

## Публична декларация във връзка със задължителните фирмени правила на GSK

### Въведение

Дейностите на GSK („ние“, „нас“, „наши“) за управление на човешките ресурси (ЧР) и научни изследвания и развитие (НИРД) са свързани с обработването на „лични данни“ (вижте речника на термините), в това число с прехвърлянето на тези лични данни между държави. Поели сме ангажимент да прилагаме високи стандарти за почтеност при работата с лични данни и приехме задължителни фирмени правила (ЗФП), за да можем да извършваме международни прехвърляния на лични данни в рамките на групата ни от компании в съответствие със законите за защита на информацията на Европейския съюз, по-специално Общия регламент за защита на данните (Регламент 2016/679) (ОРЗД).

### Какво представляват задължителните фирмени правила?

Задължителните ни фирмени правила включват няколко документа, в това число стандарта и политиките ни за поверителност, споразумение между членовете на групата на GSK и настоящата публична декларация. Те се поддържат от обучение и одити. Целта на настоящата публична декларация е да обясним правилата и да гарантираме, че лицата, чиито лични данни обработваме за дейностите по управление на ЧР и НИРД, („вие“) са информирани за правата си съгласно ЗФП и как да ги упражняват.

В края на този документ можете да намерите речник на използваните термини. Ако се нуждаете от допълнителни подробности, копие от задължителните ни фирмени правила можете да получите, като се свържете с длъжностното ни лице по защита на данните съгласно правилата на ЕС на адрес [EU.DPO@GSK.com](mailto:EU.DPO@GSK.com).

### Обхват на ЗФП

Задължителните фирмени правила ще се прилагат към личните Ви данни, събирани за дейностите ни за управление на ЧР и НИРД, както е описано по-долу, когато се прехвърлят между държави от компания на GSK, която е предмет на законите за защита на данните на Обединеното кралство или ЕС в одобрените държави на ЕС, към държава извън Европейското икономическо пространство (ЕИП), където законите не осигуряват адекватна защита за личните данни.

Държави от ЕС, за които е получено одобрение: GSK получи одобрение на задължителните си фирмени правила в следните държави: Австрия, Белгия, България, Хърватия, Кипър, Чешката република, Дания, Естония, Финландия, Франция, Германия, Гърция, Унгария, Исландия, Ирландия, Италия, Латвия, Литва, Люксембург, Малта, Нидерландия, Норвегия, Полша, Португалия, Румъния (само за НИРД), Словакия, Словения, Испания, Швеция, Швейцария и Обединеното кралство.

Дейностите ни за управление на ЧР: те включват администриране и управление на работната ни сила; дейности по набиране и подбор на персонал; влизане в трудови правоотношения; администриране на заплати и придобивки; обучение, развитие и изпълнение на работата; управление на дисциплинарни процедури и процедури по обжалване; комуникация със служителите и предоставяне на препоръки; комуникация със служителите при спешни случаи; управление на процеса [Speak Up](#), който дава възможност за повдигане или докладване на опасения вътрешно; поддържане на бизнес операциите и осигуряване на достъпа на служителите до системите и изпълнението на задълженията им; скрининг и наблюдение на съобщенията на служителите; спазване на правните, регулаторни и други изисквания, приложими за нас, включително онези, свързани със законите и наредбите относно данъци, здраве и безопасност, дискриминация, поверителност на данните, трудови правоотношения и имиграция, задължения за съхранение на записи и отчетност, одит и държавни проверки; както и реагиране на съдебни процеси, търсене на законни права и средства за защита, защита при съдебни спорове и управление на вътрешни жалби или иски. Обработваната лична информация обхваща информация, свързана с настоящи, бивши или потенциални служители или „допълнителни работници“ на GSK (вижте речника на термините), както и на техните брачни партньори и зависими лица, в зависимост от случая.

Дейностите ни за управление на НИРД: те включват интервенционни и неинтервенционни клинични

проучвания, които са организирани, управлявани или финансирани от нас самостоятелно или съвместно с други организации, както и свързаните с тях дейности по спазване на нормативните изисквания, като например мониторинг на безопасността на пациентите и докладване на нежелани реакции. Обработваната лична информация включва информация, свързана с външни изследователи и участници в изследванията (вижте речника на термините).

Извън обхвата: Задължителните ни фирмени правила не уреждат обработването и прехвърлянето на лични данни от търговските ни подразделения (напр. лични данни, свързани с потребители или лица, свързани с доставчици на търговските ни подразделения). Тези данни са защитени в съответствие с различни законосъобразни механизми. Те не обхващат прехвърляния на лични данни от компании на GSK, намиращи се извън ЕИП, където не се подчиняват на законите за защита на данните на Обединеното кралство или ЕС.

Компании на GSK, обхванати от задължителните ни фирмени правила: Задължителните ни фирмени правила са обвързващи за всички компании в групата ни, които са подписали споразумението между членовете на групата, споменато по-горе. GlaxoSmithKline PLC, компания със седалище в Обединеното кралство, носи общата отговорност за това другите компании от групата по целия свят да спазват ЗФП, включително за отстраняване на нарушения на ЗФП.

## Нашите правила (според стандарта ни за поверителност)

### 1. Обработваме личните данни добросъвестно и законосъобразно

Спазваме приложимите закони по отношение на обработването на лични данни. В случай на конфликт между настоящите ЗФП и приложимите закони, а това вероятно ще има значителен отрицателен ефект, той трябва да бъде докладван на органа по защита на данните.

Причина за обработването: Обработваме лични данни само ако имаме законна бизнес цел и обработването е необходимо за тази цел. Цялото обработване е в съответствие с подходящо правно основание съгласно ОРЗД.

Правно основание за обработването: Обработваме лична информация въз основа на следните правни основания. Обработването трябва да е необходимо:

- (i) за изпълнението на договор, по който Вие сте страна, или за да предприемем действия по Ваше искане преди сключването на договор;
- (ii) за спазването на правните ни задължения;
- (iii) за изпълнението от нас на задача от обществен интерес;
- (iv) за защитата на Вашите жизненоважни интереси; или
- (v) за законни интереси, преследвани от нас или от трета страна, при условие че пред тези интереси нямат преимущество Вашите собствени интереси, права и свободи.

Специални категории данни: Предвид естеството на „специалните категории данни“ (вижте речника на термините), към тях трябва да се прилагат допълнителни предпазни мерки. Обработваме специални категории данни само в следните случаи:

- (i) когато е необходимо да спазваме правните си задължения и да упражняваме законните си права съгласно трудовото законодателство;
- (ii) когато е необходимо да защитаваме жизненоважните Ви интереси, когато сте физически или юридически неспособни да дадете своето съгласие;
- (iii) обработването включва лични данни, които явно са направени обществено достояние от Вас;
- (iv) когато е необходимо за установяване, упражняване или защита на правни претенции;
- (v) когато е необходимо по причини от важен обществен интерес; или
- (vi) за целите на превантивната или трудовата медицина, за оценка на трудоспособността на един от служителите ни, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управление на услугите и системите за здравеопазване и социални грижи съгласно приложимите закони или договор със здравен специалист. При тези обстоятелства обработването ще бъде извършено от здравен специалист, длъжен да спазва професионална тайна, или от друго лице, което има съответните задължения за пазене на тайна.

Искаме недвусмисленото Ви съгласие, за да обработваме личните Ви данни и специалните категории данни в случаите, когато това се изисква от закона или когато не можем да разчитаме на едно от горните основания.

## **2. Събираме и съхраняваме минималното количество лични данни, необходимо за постигане на конкретни и законни бизнес цели**

Събираме и съхраняваме минималното количество лични данни, необходимо за постигане на всяка законна бизнес цел. Вземаме мерки личните данни да са подходящи, уместни и да не са прекомерни по отношение на целите, за които събираме и/или ги обработваме допълнително. Когато е възможно, предпочитаме да използваме анонимизирана информация вместо лични данни, за да постигаме целите си. Полагаме усилия личните данни да са точни и, където е необходимо, поддържани в актуално състояние.

Съхраняваме личните данни само за периода, необходим за постигането на законна бизнес цел. След това изтриваме, унищожаваме или анонимизираме личните данни.

## **3. Обясняваме как ще се използват личните данни и какви са правата Ви**

Прозрачност: Дейностите ни за обработване на лични данни са прозрачни. Предоставяме информацията, изисквана съгласно приложимите закони, в момента на събиране на личните данни. Като минимум осигуряваме минималната информация, изисквана по силата на членове 13 и 14 от ОРЗД. Ако сме получили лични данни от трети страни, а не директно от Вас, възможно е (в зависимост от приложимото законодателство) да не Ви предоставим тези данни, ако това се окаже невъзможно или изисква несъразмерно големи усилия.

Управление на отделните права: Предоставяме Ви възможност да упражнявате правата съгласно ОРЗД, включително правото да:

- (i) имате достъп до личните си данни;
- (ii) да коригирате личните си данни;
- (iii) да изтривате личните си данни;
- (iv) да ограничавате или прекратявате обработването на личните си данни;
- (v) да предоставим копие от личната Ви информация на Вас или на трета страна;
- (vi) да не бъдат вземани автоматизирани решения за Вас (вижте по-долу);
- (vii) да оттегляте съгласието си; и
- (viii) да се откажете от получаването на маркетингови съобщения.

Освен това спазваме приложимите закони в държавите, които Ви дават и други права по отношение на личните Ви данни. Може да ограничим правото Ви на достъп до личните Ви данни с цел да защитим други (напр. правото на поверителност на друго лице).

Автоматизирано вземане на решения: При обработване на лични данни използваме в ограничена степен процедурите за автоматизираното вземане на решения. Използваме автоматизирано вземане на решения само ако:

- (i) то е необходимо за сключване или изпълнение на договор между нас и Вас;
- (ii) разрешено е по силата на конкретен закон на ЕС или на държава членка и са приложени предпазните мерки, предвидени по този закон; или
- (iii) Вие сте дали изрично съгласие.

## **4. Не използваме лични данни за допълнителни цели, които са несъвместими с целта, за която са били събирани първоначално**

Ограничаване на целта: Ще обработваме личните данни само по начин, който е съвместим със законната бизнес цел, за която са били събирани първоначално. Ще Ви уведомим, ако има нова цел за обработване на личните Ви данни.

## 5. Използваме подходящи предпазни мерки за сигурност

Защита на поверителността Ви: Внедряваме подходящи технически и организационни мерки за сигурност, за да предотвратим случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване или достъп до лични данни. Тези мерки са съобразени с рисковете, свързани с използването на лични данни, и включват най-съвременни технологии.

Управление на инциденти и нарушения: Ще уведомим органите по защита на данните в случай на нарушения на сигурността на личните данни, освен ако е малко вероятно тези нарушения да доведат до риск за правата и свободите Ви. Ще Ви уведомим в случай на нарушения на сигурността на личните данни, ако тези нарушения има вероятност да доведат до висок риск за правата и свободите Ви и (по наша преценка) при определени други обстоятелства. Поддържаме регистър на нарушенията на сигурността на личните данни, който включва подробности за нарушението, последиците (ако има такива) върху Вас, върху нас или друга страна, както и предприетите действия за справяне с него. Ще предоставим тези записи на компетентните органи по защита на данните при поискване от тяхна страна.

## 6. Внимателно контролираме разкриването на лични данни на трети страни

Управление на поверителността на трети страни: Разкриваме лични данни извън групата ни от компании в случаите, когато това се изисква по закон, във връзка със съдебно производство и в други ограничени и законосъобразни случаи. Възможно е също така да прехвърляме лични данни извън групата ни от компании до: (а) трети страни, действащи от наше име, включително доставчици; или (б) други независими трети страни, като например партньори, занимаващи се с изследвания и търговия, или регулаторни органи.

Когато разчитаме на трета страна да обработва лични данни от наше име, прилагаме подходящи договорни, организационни и оперативни механизми за контрол по отношение на тях, с цел да гарантираме поверителността и сигурността на личните Ви данни. Изискваме от тези трети страни да приемат всички разпоредби, посочени в член 28 на ОРЗД. Ако установим, че трета страна обработва лични данни, без напълно да спазва изискванията, наложени от нас, или приложимите закони, ще предприемем всички оправдани стъпки, за да бъдат нарушенията отстранени възможно най-бързо.

Прехвърляне на данни на трети страни: Когато прехвърляме лични данни между държави към трети страни, намиращи се в държави извън ЕИП, където законите за защита на данните не предлагат адекватно ниво на защита за личните данни, прилагаме одобрените стандартни договорни клаузи, подробности за които можете да намерите [тук](#), или разчитаме на друго законосъобразно изключение за прехвърляне на личната информация.

Подаване на информация до регулаторни органи: Когато се изисква от приложимите закони за защита на данните в държавите членки, уведомяваме или получаваме одобрение от съответния орган по защита на данните за обработването на лични данни (включително прехвърляне на лични данни между държави) и поддържаме тези уведомления и одобрения актуални в случай на промяна.

## 7. Прилагаме процедура на обжалване и уважаваме правото Ви на защита

Подаване на жалба до нас: Ако смятате, че може да не сме спазили правилата, заложили в нашите ЗФП, имате възможност да изкажете опасенията си директно към нас и Вашето оплакване ще бъде разгледано по вътрешната ни процедура за разрешаване на жалби. Приканваме Ви да подавате жалбите си във връзка с поверителността чрез [линията Speak Up](#).

Дейности за управление на ЧР: За служителите и останалите лица, чиито данни се обработват във връзка с дейности по управление на ЧР, можете да регистрирате жалба във връзка с поверителността до прекия си ръководител (в случая на служители на GSK), до длъжностното лице по съответствието за държавата, до местния представител за управление на ЧР или юридически представител, или до регионалния еквивалент на която и да е от тези функции, като всеки от тях ще я докладва по канала за жалби в рамките на GSK. Така жалбата ще стигне до групата по съответствие на бизнес звеното и до Центъра за високи постижения в областта на поверителността. Те независимо ще преценят правилния

начин на действие в отговор на жалбата Ви.

Управление на НИРД: За лица, чиито лични данни се обработват във връзка с НИРД, ако сте участник в проучване (вижте речника на термините), трябва да се свържете с лекаря или изследователя, провеждащ проучването, който ще препрати жалбата до нашия Център за високи постижения в областта на поверителността. Ако сте външен изследовател (вижте речника на термините), жалбата във връзка с поверителността може да се регистрира при длъжностното лице на GSK по съответствието за държавата или юридическия представител, или регионалния им еквивалент, като всеки от тях ще я докладва по канала за жалби в рамките на GSK. Те независимо ще преценят правилния начин на действие в отговор на жалбата Ви.

Ескалиране: Независимо откъде идват жалбите във връзка с поверителността, ако не могат да бъдат решени, те ще бъдат отнесени до по-високо ниво: (i) до съветник по поверителността на GSK за съответната държава, чиито данни за връзка са публикувани в уебсайта ни [тук](#); или (ii) след това до длъжностното лице на GSK по защита на данните за ЕС на адрес [EU.DPO@GSK.com](mailto:EU.DPO@GSK.com). Длъжностното лице по защита на данните за ЕС е последната инстанция в рамките на GSK за разрешаване на жалби, свързани със задължителните ни фирмени правила. Стремим се да решаваме жалбите експедитивно и, освен при възникване на извънредни обстоятелства, GSK ще се свърже писмено с Вас в срок до месец. Това съобщение може да съдържа следното: а) ще бъде изложена позицията ни относно жалбата и действията, които сме предприели или предстои да предприемем в отговор на жалбата; или (б) ще посочва кога ще бъдете информирани за позицията ни, което ще бъде не по-късно от два месеца след това. Ако желаете, можете да се свържете директно с длъжностното ни лице по защита на данните за ЕС.

Подаване на жалба до орган по защита на данните или съд: Имате право да подадете оплакване до: (i) компетентния орган по защита на данните в държавата на основното Ви местопребиваване, месторабота или където е възникнало предполагаемото нарушение; (ii) до комисаря по информационните въпроси или съдилищата на Обединеното кралство (като място, където се намира GlaxoSmithKline plc); (iii) съдилищата в държавата от ЕИП, от която личните Ви данни са прехвърлени от нас; и (iv) съдилищата в държавата от ЕИП, където е обичайното Ви местопребиваване. Използването на вътрешната ни процедура за жалби по никакъв начин не засяга правото Ви да използвате някоя от тези възможности.

Ако подадете жалба и можете да докажете, че сте претърпели материална или нематериална щета най-вероятно поради нарушение на задължителните ни фирмени правила, ние ще трябва да докажем, че не е имало такова нарушение. Ако орган по защита на данните или съд издаде заповед срещу компания на GSK извън ЕИП и тя не е в състояние или не желае поради каквато и да е причина да плати обезщетението или да спази разпоредбата в рамките на приложимия гратисен период, GlaxoSmithKline plc ще изплати присъденото Ви обезщетението директно или ще вземе мерки съответната компания на GSK да се съобрази със съдебното разпореджане.

### Речник на термините

„Анонимизирани данни“ означава лични данни, които са превърнати в анонимни по такъв начин, че лицето не може или вече не може да бъде идентифицирано.

„Външен изследовател“ означава външни лекари или други здравни специалисти, които участват или може да участват в НИРД.

„Допълнителен работник“ за GSK означава лице, с изключение на служителите на GSK, което предоставя услуги за или от името на GSK, включително лица без постоянен договор, които работят на място или от разстояние, професионални консултанти, временен персонал, доставчици и подизпълнители за предоставяне на услуги.

„Лични данни“ означава данни, отнасящи се до физическо лице, което е идентифицирано или може да бъде идентифицирано.

„Специални категории данни“ означава част от личните данни, свързани с расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни, обработвани с цел уникалното идентифициране на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

„Участник в проучване“ означава кандидати за участие или лица, участващи в изследователски дейности, или лица, приемащи продуктите или леченията ни, чиито лични данни обработваме в контекста на



---

лекарствената безопасност. Участниците в проучване включват лица, които са както външни, така и вътрешни спрямо GSK.

**[юни 2018 г.]**