**1. Общ Регламент за защита на личните данни**

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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, наричан за краткост „Общ регламент за защита на данните“ или „ОРЗД“, осигурява защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

**2. Система за защита на личните данни**

**2.1.** Системата за защита на личните данни е разработена в съответствие с изискванията на ОРЗД и Закона за защита на личните данни (ЗЗЛД), публикуван в ДВ, бр. 1 от 4.01.2002 г. и друга приложима нормативна уредба в РБългария.

**2.2.** Системата е разработена и се прилага от СТИНГ АД.

**2.3.** Системата включва настоящата политика и процедурите, които следва СТИНГ АД като администратор на лични данни, наричан за краткост „администратор“.

**2.4.** Системата включва и инструкции и регистри за обработване на лични данни, както и други документи.

**3. Политика за защита на личните данни**

**3.1** Политиката за защита на личните данни се прилага за всички дейности по обработването на лични данни , включително тези, които се извършват относно лични данни на клиенти, служители, доставчици и партньори.

**3.2.** Тази политика се прилага от всички служители/работници на СТИНГ АД. Всяко нарушение на политиката и документите по конкретното й прилагане, ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, администраторът ще предостави наличните документи за разглеждане в най-кратък възможен срок на компетентните органи.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Фамилия** | **Длъжност** | **Дата** | **Подпис** |
| **Разработена** | **Младен Минев/ Мустафа Кючуков** | **Р-л АПО**  **Р-л ФО** | **12.11.2023г**  **15.11.2023г** |  |
| **Проверена** | **Любенова** | **ОДЛ** | **02.12.2023г** |  |
| **Одобрена** | **Георгиев** | **ИД** | **15.12.2023г** |  |

**4. Понятия**

***„Лични данни"*** - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано. Физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната,

психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

***„Данни за здравословното състояние“*** означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

***„Обработване***" - означава 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;

***„Администратор на лични данни"*** - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други, определя целите и средствата за обработването на лични данни;

***„Обработващ лични данни“*** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

***„Субект на данните“*** – всяко живо идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, чиито лични данни се обработват от администратора;

***„Съгласие на субекта на данните"*** - всяко 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 обработвани;

***„Дете“*** –Всяко физическо лице на възраст под 16 години;

***„Регистър с лични данни“*** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

***„Нарушение на сигурността на лични данни"*** - 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;

***„Основно място на установяване “***:

* за администратор, установен в една държава членка - мястото, където се намира централното му управление;
* за администратор, установен в повече от една държава членка - мястото, където се намира централното му управление, освен в случаите, когато решенията по отношение на целите и средствата за обработването на лични данни се вземат на друго място на установяване на администратора в ЕС и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване;
* за администратор със седалище извън ЕС основното място на установяване е мястото, на което е установено физическо или юридическо лице, установено в Съюза, което е назначено от администратора или обработващия лични данни в писмена форма, представлява администратора или обработващия лични данни във връзка със съответните им задължения по ОРЗД.

***„Получател"*** - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

***„Трета страна“*** – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни, имат право да обработват личните данни.

**5.** **Основни отговорности**

**5.1.** СТИНГ АД е администратор на лични данни съгласно ОРЗД, ЗЗЛД и настоящата политика.

**5.2.** Катоадминистратор на лични данни, СТИНГ АД самостоятелно определя целите и средства за обработване на личните данни.

**5.3.** СТИНГ АД е отговорно за разработване и насърчаване на добри практики в областта на обработване на лични данни.

**5.4.** СТИНГ АД е отговорно за осигуряване на ежегоден преглед на дейностите по обработка на данните и за извършване на необходимите актуализации на политиката и документите по конкретното й прилагане.

**5.5.** Данните за контакт със СТИНГ АД са:

- пощенски адрес: гр. София, п. код 1592, район Младост, бул. „Асен Йорданов“ № 6;

- имейл адрес: [office.sofia@stingpharma.com](mailto:office.sofia@stingpharma.com);

- телефон: 02 970 31; + 359 2 970 31;

- интернет страница: [www.stingpharma.com](http://www.stingpharma.com).

**5.6.** СТИНГ АД носи самостоятелно пълната отговорност в своите дейности по обработване на лични данни за спазването на законодателството за защита на данните и настоящата политика.

6. Принципи за защита на данните

Обработката на лични данни се извършва в съответствие с принципите за защита на данните, посочени в [член 5](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art5) от ОРЗД. Системата за защита на личните данни има за цел да гарантира спазването на тези принципи.

**6.1**. **Личните данни трябва се обработват законосъобразно, добросъвестно и прозрачно**

**6.1.1. Законосъобразно** – спазването на този принцип изисква идентифициране на законна основа (основания за обработване), преди да започне обработването на лични данни.

Обработването на лични данни е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

a) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

г) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

**Под „съгласие“ се разбира:**

- всяко 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;

- само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, не е валидно основание за обработване на лични данни;

- наличие на активна комуникация между администратора и субекта на данни;

- наличие на изрично писмено съгласие за специални категории данни, освен ако не съществува алтернативно законно основание за обработване.

**Субектът на данните може да оттегли своето съгласие по всяко време.**

д) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

е) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

**6.1.2. Добросъвестно** - спазването на този принцип изисква да се предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

**6.1.3. Прозрачно** – спазването на този принцип изисква предоставяне на информация на субектите на данни. Предоставяната информация следва да бъде подробна, в разбираема форма за лицето, на което се предоставя, конкретна, достъпна на ясен и разбираем език.

Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства.

С оглед реализиране правата на субекта на данни, информацията се предоставя без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията.

**6.2. Лични данни могат да се събират само за конкретни, изрично указани и легитимни цели и не се обработват по начин, несъвместим с тези цели**

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от официално обявените на надзорния орган като част от съответния Регистър на дейностите по обработване лични данни.

**6.3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел.**

**6.3.1.** Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация за поверителност и да бъдат одобрени от представляващ дружеството.

**6.3.2.** СТИНГ АД гарантира, че на годишна основа всички способи за събиране на данни се преглеждат, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни.

**6.4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент, както и да са положени необходимите усилия, за да е възможно своевременно изтриване или коригиране.**

**6.4.1.** Субектът на данните декларира, че данните, които предава за съхраняване са точни и актуални към датата на подаване.

**6.4.2.** Субектът на данните е задължен да уведомява администратора за всякакви промени в обстоятелствата, които водят до актуализиране на записите на лични данни.

**6.4.3.** СТИНГ АД е отговорен да осигури подходящо обучение на своя персонал и да гарантира, че този персонал е обучен в значението на събирането на точни данни и поддържането им в актуален вид и размер.

**6.4.4.** СТИНГ АД гарантира, че са налице подходящи правила за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която могат да бъдат променяни и други относими фактори.

**6.4.5.** Данните, които се съхраняват трябва да бъдат прегледани и актуализирани при необходимост от отговорника за обработване на лични данни в съответния регистър. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.

**6.4.6.** СТИНГ АД е отговорен за съответствие с исканията за корекция на данни в рамките на един месец

**6.4.7.** В случай че реши да не се съобрази с искането, СТИНГ АД информира за това субекта на данните, като обяснява мотивите за отказа и го информира за правото му да подаде жалба пред надзорния орган и/или да потърси правна защита.

**6.5. Личните данни трябва да се съхраняват в такава форма, че субектът на данните да може да бъде идентифициран само толкова дълго, колкото е необходимо за целите на обработването.**

**6.5.1.** Личните данни се съхраняват в съответствие със сроковете за съхраняване на записи и документи, съдържащи лични данни, посочени в регистрите на дейностите по обработване на данни и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания ред в ST OD 2-5.8/ (PROC 05).

**6.5.2.** СТИНГ АД прави преглед на сроковете на съхранение на личните данни, най-малко на годишна база и идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни ще бъдат надеждно унищожени в съответствие с действащите процедури и правила.

**6.5.3.** Всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в регистрите на дейностите по обработване на данни може да бъде направено само след изрично одобрение от Изпълнителен директор на база писмено искане от отговорника по обработване на данни в съответния регистър.

**6.5.4.** Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин*,* за да се защити самоличността на субекта на данните в случай на нарушение на данните.

**6.6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност**

**6.6.1.** За определяне формата и нивото за осигуряване на подходяща сигурност, отговорникът за обработване на данни в съответния регистър ще извършва оценка на въздействието (когато това е приложимо), като взема предвид всички обстоятелства, свързани с операциите по управление или обработване на тези данни, както и степента на евентуална вреда или загуба, която може да бъде причинена на физически лица, ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на дружеството. Извършването на оценка на въздействието се извършва съгласно реда, посочен в ST SOP 2-5 точка 8 за оценка на риска и въздействието върху защитата на данните (PROC 06).

**6.6.2.** При оценяването на подходящи технически мерки за осигуряване на подходяща сигурност, СТИНГ АД взема предвид следните възможности:

* Защита с парола;
* Автоматично заключване на бездействащи работни станции в мрежата;
* Премахване на права на достъп за USB и други преносими носители с памет;
* Антивирусен софтуер и защитни стени;
* Предоставяне на права за достъп основани на роли, включително тези на назначен временно персонал;
* Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
* Нивото на сигурност на локални и широкообхватни мрежи;
* Технологиите за подобряване на поверителността, като например псевдонимизиране, анонимизиране, криптиране;
* Прилагането на подходящи международни стандарти за сигурност, подходящи за администратора;
* Ограничаване изнасянето на лични данни извън територията на администратора;
* Физическа охрана и видеонаблюдение;
* Ограничаване достъпа до помещения на администратора.

**6.6.3.** При оценяването на подходящите организационни мерки администраторът взема предвид следните възможности:

* Възможностите за подходящо обучение;
* Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
* Включването на отговорностите за защита на данните в трудовите договори и длъжностните характеристики;
* Прилагане на дисциплинарни мерки за нарушения по отношение на обработването на данни;
* Проверка на персонала за спазване на съответните правила за сигурност;
* Контрол на физическия достъп до електронни и хартиено базирани записи;
* При напускане на работното място, цялата работна документация е премахната или прибрана в подходящи за това и с ограничен достъп места - специални шкафове, заключени помещения, унищожаване на вече ненужни документи и т.н. Съхраняване на данните на хартия в заключващи се шкафове;
* Ограничаване използването на служебни портативни електронни устройства извън работното място;
* Забрана за използването от служителите на лични устройства на работното място за целите на обработването на лични данни;
* Приемане на ясни правила за създаване, ползване, актуализация и съхранение на пароли;
* Поддържане на резервни копия на личните данни;
* Включване договорни задължения на контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на лични данни извън ЕС.

**6.6.4.** Служителите на СТИНГ АД са отговорни за гарантирането сигурността на данните, които те обработват, както и че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако администраторът не е дал такива права на съответния служител.

**6.6.5.** Всички лични данни трябва да бъдат достъпни само за тези служители, които се нуждаят от тях при изпълнение на служебните си задължения и във връзка с това са изрично упълномощени да обработват определени лични данни.

**6.6.6.** Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

* на хартиен носител – по възможност - в самостоятелна стая с контролиран достъп и/или в заключен шкаф или в картотека;
* на електронен носител - с парола за достъп в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация и/или в специализирана база данни изградена чрез Microsoft SQL Server технология.
* на преносими носители, които са защитени в съответствие с организационните и техническите мерки за контролиране на достъпа до информация.

**6.6.7.** Всеки служител/работник е длъжен да премине обучение и да приеме съответните договорни клаузи и мерки за достъп, както и правилата за приключване на дейностите по обработване на лични данни, преди да им бъде предоставен достъп до информация от всякакъв вид.

**6.6.8.** Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат унищожени.

**6.6.9.** Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данни (PROC 05). Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани или унищожени по друг начин. Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури.

**6.6.10.** Персоналът трябва да бъде изрично упълномощен да обработва лични данни извън територията на обектите на СТИНГ АД.

**6.6.11.** Изборът на подходящи мерки за защита на лични данни се извършва въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват, с изричното одобрение на представляващ СТИНГ АД по писмено предложение от отговорника за обработване на данни в съответния регистър.

**6.6.12.** При установено нарушение на сигурността се прилага ST SOP 2-5 точка 6.1.8 съобразно член 33 от ОРЗД – „Уведомяване на надзорния орган за нарушение на сигурността на личните данни“, и член 34 от ОРЗД – „Съобщаване на субекта на данните за нарушение на сигурността на личните данни“(PROC 07).

**6.7. Спазване на принципа на отчетност**

СТИНГ АД ще доказва спазването на принципите за защита на данните чрез практическото прилагане на системата за защита на личните данни, чрез приемане на техники по защита на данните на етап проектиране обработването на лични данни и/или като се присъединява към кодекси за поведение в приложимите случаи.

7. Права на субектите на данни

**7.1.** Субектът на данни има следните права по отношение на обработването на данни от СТИНГ АД:

* Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;
* Да поиска копие от своите лични данни, които се обработват;
* Да иска коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
* Да изиска изтриване на лични данни (право „да бъдеш забравен");
* Да иска ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
* Да направи възражение срещу обработване на негови лични данни;
* Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
* Да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на ОРЗД или ЗЗЛД е нарушена;
* Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат. При предаване или прехвърляне на лични данни към друг администратор се прилага ST SOP 2-5 точка 6.1.3 за преносимост на данни (PROC 03);
* Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане;
* Да не е обект на автоматизирано взети решения, които го засягат в значителна степен, без възможност за човешка намеса;
* Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие.

**7.2**. СТИНГ АД осигурява условия, които да гарантират упражняването на тези права от субекта на данни съгласно правилата, посочени в ST SOP 2-5 точка 6.1.4 за управлeниe на исканията и жалбите от субектите на лични данни (PROC 02):

* Субектите на данни могат да направят искания за достъп до данни и да получат отговор;
* Субектите на данни имат право да подават жалби, свързани с обработването на личните им данни, с обработването на искане от субекта на данни и с начина на обработване на жалбите.

8. Разкриване на данни

**8.1.** СТИНГ АД осигурява условия, при които личните данни не се разкриват на неупълномощени трети страни.

**8.2.** Необходимо е на служителите да се извършва специално обучение и при необходимост инструктажи, с цел да се избегне рискът от неправомерно разкриване на данни.

**8.3.** Всички искания от трети страни за предоставяне на данни трябва да бъдат мотивирани с подходяща документация и всички такива разкривания на данни да бъдат специално разрешени от представляващ СТИНГ АД.

9. Съхраняване и унищожаване на данните

**9.1.** Не се съхраняват лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

**9.2.** Може да съхраняват данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

**9.3.** Периодът на съхранение за всяка категория лични данни е посочен в регистрите на дейностите по обработване на данни, както и критериите, използвани за определяне на този период, включително законови задължения.

**9.4.** Правилата за унищожаване на информацията върху вече неизползвани записващи носители ще се прилагат във всички случаи.

**9.5.** Личните данни трябва да бъдат унищожени съгласно принципа за гарантиране подходящо ниво на сигурност, включително и защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. Прилага се ST SOP 2-5 точка 6.1.5 за съхраняване и унищожаване на данни (PROC 05).

10. Трансфер на данни

**10.1.** Всеки износ на лични данни от рамките на ЕС към страни извън ЕС, страните по Споразумението за Европейското икономическо пространство и Конфедерация Швейцария (посочени в Общия регламент като "трети държави") са незаконни, освен ако няма подходящо ниво на защита на основните права на субектите на данни. Прехвърлянето на лични данни към трети държави е забранено, освен ако не се прилагат една или повече от посочените по-долу гаранции или изключения.

**10.2. Решение за адекватност**

Европейската комисия може да оцени трети държави, територия и/или специфични сектори в трети държави, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица.

СТИНГ АД може да трансферира данни в случай на положително решение на Европейската комисия.

**10.3. Щит за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield)**

Администраторът може да прехвърли лични данни в САЩ след проверка и потвърждение, че организацията, пожелала получаването на такива данни е подписала и поддържа валидно Рамковото споразумение „Privacy Shield“ с Министерство на търговията на САЩ.

**10.4. Стандартни договорни клаузи**

СТИНГ АД може да прилага приети от Европейската комисия или от съответния надзорен орган и одобрени от Комисията стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство.

**10.5. Изключения**

При липса на решение за адекватност, членство в US Privacy Shield, и/или стандартни договорни клаузи, СТИНГ АД може да прехвърли лични данни в трета държава или международна организация само при едно от следните условия:

* субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такова прехвърляне;
* предаването е необходимо за изпълнението на договор между субекта на данните и СТИНГ АД или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
* предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данни между СТИНГ АД и друго физическо или юридическо лице;
* предаването е необходимо поради важни причини от обществен интерес;
* предаването е необходимо за установяването, упражняването или защитата на правни претенции;
* предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
* предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

В случаите на трансфер на лични данни към трети страни и/или международни организации се прилага ST SOP 5-2 точка 6.1.9 за предаване на лични данни на трети държави или на международни организации (PROC 08).

11. Регистър на обработванията на данни (инвентаризация на данните)

**11.1.** СТИНГ АД е извършил първоначална инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с ОРЗД.

**11.2.** В процеса на оперативната дейност СТИНГ АД извършва анализ на обработваните данни, за да установи:

* бизнес процесите, които използват лични данни;
* източниците на лични данни;
* ориентировъчен брой на субектите на данни;
* описание на категориите лични данни и елементите във всяка категория;
* дейностите по обработване;
* целите на обработването, за което личните данни са предназначени;
* правното основание за обработването;
* получателите или категориите получатели на личните данни;
* основните системи и места за съхранение;
* всички лични данни, които подлежат на трансфери извън ЕС;
* сроковете за съхранение и унищожаване.

**11.3.** Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване, СТИНГ АД извършва оценка на въздействието на предвидените операции по обработване върху защитата на личните данни.

**11.4.** Когато в резултат на оценката на въздействието е ясно, че СТИНГ АД ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, се взема от представляващ дружеството.

**Приложими документи:**

1. Процедура за правилата за администриране на личните данни
2. Оперативни документи по ИСУ свързани с изискванията заложени в Закона за защита на личните данни.