

Договор за обработка на лични данни*

СТРАНИ

- 1) [ПЪЛНО ИМЕ НА ОРГАНИЗАЦИЯТА с идентификационен номер [...]] и адрес на управление [...], представлявано от [...] (**наричано по-долу за краткост Възложител или Администратор на лични данни**)
- 2) [ПЪЛНО ИМЕ НА ОРГАНИЗАЦИЯТА] с идентификационен номер [...] и адрес на управление [...], представлявано от [...] (**наричано по-долу за краткост Изпълнител или Обработващ лични данни**)

ВЪВЕДЕНИЕ

Възложителят и Изпълнителят са сключили договор за [*ПРЕДМЕТ НА ОСНОВНИЯ ДОГОВОР МЕЖДУ СТРАНИТЕ*] (**Основен Договор**), който налага Изпълнителят (в качеството му на обработващ лични данни) да обработва данни от името на Възложителя (в качеството му на администратор на лични данни).

Този договор за Обработка на лични данни регламентира допълнителните условия и изисквания, въз основа на които Изпълнителят ще обработва лични данни за целите на изпълнение на своите задължения по Основния договор. Този договор съдържа задължителните клаузи съгласно чл. 28 (3) от Общия регламент за защита на данните (ЕС) 2016/679 (**ОРЗД**) за договори между администратори и обработващи лични данни.

1. ДЕФИНИЦИИ

Бизнес цели: услугите, описани в Основния договор

Законодателство по защита на данните: всяко приложимо законодателство в областта на защита на данните, включително ОРЗД, както и всяко друго приложимо местно законодателство в Република България, свързано със защитата на личните данни и неприкосновеността на електронните комуникации.

Лични данни: всяка информация относно идентифицирано физическо лице или такова, което може да бъде идентифицирано, която бива обработвана от Изпълнителя, в резултат на или във връзка с доставката на услугите, уговорени в Основния договор.

Физическо лице, което може да бъде идентифицирано: лице, което може да бъде идентифицирано директно или индиректно, най-вече чрез идентификатор като: име, идентификационен номер, данни относно местоположението, онлайн идентификатор или един, или повече фактори, специфични за неговата

* Целта на този стандартен договор за обработка на лични данни е да се използва като допълнение към основен договор за доставка на стоки/услуги, когато изпълнението на задълженията по основния договор е свързано с обработване на лични данни. Договорът е изготвен в съответствие с Общия Регламент за Защита на Данните (ЕС) 2016/679 (GDPR).

физическа, психологическа, генетична, умствена, икономическа, културна или социална идентичност.

Нарушение на защитата на данните: нарушение на сигурността, което води до случайно или незаконосъобразно унищожаване, загуба, промяна, неоторизирано предаване или достъп до лични данни, предмет на обработване.

Обработване на лични данни: всяка дейност, която изисква употребата на лични данни. Това включва всяка операция или серия от операции (без значение дали са автоматизирани или не), свързани с лични данни, като например: събиране, записване, организация, структуриране, съхранение, адаптиране или промяна, възстановяване, употреба, предаване, разпространяване, комбиниране, ограничаване, изтриване или унищожаване. Обработката също включва и трансфер на лични данни до трети лица.

Оторизирани лица: лицата или категории лица, които, след одобрение от страна на Възложителя, могат да дават инструкции на Изпълнителя относно дейностите по обработване на лични данни.

Стандартни Договорни Клаузи (СДК): Стандартните Договорни Клаузи, одобрени от Европейската Комисия чрез Решение 2010/87/ЕС за трансфер на Лични Данни от страна – членка на Европейския Съюз към обработващ, установен в трета страна.

В случай на конфликт или неяснота между клауза в този Договор и:

- клауза в Основния Договор, клаузата в този Договор има предимство;
- клауза в СДК, СДК има предимство.

Субект на Данни: физическо лице, което е субект на лични данни.

2. ВИДОВЕ ЛИЧНИ ДАННИ И ЦЕЛИ НА ОБРАБОТКА

2.1. Възложителят и Изпълнителят приемат, че за целите на законодателството по защита на данните Възложителят е администратор, а Изпълнителят е обработващ лични данни.

2.2. Възложителят запазва контрол върху личните данни и остава отговорен за спазването на изискванията на законодателството по защита на данните, включително за предоставяне на необходимите изявления до субектите на данни и получаване на необходимите съгласия от субектите, както и за инструкциите за обработка, които предоставя на Изпълнителя.

2.3. *Приложение А* към този договор описва предмета, продължителността, вида и целите на обработване и видовете лични данни и категориите субекти на данни, спрямо които Изпълнителят може да извършва дейности по обработване с цел изпълняване на бизнес целите по Основния договор.

3. ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ (ОБРАБОТВАЩИЯ)

3.1. Изпълнителят се задължава да обработва предоставените му лични данни само до степента и по начина, които са необходими за изпълнението на бизнес целите и съобразно писмените инструкции на Възложителя. Той няма да обработва лични данни по начин, който не съответства на условията по този договор или на законодателството по защита на данните. Изпълнителят следва

да уведоми Възложителя без забавяне, ако според него инструкциите на Възложителя не са в съответствие със законодателството по защита на данните.

3.2. Изпълнителят следва да изпълни без забавяне всяка молба или инструкция на Възложителя, да промени, предаде, изтрие или да обработи по друг начин личните данни, или да спре, ограничи или поправи последствията от евентуално неоторизирано обработване.

3.3. Изпълнителят ще съхрани конфиденциалността на личните данни и няма да ги предоставя на трети лица, освен ако Възложителят или условията по този договор изрично не позволяват това предоставяне, или ако то не се изисква по закон. Ако съдебен или друг публичен орган изискат от Изпълнителя да обработи или предостави лични данни, той следва първо да уведоми Възложителя какво е правното основание за това и да даде възможност на Възложителя да възрази, освен ако не съществува законова забрана за извършването на такова уведомяване.

3.4. Изпълнителят ще положи разумни усилия да подпомогне Възложителя в спазването на задълженията му в областта на защита на данните, вземайки предвид същността на обработването и информацията, с която разполага.

3.5. Изпълнителят следва да уведоми Възложителя без забавяне за всякакви промени в законодателството по защита на данните, които могат да се отразят негативно на изпълнението на ангажиментите на Изпълнителя по този договор.

4. СЛУЖИТЕЛИТЕ НА ИЗПЪЛНИТЕЛЯ

4.1. Изпълнителят ще се увери, че всички негови служители:

- са информирани за това, че личните данни са обект на конфиденциалност и ограничения относно тяхната употреба;
- са преминали обучение по законодателството по защита на данните, и
- разбират както своите задължения, така и тези на Изпълнителя, във връзка със спазването на законодателството по защита на данните и този договор.

5. СИГУРНОСТ

5.1. Изпълнителят е длъжен да въведе необходимите технически и организационни мерки срещу неоторизирана или незаконна обработка, достъп, предоставяне, копиране, промяна, съхранение, възпроизвеждане, показване или дистрибуция на лични данни, включително, но не само, мерките за сигурност, описани в *Приложение В*.

5.2. Изпълнителят е длъжен да въведе такива мерки за сигурност, които са подходящи спрямо нивото на риска, включително, ако е подходящо:

- Псевдоминизация или криптиране на данните, както и други методи, които осигуряват конфиденциалността, целостта и устойчивостта на системите за обработка на данни.
- Изпълнителят следва да може да възстанови навременно достъпа до личните данни в случай на инцидент.
- Изпълнителят следва регулярно да тества и оценява ефективността на избраните мерки за сигурност.

6. НАРУШЕНИЕ НА СИГУРНОСТТА НА ДАННИТЕ

6.1. Изпълнителят следва да уведоми Възложителя без излишно забавяне, ако личните данни бъдат унищожени, загубени, увредени или станат негодни за

употреба. Изпълнителят трябва да положи всички разумни усилия да възстанови данните за своя сметка.

6.2. Изпълнителят следва да уведоми Възложителя [незабавно ИЛИ в рамките на [ОПРЕДЕЛЕН БРОЙ] часа] и без излишно забавяне, ако установи, че е налице:

- инцидентна, неоторизирана или незаконна обработка на лични данни, или
- нарушение на сигурността на данните.

6.3. В случай на възникване на инцидент Изпълнителят следва без излишно забавяне да предостави следната информация на Възложителя:

- описание на естеството на инцидента, включително категориите и приблизителния брой на засегнатите субекти на данни и масиви от лични данни;
- вероятните последици от инцидента, и
- описание на мерките, които Изпълнителят е взел или предлага да вземе за преодоляване на негативните последици от инцидента.

6.4. Непосредствено след всяка неоторизирана или незаконна обработка на лични данни или нарушение на сигурността на данните страните ще координират действията си по разследване на проблема. Изпълнителят ще предприеме разумни стъпки да съдейства на Възложителя, включително като:

- съдейства за разследването на инцидента;
- осигури физически достъп на Възложителя до засегнатите съоръжения и системи;
- организира разговори между своите служители и Възложителя (това може да включва и бивши служители на Изпълнителя);
- предостави достъп до документацията, която е създал, с цел спазване на законодателството за защита на данните, и
- вземе разумни и навременни мерки да ограничи вредните последици от нарушението на защитата на данните или незаконната обработка на лични данни.

6.5. Изпълнителят няма да уведомява трети лица за установено нарушение на защитата на данните, без първо да е получил писмено одобрение от страна на Възложителя, освен когато уведомяването им е задължително по закон.

6.6. Изпълнителят е съгласен, че единствено Възложителят има право да определи:

- дали да бъдат уведомени за нарушението на сигурността субектите на данни или регулаторния орган, когато това се изисква от закон или е решение на Възложителя, включително съдържанието и начина на изпращане на такова уведомление;
- дали да бъде предложена компенсация на субектите на данни и от какво естество.

6.7. Изпълнителят ще поеме всички разумни разходи, свързани с изпълнение на задълженията си при нарушение на сигурността на данните, освен ако инцидентът не е в резултат от изричните инструкции на Възложителя, небрежност или умишлено нарушение на този договор от страна на Възложителя. В тези случаи всички разходи са за сметка на Възложителя.

6.8. Изпълнителят следва да възстанови на Възложителя реалните и разумни разходи, които Възложителят е направил в резултат на нарушение на сигурността по вина на Изпълнителя, включително всички разходи по

уведомяване на субектите и/или регулаторния орган и предоставяне на обезщетения.

7. ТРАНСФЕР НА ЛИЧНИ ДАННИ ИЗВЪН ЕС/ЕИП

7.1. Изпълнителят (както и всеки подизпълнител на Изпълнителя) не може да извършва трансфери или друга форма на обработване на лични данни извън Европейския съюз (ЕС)/ Европейското Икономическо Пространство (ЕИП), без да получи писмено съгласие от Възложителя.

7.2. Когато такова съгласие е получено, Изпълнителят може да обработва, или да разреши да бъдат обработвани лични данни извън ЕС/ЕИП при следните условия:

- Изпълнителят обработва лични данни на територията на държава, за която има решение на Европейската Комисия, че е осигурено адекватно ниво на защита, или
- Изпълнителят участва в друг валиден механизъм за трансфер на данни извън ЕС/ЕИП, съгласно законодателството за защита на данните, който осигурява подходящи защиты, опазващи правото на защита на данните и неприкосновеността на личния живот на лицата. [Изпълнителят следва да посочи в *Приложение А* трансферния механизъм, който ще прилага, и да уведоми Възложителя незабавно за всяка промяна.], [или]
- Ако трансфер на лични данни между Възложителя и Изпълнителя изисква включването на СДК към този договор в резултат на това, че Изпълнителят е установен извън ЕС/ЕИП, страните ще попълнят необходимата информация и подпишат СДК в *Приложение Б*, и ще вземат всички други мерки да осигурят легитимността на трансфера.

8. ПОДИЗПЪЛНИТЕЛИ

8.1. Изпълнителят няма да оторизира трети лица или подизпълнители с обработването на лични данни.

ИЛИ (алтернативно)

8.2. Изпълнителят може да оторизира трето лице (подизпълнител) да обработва лични данни, ако:

- Възложителят предостави писмено съгласие преди всяко възлагане на обработването на подизпълнител **ИЛИ** има възможност да възрази срещу такова възлагане в рамките на [БРОЙ дни] след като Изпълнителят предостави пълна информация относно подизпълнителя;
- Изпълнителят ще сключи писмен договор с подизпълнителя, съдържащ условия, които по същество не се различават от тези в настоящия договор, по-специално условията, изискващи подходящи технически и организационни мерки. При писмено искане от страна на Възложителя, Изпълнителят ще предостави на Възложителя копия от такива договори;
- Изпълнителят ще запази контрол върху личните данни, чието обработване възлага на подизпълнителя; и
- Договорът с подизпълнителя се прекратява автоматично при прекратяване на този договор по каквото и да е било причина.

8.3. Информация за подизпълнителите, одобрени в момента на сключване на този договор, се съдържа в *Приложение А* и включва име и адрес на подизпълнителя и контактна информация на лицето, отговорно за спазване на правилата за защита на данните.

8.4. В случай че подизпълнителят не спази някое от задълженията си по договора си с Изпълнителя, последният остава изцяло отговорен пред Възложителя за изпълнението на задълженията на подизпълнителя.

9. ОПЛАКВАНИЯ, ИСКАНИЯ ЗА ДОСТЪП ДО ИНФОРМАЦИЯ И ПРАВА НА ТРЕТИ ЛИЦА

9.1. Изпълнителят е длъжен, без да изисква допълнително заплащане, да вземе подходящи технически и организационни мерки и да предостави навременно на Възложителя информация, която да му даде възможност да спазва задълженията си, свързани с:

- правата на субектите на данни по силата на законодателството по защита на данните, включително искания за достъп до информация, правото на поправка или изтриване на данни, възражение срещу обработване и автоматизирано обработване, и ограничаване на обработването;
- искания за информация от страна на регулаторния орган.

9.2. Изпълнителят следва да уведоми Възложителя незабавно, ако получи оплакване, искане или друга информация, свързана директно или индиректно с обработването на лични данни или със спазването на изискванията на законодателството по защита на данните.

9.3. Изпълнителят следва да уведоми Възложителя в рамките на [БРОЙ] работни дни след получаването на искане от субект на данни за упражняване на правото му на достъп до личните му данни или на някое друго от правата, дадени му по силата на законодателството по защита на данните.

9.4. Изпълнителят ще осигури на Възложителя пълно съдействие за отговора на всяко постъпило оплакване или искане.

9.5. Изпълнителят няма да предоставя лични данни на субект на данни или на трета страна, ако не е получил такава инструкция от Възложителя или не е длъжен да предостави данните по закон.

10. СРОК И ПРЕКРАТЯВАНЕ

10.1. Този договор ще бъде в сила докато:

- Основният договор е в сила, или
- Изпълнителят продължава да има контрол върху лични данни, свързани с основния договор.

10.2. Всяко нарушение на условията по този договор от страна на Изпълнителя представлява нарушение и на Основния договор, което дава основание на Възложителя да прекрати [Основния договор **ИЛИ** всяка част от Основния договор, оторизираща обработването на лични данни] без предизвестие и последващи задължения, при условие, че уведоми за това Изпълнителя писмено.

10.3. Ако в резултат на промяна на законодателството по защита на данните, която и да е от страните не може да продължи да изпълнява задълженията си по този договор, страните ще преустановят обработването на лични данни докато не се уверят, че съответната страна е в съответствие с новите изисквания.

11. ВРЪЩАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ

11.1. При искане от страна на Възложителя, Изпълнителят ще предостави на Възложителя копие или достъп до всички или част от личните данни, които Възложителят му е предоставил, по начин и във формат, в който Възложителят е разумно да ги изиска.

11.2. При прекратяване на Основния договор по каквото и да е причина или изтичане на договорния срок, Изпълнителят ще изтрие или унищожи по сигурен начин или, въз основа на писмени инструкции от Възложителя, ще върне всички лични данни, свързани с този договор.

11.3. Ако Изпълнителят има законово задължение да запази документи или други материали, които в противен случай би бил длъжен да върне или унищожи, Изпълнителят ще уведоми Възложителя писмено за това изискване, давайки подробна информация относно документите или материалите, които трябва да съхрани, законовото основание за съхранението, както и информация за това кога унищожаването ще бъде възможно.

11.4. Изпълнителят ще потвърди писмено, че е унищожил надлежно личните данни, в срок до [БРОЙ] дни след като е завършил процеса по унищожаване.

12. ОТЧЕТНОСТ

12.1. Изпълнителят ще води детайлна, точна и актуална писмена отчетност относно всяка дейност по обработка на лични данни, включително, но не само, информация за достъпа, контрола и сигурността на личните данни, одобрени подизпълнители, цели и категории обработки, трансфери до страни извън ЕИП и общо описание на предприетите технически и организационни мерки.

12.2. При искане от страна на Възложителя, Изпълнителят ще му предостави копия от поддържаната документация във връзка с обработването на лични данни.

12.3. Възложителят и Изпълнителят извършват преглед на информацията, съдържаща се в Приложенията към този договор, [веднъж годишно ИЛИ друг период] с цел да потвърдят нейната точност и да я актуализират при нужда.

13. ГАРАНЦИИ

13.1. Изпълнителят гарантира, че:

- Всички негови служители, подизпълнители или всяко друго лице или лица с достъп до лични данни са получили необходимото обучение по законодателството по защита на данните;
- Той, както и всяко друго лице, което обработва лични данни от негово име, ще спазват изискванията на законодателството по защита на данните;
- Имайки предвид съществуващите технологични решения и разходите за тяхното въвеждане, ще вземе подходящи технически и организационни мерки, за да предотврати неоторизирано или незаконно обработване на лични данни и случайна загуба или унищожаване или увреждане на лични данни, и ще осигури подходящо ниво на сигурност, съобразено с:
 - а) вредата, която може да произтече от такова неоторизирано и незаконно обработване или случайна загуба, унищожаване или повреждане;
 - б) естеството на личните данни; и
 - в) задължението си да спази приложимото законодателство по защита на данните и политиките си по информационна сигурност.

13.2. Възложителят гарантира, че очакваната употреба на личните данни от Изпълнителя за Бизнес целите по Основния договор е в съответствие със законодателството по защита на данните.

14. ИЗВЕСТИЯ

14.1. Всяко известие или друга комуникация до всяка от страните във връзка с този Договор следва да бъде в писмена форма и да е доставена до:

- За Възложителя: [...]
- За Изпълнителя: [...]

Този договор е сключен и влиза в сила от дата: [ДАТА]

Подпис:

[ЗА ВЪЗЛОЖИТЕЛЯ]

Подпис:

[ЗА ИЗПЪЛНИТЕЛЯ]

ПРИЛОЖЕНИЕ А

Цели на обработката

Предмет на Обработката:

Естество на Обработката:

Бизнес Цели:

Категории лични данни:

Категории субекти на данни

Оторизирани лица:

[Посочете законовата база, въз основа на която Изпълнителят обработва лични данни извън ЕИП (изберете една):

- *Установен е в държава, спрямо която има в сила решение за адекватност: [ДЪРЖАВА]*
- *Обвързващи Корпоративни Правила*
- *Стандартни Договорни Клаузи*
- *Сертификация по EU-US Privacy Shield*
- *Друго: [ОПИШЕТЕ ДЕТАЙЛНО]*

[Одобрени подизпълнители:

- *[ПОСОЧЕТЕ ВСИЧКИ ОДОБРЕНИ ПОДИЗПЪЛНИТЕЛИ]*

ПРИЛОЖЕНИЕ Б

Стандартни Договорни Клаузи

[Стандартните Договорни Клаузи при предаване на Лични Данни до Обработващи, установени в трети страни, които да включите в това Приложение и които са одобрени от Европейската Комисия, може да намерите в приложението към Решение 2010/87/ЕС, чиято българска версия е достъпна тук - <http://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32010D0087&from=en>]

Приложение В

Мерки за сигурност

Изпълнителят е осигурил следните технически и организационни мерки за осигуряване на сигурността на данните:

[Опишете конкретните мерки тук – те могат да включват: контрол на физическия достъп, достъпа до системи и бази данни; контрол върху предаването, back-up на данните и др.]