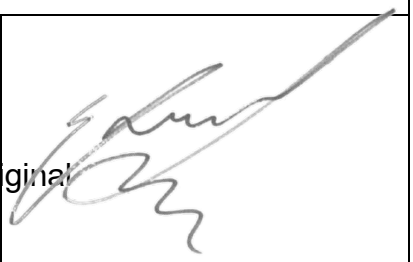
STADA	**Local Policy (LP)**	Номер: 007 Версия 01 В сила от: 01.06.2021 г.

Заглавие:	**SOP 007 - Политика за неприкосновеност на данните**
Отговорен корпоративен отдел:	Compliance/DPO
Автор:	Local Data Protection Coordinator & Local Compliance Coordinator
Списък за разпространение:	STADA България ЕООД - целия екип
Приложимо за:	STADA България ЕООД

Подписи / одобрение:		
Stefan Dinev signed original General Manager	Plamena Uzunova signed original Local Data Protection Coordinator	 Local Compliance Coordinator

Съдържание

1 Цел

(1) Целта на тази Политика е да гарантира, че *Личните данни* не се събират, обработват и използват произволно, а само до степента, необходима и законно допустима. Най-важните принципи от приложимите регламенти за защита на данните (в частност Общият регламент относно защита на данните (ОРЗД) и местния закон - Закон за защита на личните данни)) трябва да бъдат посочени и обобщени.

(2) Освен това, тази Политика е предназначена да защитава и подкрепя установената ценност INTEGRITY „почтеността“ в STADA. Почтеността е една от нашите ключови ценности и е от централна важност за нас като фармацевтично дружество, тъй като пациентите и потребителите се доверяват на STADA и продуктите му във връзка със здравето и благосъстоянието си. Тя е също така от голямо значение за нашите бизнес партньори, органите и другите заинтересовани страни.

(3) Тази Политика за защита на данните е ключов стълб на Системата за управление на съответствието на STADA (Compliance Management System) и цели допълнително да уточни главните принципи в тази чувствителна област, които вече са били изложени в Кодекса за поведение и Глобалната политика за защита на данните на STADA.

2 Обхват

(1) Тази Политика постановява защитата на

1. *Личните данни* (конкретно на служители, клиенти и бизнес партньори) и
2. *Специални категории лични данни* (конкретно на пациенти в случаите на клинични изпитвания или обсервационни проучвания).

(2) Тази Политика е валидна за STADA България ЕООД и трябва да бъде спазвана от цялото ръководство и от всички служители (заедно „Адресатите“).

3 Съдържание

3.1 Определения

(1) *Лични данни* означава всяка информация, свързана с идентифицирано или възможно да бъде идентифицирано лице (субект на данни).

(2) *Специални категории лични данни* са *Личните данни*, разкриващи расов или етнически произход, политически убеждения, религиозни или философски вярвания, както и генетични данни, биометрични данни, здравни данни или данни относно половия живот или сексуалната ориентация на физическо лице. *Специалните категории лични данни* са специално защитени данни.

(3) *Обработването на данни* се отнася до събирането, съхранението, модифицирането, предаването, използването, ограничаването, изтриването, псевдонимизирането и анонимизирането на личните данни.

(4) *Носители на данни* за целите на тази Политика са всички носители, на които може да се или се съхранява информация. Това определение включва в частност хартия, CD, DVD, USB флашка, SSD, чип карта, твърд диск или сървър.

3.2 Data Protection Coordinator

(1) STADA България ЕООД по закон не е задължена да назначи DPO (data protection officer). Независимо от това, ние приемаме сериозно защитата на данните. Затова сме назначили **местен** data protection coordinator. Data protection coordinator наблюдава съответствието с разпоредбите за защита на данните и консултира по въпросите за защита на данните.
С data protection coordinator можете да се свържете на адрес: plamena.uzunova@stada.bg.
С compliance coordinator можете да се свържете на адрес: elena.mangarova@stada.bg

3.3 Основни принципи за неприкосновеност на данните

(1) Всяко лице в обхвата на тази Политика трябва да се информира за разпоредбите за защита на данните, за да бъде в съответствие. Това задължение за информиране включва участие в курсове за обучение и запитване относно приложимите регламенти за защита на данните в индивидуалните случаи.

(2) *Избягване на данни* и *минимизиране на данни*: Трябва да се събират, обработват и използват възможно най-малко лични данни. На всеки е разрешено само да получи или прегледа информацията, която му е необходима за неговата работа, но не повече (**принцип за минимум информация**). Това включва например съхраняване на данни на устройства с ограничен достъп или използването на функцията за копия BCC при изпращане на имейли до неизвестна, хетерогенна група получатели.

(3) *Ограничаване на предназначението:* Личните данни могат да бъдат използвани само за целта, за която са събрани или съхранявани.

(4) *Сигурност на данните*: Трябва да се вземат технически и организационни мерки за предотвратяване на неупълномощеното обработване. Това включва например заключване на екрана при напускане на работното място или използване на сигурни пароли/ПИН.

(5) *Точност и актуалност на данните*: Личните данни трябва да бъдат съхранявани правилно, цялостно и актуално. Неточните, непълни или неактуални данни трябва да бъдат изтривани, коригирани, допълвани или актуализирани.

(6) *Изтриване на данните: Личните данни* трябва да бъдат изтрити веднага щом целта, за която са били събрани, вече не е валидна или повече не са необходими за целта. Преди изтриване на данните е необходимо да се провери дали регламентите за съхранение не се противопоставят на изтриването. Ако не е възможно да се изтрият данните, обработването на данните трябва да бъде ограничено като алтернатива.

(7) *Поверителност*: Секретността на данните се прилага към *Личните данни.* Те трябва да бъдат третирани поверително. Поверителността също важи след края на трудовите правоотношения.

(8) Просто правило: При работа със *Специални категории лични данни* трябва да се спазват по-строги условия/изисквания при всички горепосочени области.

3.4 Ангажиране на местен Compliance Coordinator и местен Data Protection Coordinator

(1) Местният Data Protection Coordinator или местният Compliance Coordinator трябва да бъдат легитимно ангажирани и информирани преди въвеждането или модифицирането на нова процедура за обработване на *Лични данни* в конкретен софтуер.

(2) Местният Data Protection Coordinator или местният Compliance Coordinator трябва да се включи в прехвърлянията на данни до трети страни за обработване на данните (вижте Раздел 3.7.)

(3) Искания на субекта на данни: Всеки субект на данни има правото да получи информация относно обработените лични данни, които го/я касаят, право да коригира тези данни или - обект на определени допълнителни изисквания - правото да накара те да бъдат изтрити (правото да бъдеш забравен). В допълнение, всеки субект на данни има следните права: право на ограничаване на обработването, право на преносимост на данните, възражение на обработването и право на оплакване пред компетентния надзорен орган. Исканията от субектите на данни, в частност искания за информация и/или изтриване, трябва да се докладват веднага на местния Data Protection Coordinator, тъй като те трябва да бъдат обработени в рамките на един месец от получаването.

(4) Нарушения на сигурността на данните: Местният Data Protection Coordinator и местният Compliance Coordinator трябва да бъдат информирани веднага, ако се подозира инцидент съгласно Раздел 3.8. Местният Data Protection Coordinator и местният Compliance Coordinator трябва незабавно да информират Службата „Корпоративно съответствие“-Corporate

Compliance Office, както и - в зависимост от типа на нарушението на данните - друг корпоративен отдел за нарушението.

3.5 Обработване на носители на данните

(1) *Носители на данните* трябва да се съхраняват, унищожават- като се унищожават по такъв начин, че да не може до тях да имат достъп неупълномощени трети страни.
(2) *Носителите на данните* трябва да се съхраняват в заключени шкафове или подходящи помещения. Ако носителите на данните се транспортират извън офиса, носителите на данни трябва да бъдат в затворен контейнер и криптирани по време на транспортирането.
(3) Ако *носителят на данни*, съдържащ лични данни, повече не е необходим, той трябва да се съхранява сигурно, а ако трябва да бъде унищожен, да се изтрие сигурно или унищожи предварително от IT отдела.
(4) При унищожаването на *лични данни* на хартия винаги трябва да се използват запечатани контейнери за унищожаване на данни или подходящи шредери за документи.

3.6 Гарантиране на сигурността на данните при напускане на компания

Ако дадено лице в обхвата на тази политика напусне дадена компания в обхвата на тази политика, трябва да се гарантира, че всички регламенти за защита на данните са спазени. Това включва в частност връщането на ключове и преобразуватели на непрекъснати данни в цифрови, носители на данни и изтриването на ИТ достъп.

3.7 Външни доставчици на услуги

(1) В случай че *Личните данни* се обработват от името на STADA България ЕООД като трета страна, STADA България ЕООД все още е „Администратор на лични данни“ на данните и отговаря за гарантиране на съответствието със законите за защита на данните.
(2) Следните услуги в частност са обработване на данни (в съответствие с Чл. 28 на ОРЗД):

- Техническа работа по обработване на данни за отчитане на платежна ведомост или финансово осчетоводяване,
- Аутсорсинг на обработване на лични данни в контекста на облачните компютърни изчисления,
- Обработване на рекламен адрес в пункт за разпределение на писма,
- Събирането на данни за контакт от кол-център,
- Използването на външен доставчик на телефонна система,
- Аутсорсинг на управление на имейлите или услуги на данните до уебсайтове,
- Получаване на данни, преобразуване на данни или сканиране на документи,
- Резервно съхранение за сигурност и друго архивиране
- Унищожаване на носители на данни
- Тестване или поддръжка на автоматизирани процеси или оборудване за обработване на данни (в частност копирни машини, сървъри или софтуер), ако достъпът до лични данни не може да бъде изключен по време на тези дейности,
- CRO.

(3) Следните услуги типично не са обработване от името на друг:

- Администриране на персонала,
- Набиране на служители,
- Договорна услуга на клиенти,
- Консултантски услуги или одитиране,
- Свикване на експерти или наблюдатели.
- Транспортни услуги на пощенски или куриерски услуги,
- Транспортни услуги на публични телекомуникационни услуги,
- Банкови услуги като управление и транспортни услуги на пари,

- Услуги за охрана,
- Услуги за почистване,
- Услуги по ремонт или поддръжка.

(4) Ако са спазени условията за обработване на данните, **трябва да се сключи писмено споразумение с доставчика на услугите** в съответствие с Чл. 28 на ОРЗД (GDPR).

3.8 Нарушения на сигурността на данните

(1) Инцидент със защитата на данните или потенциално нарушение на сигурността на данните може да възникне в следните случаи, например:
   - Хакерска атака,
   - (Неумишлено) разкриване на информация пред неупълномощени получатели,
   - (Неумишлена) загуба на информация,
   - Загуба/кражба на лаптоп/таблет/USB флашка/ мобилни телефони и др.

(2) Като просто правило, задължение за уведомяване на надзорния орган по защита на данните може да се прилага веднага щом се установи възможност за негативни последици за субектите на данни. Оценяването на такава възможност е отговорност на местния Data Protection Coordinator и местния Compliance Coordinator при съгласуване с Корпоративния къмплайънс отдел - Corporate Compliance Office.

(3) Ако е необходимо, известието до органа за защита на данните трябва да се направи „без ненужно закъснение и в рамките на 72 часа от узнаването за инцидента със сигурността“. Следователно, местният Data Protection Coordinator и местният Compliance Coordinator трябва да бъдат ангажирани веднага, след като инцидентът е поднесен на вниманието на някой служител на STADA България ЕООД или на Corporate Compliance Office. Докладът до компетентния орган се прави от местния Data Protection Coordinator и местния Compliance Coordinator. Местният Data Protection Coordinator и местният Compliance Coordinator също ще преценят съществуващите задължения да уведомят лицата, засегнати от инцидента със защита на данните.

4 Финални забележки

Всички *Адресати* са задължени да спазват вътрешните политики като част от техните трудови правоотношения.

Ако даден *Адресат* не спазва разпоредбите на тази Политика, това може да доведе до дисциплинарна мярка и може да доведе до прекратяване на трудовото правоотношение и/или подобни последствия. Без да се омаловажава горното, ограничено или никакво дисциплинарно действие може да се предприеме, ако даден Адресат, който е нарушил тази Политика, бързо уведоми своя началник и/или местния Compliance Coordinator или Корпоративния къмплайънс отдел Corporate Compliance Office (compliance@stada.com), и може да се докаже, че адресатът е действал добросъвестно, за да спази правилата на STADA и напълно е подкрепял STADA в своите коригиращи мерки.

Настоящата политика съдържа поверителна информация на STADA и следва да се използва само за вътрешни цели. Разкриването пред трета страна е обект на одобрение от Compliance.