



## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

### I. Въведение

#### 1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 (Общ регламент за защита на данните) замества Директивата 95/46 / ЕО за защита на данните. Има пряко действие и предполага изменение в законодателството на страните - членки в областта на защитата на личните данни. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработват с тяхно съгласие.

#### 2. Обхват очертан от Общия регламент за защита на данните

**Материален обхват (член 2)** – настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

**Териториален обхват (член 3)** – правилата на Общия Регламент ще важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Ще се прилага и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

#### 3. Понятия

**„Лични данни“** - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); 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.

**„Специални категории лични данни“** – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.

**„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“** - 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; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29



## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

**„Субект на данните“** – всяко живо физическо лице, което е предмет на личните данни съхранявани 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 обработени.

**„Дете“** – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

**„Профилиране“** - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

**„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“** – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.

Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи. (Член 4 т.16) от 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. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

**„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;

## II. Декларация относно политиката по защита на личните данни

1. Ръководството на „СОФИАНА“ ООД, се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на "правата и свободите" на лицата, чиито лични данни „СОФИАНА“ ООД събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

Контакт с Администратора на лични данни: "СОФИАНА" ООД  
Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)  
E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)  
Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

2. В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.

3. Регламент (ЕС) 2016/679 и тази политика се отнасят до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на клиенти, служители, доставчици и партньори и всякакви други лични данни, които организацията обработва от различни източници.

4. Отговорникът по защита на данните отговаря за преразглеждането на „Регистъра на дейностите по обработване“ ежегодно в светлината на всякакви промени в дейностите на „СОФИАНА“ ООД, както и всички допълнителни изисквания, оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган.

5. Тази политика се прилага за всички служители/работници, наети лица на граждански договори, както и за счетоводната къща, фирмата за трудова медицина и фирмата за поддръжка на ИТ системите и процесите на „СОФИАНА“ ООД като външни доставчици. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-къс възможен срок на съответните държавни органи.

6. Партньори и трети лица, които работят с или за „СОФИАНА“ ООД, както и които имат или могат да имат достъп до личните данни, ще се очаква да се запознаят, разбират и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от „СОФИАНА“ ООД, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които „СОФИАНА“ ООД е поела, и което дава право на „СОФИАНА“ ООД да извършва проверки на спазването на наложените със споразумението задължения.

### III. Задължения и роли по Регламент (ЕС) 2016/679

1. „СОФИАНА“ ООД е *администратор на данни* съгласно Регламент (ЕС) 2016/679.

2. Висшето ръководство и всички членове на управителните или надзорните органи на „СОФИАНА“ ООД са отговорни за разработване и насърчаване на добри практики в областта на обработване на информация в „СОФИАНА“ ООД;

3. Отговорникът по защита на данните с роля определена в Регламент (ЕС) 2016/679, трябва да бъде част от висшето ръководство, и да се отчита пред *Висшето ръководство / Съвета на директорите* на „СОФИАНА“ ООД за управлението на личните данни в рамките на организацията и за гарантирането на възможността за доказване на съответствието със законодателството за защита на данните и добрите практики.

Тази отчетност на Отговорника по защита на данните включва:

- разработване и внедряване на изискванията на РЕГЛАМЕНТ (ЕС) 2016/679 както се изисква от настоящата политика;
- управление на сигурността и риска по отношение на съответствието с политиката.

4. Отговорника по защита на данните, което (Висшето ръководство/Съвета на директорите/друго)

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29



## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

счита за подходящо, квалифицирано и опитно, е назначено, за да поеме отговорността за съответствието на „СОФИАНА“ ООД с тази политика на ежедневна основа. Отговорникът по защита на данните е пряко отговорно да гарантира, че както като цяло организацията на „СОФИАНА“ ООД, така и дейността на всеки член на ръководния състав, която се извършва в рамките на неговата област на отговорност, съответстват на изискванията на Регламент (ЕС) 2016/679.

5. Отговорникът по защита на данните има специфични отговорности по отношение на процедури като „Процедура за управление на исканията от субектите“ и е контактна точка за служителите на администратора, които искат разяснения по всеки аспект на спазването на защитата на данните.

6. Спазването на законодателството за защита на данните е отговорност на всички служители на „СОФИАНА“ ООД, които обработват лични данни.

7. Политиката за обучение на „СОФИАНА“ ООД (Политика за провеждане на обучение) определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите/работници на „СОФИАНА“ ООД.

### IV. Принципи за защита на данните

Цялата обработка на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на „СОФИАНА“ ООД имат за цел да гарантират спазването на тези принципи.

#### **1. Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно**

**Законосъобразно** – да идентифицира законна основа, преди да може да обработва лични данни. Те често са посочени като "основания за обработване", например „съгласие“.

**Добросъвестно** - за да може обработването да бъде добросъвестно, администраторът на данни трябва да 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.

Регламент (ЕС) 2016/679 увеличава изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхваната от изискването за "прозрачност".

**Прозрачно** – Общият регламент включва правила относно предоставяне на поверителна информация на субектите на данни в членове 12, 13 и 14 от ОРЗД. Те са подробни и конкретни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

Правилата за уведомяване на субекта на данни от „СОФИАНА“ ООД са определени в Процедура за прозрачност при обработката на лични данни и уведомлението се записва в Образец на Декларация за поверителност (уведомление за поверително третиране на личните данни).

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

- контактите на ДЛЗД / Отговорника по защита на данните;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както и право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

### **2. Лични данни могат да се събират само за конкретни, изрично указани и законни цели**

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, официално обявени на надзорния орган като част от Регистъра на дейностите по обработване на данни (чл. 30 ОРЗД) на „СОФИАНА” ООД. Процедура за прозрачност при обработката на лични данни определя съответните правила.

### **3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел. (принцип на минимално необходимото)**

- Отговорникът по защита на данните е отговорен да осигури „СОФИАНА” ООД да не събира информация, която не е строго необходимо за целта, за която тя е получена.
- 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 добросъвестно обработване или Декларация за поверителност (уведомление за поверително третиране на личните данни) и да бъдат одобрени от Отговорникът по защита на данните.
- Отговорникът по защита на данните ще гарантира, че на годишна основа всички способи за събиране на данни се преглеждат от (вътрешен одит/външни експерти), за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни (Процедура за оценка на въздействието върху защитата на данните и използваната от вас методология за оценка на въздействието).

### **4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.**

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

- Данните, които се съхраняват от администратора на данни, трябва да бъдат прегледани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.
- Отговорникът по защита на данните е отговорно да гарантира, че целият персонал е обучен в значението на събирането на точни данни и поддържането им.
- Също така, задължение на субекта на данните е да декларира, че данните, които предават за съхраняване от „СОФИАНА“ ООД са точни и актуални. Попълването на формуляр от субекта на данни, предназначени за администратора, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване.
- От служителите / работниците / клиентите / доставчиците трябва да се изисква, да уведомяват „СОФИАНА“ ООД за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на „СОФИАНА“ ООД е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.
- Отговорникът по защита на данните носи отговорност да се гарантира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени, други относими фактори.
- Най-малко на годишна база отговорникът по защита на данните ще прегледа сроковете на съхранение на всички лични данни, обработвани от „СОФИАНА“ ООД, като се позовава на инвентаризацията на данните и ще идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.
- Отговорникът по защита на данните е отговорно за съответствие с искания за корекция на данни в рамките на един месец (Процедура за управление на исканията от субектите ). Този срок може да бъде удължен с още два месеца за сложни заявки. Ако „СОФИАНА“ ООД реши да не се съобрази с искането, Отговорникът по защита на данните трябва да отговори на субекта на данните, за да обясни мотивите си и да го информира за правото му да подаде жалба пред надзорния орган, и да потърси правна защита.
- Отговорникът по защита на данните е отговорно за вземане на подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни, да ги информира, че информацията е неточна или остаряла и е да не се използва за вземане на решения относно лицата, да информира съответните страни; и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

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

- Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин (*изнесени на външен носител без достъп до интернет*), за да се защити самоличността на субекта на данните в случай на нарушение на данните.
- Лични данни ще бъдат пазени в съответствие с Процедура за съхраняване и унищожаване на данните и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

унищожени по указания в тази процедура ред.

- Отговорникът по защита на данните специално трябва да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в Процедура за съхраняване и унищожаване на данните и трябва да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

### **6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност (чл. 24, чл. 32 от ОРЗД)**

Отговорникът по защита на данните ще извърши оценка на въздействието <sup>1</sup> (оценка на риска) , като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от „СОФИАНА” ООД.

При определянето на това доколко уместно е обработването, отговорникът за защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или клиенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите.

При оценяването на подходящи технически мерки, длъжностното лице по защита на данните ще разгледа следното:

- 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;
- Правата за достъп основани на роли, включително тези, на назначен временно персонал
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални и широкообхватни мрежи;
- Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за „СОФИАНА” ООД;

При оценяването на подходящите организационни мерки отговорникът за защита на данните ще вземе предвид следното:

- Нивата на подходящо обучение в „СОФИАНА” ООД;

---

1

Препоръчително е в документите относно използваната от Вас методология за оценка на въздействието да посочите този пункт от политиката Ви.

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Приемането на политика на „чисто работно място“<sup>2</sup>;
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Приемане на ясни правила за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

Тези контроли са избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват.

### **7. Спазване на принципа на отчетност**

Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в [чл. 5, пар. 2](#) изисква от администратора да докаже, че спазва останалите принципи в ОРЗД и изрично заявява, че това е негова отговорност.

„СОФИАНА” ООД ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към кодекси за поведение, внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

## **v. Права на субектите на данни**

**1.** Субектите на данни имат следните права по отношение на обработването на данни, както и на

---

2

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.

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29





## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

данните, които се записват за тях:

- 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 от администратора;
- Да иска от администратора коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен”);
- Да иска от администратора 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 е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

2. „СОФИАНА” ООД осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е описано в процедурата Процедура за управление на исканията от субектите. Тази процедура също така описва как „СОФИАНА” ООД ще гарантира, че отговора на искането на субекта на данни отговаря на изискванията на Общия регламент.
- Субектите на данни имат право да подават жалби до „СОФИАНА” ООД, свързани с обработването на личните им данни, обработването на искане от субекта на данни и обжалване от страна на субекта на данни, относно начина на обработване на жалбите в съответствие с Процедура за начините на комуникация при жалби и искания от субекта на данни.

## VI. Съгласие

1. Под „съгласие“ „СОФИАНА” ООД ще разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.

**2.** „СОФИАНА“ ООД разбира под "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

**3.** Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие<sup>3</sup> за дейностите по обработване.

**4.** За специални категории данни трябва да се получи изрично писмено съгласие (Процедура по получаване на съгласие за обработване на лични данни на субектите на данни), освен ако не съществува алтернативно законно основание за обработване.

**5.** В повечето случаи съгласието за обработка на лични и специални категории данни се получава рутинно от „СОФИАНА“ ООД, като се използват стандартни документи за съгласие (посочете) напр. когато нов клиент подписва договор или по време на набиране на нов персонал и т.н.

**6.** Когато „СОФИАНА“ ООД обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години (освен ако държавата-членка не е предвидила по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

### **VII. Сигурност на данните**

**1.** Всички служители / работници са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които „СОФИАНА“ ООД държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако „СОФИАНА“ ООД не е дал такива права на тази трета страна, като са сключили договор/клауза за поверителност.

**2.** Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа.<sup>4</sup> Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или

---

3

Администраторът трябва да реши как иска да направи това. Възможно е чрез формуляр, който трябва да бъде подписан. Възможно е също така с известие за поверителност, което трябва да бъде изрично прието от някого, преди да се обработва информацията или пък по някакъв друг способ. Каквото и да е решението, трябва да бъде посочено тук.

4

Препоръчително е ако няма, да се създадат такива правила като отделен документ и в съответствие с характерните особености на вашата организация.

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

- ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (*например правила за контрол на достъпа*) ; и / или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

**3.** Да се създаде организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизирани служители / работници на „СОФИАНА” ООД. От всички служители / работници се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

**4.** 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 по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.<sup>5</sup>

**5.** Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данните. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтривани или дисковете унищожени, съгласно изградените правила/процедури.<sup>6</sup>

**6.** Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

### **VIII. Разкриване на данни**

**1.** „СОФИАНА” ООД трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители / работници трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността извършвана от организацията.

Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с

---

5

Препоръчително е да се създадат правила за унищожаване на хартиени документи след изтичане на периода за съхранение – начин на унищожаване, отговорни лица, запис (протокол, друго) за извършеното, дата и т.н.

6

Препоръчително е да се създадат правила за унищожаване на информацията върху неизползвани (бракувани) записващи носители, било чрез сигурно изтриване, било чрез унищожаване на самите носители.

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Длъжностното лице за защита на данните / Отговорникът за защита на данните.

### ix. Съхраняване и унищожаване на данните

1. „СОФИАНА“ ООД не съхранява 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.

2. „СОФИАНА“ ООД може да съхранява 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.

3. Периода на съхранение за всяка категория на лични данни ще бъдат изложени в процедурата за Процедура за съхраняване и унищожаване на данните както и на критериите, използвани за определяне на този период, включително всякакви законови задължения на „СОФИАНА“ ООД да се запазят данните.

4. Процедурата за съхраняване и унищожаване на данните на „СОФИАНА“ ООД ще се прилага във всички случаи.

5. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1 б. е) от Общия регламент) – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

### x. Трансфер на данни

1. Всеки износ на данни от рамките на ЕС към страни извън ЕС (посочени в Общия регламент като "трети страни") са незаконни, освен ако няма подходящ "ниво на защита на основните права на субектите на данни.

Прехвърлянето на лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от възможните гаранции или изключения.

#### 2. Решение за адекватност

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. В тези случаи не се изисква разрешение.

Държавите, които са членки на Европейското икономическо пространство (ЕИП), но не и на ЕС, се приемат като отговарящи на условията за решение за адекватност.

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

Ако Организацията желае да прехвърли лични данни от ЕС на трета страна в САЩ, тя трябва да

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА“ ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

провери дали организацията е подписала Рамковото споразумение „Privacy Shield“ с Министерство на търговията на САЩ.

Американското министерство на търговията отговаря за управлението и администрирането на Privacy Shield и гарантира, че компаниите изпълняват своите ангажименти. За да могат да се сертифицират пред министерството, фирмите трябва да имат политика за защита на личните данни в съответствие с принципите на ОРЗД, напр. използват, съхраняват и прехвърлят личните данни в съответствие набор от строги правила и предпазни мерки за защита на данните.

#### 4. Задължителни фирмени правила

„СОФИАНА“ ООД може да приеме одобрени задължителни корпоративни правила за прехвърляне на данни извън ЕС. Това изисква подаването им за одобрение до съответния надзорен орган.

#### 5. Стандартни договорни клаузи

„СОФИАНА“ ООД може да приеме утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство. Ако „СОФИАНА“ ООД приема стандартни договорни клаузи, одобрени от съответния надзорен орган, има автоматично признаване на адекватността.<sup>7</sup>

#### 6. Изключения

При липса на решение за адекватност, членство в US Privacy Shield, задължителни фирмени правила и / или договорни клаузи, прехвърляне на лични данни в трета страна или международна организация се извършва 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 такива прехвърляния;
- предаването е необходимо за изпълнението на договор между субекта на данните и администратора 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 данните между администратора 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

---

7

При положение, че използвате такива клаузи, посочете ги тук като връзка към документ.

## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076

ДЛЗД/Отговорник: Анна Чобанова - Управител

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.

### **XI. Регистър на обработванията на данни (инвентаризация на данните)**

1. „СОФИАНА” ООД е създала процес на инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламент (ЕС) 2016/679. При инвентаризацията на данните в „СОФИАНА” ООД и в работният поток от данни се установяват:

- бизнес процесите, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на 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 заличаване.

2. „СОФИАНА” ООД е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. „СОФИАНА” ООД оценява нивото на риска за лицата, свързани с обработването на личните им данни. Извършват се оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от „СОФИАНА” ООД и във връзка с обработването, предприето от други организации от името на „СОФИАНА” ООД (Процедура за оценка на въздействието върху защитата на данните и използваната Методология за оценка на въздействието).

4. „СОФИАНА” ООД управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с тези правила.

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 „СОФИАНА” ООД следва да извърши оценка на въздействието на предвидените операции по обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

5. Когато в резултат на Оценката на въздействието е ясно, че „СОФИАНА” ООД 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, трябва да бъде предадено за преглед

Контакт с Администратора на лични данни: "СОФИАНА" ООД

Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)

E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)

Телефон: 02 946 14 29



## ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

Администратор: „СОФИАНА” ООД, ЕИК: 040277076  
ДЛЗД/Отговорник: Анна Чобанова - Управител

от страна на отговорникът за защита на данните.

**6.** Ако отговорникът за защита на данните има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да ескалира въпроса пред надзорния орган.

**7.** Отговорникът по защита на данните, прави периодичен ежегоден преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ в светлината на всякакви промени в дейностите на „СОФИАНА” ООД.

Контакт с Администратора на лични данни: "СОФИАНА" ООД  
Уебсайт: [www.sofiana-bg.com](http://www.sofiana-bg.com)  
E-mail: [office@sofiana-bg.com](mailto:office@sofiana-bg.com)  
Телефон: 02 946 14 29