Споразумение за обработка на данни

https://scratcher.io/bg/data-processing-agreement

Стандартна версия, последна актуализация: 22 октомври 2026 г. Това Споразумение за обработка на данни е неразделна част от споразумението между Вас и Scratcher ApS (CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Дания), когато използвате Scratcher. То е съставено в съответствие с изискванията на член 28 от GDPR.

Споразумение за обработка на данни

Това Споразумение за обработка на данни е неразделна част от Споразумението между Клиента и Scratcher. Ако това Споразумение за обработка на данни е приложено към Споразумението, клауза 10 от Общите условия не се прилага и се прилага настоящото Споразумение за обработка на данни.

1. Дефиниции

1.1. Освен ако контекстът изрично не изисква друго, следните термини с главна буква в настоящото Споразумение за обработка на данни имат следното значение:

- „Нарушение на сигурността на данните“ е всяко случайно или неправомерно унищожаване, загуба, промяна, неоторизирано разкриване или достъп до предавани, съхранявани или обработвани по друг начин Лични данни.
- „Администратор на лични данни“ означава Клиента, когато той определя целите и средствата за обработката на Лични данни съгласно дефиницията в GDPR.
- „Обработващ лични данни“ означава Scratcher, когато той обработва Лични данни от името на Администратора на лични данни.
- „Лични данни“ означава всяка информация, свързана с идентифицирано или идентифицируемо физическо лице (член 4, точка 1 от GDPR), която Обработващият лични данни обработва от името на Администратора на лични данни съгласно Споразумението.
- „GDPR“ означава Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).
- „Подобработващ лични данни“ означава всяко лице, с изключение на служител на Обработващия лични данни, ангажирано от Обработващия лични данни за обработката на Лични данни от името на Обработващия лични данни и в съответствие с неговите указания до степента и за целите, посочени в Споразумението за обработка на данни.

1.2. Термините с главна буква, които не са дефинирани по-горе, имат същото значение, както са дефинирани в Споразумението, освен ако контекстът изрично не изисква друго.

2. Обхват

2.1. Условията, съдържащи се в настоящото Споразумение за обработка на данни, се прилагат за обработката на Лични данни от Обработващия лични данни от името и по указания на Администратора на лични данни.

2.2. Когато в настоящото Споразумение за обработка на данни се прави позоваване на Обработващия лични данни, съответните разпоредби от Споразумението за обработка на данни се прилагат и за всеки Подобработващ лични данни, ангажиран от Обработващия лични данни.

3. Указания на Администратора на лични данни и условия за обработка

3.1. Обработващият лични данни обработва Личните данни само в съответствие с документираните указания на Администратора на лични данни, включително по отношение на предаването на Лични данни на трета държава, освен ако това не се изисква от правото на Съюза или правото на държава членка, което се прилага спрямо Обработващия лични данни. В такъв случай Обработващият лични данни информира Администратора на лични данни за това правно изискване преди обработката, освен ако това право забранява такова информиране на важни основания от обществен интерес.

3.2. Обработващият лични данни обработва Личните данни на тези категории субекти на данни, които Администраторът на лични данни (включително неговите клиенти) качва или изпраща при използване на Услугите. Видовете Лични данни и категориите субекти на данни, обработвани от името на Администратора на лични данни, са посочени в Приложение А към настоящото Споразумение за обработка на данни.

3.3. Страните се съгласяват да считат настоящото Споразумение за обработка на данни и Споразумението, което може да бъде сключено от Администратора на лични данни при използване на Услугите, за документирани указания на Администратора на лични данни. Администраторът на лични данни може да предостави на Обработващия лични данни допълнителни документирани указания за събирането на лични данни чрез коригиране на настройките на Услугите. Страните могат също така да се договорят писмено за изпълнението на допълнителни указания на Администратора на лични данни и цената за това.

3.4. Обработващият лични данни обработва Личните данни от момента на тяхното качване или предаване от Администратора на лични данни при използване на Услугите до премахването им, но не за по-дълъг период от посочения в член 12 от настоящото Споразумение за обработка на данни.

3.5. Обработващият лични данни незабавно информира Администратора на лични данни, ако според него дадено указание нарушава GDPR или други разпоредби на Съюза или на държава членка относно защитата на данните.

3.6. Администраторът на лични данни се задължава при поискване от Обработващия лични данни незабавно да предостави всяка информация, документи или съдействие, необходими на Обработващия лични данни, за да спази надлежно всички изисквания на GDPR при обработката на Личните данни от името на Администратора на лични данни.

4. Конфиденциалност на Личните данни

4.1. Обработващият лични данни използва Личните данни само за целите на предоставянето на Услугите и упражняването на правата си по Споразумението. Освен ако не се изисква друго от закона, Обработващият лични данни не разкрива Личните данни на трети страни.

4.2. Обработващият лични данни гарантира, че достъп до Личните данни се предоставя само на тези служители или доставчици на Обработващия лични данни, за които тези данни са необходими за изпълнение на техните задължения или за предоставяне на услуги на Обработващия лични данни, и че всички лица, упълномощени да обработват Личните данни, са поели ангажимент за конфиденциалност или са обвързани от съответно законово задължение за конфиденциалност.

4.3. Ако Обработващият лични данни е длъжен да разкрие Личните данни на трети страни (напр. правоприлагащи органи), за да спази изискванията на закона, Обработващият лични данни незабавно информира Администратора на лични данни за изискванията за разкриване на Личните данни, освен ако в закона не е предвидено друго.

4.4. Тези задължения за конфиденциалност остават в сила и след прекратяването на настоящото Споразумение за обработка на данни.

5. Технически и организационни мерки

5.1. Като взема предвид достигането на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработката, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, Обработващият лични данни прилага, преди обработката на Личните данни и по всяко време по време на обработката на Личните данни, подходящи технически и организационни мерки, необходими за гарантиране на сигурността на Личните данни. При избора и прилагането на технически и организационни мерки за осигуряване на подходящо ниво на сигурност Обработващият лични данни взема предвид по-специално рисковете, произтичащи от обработката на Личните данни на субекта на данните, от случайно или неправомерно унищожаване, загуба, промяна, неоторизирано разкриване или неправомерен достъп до предавани, съхранявани или обработвани по друг начин данни.

5.2. Тъй като Обработващият лични данни е професионалист в своята област и притежава знания и опит в предоставянето на Услугите, Обработващият лични данни избира и определя техническите и организационните мерки, необходими за постигане на целите, посочени в клауза 5.1 от настоящото Споразумение за обработка на данни, но тези мерки във всеки случай трябва да съответстват на изискванията на приложимото законодателство. Въпреки това Администраторът на лични данни има право да дава указания и предложения на Обработващия лични данни относно прилагането на технически и организационни мерки за сигурност. Обработващият лични данни взема предвид тези предложения на Администратора на лични данни, разглежда ги и (i) предоставя на Администратора на лични данни мотивиран отговор за това как Обработващият лични данни ще изпълни указанията на Администратора на лични данни (ii) предприема незабавни стъпки за прилагането на такива мерки.

5.3. Техническите и организационните мерки, приложени от Обработващия лични данни към момента на сключване на настоящото Споразумение за обработка на данни, са описани в Приложение B.

Обработващият лични данни поддържа система за управление на сигурността на информацията, сертифицирана по ISO/IEC 27001, и може да актуализира мерките с течение на времето, при условие че общото ниво на сигурност не се намалява.

5.4. Като взема предвид естеството на обработката и наличната информация, Обработващият лични данни съдейства на Администратора на лични данни за осигуряване на спазването на задълженията съгласно член 32 от GDPR.

6. Одит на обработката на данни

6.1. Обработващият лични данни предоставя на Администратора на лични данни цялата информация, необходима за доказване на спазването на задълженията, предвидени в член 28 от GDPR, включително текущия си сертификат по ISO/IEC 27001 и при поискване своята Декларация за приложимост (Statement of Applicability).

6.2. За да провери дали Обработващият лични данни обработва надлежно Личните данни, Администраторът на лични данни има право да извършва проверки на тази обработка при следните условия: (i) одитът трябва да се отнася само до обработката на Личните данни; (ii) Администраторът на лични данни трябва да уведоми Обработващия лични данни за желанието си да извърши одит в разумен срок, който не трябва да бъде по-малък от 4 седмици; (iii) одитът трябва да се извършва по такъв начин, че да не пречи на ежедневната дейност на Обработващия лични данни; (iv) одитът трябва да се извършва за сметка на Администратора на лични данни; (v) одитът трябва да се извършва от независимо лице, чиято кандидатура трябва да бъде предварително одобрена от Обработващия лични данни, като това одобрение не трябва да бъде неоснователно отказвано, и което трябва да се задължи да защитава Конфиденциалната информация на Обработващия лични данни.

6.3. Обработващият лични данни има право да получи възнаграждение за съдействието си при извършването на одита. Размерът на това възнаграждение се определя от Обработващия лични данни, като се вземат предвид разходите, направени от Обработващия лични данни във връзка с одита. Обработващият лични данни информира Администратора на лични данни за размера на възнаграждението преди одита.

6.4. Одитите и проверките, извършвани от компетентен надзорен орган, не подлежат на условията по клаузи 6.2 и 6.3.

6.5. Ако Администраторът на лични данни не е удовлетворен от резултатите от одита, Администраторът на лични данни има право едностранно, извънсъдебно, да прекрати настоящото Споразумение за обработка на данни и Споразумението. В такъв случай прекратяването на Споразуменията е единствената мярка, която може да бъде предприета от Администратора на лични данни, и Обработващият лични данни не е длъжен да обезщетява каквито и да било вреди на Администратора на лични данни.

7. Подобработващи лични данни

7.1. С настоящото Администраторът на лични данни дава на Обработващия лични данни общо предварително съгласие да ангажира Подобработващи лични данни, които ще обработват Личните данни от името на Обработващия лични данни в обхвата и за целите, посочени в настоящото Споразумение за обработка на данни.

7.2. Обработващият лични данни гарантира, че с ангажираните Подобработващи лични данни е сключено писмено споразумение, съгласно което Подобработващите лични данни се задължават да спазват същите задължения за защита на данните като тези, посочени в настоящото Споразумение за обработка на данни, и по-специално да предоставят достатъчно гаранции за прилагане на подходящи технически и организационни мерки по такъв начин, че обработката да отговаря на изискванията на GDPR. Обработващият лични данни носи отговорност пред Администратора на лични данни за изпълнението на задълженията на Подобработващите лични данни.

7.3. Актуалният списък на Подобработващите лични данни е посочен в Приложение Б към настоящото Споразумение за обработка на данни. Обработващият лични данни уведомява Администратора на лични данни за плановете си да замени или ангажира нов Подобработващ лични данни, като предостави тази информация на Администратора на лични данни не по-късно от 14 календарни дни преди планираното събитие.

7.4. Ако Администраторът на лични данни продължи да използва Услугите след замяната или ангажирането на нов Подобработващ лични данни, след като е бил уведомен от Обработващия лични данни в съответствие с процедурата, посочена в клауза 7.3 от настоящото Споразумение за обработка на данни, се счита, че Администраторът на лични данни е дал съгласие за тези действия на Обработващия лични данни. Ако Администраторът на лични данни не е съгласен с такава замяна или ангажиране на Подобработващия лични данни, Администраторът на лични данни има право да прекрати Споразумението едностранно по извънсъдебен ред. В такъв случай прекратяването на Споразумението е единствената мярка, която може да бъде предприета от Администратора на лични данни, и Обработващият лични данни не е длъжен да обезщетява Администратора на лични данни за каквито и да било вреди.

7.5. Ако Администраторът на лични данни оттегли общото си съгласие за ангажиране на Подобработващия лични данни, Обработващият лични данни има право едностранно да прекрати Споразумението по извънсъдебен ред, като това прекратяване се счита за извършено по важни причини и се счита, че Администраторът на лични данни не е претърпял вреди в резултат на това прекратяване.

8. Нарушение на сигурността на данните

8.1. Обработващият лични данни уведомява Администратора на лични данни за всяко Нарушение на сигурността на данните, засягащо Личните данни, на имейл адреса, посочен в Търговското предложение (Sales Proposal), или, ако такъв не е посочен, на имейл адреса на собственика на акаунта на Администратора на лични данни, без излишно забавяне, но не по-късно от 24 часа след като е научил за Нарушението на сигурността на данните, и като взема предвид естеството на предоставяните Услуги и обработката на Личните данни и наличната информация, предоставя

следната информация на Администратора на лични данни: (i) естеството на Нарушението на сигурността на данните, включително, когато е възможно, категориите и приблизителния брой на засегнатите субекти на данни; (ii) евентуалните последици от Нарушението на сигурността на данните; (iii) мерките, приложени или предложени за предприемане от Обработващия лични данни за справяне с Нарушението на сигурността на данните, включително, където е подходящо, мерки за смекчаване на евентуалните отрицателни последици от Нарушението на сигурността на данните; (iv) трите имена и информация за контакт на длъжностното лице по защита на данните или друго лице за контакт, което би могло да предостави допълнителна информация.

8.2. Обработващият лични данни документира всички Нарушения на сигурността на данните, включително фактите, свързани с Нарушението на сигурността на данните, неговите последици и предприетите коригиращи мерки. В случаите, предвидени в GDPR или друго приложимо законодателство, Обработващият лични данни предоставя тази документация на надзорния орган.

8.3. Като взема предвид естеството на обработката и наличната информация, Обработващият лични данни съдейства на Администратора на лични данни за осигуряване на спазването на задълженията му съгласно членове 33 и 34 от GDPR. Администраторът на лични данни носи отговорност за уведомяването на надзорния орган и, когато се изисква, на субектите на данни. Освен когато Нарушението на сигурността на данните е причинено от нарушение на задълженията на Обработващия лични данни съгласно настоящото Споразумение за обработка на данни, съдействието на Обработващия лични данни извън уведомлението по клауза 8.1 може да подлежи на допълнително заплащане.

9. Предаване на Лични данни на трети държави

9.1. Всяко предаване на лични данни на трети държави (извън ЕС/ЕИП) от Обработващия лични данни се извършва само въз основа на документирани указания от Администратора на лични данни и винаги в съответствие с Глава V от GDPR.

9.2. Одобрението от страна на Администратора на лични данни на Подобработващите лични данни, изброени в Приложение Б, представлява документирано указание за предаванията, които тези Подобработващи лични данни извършват, както е описано там. Всяко такова предаване се основава на решение относно адекватността на Европейската комисия (включително Рамката за поверителност на данните между ЕС и САЩ / EU–US Data Privacy Framework за сертифицирани получатели), Стандартните договорни клаузи на Европейската комисия или друг инструмент за предаване съгласно Глава V от GDPR.

10. Сътрудничество

10.1. Като взема предвид естеството на предоставяните Услуги и обработката на Данните на Клиента и наличната информация, Обработващият лични данни сътрудничи с Администратора на лични данни за осигуряване на изпълнението на задълженията, посочени в членове 32–36 от GDPR. За тази цел и само до степента, посочена в настоящото Споразумение за обработка на данни, Обработващият лични данни предоставя на Администратора на лични данни поисканата информация, необходима за надлежното изпълнение на задълженията на Администратора на лични

данни съгласно GDPR.

10.2. Когато даден вид обработка, по-специално при използване на нови технологии, и предвид естеството, обхвата, контекста и целите на обработката, има вероятност да доведе до висок риск за правата и свободите на физическите лица, Обработващият лични данни оказва подкрепа на Администратора на лични данни преди обработката при извършването на оценка на въздействието на предвидените операции по обработка върху защитата на Личните данни.

10.3. Ако субектът на данните, надзорният орган или трета страна поиска от Обработващия лични данни да предостави каквато и да е информация за обработваните Лични данни съгласно законите, Обработващият лични данни препраща тези искания на Администратора на лични данни без излишно забавяне. Обработващият лични данни се задължава да съдейства на Администратора на лични данни до необходимата степен при отговора на исканията на субектите на данни, надзорните органи или трети страни и при изпълнение на задълженията на Администратора на лични данни, свързани с упражняването на правата на субектите на данни, включително, но не само, правото на коригиране и изтриване на лични данни, правото на преносимост на лични данни, правото на възражение и ограничаване на обработката. Обработващият лични данни гарантира, че информацията, с която разполага, се съобщава в установените от закона срокове.

11. Задължения на Администратора на лични данни

11.1. Администраторът на лични данни определя по своя собствена преценка и на своя собствена отговорност видовете Лични данни и категориите субекти на данни, които да бъдат предоставени на Обработващия лични данни, и предоставя на Обработващия лични данни само Личните данни, необходими за надлежното предоставяне на Услугите от Обработващия лични данни. Администраторът на лични данни поема всички свързани рискове, включително рисковете Обработващият лични данни да получи повече Лични данни от необходимото.

11.2. Администраторът на лични данни декларира и гарантира, че е получил и ще поддържа през целия срок на Споразумението всички необходими разрешения и разрешителни, изисквани за предоставяне на Личните данни на Обработващия лични данни и за ангажиране на Обработващия лични данни да обработва Личните данни съгласно Споразумението.

12. Изтриване и връщане на Лични данни

12.1. При прекратяване на Споразумението или на настоящото Споразумение за обработка на данни, Обработващият лични данни, по избор на Администратора на лични данни, изтрива всички Лични данни, обработвани от името на Администратора на лични данни, или връща всички Лични данни на Администратора на лични данни (Администраторът на лични данни може да експортира данните си от Услугите по всяко време) и изтрива всички съществуващи копия и потвърждава пред Администратора на лични данни, че е направил това, освен ако правото на Съюза или на държава членка не изисква съхраняването на Личните данни. Копията в резервните копия се изтриват с изтичането на техния обичаен цикъл и междувременно не се използват за никакви други цели.

13. Отговорност

13.1. Независимо от каквито и да било вреди, претърпени от Администратора на лични данни, цялата отговорност на Обработващия лични данни съгласно настоящото Споразумение за обработка на данни се ограничава, както следва: общата отговорност на Обработващия лични данни и на всеки от неговите доставчици за всички претенции, произтичащи от или във връзка с настоящото Споразумение за обработка на данни, не надвишава сумата, действително платена от Администратора на лични данни на Обработващия лични данни за Услугите през дванадесетте (12) месеца, предхождащи датата на събитието, породило претенцията. В максималната степен, разрешена от приложимото право, в никакъв случай Обработващият лични данни или неговите доставчици не носят отговорност за каквито и да било специални, случайни, косвени или последващи вреди (включително, но не само, вреди от пропуснати ползи, загуба на данни или друга информация, прекъсване на стопанската дейност, телесна повреда, нарушаване на поверителността), дори ако Обработващият лични данни или доставчикът е бил уведомен за възможността от такива вреди и дори ако правната защита не постигне основната си цел.

13.2. Ограниченията в клауза 13.1 се прилагат само между страните. Те не се прилагат за отговорност, която не може да бъде ограничена съгласно приложимото право, и не засягат правата на субектите на данни съгласно член 82 от GDPR.

14. Валидност и прекратяване

14.1. Настоящото Споразумение за обработка на данни влиза в сила от влизането в сила на Споразумението и остава в сила, докато Споразумението остава в сила. Задълженията на Обработващия лични данни продължават, докато той обработва Лични данни от името на Администратора на лични данни.

15. Заключителни разпоредби

15.1. Обработващият лични данни уведомява за всяка промяна в Споразумението за обработка на данни най-малко 30 дни преди възнамеряваната промяна. Ако Администраторът на лични данни продължи да използва Услугите след обявяването на промените в Споразумението за обработка на данни, се счита, че Администраторът на лични данни се съгласява с промените в Споразумението за обработка на данни. Ако Администраторът на лични данни не е съгласен с промените, Администраторът на лични данни няма да може да използва Услугите и ще има право да прекрати Споразумението.

15.2. В случай на противоречие между настоящото Споразумение за обработка на данни и Споразумението, настоящото Споразумение за обработка на данни има предимство по отношение на обработката на Лични данни.

15.3. Настоящото Споразумение за обработка на данни се управлява от същото право и споровете се решават по същия начин, както е посочено в Споразумението.

15.4. Приложения:

- Приложение А: Подробности за обработката на Лични данни;
- Приложение Б: Одобрени Подобработващи лични данни;

- Приложение B: Технически и организационни мерки

Приложение A – Подробности за обработката на Лични данни

Предмет и времетраене	Обработката на Лични данни във връзка с Услугите за срока на Споразумението, а след това до изтриването или връщането на Личните данни съгласно клауза 12.
Естество на обработката	Хостинг и съхранение; събиране на Лични данни чрез кампаниите и формите на Администратора на лични данни; показване, експортиране и изтриване в Услугите; изпращане на имейли и съобщения до участници, които Администраторът на лични данни настройва (например потвърждения, кодове и известия за награди); предаване към собствените системи на Администратора на лични данни чрез интеграции, webhooks и API по указание на Администратора на лични данни; поддръжка и отстраняване на грешки.
Цел на обработката на Лични данни	За да се даде възможност на Администратора на лични данни да използва Услугите на Обработващия лични данни, както е договорено в Споразумението
Операция по обработка на Лични данни	Събиране и съхранение на Данните на Клиента, включително Лични данни, предоставени при използване на Услугите
Видове Лични данни	Собствено име, фамилия, имейл, IP адрес и приблизително местоположение, извлечено от него, дата и час на регистрацията (created at) и допълнителни данни като дата на раждане и телефонен номер (ако са събрани от Клиента). В зависимост от това как Администраторът на лични данни настройва своите кампании, също така отговори на въпроси в кампании, резултати от игри и спечелени награди, кодове, записи за съгласие, файлове, качени от участници (например изображения), и технически данни като информация за браузъра и устройството.
Специални категории данни	Не са предвидени. Администраторът на лични данни не събира специални категории лични данни (член 9 от GDPR) или данни за присъди и нарушения (член 10 от GDPR) чрез Услугите, освен ако не е договорено писмено.
Категории субекти на данни	Участниците в кампаниите на Администратора на лични данни (Клиента), посетителите на кампаниите на Администратора на лични данни, които не се регистрират (IP адрес, приблизително местоположение и информация за браузъра), и потребителите на Услугите на Администратора на лични данни, доколкото техните данни се обработват от името на Администратора на лични данни.
Място на обработка на Личните данни	Личните данни се обработват в помещенията на Обработващия лични данни и на виртуални сървъри, разположени в Европейския съюз, както и от Подобработващите лични данни, изброени в Приложение Б, на посочените там места.

Продължителност на обработката / Период на съхранение	Както е зададено от Администратора на лични данни в Услугите. В съответствие с клауза 9.4 от Общите условия, Обработващият лични данни може да изтрива Лични данни, които са по-стари от три (3) години.

Приложение Б – Одобрени Подобработващи лични данни

Към момента на сключване на Споразумението за обработка на данни Администраторът на лични данни одобрява ангажирането на Подобработващите лични данни, изброени по-долу. Предаванията извън ЕС/ЕИП се основават на Рамката за поверителност на данните между ЕС и САЩ (EU–US Data Privacy Framework), когато получателят е сертифициран, или на Стандартните договорни клаузи на Европейската комисия (клауза 9.2).

Подобработващ лични данни	Описание на обработката	Място на обработка
Amazon Web Services EMEA SARL, Люксембург (AWS)	Хостинг на Услугите: сървъри, бази данни, файлово съхранение, резервни копия, кеширане и логове	Европейски съюз (Стокхолм, Швеция). Съдържанието се доставя чрез мрежата Amazon CloudFront, която може да обработва трафик в периферни локации (edge locations) извън ЕС/ЕИП.
ClickHouse, Inc. (ClickHouse Cloud)	Аналитична база данни за статистика на кампаниите, като посещения, участия и регистрации, включително IP адрес и информация за браузъра	Европейски съюз (Франкфурт, Германия), хоствано в AWS.
Mailgun Technologies, Inc. (част от Sinch)	Изпращане на имейли, които Администраторът на лични данни настройва до участниците, като потвърждения, кодове и известия за награди, включително доставка, отваряне и кликвания, когато проследяването е активирано	Европейски съюз (регион ЕС за данни за съобщения); ограничена информация за акаунта може да се обработва в световен мащаб.
ip-api.com	Проверка на приблизителното местоположение на IP адресите на участниците и откриване на трафик от прокси сървъри и центрове за данни с цел спиране на измами и ботове	Румъния (ЕС); обработка или предаване на данни извън ЕС/ЕИП не може да бъде изключено.
Google (Gemini API)	ИИ функции в Услугите, като ИИ асистент, преводи и генериране на текст. Данните за участниците се изпращат само в псевдонимизирана или агрегирана форма (например инициали, имейл домейн и час на регистрация), освен ако потребителите на Администратора на лични данни не ги въведат сами	Съединени щати и потенциално други държави в зависимост от крайната точка на API и конфигурацията на обработката.

Подобработващ лични данни	Описание на обработката	Място на обработка
Functional Software, Inc. (Sentry)	Мониторинг на грешки и презаписване на сесии (session replays) за Услугите с цел намиране и отстраняване на грешки. Отчетите могат да включват вътрешни идентификатори на потребители и акаунти и технически данни за браузъра на потребителите на Администратора на лични данни. Текстът в презаписването на сесии е маскиран	Европейски съюз (Германия, регион Sentry EU).
Cloudflare, Inc. (Turnstile)	Защита от ботове във формите на кампании, само когато Администраторът на лични данни я включи за дадена кампания. Получава IP адреса и сигналите от браузъра на участника	Глобална мрежа; обработката може да се извършва извън ЕС/ЕИП.
Features & Labels, Inc. (fal.ai)	ИИ генериране и редактиране на изображения, премахване на фон и дублаж (voice-overs) в Услугите. Получава подканите (prompts) и изображенията, които потребителите на Администратора на лични данни изпращат	Съединени щати.
Adressevælger (adressevaelger.dk)	Предложения за адреси във формите на кампании, само когато Администраторът на лични данни ги включи за дадена кампания. Получава текста на адреса, който участникът въвежда, и IP адреса на участника	Дания (ЕС).

Приложение B – Технически и организационни мерки

Обработващият лични данни поддържа система за управление на сигурността на информацията, сертифицирана по ISO/IEC 27001:2022 от Bureau Veritas (сертификат № FIHSK27150F). Мерките включват:

- **Хостинг и физическа сигурност:** всички данни на клиентите се съхраняват в центрове за данни на Amazon Web Services (AWS) в Европейския съюз. Обработващият лични данни не оперира собствени сървъри; физическата сигурност и сигурността на околната среда се осигуряват от AWS, която е сертифицирана по ISO 27001 и SOC 2.
- **Мрежова сигурност:** сървърите и базите данни работят в частна мрежа (Amazon VPC), до която няма достъп от интернет. Само балансьорите на натоварването (load balancers) и мрежата за доставка на съдържание са публични, защитени от защитна стена за уеб приложения (AWS WAF) и защита от DDoS атаки.
- **Криптиране:** целият трафик се криптира с TLS (HTTPS). Базите данни, файловете и резервните копия са криптирани при съхранение (at rest) с AES-256. Данните за достъп за интеграции

допълнително се криптират на ниво приложение. Паролите са хеширани и подсилени (salted) с bcrypt.

- **Контрол на достъпа:** ролево базиран контрол на достъпа за потребителите на клиентите, двуфакторна автентификация и еднократен вход с Google (Google single sign-on), изтичане на сесиите и ограничен брой опити за вход. Достъпът на служителите следва принципа на най-малките привилегии и необходимостта да се знае (least privilege and need-to-know), използва уникални акаунти и мултифакторна автентификация, където е възможно, преразглежда се поне веднъж годишно и се отнема при напускане.
- **Разделение:** данните на клиентите са логически разделени по акаунти (изолация на наемателите / tenant isolation) и всяка заявка се авторизира.
- **Логване и мониторинг:** промените в инфраструктурата се записват в одиторска следа със защита срещу подправяне, логовете на приложенията се събират централно, платформата се наблюдава денонощно, а клиентите могат да виждат дневника с активността на своите потребители.
- **Наличност и устойчивост:** ежедневни криптирани резервни копия, съхранявани за най-малко седем дни и съхранявани отделно от продукционната среда, възстановявания, тествани поне веднъж годишно, и планове за непрекъсваемост на дейността и възстановяване при бедствия, които се преразглеждат и проиграват всяка година.
- **Управление на инциденти:** документиран процес за докладване, оценка, ограничаване, анализ и последващи действия при инциденти със сигурността, включително уведомяване за Нарушения на сигурността на данните съгласно клауза 8.
- **Сигурна разработка и операции:** сървърите работят като неизменяеми контейнери без SSH достъп, които никога не се променят ръчно, а промените се тестват преди пускане в експлоатация.
- **Хора:** служителите са обвързани от конфиденциалност и преминават обучение за осведоменост относно сигурността на информацията като част от системата за управление на сигурността на информацията. Партньорите с достъп до инфраструктурата самите те са сертифицирани по ISO 27001 и получават само достъпа, който работата им изисква.
- **Минимизиране на данни и инструменти за изтриване:** Администраторът на лични данни решава кои данни събира всяка кампания и може да експортира, изтрива или автоматично да изтрива данни за участниците.