



## Задължителни корпоративни правила на Amgen за ЕС – Администратор (ЗКП ЕС)

Последна актуализация: 12 декември 2023 г.

### Увод

- (A) Amgen е лидер в областта на биотехнологиите, ангажирана с обслужването на пациенти с тежки заболявания. Настоящите задължителни корпоративни правила за ЕС – Администратор („ЗКП ЕС“) изразяват ангажимента на Amgen към поверителността и защитата на Личните данни в стремежа на дружеството да осигури адекватна защита за предаването и обработването на Лични данни между Участващите дружества.
- (B) Всички Участващи дружества и всички служители се задължават и са длъжни по закон да спазват настоящите ЗКП ЕС по отношение на личните данни, които попадат в обхвата на ЗКП ЕС. Неспазването може да доведе до предприемане на дисциплинарни наказания, допустими спрямо местното законодателство. Главният директор по съответствието в сътрудничество с главния директор по поверителност на Личните данни гарантира, че ЗКП ЕС ще бъдат прилагани. Списък на Участващите дружества ще намерите тук: <https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf>. До всички Участващи дружества можете да пишете на адрес [privacy@amgen.com](mailto:privacy@amgen.com) за всякакви въпроси, свързани с настоящите ЗКП ЕС.
- (C) Настоящите ЗКП ЕС са приети във връзка със законите на ЕС за защита на данните. Amgen Франция отговаря за гарантиране на спазването на настоящите ЗКП ЕС от Участващите дружества. Физическите лица имат право да изискват спазването на ЗКП ЕС от Amgen Франция като трети страни, както е описано по-долу. Настоящите ЗКП ЕС са на разположение на уебсайта на Amgen: [www.amgen.com/bcr](http://www.amgen.com/bcr). Можете също да пишете до Amgen на адрес [privacy@amgen.com](mailto:privacy@amgen.com) и да поискате копие.

### 1. Обхват

- 1.1. ЗКП ЕС на Amgen се прилагат за прехвърлянето и обработването, автоматично или ръчно, на всички Лични данни на Субекти на данни от Участващо дружество, което действа в качеството си на Администратор на данни или на Обработващ данни от името на друго Участващо дружество, което действа като Администратор на данни във всеки от следните случаи:
- 1.1.1. Участващото дружество, което обработва Личните данни, е установено в ЕС; или
- 1.1.2. Участващото дружество, което обработва Личните данни, не е установено в ЕИП и е получило Личните данни от Участващо дружество, установено в ЕИП; или
- 1.1.3. за последващи предавания на Лични данни от Вносител на данни на Вносител на данни.

- 1.2. Общ преглед на потоците от данни съгласно настоящите ЗКП ЕС ще намерите в Приложение 1.

## 2. Дефиниции

<b>Термини</b>	<b>Дефиниции</b>
<b>Amgen Франция</b>	Amgen S.A.S., дружество, учредено във Франция със седалище и адрес на управление: 25 quai du Président Paul Doumer, 92400 Курбевоа.
<b>Приложимо законодателство</b>	Законодателството на ЕС и/или (според случая) националното или местното законодателство на държавите членки на ЕИП (включително, без ограничение, законите на ЕС за защита на данните).
<b>Ръководител съответствие</b>	Представител на звеното за спазване на здравните изисквания към отдел „Световно съответствие и бизнес етика“ на Участващо дружество, който е делегирал отговорността за защита на данните и поверителността, когато е различен от местния служител по защита на данните, подпомага местния служител по защита на данните в изпълнението на неговите отговорности и задачи.
<b>Съгласие</b>	Свободно изразено, конкретно, информирано и недвусмислено указание за волята на Субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него Лични данни да бъдат обработени.
<b>Администратор на данни</b>	Юридическо лице, което взема решения във връзка със събирането и обработването на Лични данни, включително решения относно целите и начина, по който се обработват личните данни.
<b>Износител на данни</b>	Участващо дружество, действащо като Администратор на данни, установен в ЕИП, което прехвърля Лични данни на Вносител на данни.
<b>Вносител на данни</b>	Участващо дружество, което не е установено в ЕИП и което (а) получава Лични данни от Износител на данни или (б) получава последващо предаване на Лични данни съгласно член 1, буква в) от настоящите ЗКП ЕС.
<b>Обработващ данни</b>	Физическо или юридическо лице, което обработва Лични данни от името на Администратор на данни.
<b>Орган за защита на данните (ОЗД)</b>	Независим публичен орган за защита на данните, създаден от държава членка на ЕИП.
<b>Служител по защита на данните (СЗД)</b>	Лице, назначено от главния директор по поверителност на данните на Amgen за отговорник за надзора върху поверителността и защита на личните данни на местно ниво, както и за упражняването на

<b>Термини</b>	<b>Дефиниции</b>
	подходящ и задължителен контрол.
<b>Субект на данни</b>	<p>Физическо лице, което може да бъде идентифицирано, пряко или непряко, чрез позоваване на Лични данни. Субект на данни може да бъде (без ограничения):</p> <ul style="list-style-type: none"> <li>• пациент/субект на данни от клинично изпитване (което може да включва дете на възраст под 18 години)</li> <li>• здравен специалист</li> <li>• служител</li> <li>• продавач или доставчик</li> </ul>
<b>ЕИП</b>	Държавите членки на Европейския съюз (Австрия, Белгия, България, Хърватия, Република Кипър, Чехия, Дания, Естония, Финландия, Франция, Германия, Гърция, Унгария, Ирландия, Италия, Латвия, Литва, Люксембург, Малта, Холандия, Полша, Португалия, Румъния, Словакия, Словения, Испания и Швеция), както и Исландия, Лихтенщайн и Норвегия (всички те са „Държави членки на ЕИП“).
<b>Закони на ЕС за защита на данните</b>	ОРЗД и (според случая) местното или националното законодателство, свързано със защитата на данните и обработването на Лични данни и прилагащо ОРЗД на съответната държава членка на ЕИП.
<b>ОРЗД</b>	Общият регламент относно защитата на данните ((ЕС) 2016/679).
<b>Участващо дружество</b>	Юридическо лице от групата Amgen, което е обвързано със спазването на ЗКП ЕС.
<b>Лични данни</b>	<p>Всяка информация, свързана със Субект на данни, като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или с един или повече фактори, специфични за физическата, физиологичната, генетичната, умствената, икономическата, културната или социалната идентичност на това физическо лице, или информация, свързана със същите. Сред примерите за Лични данни могат да бъдат следните:</p> <ul style="list-style-type: none"> <li>• Име, адрес, социалноосигурителен номер, номер на шофьорска книжка, информация за финансови сметки, семейна информация или медицински данни на Субекта на данните,</li> <li>• Името, професионалното образование и практиките за предписване на медицински специалист,</li> <li>• Емейл адресът и друга идентифицираща информация, предоставена от посетител на уебсайт на Amgen.</li> </ul>

<b>Термини</b>	<b>Дефиниции</b>
	Горният списък е само ориентировъчен и не е изчерпателен.
<b>Нарушение на сигурността на личните данни</b>	Всяко нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до Лични данни, които се предават, съхраняват или обработват по друг начин.
<b>Персонал</b>	Всички щатни и нещатни членове на персонала (включително консултанти, работници от агенции за временна заетост и договорни работници) на всяко Участващо дружество.
<b>Обработване</b>	Всяка операция или съвкупност от операции, извършвана с Лични данни (или набор от Лични данни) чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.
<b>Чувствителни лични данни</b>	<p>Лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическо лице.</p> <p>Отделно от законите на ЕС за защита на данните Amgen счита финансовата информация и информацията, която може да бъде използвана за кражба на самоличност (напр. социалноосигурителен номер, номер на шофьорска книжка, информация за кредитна карта или друга банкова сметка), за Чувствителни лични данни.</p>
<b>Технически и организационни мерки за сигурност</b>	Технологични и организационни мерки, целящи осигуряване на защита на Личните данни срещу случайно или неправомерно унищожаване, или случайна загуба, промяна, неразрешено разкриване или достъп, по-специално когато обработването включва предаване на данни по мрежа, както и срещу всички други незаконни форми на обработване.
<b>Трета страна</b>	<p>Физическо или юридическо лице, публичен орган, агенция или друг орган, различен от Субекта на данните, Участващото дружество, действащо като Администратор на данни и Участващото дружество, действащо като Обработващ данни.</p> <p>В Amgen Доставчиците се считат за трета страна. В зависимост от обстоятелствата дадена трета страна може да действа като Администратор на данни или Обработващ данни във връзка с обработването на Лични данни.</p>
<b>Доставчик</b>	Всяко физическо или юридическо лице, фирма или организация, която предоставя стоки и/или услуги на Участващо дружество по

<b>Термини</b>	<b>Дефиниции</b>
	силата на договорни отношения и/или е получател на Лични данни от такова Участващо дружество с цел предоставяне на тези стоки и/или услуги.

Amgen тълкува термините в настоящите ЗКП ЕС в съответствие със законите на ЕС за защита на данните.

### **3. Ограничаване на целите**

- 3.1. Личните данни се обработват за ясно формулирани, конкретни и законни цели в съответствие с чл. 5, параграф 1, буква б) от ОРЗД.
- 3.2. Личните данни не се обработват по начини, които противоречат на законните цели, за които Личните данни са събрани, или на приложимото законодателство. Вносителите на данни са длъжни да се придържат към първоначалните цели при съхранението и/или допълнителното обработване на Лични данни или обработването на Лични данни, предадени им от друго Участващо дружество. Целите на обработването на личните данни могат да бъдат променени само със съгласието на Субекта на данните или до степента, позволена от приложимото законодателство.
- 3.3. За Чувствителните данни се осигуряват допълнителни предпазни мерки, като предвидените в законите на ЕС за защита на данните.

### **4. Качество на данните и пропорционалност**

- 4.1. Личните данни трябва да бъдат точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни Лични данни, като се имат предвид целите, за които те се обработват.
- 4.2. Личните данни трябва да бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват в съответствие с чл. 5, параграф 1, буква в) от ОРЗД.
- 4.3. Обработването на Лични данни се ръководи от целта да се ограничи събирането, обработването и/или използването на Лични данни само до необходимото, т.е. възможно най-малко Лични данни. Трябва да се разгледа възможността за анонимни или псевдонимни данни, при условие че свързаните с това разходи и усилия съответстват на желаната цел.
- 4.4. Личните данни, които вече не са необходими за стопанските цели, за която първоначално са били събрани и съхранявани, трябва да се заличат според графика за съхраняване на документация на Amgen. В случай че се прилагат законови срокове за съхранение или изисквания за съхранение за съдебни нужди, данните се блокират вместо да бъдат заличени. В края на срока за съхранение или при отпадане на изискването за съхранение за съдебни нужди данните се заличават.

### **5. Правно основание за обработване на Лични данни**

- 5.1. Обработването на Лични данни е позволено само ако е изпълнена поне една от следните предпоставки:
- 5.1.1. Субектът на данните е дал съгласието си за обработване на своите Лични данни за една или повече конкретни цели.
  - 5.1.2. Обработването е необходимо за изпълнението на договор, по който Субектът на данни е страна, или за да се предприемат стъпки по искане на Субекта на данни преди сключването на договора.
  - 5.1.3. Обработването е необходимо за спазването на правно задължение, на което Администраторът на данни подлежи съгласно приложимото законодателство.
  - 5.1.4. Обработването е необходимо, за да бъдат защитени жизненоважни интереси, като например живота, здравето или безопасността, на Субекта на данни или на друго физическо лице.
  - 5.1.5. Обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официалните правомощия, предоставени на Администратора на данни.
  - 5.1.6. Обработването е необходимо за целите на законните интереси на Администратора на данни или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на Субекта на данни.
- 5.2. Обработването на Лични данни, свързани с наказателни присъди и престъпления, се извършва само когато обработването е разрешено от приложимото законодателство, предоставящо подходящи гаранции за правата и свободите на Субектите на данни.

## **6. Обработване на Чувствителни лични данни**

- 6.1. В случай че за конкретна и законна цел Участващото дружество трябва да обработи Чувствителни данни, Участващото дружество ще направи това само ако:
- 6.1.1. Субектът на данните е дал изрично съгласие за обработването на тези Чувствителни лични данни за една или повече конкретни цели, освен когато приложимото законодателство предвижда, че забраната в член 9, параграф 1 от ОРЗД не може да бъде отменена от Субекта на данните.
  - 6.1.2. Обработването е необходимо за целите на изпълнението на задълженията и конкретните права на Администратора на данни в областта на трудовото право и правото в областта на социалното осигуряване и социалната защита, доколкото то е разрешено от приложимото право или от колективен трудов договор съгласно приложимото право, предвиждащ подходящи гаранции за основните права и интереси на Субекта на данни.
  - 6.1.3. Обработването е необходимо за защита на жизнените интереси на Субекта на данни или на друго физическо лице, когато Субектът на данни е физически или юридически неспособен да даде своето съгласие.

- 6.1.4. Обработването се извършва в хода на законосъобразната му дейност и с подходящи гаранции от фондация, сдружение или друга организация с нестопанска цел, с политическа, философска, религиозна или профсъюзна цел, при условие че обработването е свързано единствено с членовете на тази организация или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че данните не се разкриват извън тази организация без съгласието на Субектите на данни.
- 6.1.5. Обработват се Чувствителни лични данни, които явно са направени публично достояние от Субекта на данни.
- 6.1.6. Обработването на Чувствителни лични данни е необходимо за установяването, упражняването или защитата на правни искове.
- 6.1.7. Обработването е необходимо по причини от важен обществен интерес на основание приложимото законодателство, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на Субекта на данните.
- 6.1.8. Обработването на Чувствителните лични данни е необходимо за целите на профилактиката или трудовата медицина, за оценка на работоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на приложимото законодателство или по силата на договор със здравен специалист, а когато тези Чувствителни лични данни се обработват от здравен специалист или на негова отговорност, този специалист трябва да е обвързан от задължението за опазване на професионална тайна съгласно приложимото законодателство или правилата, установени от компетентните органи в държава членка на ЕИП, или от друго лице, което също е обвързано от задължението за опазване на тайна съгласно приложимото законодателство или правилата, установени от компетентните органи в държава членка на ЕИП.
- 6.1.9. Обработването на Чувствителни лични данни е необходимо по причини от обществен интерес в областта на общественото здраве, като например защита срещу сериозни трансгранични заплахи за здравето или осигуряване на високи стандарти за качество и безопасност на здравните грижи и на лекарствените продукти или медицинските изделия, въз основа на приложимото законодателство, което предвижда подходящи и конкретни мерки за защита на правата и свободите на Субекта на данните, по-специално професионална тайна.
- 6.1.10. Обработването на Чувствителни лични данни е необходимо за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания в съответствие с член 89, параграф 1 от ОРЗД, въз основа на приложимото законодателство, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на Субекта на данните.

## **7. Прозрачност и право на информация**

- 7.1. Всички Участващи дружества обработват личните данни по прозрачен начин. Amgen е ангажирана да направи ЗКП ЕС, включително информацията за връзка, леснодостъпни за всеки Субект на данни и да информира Субектите на данни за предаването и обработването на техните Лични данни. Настоящите ЗКП ЕС са на разположение на уебсайта на Amgen: [www.amgen.com/bcr](http://www.amgen.com/bcr). Можете също да пишете до Amgen на адрес [privacy@amgen.com](mailto:privacy@amgen.com) и да поискате копие. Също така Amgen ще използва различни комуникационни средства, като корпоративни уебсайтове, включително вътрешни уебсайтове, бюлетини, договори и конкретни съобщения за поверителност, за да изпълни това изискване за достъпност. Освен това Amgen ще информира своевременно Субектите на данни чрез тези средства за комуникация за всички актуализации или промени в ЗКП ЕС или в списъка на Участващите дружества.
- 7.2. На Субектите на данни, чиито Лични данни се обработват от Участващо дружество, се предоставя информацията, посочена в членове 13 и 14 от ОРЗД.
- 7.3. Когато Личните данни не са получени от Субект на данни, задължението за информирание на Субекта на данни не се прилага, ако предоставянето на тази информация се окаже невъзможно или е свързано с прекомерно усилие, или ако записът или разкриването е изрично постановено от закона.

## **8. Права на достъп, коригиране, изтриване и ограничаване на данни**

- 8.1. Всеки Субект на данни има право да получи от Участващото дружество потвърждение дали се обработват Лични данни, свързани с него, и когато това е така, да получи достъп до Личните данни и информацията, която се предоставя задължително съгласно член 15, параграф 1 от ОРЗД. Последващите действия по това искане, включително възможността за начисляване на такса или срокът за отговор на искането, се извършват при спазване на приложимото законодателство и се съобщават по подходящ начин на Субекта на данни, когато той подаде своето искане.
- 8.2. Всеки Субект на данни има право да поиска коригиране, изтриване или ограничаване на личните данни, по-специално когато данните са непълни или неточни.
- 8.3. Всеки Субект на данни има право да възрази по всяко време и на основания, свързани с неговата конкретна ситуация, срещу обработването на неговите Лични данни въз основа на изпълнението на задача, извършвана в обществен интерес или на законните интереси на Участващото дружество или на трета страна (включително профилиране, основаващо се на тези разпоредби). Участващото дружество прекратява обработването на Личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на Субекта на данни, или за установяването, упражняването или защитата на правни претенции.
- 8.4. Всеки Субект на данни има право да възрази (безплатно) срещу обработването на Лични данни, отнасящи се до него, за целите на директен маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг. Когато Субектът на данни упражни правото си на възражение срещу обработването на свързани с него Лични данни за целите на директния маркетинг, Участващото дружество е длъжно да преустанови обработването на Личните данни за тези цели.



- 8.5. Всеки Субект на данни има право да получи уведомлението до трети страни, на които са разкрити личните данни, за каквото и да е коригиране, изтриване или ограничаване, извършено в съответствие с чл. 19 от ОРЗД.
- 8.6. Всеки Субект на данни има право да е запознат с логиката на всяко автоматизирано обработване на Лични данни в съответствие с чл. 13, параграф 2, буква е) от ОРЗД.
- 8.7. Когато обработването се основава на съгласие, всеки Субект на данни има право да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне.
- 8.8. Всеки Субект на данни има право да подаде жалба до Участващото дружество относно обработването на Лични данни чрез вътрешния механизъм за подаване на жалби, предвиден в член 17.
- 8.9. Всички искания по настоящия член 8 (или по член 9 по-долу) се изпращат до Участващото дружество на адрес: [privacy@amgen.com](mailto:privacy@amgen.com). Въпреки че подаването на искания по електронна поща е силно препоръчително, това не изключва възможността Субект на данни да подаде устно искане. Участващото дружество информира без закъснение Субекта на данните за резултата от неговото искане и не по-късно от един месец от получаването на искането (включително, според случая, причините да не бъдат предприети действия и възможността за подаване на жалба до компетентния ОЗД и/или за търсене на съдебна защита). Този едномесечен срок може да бъде удължен с още два месеца, когато е необходимо, като се вземат предвид сложността и броят на исканията. Участващото дружество информира Субекта на данните за всяко такова удължаване в срок до един месец от получаването на искането, като посочва причините за забавянето. Всяко съобщение, действие и/или информация, предоставени във връзка с искане по настоящия член 8 (или член 9 по-долу), се предоставят на Субекта на данни безплатно. Когато исканията на Субект на данни са явно неоснователни или прекомерни, по-специално поради своята повтораемост, Участващото дружество може или: (а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или съобщението или предприемането на исканите действия, или (б) да откаже да предприеме действия по искането. Участващото дружество носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

## **9. Автоматизирани индивидуални решения**

- 9.1. Субектът на данни има право да не бъде обект на решение, основано единствено на автоматизирано обработване, включително профилиране, което поражда правни последици за него или по подобен начин го засяга в значителна степен, освен ако това решение:
  - 9.1.1. е необходимо за сключването или изпълнението на договор между Субекта на данни и Участващото дружество;
  - 9.1.2. се изисква или е разрешено от приложимото законодателство, което също така предвижда подходящи мерки за защита на правата, свободите и законните интереси на Субекта на данните (включително най-малко правото да получи човешка намеса от страна на Участващото дружество, да изрази своята гледна точка и да оспори решението); или

9.1.3. се основава на изричното съгласие на Субекта на данните.

## **10. Сигурност и поверителност**

- 10.1. Amgen прилага подходящи технически и организационни мерки за сигурност, за да се предпази от и да открие нарушения на сигурността на Личните данни. Amgen използва международни рамки, като ISO/IEC 27002, за определянето на тези мерки за сигурност.
- 10.2. Amgen е въвела процедури, за да гарантира, че нарушенията на сигурността на Личните данни подлежат на съобщаване, проследяване и подходящи коригиращи действия, когато такива са необходими. Всяко нарушение на сигурността на Личните данни се документира (включително фактите, свързани с нарушението на сигурността на Личните данни, последиците от него и предприетите коригиращи действия) и документацията се предоставя на компетентния ОЗД при поискване. Участващите дружества уведомяват своевременно за всяко нарушение на сигурността на Личните данни Amgen Франция, главния директор по поверителност на данните и другия съответен служител/функция по защита на личните данни, както и (когато Участващото дружество, претърпяло нарушение на сигурността на Личните данни, действа като Обработващ лични данни) Участващото дружество, действащо като Администратор на лични данни. За нарушенията на сигурността на личните данни едновременно с главния директор по поверителност на данните своевременно се уведомява компетентният ОЗД (и когато е възможно, не по-късно от 72 часа след узнаването на нарушението на сигурността на личните данни), освен ако няма вероятност то да доведе до риск за правата и свободите на Субектите на данни. Когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на Субектите на данни, за него се уведомяват своевременно и Субектите на данни.
- 10.3. Оценки на риска за сигурността на данните се правят за идентифициране на потенциални заплахи за Чувствителни лични данни и за прилагане на допълнителни контролни мерки за сигурност, когато това е подходящо.
- 10.4. Прилагането на мерките ще бъде съобразено с достиженията на техническия прогрес в съответствие с член 32 от ОРЗД.
- 10.5. Главният директор по сигурност на информацията работи съвместно с главния директор по поверителност на личните данни, за да гарантира сигурността и поверителността на личните данни.
- 10.6. Техническите и организационните мерки за сигурност трябва да бъдат разработени така, че да прилагат принципите за защита на данните съгласно член 5 от ОРЗД, принципите за защита на данните на етапа на проектирането и по подразбиране съгласно член 25 от ОРЗД и да улесняват спазването на практика на изискванията, определени от настоящите ЗПК ЕС.

## **11. Отношения с Обработващи данни (Вносител на данни на Amgen или Доставчик)**

- 11.1. Участващото дружество (действащо като Администратор на данни) избира внимателно Обработващ данните, който може да бъде друго Участващо дружество или Доставчик. Обработващият данни трябва да предостави достатъчни гаранции по отношение на

своите технически и организационни мерки за сигурност, уреждащи обработването, което ще се извършва, и трябва да осигури съответствието на тези мерки.

- 11.2. Когато възлагането на външни лица бъде счетено за необходимо след оценка на стопанските нужди и рисковете от такова възлагане, процесът на избор на Обработващ данни включва оценка на рисковите фактори за поверителността на личните данни и постигане на баланс между стопанските нужди и потенциалните рискове.
- 11.3. Участващото дружество, действащо като Администратор на данни, чрез писмени договори в съответствие с приложимото законодателство (и по-специално изискванията на член 28, параграф 3 от ОРЗД) дава указания на Обработващия данни, наред с други неща:
  - 11.3.1. Обработващият данни действа само по указания на Участващото дружество, действащо като Администратор на данни, а обработването на Лични данни за личните цели на обработващия или за целите на трета страна е забранено;
  - 11.3.2. относно правилата, свързани със сигурността и поверителността, които са задължение на Обработващия данни, и да прилага подходящи технически и организационни мерки, за да гарантира степен на сигурност, съответстваща на риска от обработването;
  - 11.3.3. лицата, упълномощени да обработват Личните данни, са поели ангажимент за поверителност или са обвързани с подходящо правно задължение за поверителност;
  - 11.3.4. Обработващият данни не включва друг Обработващ лични данни без предварителното изрично или общо писмено разрешение на Участващото дружество, действащо като Администратор на данни, а когато такова разрешение е дадено, на този друг Обработващ лични данни се налагат същите задължения за защита на данните, които са определени в договора или друг правен акт между Участващото дружество, действащо като Администратор на данни, и Обработващия данни;
  - 11.3.5. като взема предвид естеството на обработването, то трябва да подпомага Участващото дружество, действащо като Администратор на данни, чрез подходящи технически и организационни мерки, доколкото това е възможно, за изпълнение на задължението на Участващото дружество да отговаря на искания за упражняване на правата на Субекта на данни;
  - 11.3.6. трябва да помага на Участващото дружество, действащо като Администратор на данни, да осигури спазването на задълженията, свързани със сигурността на обработването, уведомяването на компетентния ОЗД за нарушение на сигурността на личните данни, съобщаването на Субекта на данните за нарушение на сигурността на Личните данни, оценките на въздействието върху защитата на данните и предварителната консултация с компетентния ОЗД, като се вземат предвид естеството на обработването и информацията, с която разполага Обработващият данни;
  - 11.3.7. по избор на Участващото дружество, действащо като Администратор на данни, то трябва да изтрие или да върне всички Лични данни на Участващото дружество, действащо като Администратор на данни, след приключване на

предоставянето на услуги, свързани с обработването, и да изтрие съществуващите копия, освен ако законите на ЕС за защита на данните не изискват съхраняването на Личните данни;

- 11.3.8. трябва да предостави на Участващото дружество, действащо като Администратор на данни, цялата информация, необходима за доказване на изпълнението на задълженията, предвидени в настоящия член 11, и да позволи и да допринесе за одити, включително проверки, извършвани от Участващото дружество, действащо като Администратор на данни, или от друг одитор, упълномощен от него.
- 11.4. Участващото дружество, действащо като Администратор на данни, гарантира, че Обработващият данни продължава напълно да изпълнява договорените технически и организационни мерки за сигурност.
- 11.5. Участващото дружество, действащо като Администратор на данни, запазва отговорността за законсъобразността на обработването и продължава да носи отговорност за правата на Субекта на данни. В степента, в която Обработващият данни е подчинен на законите на ЕС за защита на данните, той също носи отговорност за своите задължения и отговорности като Обработващ данни съгласно тези закони.
- 11.6. За да се осигурят договорните задължения на Обработващите данни, посочени в настоящия член, на Участващите дружества, действащи като Администратор на данни, се предоставя за ползване образец на договор, озаглавен „Приложение за поверителност на данните“. Участващото дружество, действащо като Администратор на данни, може, в зависимост от конкретните обстоятелства на всяко договорно споразумение, да договори разпоредби, различни от тези, посочени в Приложението за поверителност на данните, но договорните разпоредби все пак трябва да обхващат най-малко задълженията, посочени по-горе в настоящия член 11.
- 11.7. Всяко Участващо дружество, действащо като Обработващ данни, което е подчинено на законите на ЕС за защита на данните, е длъжно да поддържа регистър на всички категории дейности по обработване, извършени от името на Участващо дружество, действащо като Администратор на данни. Този регистър следва да се води в писмен вид, включително в електронна форма, да се предоставя на главния директор по поверителност на данните и на компетентния ОЗД при поискване и да съдържа следната информация: (а) името и данните за връзка с Участващото дружество, действащо като Обработващ данни, както и на всяко Участващо дружество, действащо като Администратор на данни, от чието име то действа, и когато е приложимо, на неговия представител и СЗД; (б) категориите обработване, извършвани от името на всяко Участващо дружество, действащо като Администратор на данни; и (в) когато е приложимо, предаването на Лични данни на трета държава или международна организация, включително посочване на тази трета държава или международна организация, а в случай на предаване, което се основава на дерогация съгласно член 49 от ОРЗД, документиране на съответните гаранции; и (г) когато е възможно, общо описание на техническите и организационните мерки за сигурност.

## **12. Ограничения за предаване и последващо предаване**

- 12.1. При всички предавания на Лични данни, които са предмет на настоящите ЗКП ЕС, на Трети страни, намиращи се извън ЕИП, се спазват законите на ЕС за защита на данните

относно предаването и последващото предаване на Лични данни, чрез стандартните договорни клаузи, разрешени съгласно Решение за изпълнение (ЕС) на Комисията от 4 юни 2021 г. относно стандартните договорни клаузи за предаване на Лични данни на трети държави съгласно ОРЗД, или чрез други подходящи средства съгласно глава V от ОРЗД (включително по изключение, ако за конкретна ситуация се прилага дерогация в съответствие с член 49 от ОРЗД).

12.2. При всички предавания на Лични данни, предмет на настоящите ЗКП ЕС, на Обработващи данни, разположени извън ЕИП, се спазват Законите на ЕС за защита на данните, отнасящи се до Обработващите данни (и изискванията, посочени в член 11 по-горе), в допълнение към правилата за предаване и последващо предаване на Лични данни, посочени в настоящия член 12 и в Законите на ЕС за защита на данните.

12.3. Преди предаването на Лични данни на Вносител на данни или (по отношение на последващи предавания) преди влизането в сила на актуализирано местно национално законодателство Износителят на данни, съвместно с главния директор по поверителност на данните и Amgen Франция, със съдействието на Вносителя на данни и като взема предвид обстоятелствата на предаването, преценява дали местното национално законодателство ще попречи на Вносителя на данни да изпълни задълженията си по ЗКП ЕС и определя дали следва да бъдат приложени необходимите допълнителни мерки. Тази оценка отчита:

12.3.1. конкретните обстоятелства на предаването (включително целите, за които Личните данни се предават и обработват, видовете субекти, участващи в обработването, икономическия сектор, в който се извършва предаването, категориите и формата на предадените Лични данни, местоположението на обработването (включително съхранението) и използваните канали за предаване);

12.3.2. законите и практиките на третата държава на местоназначение, които са от значение с оглед на конкретните обстоятелства на предаването (включително тези, които изискват разкриване на данни пред публични органи или разрешаване на достъп на такива органи), и приложимите ограничения и гаранции; и

12.3.3. всички съответни договорни, технически или организационни гаранции, въведени по отношение на предаването, включително мерките, прилагани по време на предаването и обработването на Личните данни в държавата на местоназначение.

Освен това тази оценка се основава на разбирането, че законите и практиките на третата държава на местоназначение зачитат основните права и свободи на Субекта на данни и не надхвърлят необходимото и пропорционалното в едно демократично общество за гарантиране на една от следните цели: (а) националната сигурност; (б) отбраната; (в) обществената сигурност; (г) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции, включително предпазването от и предотвратяването на заплахи за обществената сигурност; (д) други важни цели от общ обществен интерес, по-специално важни икономически или финансови интереси, включително парични, бюджетни и данъчни въпроси, обществено здраве и социално осигуряване; (е) защита на независимостта на съдебната власт и съдебните производства; (ж) предотвратяване, разследване, разкриване и преследване на нарушения на етичните

норми за регулираните професии; (з) функции за надзор, проверка и регулиране, свързани с упражняването на официални правомощия в случаите, посочени в предходните цели; (и) защита на Субекта на данни или на правата и свободите на други лица; и/или (й) изпълнение на гражданскоправни искове.

Главният директор по поверителност на данните преглежда и одобрява документираната оценка и всички предложени допълнителни мерки. Когато резултатът от оценката показва необходимостта от прилагане на допълнителни мерки, Износителят на данни прилага тези мерки. Ако не могат да се въведат допълнителни мерки (или по нареждане от главния директор по поверителност на данните или от компетентен ОЗД), Износителят на данни преустановява предаването. Резултатът от оценката и предложените допълнителни мерки се документират и се предоставят на компетентния ОЗД, когато това се изисква.

Главният директор по поверителност на данните и Amgen Франция информират всички Участващи дружества за извършената оценка и за резултатите от нея, за да могат определените допълнителни мерки да бъдат приложени, когато други Участващи дружества извършват същия вид предавания, или когато не могат да бъдат въведени ефективни допълнителни мерки, тези предавания да бъдат спрени или прекратени.

- 12.4. Вносителят на данни незабавно уведомява Износителя на данни, Amgen Франция и главния директор по поверителност на данните, ако има основания да смята, че е или е станал обект на закони или практики, които биха му попречили да изпълни задълженията си по настоящите ЗКП ЕС, включително след промяна в местното национално законодателство в третата държава, както е описано в член 12.3, или мярка като искане за разкриване на информация, както е описано в член 16.3. Освен това Износителите на данни (съвместно с главния директор по поверителност на данните) наблюдават непрекъснато и когато е уместно, със съдействието на Вносителите на данни, промените в третите държави, в които Износителите на данни са предали Лични данни, които биха могли да повлияят неблагоприятно на първоначалната оценка на степента на защита на Личните данни и на решенията, взети във връзка с това предаване.
- 12.5. След спиране на предаването Износителят на данни трябва да прекрати предаването или съвкупността от предавания, ако Вносителят на данни не е в състояние да спазва ЗКП ЕС и/или спазването не е възстановено в срок до един месец от спирането. В такъв случай Вносителят на данни трябва, по избор на Износителя на данни, да върне или унищожи всички Лични данни, които са били предадени преди спирането, както и всички техни копия.
- 12.6. Всички потоци от Лични данни, които не са предмет на настоящите ЗКП ЕС и/или не произхождат от Участващо дружество, установено в държава членка на ЕИП, не се считат за предаване на Лични данни съгласно настоящите ЗКП ЕС и съответно не са предмет на изискванията на настоящите ЗКП ЕС.

### **13. Програма за обучение**

- 13.1. Както е описано в Приложение 2, Amgen осигурява подходящо и актуално обучение на целия персонал относно принципите за защита на Личните данни и по-конкретно относно ЗКП ЕС. Това обучение включва и информация относно последиците от наказателното и трудовото право и/или договора за услуги за персонала, който нарушава ЗКП на ЕС.

- 13.2. Обучението е задължително и се повтаря всяка година. Успешното преминаване на обучението се документира.
- 13.3. Конкретни обучения се предоставят според случая на персонала, който има постоянен или редовен достъп до Лични данни или който участва в събирането на Лични данни или с разработването на инструменти, използвани за обработване на Лични данни.
- 13.4. В допълнение, Централният отдел за спазване на изискванията за поверителност на Amgen предоставя подходяща информация и ресурси, свързани с поверителността, включително на вътрешния портал на Amgen.

#### **14. Програма за одитиране и текущ контрол**

- 14.1. Главният директор по поверителност гарантира, че всички Участващи дружества (и спазването на ЗКП ЕС от тях) са включени в програмата за одит и текущ контрол от гледна точка на поверителността и защитата на данните. Цялостни одити се извършват редовно, не по-рядко от веднъж на 2 – 3 години (за Участващите дружества със среден и висок рисков профил въз основа на методологията за оценка на риска на отдела за одит) и веднъж на 4 – 5 години (за Участващите дружества с нисък рисков профил въз основа на методологията за оценка на риска на отдела за одит), от отдела за вътрешен одит или от независими външни сертифицирани одитори. Цялостните одити включват в обхвата си въпроси, свързани със защитата на данните и поверителността (включително спазването на настоящите ЗКП ЕС, когато те са приложими за Участващото дружество и се прилагат от него). В допълнение към цялостните одити и без да се засягат сроковете, посочени по-горе, се извършват одити с друг обхват, включително интердисциплинарни одити или одити по специфичен проблем (напр. спазване на ЗКП ЕС), ограничен одит на една или повече системи за обработване на Лични данни и/или ограничен одит на един или повече функционални отдели (напр. Централния отдел за спазване на изискванията за поверителност). Програмата за одитиране е разработена и съгласувана в сътрудничество с главния директор по одитирането и главния директор по съответствието, който е и старши вицепрезидент. Главният директор по поверителност на личните данни, главният директор по съответствието и главният директор по информацията могат по всяко време да започнат ad hoc одити, свързани със ЗКП ЕС. Например като реакция на всеки установен проблем със съответствието или доклад за съществено несъответствие, нарушение на сигурността на личните данни и/или съществена промяна в законите на ЕС за защита на данните. Програмата за одитиране обхваща всички аспекти на ЗКП ЕС, включително начините за гарантиране, че ще се предприемат коригиращи действия.
- 14.2. Всички одитни доклади за ЗКП ЕС се предоставят своевременно на главния директор по съответствието и главния директор по поверителност на Личните данни. Обобщенията и констатациите от одита на ЗКП на ЕС, както и друга важна информация, се докладват редовно и на Съвета на директорите на Amgen Inc. чрез съответните комисии (например Комисията по корпоративна отговорност и съответствие и/или Одитната комисия на Съвета на директорите), на Съвета на директорите на Amgen Франция и (когато е уместно, например във връзка с констатация, изискваща коригиране) на съответното Участващо дружество. Комисията по корпоративна отговорност и съответствие към Съвета на директорите на Amgen, Inc. заседава пет пъти годишно. Поверителността и защитата на данните се разглеждат ежегодно, обикновено на заседанието през октомври.

- 14.3. При поискване компетентните ОЗД могат да получат копие от одитните доклади, свързани със ЗКП ЕС.
- 14.4. Всяко Участващо дружество оказва съдействие и без ограничения приема да бъде одитирано от компетентните ОЗД. Всяка одитирана структура трябва незабавно да информира главния директор по поверителност, ако получи известие за такъв одит или ако такъв одит бъде извършен.

#### **15. Спазване на правилата и надзор на спазването**

- 15.1. Amgen назначава подходящи членове на персонала, включително, според случая, мрежа от служители по защита на данните, които с подкрепа от висшето ръководство контролират и гарантират спазването на правилата за защита на данните. Главният директор по поверителност отговаря за Централния отдел за спазване на изискванията за поверителност, който е централен отдел, оказващ експертна подкрепа на юридическите лица от групата Amgen в целия свят (включително Участващите дружества).
- 15.2. В Amgen задълженията на главния директор по поверителност на личните данни включват, наред с други:
- 15.2.1. консултиране на управителния съвет;
  - 15.2.2. осигуряване на спазването на изискванията за защита на данните на световно ниво (включително цялостна отговорност за ЗКП ЕС);
  - 15.2.3. редовно докладване за спазването на изискванията за защита на данните (включително на главния директор по съответствието); и
  - 15.2.4. работа по проучванията на компетентните ОЗД.
- 15.3. Централният отдел за спазване на изискванията за поверителност включва главния директор по поверителност (който, в допълнение към отговорностите, посочени по-горе, наблюдава глобалната мрежа от служители по защита на данните), европейския служител по защита на данните и други местни служители по защита на данните. Централният отдел за спазване на изискванията за поверителност на Amgen отговаря изцяло за спазването на изискванията за защита на данните и поверителност.
- 15.4. Европейският служител по защита на данните е назначен от Amgen за длъжностно лице по защита на данните за ЕИП, Обединеното кралство и Швейцария. Европейският служител по защита на данните има задачите, посочени в член 39 от ОРЗД. Amgen гарантира, че задачите и задълженията на Европейския служител по защита на данните няма да доведат до конфликт на интереси с такива задачи. Европейският служител по защита на данните е пряко подчинен на главния служител по защита на данните (който е част от най-високото управленско ниво на Amgen) и се подпомага от местния ръководител по съответствието във Франция. Европейският служител по защита на данните може да се свърже с главния служител по защита на личните данни, ако по време на изпълнението на задълженията му възникнат въпроси или проблеми. Можете да се свържете с европейския служител по защита на данните на адрес: [privacy@amgen.com](mailto:privacy@amgen.com)



- 15.5. На местно ниво служителите по защита на данните отговарят за разглеждането на молби, свързани с поверителността на Личните данни, от местни Субекти на данни с цел гарантиране на съответствието на местно ниво, с помощ от Централния отдел за спазване на изискванията за поверителност, както и за съобщаването на сериозни проблеми, свързани с поверителността на Личните данни, на главния директор по поверителност на личните данни. Amgen поддържа мрежа от служители по защита на данните и гарантира, че СЗД е назначен или определен за всяка държава, в която Amgen има юридическо лице (Участващото дружество) и приложимото право на юрисдикцията на това Участващо дружество изисква такова назначаване.
- 15.6. Служителите по защита на данните обикновено са или получават подкрепа от местни ръководители по съответствието, които са подчинени на отдел „Световно съответствие и бизнес етика“. Централният отдел за спазване на изискванията за поверителност е част от и е подчинен на отдел „Световно съответствие и бизнес етика“, начело на който е главният директор по съответствието. Главният директор по съответствието носи цялостната отговорност за спазването на правните и регулаторните изисквания от групата Amgen в световен мащаб. В редки случаи поради специфичните обстоятелства на Участващо дружество или други специални обстоятелства служителят по защита на данните може да е от друга функция, например регулаторна. Във всички случаи Централният отдел за спазване на изискванията за поверителност гарантира, че служителите по защита на данните и ръководителите съответствие са подходящо обучени и имат достатъчно експертни познания и опит в управлението, за да изпълняват своята роля. Освен това служителите по защита на данните са пряко подчинени на главния директор по поверителност и се подпомагат от персонала на Централния отдел за спазване на изискванията за поверителност, в случай че се нуждаят от допълнителни насоки.
- 15.7. Всяко Участващо дружество, действащо като Администратор на данни, носи отговорност и може да докаже спазването на ЗКП ЕС. Като част от това изискване всички Участващи дружества:
- 15.7.1. трябва да поддържат регистър на всички категории дейности по обработване, извършвани в съответствие с изискванията на член 30, параграф 1 от ОРЗД. Този регистър следва да се води в писмен вид, включително в електронна форма, да се предоставя на главния директор по поверителност на данните и на компетентния ОЗД при поискване и да съдържа следната информация: (а) името и данните за връзка с Участващото дружество, действащо като Администратор на данни, неговия представител и СЗД; (б) целите на обработването; (в) описание на категориите Субекти на данни и на категориите Лични данни; (г) категориите получатели, на които Личните данни са били или ще бъдат разкрити, включително получатели в трети държави или международни организации; (д) когато е приложимо, предаването на Лични данни на трета държава или международна организация, включително идентифицирането на тази трета държава или международна организация, а в случай на предаване, което се основава на дерогация, документиране на подходящите гаранции; (е) когато е възможно, предвидените срокове за изтриване на различните категории Лични данни; и (ж) когато е възможно, общо описание на техническите и организационни мерки за сигурност.
- 15.7.2. извършване на оценки на въздействието върху защитата на данните за операции по обработване, които има вероятност да доведат до висок риск за правата и свободите на физическите лица в съответствие с член 35 от ОРЗД.

Когато оценката на въздействието върху защитата на данните съгласно член 35 показва, че обработването би довело до висок риск при липса на мерки, предприети от Участващото дружество за намаляване на риска, преди обработването трябва да се проведе консултация с главния директор по защита на личните данни, който след това се консултира с компетентния ОЗД в съответствие с член 36 от ОРЗД.

## **16. Действия в случай на национално законодателство, възпрепятстващо спазването на ЗКП ЕС**

- 16.1. Когато Участващо дружество има основание да смята, че приложимото за него законодателство възпрепятства Участващото дружество да изпълни своите задължения по ЗКП ЕС и има значително въздействие върху гаранциите, предвидени от правилата, то незабавно уведомява главния директор по защита на личните данни (освен когато това е забранено от правоприлагащ орган, например наказателноправна забрана за опазване на поверителността на разследване на правоприлагащия орган) и Amgen Франция.
- 16.2. Когато има противоречие между местното национално законодателство и ангажиментите по ЗКП ЕС, главният директор по поверителност на личните данни в сътрудничество с местния юрисконсулт и местния служител по защита на данните определя какви са необходимите законосъобразни действия. Ако е необходимо, главният директор по поверителност на личните данни се консултира и с компетентните ОЗД.
- 16.3. Когато има вероятност някое правно изискване, на което е подчинено Участващо дружество в трета държава, да окаже съществено неблагоприятно въздействие върху гаранциите, предоставени от ЗКП ЕС, Вносителят на данни незабавно уведомява главния служител по защита на личните данни, Amgen Франция и Износителя на данни, а главният служител по защита на личните данни уведомява компетентния ОЗД и (когато е възможно) Субектите на данни. Това включва (а) всяко правно обвързващо искане за разкриване на Лични данни от правоприлагащ орган или орган за държавна сигурност, като в такъв случай компетентният ОЗД следва да бъде ясно информиран за искането, включително информация за исканите данни, искащия орган и правното основание за разкриването, както и за предоставения отговор (освен ако не е забранено, като например забрана съгласно наказателното право за опазване на поверителността на разследване от правоприлагащите органи), и (б) всеки пряк достъп на публични органи до Лични данни, предадени съгласно настоящите ЗКП ЕС, в съответствие със законите на държавата по местоназначение, като в такъв случай това уведомление включва цялата информация, с която разполага това Участващо дружество (освен ако не е забранено, като например забрана по силата на наказателното право за опазване на поверителността на разследване на правоприлагащите органи).
- 16.4. Ако в конкретни случаи спирането и/или уведомяването са забранени, Участващото дружество, което получава искането, полага максимални усилия, за да получи правото да се откаже от тази забрана, за да съобщи възможно най-много информация във възможно най-кратък срок и да може да докаже (по искане на Износителя на данни), че е направило това.
- 16.5. Вносителят на данни предоставя редовно на Износителя на данни възможно най-много важна информация относно получените искания (по-специално броя на исканията, вида

на исканите Лични данни, самоличността на искащите органи, дали исканията са били оспорени и резултата от тези оспорвания). Вносителят на данни съхранява тази информация, докато Личните данни са предмет на гаранциите, предвидени в ЗКП ЕС, и я предоставя на компетентния ОЗД при поискване. В случай че Вносителят на данни е получил или получи частична или цялостна забрана за предоставяне на горепосочената информация на Износителя на данни, Вносителят на данни информира своевременно Износителя на данни за това.

- 16.6. Вносителят на данни, съвместно с главния служител по защита на личните данни, преглежда законосъобразността на искане за разкриване на данни от публичен орган, за да определи дали то попада в обхвата на правомощията, предоставени на искащия публичен орган. Вносителят на данни оспорва искането, ако след такава оценка стигне до заключението (съвместно с главния служител по защита на личните данни), че има разумни основания да счита, че искането е незаконосъобразно съгласно законите на държавата по местоназначение, приложимите задължения по международното право и/или принципите на добрите международни отношения. Ако Вносителят на данни смята, че има такива разумни основания да счита искането за незаконосъобразно, той използва възможностите за обжалване. При оспорване на искане Вносителят на данни иска временни мерки с оглед спиране на действието на искането, докато компетентният съдебен орган се произнесе по неговата основателност. Вносителят на данни не разкрива исканите Лични данни, докато не бъде задължен да го направи съгласно приложимото законодателство и процедурните правила на държавата на местоназначение. Вносителят на данни документира своята правна оценка и всяко оспорване на искането за разкриване и, доколкото това е допустимо съгласно законите на държавата по местоназначение, предоставя документацията на Износителя на данни и при поискване я предоставя на компетентния ОЗД.
- 16.7. Вносителят на данни предоставя минималното допустимо количество информация, когато отговаря на искане за разкриване, въз основа на разумно тълкуване на искането.
- 16.8. Във всеки случай предаването на Лични данни от Участващо дружество на който и да е публичен орган не трябва да бъде масово, непропорционално и безразборно по начин, който да надхвърля необходимото в едно демократично общество.
- 16.9. За Участващите дружества, разположени в ЕИП, всяко решение на съд или трибунал и всяко решение на административен орган на трета държава, с което се изисква от Администратор на данни или Обработващ данни да предаде или разкрие Лични данни, може да бъде признато или изпълнено по какъвто и да е начин само ако се основава на международно споразумение, като например договор за правна взаимопомощ, в сила между изискващата трета държава и ЕС или държава членка на ЕИП, без да се засягат другите основания за предаване съгласно глава V от ОРЗД.

## **17. Вътрешни механизми за подаване на жалби**

- 17.1. Atgen ще използва своя съществуващ процес за разглеждане на жалби, за да включи разглеждането на жалби или опасения, свързани със ЗКП ЕС.
- 17.2. Всеки Субект на данни може по всяко време да подаде жалба, че някое Участващо дружество не спазва ЗКП ЕС. Тези жалби се разглеждат от Централния отдел за спазване на изискванията за поверителност под ръководството на главния директор по поверителност на личните данни и в сътрудничество със съответния местен служител по защита на данните.

- 17.3. Amgen препоръчва тези жалби да се подават писмено по пощата или по имейл директно на Централния отдел за спазване на изискванията за поверителност или на съответното Участващо дружество. Можете да се свържете с Централния отдел за спазване на изискванията за поверителност, като използвате данните за връзка по-долу:

Адрес: 25 quai du Président Paul Doumer, 92400 Курбевоа.

Имейл: [privacy@amgen.com](mailto:privacy@amgen.com)

- 17.4. Персоналът на Amgen може, когато е приемливо съгласно законите, приложими за Участващото дружество, да използва горещата телефонна линия за бизнес поведение, за да докладва жалба по ЗКП ЕС.
- 17.5. Ако жалбата е получена на място в Участващото дружество, СЗД я превежда, ако е необходимо, и незабавно я препраща на Централния отдел за спазване на изискванията за поверителност.
- 17.6. Първоначален отговор се предоставя на Субекта на данни в срок до десет (10) работни дни, като го информира, че жалбата му се разглежда и че ще получи отговор по същество своевременно и във всички случаи в срок до един месец от получаване на искането. Като се вземат предвид сложността и броя на исканията, едномесечният срок може да бъде удължен с не повече от два месеца, като в такъв случай Субектът на данни се уведомява за това. В отговора по същество се посочват подробни данни за нашите констатации и действията, които Amgen предлага да бъдат предприети. В случай че Amgen реши, че не е необходимо да се предприемат действия, това се обяснява на Субекта на данни, като се посочват основанията за това решение.
- 17.7. Ако жалбата бъде уважена от Amgen, то Amgen ще приложи подходящи коригиращи мерки. Тези мерки се определят за всеки отделен случай от главния директор по поверителност и Централния отдел за спазване на изискванията за поверителност, местния СЗД и, според случая, всеки друг засегнат отдел. Освен това, ако Централния отдел за спазване на изискванията за поверителност открие индивидуални нарушения, ще бъдат предприети съответните дисциплинарни мерки до и включително незабавно прекратяване на трудовото правоотношение, доколкото това е разрешено от приложимото законодателство.
- 17.8. Субектът на данни ще получи отговор, уведомяващ го за резултата от неговата жалба. Това ще се случи своевременно и във всеки случай до един месец от получаването на жалбата (заедно с достатъчно подробни данни, за да може Amgen да установи естеството на жалбата и само ако е основателно необходимо, заедно с необходимата информация, за да се удостовери самоличността на жалбоподателя). Като се вземат предвид сложността и броя на исканията, едномесечният срок може да бъде удължен с не повече от два месеца, като в такъв случай Субектът на данни се уведомява за това.
- 17.9. Субектът на данни ще бъде уведомен, че ако не е удовлетворен от отговора на Amgen, може да заведе иск пред съдилищата на държавата членка на ЕИП или пред компетентните ОЗД. Не е задължително обаче Субектът на данни да мине през процедурата за разглеждане на жалби на Amgen, преди да има правото да подаде жалба до компетентните ОЗД или иск пред съдилищата на държава членка на ЕИП.

- 17.10. Този процес за разглеждане на жалби ще бъде оповестен чрез публикуването на ЗКП ЕС, както е посочено в раздел 7 по-горе.

## **18. Права и отговорности на заинтересовани трети страни**

- 18.1. Субект на данни, чиито Лични данни произхождат от ЕИП или са защитени от законите на ЕС за защита на данните и са предадени на Участващи дружества извън ЕИП, има право да иска прилагането на ЗКП ЕС в качеството си на заинтересована трета страна и има право да потърси съдебна защита, да получи средства за правна защита и когато е уместно, обезщетение за действително претърпени вреди в резултат на нарушение на настоящите ЗКП ЕС. Всички подобни жалби могат да бъдат подадени от Субекта на данните до компетентните ОЗД (които могат да бъдат ОЗД в държавата членка на ЕИП по обичайно пребиваване на Субекта на данните или ОЗД по месторабота или по мястото на предполагаемото нарушение). Субектите на данни могат също така да предявят иск пред компетентен съд в държава членка на ЕИП (това могат да бъдат съдилищата на държавата членка на ЕИП, в която съответното Участващо дружество е установено, или съдилищата на държавата членка на ЕИП, в която е обичайното пребиваване на Субекта на данни). Субект на данни може да бъде представляван при упражняването на правото си на ефективна съдебна защита срещу Участващо дружество от орган, организация или сдружение с нестопанска цел, при условие че този орган, организация или сдружение е надлежно учреден в съответствие с приложимото законодателство, има законоустановени цели, които са в обществен интерес, и извършва дейност в областта на защитата на правата и свободите на Субектите на данни, свързани със защитата на техните Лични данни. Субектът на данни има възможността да изиска прилагането на следните членове като заинтересована трета страна:
- 18.1.1. Членове 1 (Обхват), 2 (Дефиниции), 3 (Ограничение на целите), 4 (Качество на данните и пропорционалност), 5 (Правно основание за обработване на лични данни) и 6 (Обработване на Чувствителни лични данни);
  - 18.1.2. Член 7 (Прозрачност и право на информация);
  - 18.1.3. Членове 8 (Права на достъп, коригиране, изтриване и ограничаване на данни) и 9 (Автоматизирани индивидуални решения);
  - 18.1.4. Член 10 (Сигурност и поверителност), 11 (Отношения с Обработващи данните (Вносител на данни или Доставчик на Amgen) и 12 (Ограничения за предаване и последващо предаване);
  - 18.1.5. Член 16 (Действия в случай на национално законодателство, възпрепятстващо спазването на ЗКП ЕС) и 21 (Връзка между националните закони и ЗКП ЕС);
  - 18.1.6. Член 18 (Права и отговорности на заинтересовани трети страни); и
  - 18.1.7. Член 19 (Взаимопомощ и сътрудничество с ОЗД).
- 18.2. За избягване на съмнение правата на заинтересованата трета страна не се разпростират върху онези членове и елементи от настоящите ЗКП ЕС, които се отнасят до вътрешни механизми, изпълнявани в рамките на Участващите дружества или групата Amgen, като

подробности относно обучение (включително Приложение 2), програми за одит, вътрешни мрежи и структура за съответствие и механизма за актуализиране на ЗКП ЕС.

- 18.3. Amgen Франция поема отговорност и се съгласява да предприеме такива действия, каквито са разумно необходими за поправяне на действията на Участващите дружества, установени извън ЕИП. Amgen Франция ще плати обезщетение за всякакви материални или нематериални щети, произтичащи от нарушаването на настоящите ЗКП ЕС, освен ако може да докаже, че Участващото дружество, установено извън ЕИП, не е отговорно за събитието, което е довело до щетите. Amgen Франция разполага с достатъчни финансови средства и застрахователно покритие, за да изплаща обезщетения, свързани със ЗКП ЕС.
- 18.4. Всеки Субект на данни, който е претърпял вреди, произтичащи от нарушение на настоящите ЗКП ЕС от страна на Участващо дружество, което не е установено в ЕИП, има право, когато е целесъобразно, да получи обезщетение от Amgen Франция за претърпените вреди, като компетентни са съдилищата или други компетентни органи в ЕИП. Субектът на данни разполага със същите права и средства за правна защита срещу Amgen Франция, както ако нарушението е причинено от Amgen Франция в ЕС, а не от Участващото дружество, което не е установено в ЕИП. В случай че Участващото дружество, установено извън ЕИП, е отговорно или бъде признато за отговорно за такова нарушение, то ще обезщети Amgen Франция до степента, до която е отговорно или бъде признато за отговорно, за всички разходи, такси, вреди, разноски или загуби, понесени от Amgen Франция във връзка с нарушението.
- 18.5. В случай на иск от Субект на данни, че е претърпял вреди и е установил, че има вероятност такава вреда да е настъпила поради нарушение на настоящите ЗКП ЕС, тежестта да докаже, че вредите, понесени от Субекта на данни поради нарушение на настоящите ЗКП ЕС, не са по вина на съответното Участващо дружество, е върху Amgen Франция. В случай че Amgen Франция докаже, че Участващото дружество, установено извън ЕИП, не е отговорно за събитието, довело до вредата, то не носи отговорност за вредата.

## **19. Взаимопомощ и сътрудничество с ОЗД**

- 19.1. Участващите дружества си сътрудничат и си оказват взаимна помощ при разглеждането на искане или жалба от Субект на данни или при разследване или проучване от страна на компетентните ОЗД.
- 19.2. Участващите дружества ще отговарят в сътрудничество с главния директор по поверителност на искания, свързани със ЗКП ЕС, от компетентните ОЗД в подходящ срок с оглед на обстоятелствата на искането (и във всеки случай не по-късно от всеки краен срок, наложен от компетентния ОЗД) и достатъчно подробно въз основа на информацията, с която разполага Участващото дружество. Във връзка с въвеждането и текущото прилагане на ЗКП ЕС Участващите дружества трябва да отделят нужното внимание на съобщенията и препоръките на компетентния ОЗД и да се съобразяват с всички официални решения или известия, издадени от компетентния ОЗД.
- 19.3. Всеки спор, свързан с упражняването на надзор от страна на компетентен ОЗД върху спазването на настоящите ЗКП ЕС, се решава от съдилищата на държавата членка на този ОЗД, в съответствие с приложимото законодателство на тази държава членка.

## **20. Актуализации и промени на ЗКП ЕС**

- 20.1. Amgen си запазва правото да променя и/или актуализира настоящите ЗКП ЕС по всяко време. Подобна актуализация на ЗКП ЕС може да е необходима конкретно в резултат на нови правни изисквания, значителни промени в структурата на групата Amgen или на официалните изисквания, наложени от компетентните ОЗД.
- 20.2. Amgen ще съобщи бързо и своевременно за всички съществени изменения на ЗКП ЕС или на списъка на Участващите дружества на всички други Участващи дружества и на компетентните ОЗД, за да вземат под внимание промени в регулаторната среда и/или структурата на групата Amgen. По-специално, когато дадено изменение би засегнало степента на защита, осигурена от ЗКП ЕС, главният директор по поверителност незабавно ще съобщи предварително за такова изменение на компетентния ОЗД с кратко обяснение на причините за изменението. За някои промени може да е необходимо ново разрешение от компетентните ОЗД.
- 20.3. Главният директор по поверителност поддържа напълно актуален списък с Участващите дружества в ЗКП ЕС и проследява всички актуализации на правилата, и при поискване предоставя необходимата информация на Субектите на данни или на компетентните ОЗД. Всички административни изменения в ЗКП ЕС се съобщават редовно на Участващите дружества.
- 20.4. Не се извършва предаване на Лични данни на ново Участващо дружество под гаранциите на ЗКП ЕС, докато новото Участващо дружество не се обвърже със спазването на ЗКП ЕС и не е приведено в съответствие със ЗКП ЕС.
- 20.5. Всякакви административни изменения в ЗКП ЕС или в списъка на Участващите дружества се съобщават редовно на Участващите дружества и поне веднъж годишно на компетентните ОЗД с кратко обяснение на причините за актуализацията.
- 20.6. Значителните изменения на ЗКП ЕС се съобщават и на Субектите на данни по който и да е от начините по чл. 7 от ЗКП ЕС.

## **21. Връзка между националните закони и ЗКП ЕС**

- 21.1. Когато местното национално законодателство, приложимо за Участващо дружество, изисква по-висока степен на защита на личните данни, то има предимство пред ЗКП ЕС. Ако местното национално законодателство, приложимо за Участващо дружество, предвижда по-ниска степен на защита на личните данни от ЗКП ЕС, се прилагат ЗКП ЕС.
- 21.2. В случай че задълженията, произтичащи от местното национално законодателство, приложимо за Участващото дружество, са в противоречие със ЗКП ЕС, Участващото дружество информира своевременно главния директор по поверителност и спазва допълнителните изисквания, посочени в член 16 по-горе.
- 21.3. Във всички случаи личните данни се обработват в съответствие с член 5 от ОРЗД и съответното местно законодателство.

## **22. Окончателни разпоредби**

- 22.1. ЗКП ЕС влизат в сила след одобрението им от компетентния ОЗД и се прилагат за Участващите дружества след подписването на споразумението за приемане на ЗКП ЕС.
- 22.2. Не се извършва предаване към Участващо дружество, ако то не е обвързано с настоящите ЗКП ЕС. Когато Вносителят на данни престане да бъде обвързан от ЗКП ЕС, той е длъжен незабавно да върне или изтрие всички Лични данни (включително техни копия), които са били предадени по силата на настоящите ЗКП ЕС, с изключение на случаите, когато Вносителят на данни поема правно обвързващи задължения за поддържане на защитата на Личните данни в съответствие с глава V от ОРЗД, в които той може да запази Личните данни, които са били предадени по силата на настоящите ЗКП ЕС.
- 22.3. Вносителят на данни е длъжен незабавно да уведоми Износителя на данни, Amgen Франция и главния директор по поверителност, ако по някаква причина не е в състояние да спазва настоящите ЗКП ЕС (включително ситуациите, описани в член 12.3 по-горе). Когато Вносителят на данни нарушава настоящите ЗКП ЕС или не е в състояние да ги спазва, Износителят на данни трябва да уведоми главния директор по поверителност и да преустанови предаването на Лични данни.
- 22.4. По избор на Износителя на данни Вносителят на данни е длъжен незабавно да върне или изтрие всички Лични данни (включително техни копия), които са били предадени по силата на настоящите ЗКП ЕС, и да удостовери същото пред Износителя на данни, когато:
- 22.4.1. Износителят на данни е преустановил предаването на Лични данни, а спазването на настоящите ЗКП ЕС не е възстановено в разумен срок и във всички случаи в срок до един месец от преустановяването; или
- 22.4.2. Вносителят на данни е извършил съществено нарушение на настоящите ЗКП ЕС; или
- 22.4.3. Вносителят на данни не изпълни задължително решение на компетентен съд или компетентен ОЗД във връзка със задълженията му по настоящите ЗКП ЕС.

Вносителят на данни е длъжен да продължи да гарантира спазването на настоящите ЗКП ЕС, докато Личните данни не бъдат изтрети или върнати. Ако местните национални закони, приложими към Вносителя на данни, забраняват връщането или изтриването на Личните данни, предадени съгласно настоящите ЗКП ЕС, Вносителят на данни е длъжен да продължи да гарантира спазването на настоящите ЗКП ЕС и да обработва Личните данни само до степента и за срока, изисквани от тези местни национални закони.

## 23. Приложения

Приложенията са неразделна част от ЗКП ЕС.

Приложение 1: Преглед на потоците от данни на Amgen

Приложение 2: Преглед на програмата за обучение на Amgen



**Приложение 1: Преглед на потоците от данни на Amgen**

Субекти на данни	Категории данни	Цели	Предаване
Служител	<p>Идентификационни данни като име, адрес, дата и място на раждане, дата на наемане, социалноосигурителен номер, номера на кредитни карти, банкова сметка и финансова информация, както и номер на шофьорска книжка и издадена от държавата лична карта</p> <p>Отпуски и обезщетения, оплаквания, бонуси, повишения, прегледи и оценки, трудови досиета, информация, свързана със здравни и социални осигуровки, пенсионен план и подробности за опции за акции</p> <p>Данъчна и финансова лична информация</p> <p>Чувствителни данни като национален произход, когато това е разрешено от местното законодателство</p>	<p>Управление на персонала, поддръжка на информационни технологии и административни цели във връзка с трудовото правоотношение и обезщетения или администриране на доходи след напускане, както и за спазване на правните, административни и корпоративни задължения на Amgen</p>	<p>Глобалните бази данни на Amgen се намират в САЩ, където се намира седалището на Amgen Inc.</p> <p>Потоците от данни текат от Amgen Франция (или съответния Износител на данни) към Amgen Inc. в Съединените щати или към Участващи дружества в Швейцария. След което данните могат:</p> <ul style="list-style-type: none"> <li>- да бъдат само съхранявани и поддържани там</li> <li>- да бъдат анализирани за осигуряване на обща статистика и отчетност</li> <li>- да бъдат споделяни по-нататък в рамките на групата на Amgen с други Участващи дружества, когато има стопанска необходимост от такъв достъп от конкретен персонал или стопански функции в тези Участващи дружества (например: служител, който кандидатства за работа извън страната си или трябва да докладва на</li> </ul>
Здравни специалисти	<p>Име, данни за служебна връзка, включително телефон и имейл, специалност</p> <p>Професионален опит (автобиография)</p> <p>Участие в други изследвания</p> <p>Финансова информация (информация за фактуриране и плащания)</p>	<p>Администриране и управление на професионалните и научните дейности на Amgen – Научноизследователска и развойна дейност (например участие в медицински изследвания, клинични проучвания, професионални срещи или конгреси)</p> <p>Рекламирање на продуктите и услугите на Amgen</p> <p>Разкриване на финансова информация, когато се изисква от приложимото законодателство или за спазване на професионалните правила</p>	<ul style="list-style-type: none"> <li>- да бъдат споделяни по-нататък в рамките на групата на Amgen с други Участващи дружества, когато има стопанска необходимост от такъв достъп от конкретен персонал или стопански функции в тези Участващи дружества (например: служител, който кандидатства за работа извън страната си или трябва да докладва на</li> </ul>

		Спазване на нормативната уредба, като следене на безопасността и отчетност на нежелани събития	ръководител, базиран извън страната му). В повечето случаи тези Участващи дружества ще действат като Администратори на данни, но в зависимост от потребностите на дейността Участващите дружества могат да действат и като Обработващи данни (например: при предоставяне на поддръжка на IT Help Desk или при предоставяне на поддръжка, свързана с Центъра за услуги HR Connect).
Търговци/доставчици	Име на физическо лице, наименование на организацията, данни за служебна връзка  Информация за фактуриране и плащания	Обработка на плащанията към търговци и доставчици  Спазване на нормативната уредба, като например данъчните закони	
Субекти на данни от клинични изпитвания (които могат да включват деца на възраст под 18 години, когато има педиатричен пациент, участващ в клинично проучване, спонсорирано от Amgen).	Кодирани данни – името на пациента и данните за връзка се заменят с вътрешногенериран идентификационен номер. Само мястото на клинично изпитване (болница/място на изследване) поддържа списъка, за да обвърже идентификационния номер с името на пациента.  Непреки идентификатори като година или дата на раждане (пълната дата на раждане се събира само за педиатрични изследвания), пол, тегло, височина.  Необходимите данни за здравословното състояние, посочени в протокола на научното изследване.  Други данни, свързани с пациента, необходими за провеждането на изследването, включително етническа принадлежност, семейно положение (като брой деца), консумация на лекарства, алкохол, наркотици, общи навици или поведение, професионална ситуация като	Администриране и управление на биомедицински изследвания (клинични изпитвания, обсерваторни изследвания)	

	<p>работа, безработица, участие в други изследвания.</p>		
<p>Пациенти (сред които може да има деца под 18-годишна възраст, когато има нежелано събитие, включващо употребата на продукт на Amgen с педиатрично показание).</p>	<p>Косвени идентификатори на пациента като възраст, година или дата на раждане, инициали на пациента (когато е разрешено от местното законодателство), пол, тегло/ръст или идентификационен номер на пациента (с изключение на националните здравни идентификатори).</p> <p>Данни, свързани с идентификацията на продукта на Amgen, като например използван продукт или устройство, серийни номера на устройствата, метод на доставка или дозировка на продукта, партидни номера на продукта.</p> <p>Данни за здравословното състояние, включително проведено лечение, резултати от прегледи, естество на всеки нежелан ефект, лична или семейна анамнеза, съпътстващи заболявания или събития, рискови фактори, информация, свързана с предписването и употребата на лекарства и с терапевтичното поведение на здравните специалисти, участващи в лечението на заболяването на пациента.</p> <p>Други данни, свързани с пациента, необходими за оценка на неблагоприятното здравно събитие в съответствие със задълженията за спазване на нормативните изисквания, като етническа принадлежност, професионален живот, консумация на лекарства, алкохол, наркотици и/или общи навици или поведение.</p>	<p>Съответствие с нормативните изисквания и фармакологична бдителност, като следене на безопасността и докладване на нежелани събития (когато е разрешено от местното законодателство)</p>	

## **Приложение 2: Преглед на програмата за обучение на Amgen**

### ***Програма за обучение/осведоменост по отношение на поверителността и защитата на данните***

Програмата за обучение за поверителност и защита на данните се стреми да гарантира, че целият персонал на Amgen е подходящо обучен относно ЗКП ЕС на Amgen, както и всички правни задължения, които оказват влияние върху обработването на Лични данни. Тази програма съдържа различни елементи.

#### **Общо обучение за целия персонал на Amgen**

Целият персонал на Amgen трябва да провежда годишно онлайн обучение за защита на данните като част от обучението по Кодекса за поведение. Това обучение е задължително, наблюдава се и обикновено отнема около 75 минути. Това обучение включва ЗКП ЕС и информация относно последиците от наказателното и трудовото право и/или договора за услуги за персонала, който нарушава ЗКП ЕС.

#### **Специфично обучение за СЗД**

Всички СЗД на Amgen се обучават редовно за новите процеси чрез редовни разговори със СЗД, провеждани от Централния отдел за спазване на изискванията за поверителност, и семинари за поверителност на място и/или онлайн според необходимостта от информация. Всички СЗД имат достъп до страница в уикипедия, която дава отговори на най-често задаваните въпроси и предоставя насоки, както и връзки към външни ресурси.

#### **Специфично обучение за персонала**

Специфично обучение може да бъде осигурено при необходимост онлайн или на място, или чрез публикуване на информация във вътрешната мрежа на Amgen. Това обучение може да бъде насочено към конкретни групи, които ежедневно обработват Лични данни или подпомагат други групи, които обработват Лични данни. Например групата за одит, функциите за научноизследователска и развойна дейност и правният отдел се обучават редовно. Това включва информация за процедурите за управление на искания за достъп до Лични данни от страна на публични органи, когато това е от значение за конкретен персонал. Това обучение може да се провежда на регионално или на национално ниво. Други обучения специално по ЗКП ЕС могат да бъдат разработени според необходимостта от информация.

#### **Осведоменост**

Amgen има специална страница в своята вътрешна мрежа, посветена на поверителността и защитата на данните, която предоставя връзки към други вътрешни или външни ресурси.

Централният отдел за спазване на изискванията за поверителност на Amgen си сътрудничи с отдела за информационна сигурност по програмата Sentinel, която е глобална програма за повишаване на осведомеността на персонала на Amgen по отношение на информационната сигурност.

#### **Подпомагане на обучението**

Всички обучения, свързани с поверителността, се разработват от Централния отдел за спазване на изискванията за поверителност и се одобряват от главния директор по поверителност. Обучението може да бъде проведено пряко от представител на Централния отдел за спазване на изискванията за поверителност или от местен СЗД по модела „обучение на обучаващи“.