MEDICLIM

GDPR

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Data Protection Policy

СЪДЪРЖАНИЕ

1. ЦЕЛ, ОБХВАТ И ПОТРЕБИТЕЛИ 3
2. РЕФЕРЕНТНИ ДОКУМЕНТИ 3
3. ОСНОВНИ ПРИНЦИПИ ОТНОСНО ОБРАБОТКАТА НА ЛИЧНИ ДАННИ 3
3.1. ЗАКОННОСТ, СПРАВЕДЛИВОСТ И ПРОЗРАЧНОСТ 3
3.2. ОГРАНИЧАВАНЕ В РАМКИТЕ НА ЦЕЛТА 3
3.3. МИНИМИЗИРАНЕ НА ДАННИТЕ 3
3.4. ТОЧНОСТ 3
3.5. ОГРАНИЧЕНИЯ ЗА СЪХРАНЕНИЕ 3
3.6. ПОВЕРИТЕЛНОСТ И НЕПРИКОСНОВЕННОСТ 4
3.7. ОТГОВОРНОСТ 4
4. ИЗГРАЖДАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ 4
4.1. УВЕДОМЯВАНЕ НА СУБЕКТИТЕ НА ДАННИ 4
4.2. ИЗБОР И СЪГЛАСИЕ НА СУБЕКТА НА ДАННИТЕ 4
4.3. СЪБИРАНЕ 4
4.4. ИЗПОЛЗВАНЕ, ЗАДЪРЖАНЕ И УНИЩОЖАВАНЕ (ЗАЛИЧАВАНЕ) 4
4.5. РАЗКРИВАНЕ ПРЕД ТРЕТИ СТРАНИ 4
4.6. ТРАНСГРАНИЧЕН ТРАНСФЕР НА ЛИЧНИ ДАННИ 5
4.7. ПРАВА НА ДОСТЪП ОТ СУБЕКТИТЕ НА ДАННИ 5
4.8. ПРЕНОСИМОСТ НА ДАННИ 5
4.9. ПРАВО ДА БЪДЕШ ЗАБРАВЕН 5
5. НАСОКИ ЗА ТОЧНА ОБРАБОТКА 5
5.1. ИЗВЕСТИЯ КЪМ СУБЕКТИ НА ДАННИ 5
5.2. ПОЛУЧАВАНЕ НА СЪГЛАСИЕ 6
6. ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ 6
7. НАСОКИ ЗА СЪЗДАВАНЕ НА ВОДЕЩ НАДЗОРЕН ОРГАН 7
7.1. НЕОБХОДИМОСТ ОТ СЪЗДАВАНЕ НА ВОДЕЩ НАДЗОРЕН ОРГАН 7
7.2. ВОДЕЩ НАДЗОРЕН ОРГАН 7
7.2.1. ОСНОВЕН ЦЕНТЪР ЗА УПРАВЛЕНИЕ ЗА АДМИНИСТРАТОРА НА ДАННИ 7
7.2.2. ОСНОВНО УЧРЕЖДЕНИЕ ЗА ОБРАБОТВАЩИЯ ДАННИ 7
8. ОТГОВОР ПРИ ИНЦИДЕНТИ С НАРУШАВАНЕ НА ЛИЧНИ ДАННИ 8
9. ОДИТ И ОТЧЕТНОСТ 8
10. ПРАВНИ КОНФЛИКТИ 8

1. ЦЕЛ, ОБХВАТ И ПОТРЕБИТЕЛИ

МЕДИКЛИМ (Администраторът) се стреми да спазва приложимите закони и разпоредби, свързани със защитата на личните данни в държавите, в които МЕДИКЛИМ (Администраторът) оперира или има служебни взаимоотношения. Тази политика определя основните принципи, чрез които МЕДИКЛИМ (Администраторът) обработва личните данни на потребители, клиенти, доставчици, партньори, служители и други лица, и посочва отговорностите на своите структурни звена и служители по време на обработката на лични данни.

Тази политика важи за МЕДИКЛИМ (Администратора) и неговите пряко или косвено контролирани изцяло притежавани дъщерни структури, които извършват дейност в рамките на Европейското икономическо пространство (ЕЕА) или обработват личните данни на субектите на данни в рамките на ЕЕА.

Потребителите на този документ са всички служители, постоянни или временни, и всички изпълнители, които работят от името на МЕДИКЛИМ (Администратора).

2. РЕФЕРЕНТНИ ДОКУМЕНТИ

- Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни
- Политика за защита на личните данни на служителите
- Политика за запазване на данни
- Описание на длъжността на служителя по защита на данните
- Насоки за инвентаризация на личните данни
- Процедура за заявка за достъп до физически лица
- Насоки за оценка на въздействието на защитата на данните
- Процедура за трансгранично прехвърляне на лични данни
- Политики за сигурност на информацията
- Процедура за уведомяване за нарушение

3. ОСНОВНИ ПРИНЦИПИ ОТНОСНО ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Принципите за защита на данните очертават основните отговорности за организациите, обработващи лични данни. Член 5, параграф 2 от GDPR постановява, че **"администраторът е отговорен и е в състояние да докаже спазването на принципите."**

3.1. Законност, справедливост и прозрачност

Личните данни са обработвани законно, справедливо и по прозрачен начин по отношение на субекта на данните.

3.2. Ограничаване в рамките на целта

Личните данни се събират за конкретни, изрични и законни цели и да не се обработват по начин, който е несъвместим с тези цели.

3.3. Минимизиране на данните

Личните данни са адекватни, уместни и ограничени до това, което е необходимо по отношение на целите, за които се обработват. МЕДИКЛИМ (Администратора) прилага анонимност или псевдонимация на личните данни, ако е възможно, за да намали рисковете за засегнатите субекти на данни.

3.4. Точност

Личните данни са точни и, при необходимост, актуализирани; предприемат се разумни стъпки, за да се гарантира, че личните данни, които са неточни (като се имат предвид целите, за които се обработват) се изтриват или коригират своевременно.

3.5. Ограничения за съхранение

Личните данни се съхраняват не повече от времето, необходимо за целите, за които се обработват личните данни.

3.6. Поверителност и неприкосновеност

Вземайки предвид състоянието на технологиите и другите налични мерки за сигурност, разходите по внедряването и вероятността и тежестта на рисковете, свързани с личните данни, МЕДИКЛИМ (Администраторът) използва подходящи технически или организационни мерки за обработка на лични данни по начин, който гарантира подходяща сигурност на личните данни, включително защита срещу случайно или незаконно унищожаване, загуба, редуване, неразрешен достъп или разкриване.

3.7. Отговорност

МЕДИКЛИМ (Администраторът) на данни отговаря за доказването на съответствие с принципите, изложени по-горе.

4. ИЗГРАЖДАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

За да се докаже съответствие с принципите за защита на данните, МЕДИКЛИМ (Администраторът) изгражда защита на данните в своите оперативни дейности.

4.1. Уведомяване на субектите на данни

МЕДИКЛИМ (Администраторът) уведомява субекта на личните данни за контрола на всички процеси, свързани с управлението и защитата на личните данни.

4.2. Избор и съгласие на субекта на данните

МЕДИКЛИМ (Администраторът) управлява и защитава личните данни на субекта, само след като субектът доброволно е избрал Администратора и е дал писмено съгласие за управление и защита на неговите лични данни.

4.3. Събиране

МЕДИКЛИМ (Администраторът) се стреми да събере възможно най-малко количество лични данни. Ако личните данни се събират от трета страна, МЕДИКЛИМ (Администраторът) гарантира, че личните данни се събират законно.

4.4. Използване, задържане и унищожаване (заличаване)

Целите, методите, ограничаването на съхранението и периодът на запазване на личните данни съответстват на информацията, съдържаща се в Общото известие за защита на данните.

МЕДИКЛИМ (Администраторът) поддържа точността, целостта, поверителността и уместността на личните данни въз основа на целта на обработката. МЕДИКЛИМ (Администраторът) използва адекватни механизми за защита, предназначени за защита на личните данни, за да се предотврати откраднването, злоупотребата или злоупотребата с личните данни и да се предотврати нарушаване на личните данни.

ДЛЗЛД отговаря за спазването на изискванията, изброени в този раздел.

4.5. Разкриване пред трети страни

Когато МЕДИКЛИМ (Администратора) използва доставчик или партньор (трета страна), за да обработва лични данни от нейно име, МЕДИКЛИМ (Администратора) гарантира, че този доставчик на специфични услуги (партньор) ще осигури необходимите мерки за сигурност за защита на личните данни, които са подходящи за свързаните с тях рискове. За тази цел Администраторът използва въпросник за оценка на съответствието на процесите по управление и защита на обработващия личните данни с изискванията на GDPR, ЗЗЛД и приложимите стандарти.

МЕДИКЛИМ (Администраторът) договорно изисква от доставчика или партньора да осигури необходимото ниво на защита на данните. Доставчикът или партньорът обработва само такива лични данни, които се изискват за изпълнение неговите договорни задължения към МЕДИКЛИМ (Администратора) или по нареждане на МЕДИКЛИМ (Администратора), а не за други цели.

Когато МЕДИКЛИМ (Администраторът) обработва лични данни съвместно с независима трета страна, МЕДИКЛИМ (Администратора) **изрично да определя съответните си отговорности и тези на третата страна в съответния договор или друг правно обвързващ документ, като например Споразумението за обработка на данни на доставчик.**

4.6. Трансграничен трансфер на лични данни

Преди да се предадат лични данни извън Европейското икономическо пространство (ЕИП), се използват адекватни мерки за сигурност и защита, включително подписване на Споразумение за прехвърляне на данни, както се изисква от Европейския съюз, и при необходимост се получава разрешение от съответния Орган за защита на данните.

МЕДИКЛИМ и всички участници в процеса спазват принципите за обработка и защита на лични данни, посочени в процедурата за трансгранично предаване на данни.

4.7. Права на достъп от субектите на данни

Когато действа като администратор на данни, МЕДИКЛИМ предоставя на субектите на данни достъп до механизъм за разумен достъп, който им позволява да имат достъп до личните им данни, и им позволява да актуализират, коригират, изтриват (заличават) или предават своите лични данни, или изисквано от закона. Механизмът за достъп е допълнително описан в **Процедура за заявка за достъп до субекта на данни.**

4.8. Преносимост на данни

Субектите на данни имат право да получат при поискване копие от данните, които им предоставят в структуриран формат, и да предадат тези данни на друг администратор безплатно.

МЕДИКЛИМ (Администраторът) гарантира, че тези молби се обработват в **рамките на един месец,** не са прекомерни и не засягат правата на лични данни на други лица.

4.9. Право да бъдеш забравен

При поискване, субектите на данни имат правото да получат от МЕДИКЛИМ (Администратора) изтриването (заличаването) на личните им данни. Когато МЕДИКЛИМ (Администратора) действа като контролиращо лице, ДЛЗЛД предприема необходимите действия (включително технически мерки), за да информира третите страни, които използват или обработват тези данни, за да се съобразят с искането.

5. НАСОКИ ЗА ТОЧНА ОБРАБОТКА

Личните данни се обработват само при изрично разрешение и под контрола на ДЛЗЛД.

МЕДИКЛИМ (Администраторът) решава дали да извърши оценката на въздействието върху защитата на данните за всяка дейност по обработка на данни съгласно насоките за оценка на въздействието върху защитата на данните.

5.1. Известия към субекти на данни

По време на събирането или преди събирането на лични данни за всякакъв вид обработка, включително, но не само, продажба на продукти, услуги или маркетингови дейности, ДЛЗЛД е отговорно да информира надлежно субектите на данни за следното: видовете лични данни събраните данни, целите на обработката, методите за обработка, правата на субектите на данни по отношение на техните лични данни, периода на задържане, потенциалните международни трансфери на данни, ако данните се споделят с трети страни и мерките за сигурност на дружеството за защита на личните данни. Тази информация се предоставя чрез Общото известие за защита на данните.

Ако МЕДИКЛИМ (Администратора) има няколко дейности за обработка на данни, се прилагат **различни известия**, които се различават в зависимост от обработващата дейност и категориите събрани лични данни - например едно известие може да бъде написано за пощенски цели, а друго - за изпращане цели.

Когато се споделят лични данни с трета страна, ДЛЗЛД гарантира, че субектите на данни са били уведомени за това чрез Обща бележка за защита на данните.

Когато се прехвърлят лични данни на трета държава в съответствие с Политиката за трансгранично прехвърляне на данни, общото известие за защита на данните следва да отразява това и ясно да посочва къде и кои лични данни се прехвърлят.

Когато се събират чувствителни лични данни, ДЛЗЛД трябва да се увери, че Общото известие за защита на данните изрично посочва целта, за която се събират тези чувствителни лични данни.

5.2. Получаване на съгласие

Когато обработването на лични данни се основава на съгласието на субекта на данните или на други законови основания, ДЛЗЛД е отговорно за запазването на такова съгласие. ДЛЗЛД отговаря за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласието си, и трябва да уведомят и да гарантират, че тяхното съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време.

Когато събирането на лични данни е свързано с дете на възраст под 16 години, ДЛЗЛД гарантира, че родителското съгласие е дадено преди събирането, като се използва формулярът за съгласие за родител.

Когато се искат да се коригират, изменят или унищожат записите с лични данни, ДЛЗЛД гарантира, че тези искания се обработват в разумен срок. ДЛЗЛД записва **заявките** и води **Дневник** за тях.

Личните данни се обработват само за целите, за които първоначално са били събрани. В случай, че МЕДИКЛИМ (Администраторът) желае да обработва събрани лични данни за друга цел, МЕДИКЛИМ (Администраторът) търси съгласието на своите субекти на данни в ясни и кратки срокове. Всяко такова искане включва **първоначалната цел**, за която са събрани данните, както и **новата или допълнителната (ите) цел (и)**. Искането включва и причината за промяната на целта/целите. ДЛЗЛД отговаря за спазването на правилата в този параграф.

Сега и в бъдеще, ДЛЗЛД гарантира, че методите за събиране са в съответствие със съответните закони, добри практики и приложими стандарти.

ДЛЗЛД е отговорен за създаването и поддържането на **Регистър на Общите известия за защита на данните.**

6. ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ

Отговорността за осигуряване на подходяща обработка на лични данни се носи от всеки, който работи за или с МЕДИКЛИМ (Администратора) и има достъп до обработваните от компанията лични данни.

Основните области на отговорности при обработването на лични данни са следните организационни роли:

Комисия за управление на сигурността и защита на личните данни взема решения и одобрява общите стратегии на компанията за защита на личните данни.

ДЛЗЛД отговаря за управлението на програмата за защита на личните данни и отговаря за разработването и популяризирането на политики за защита на личните данни "от край до край", определени в описанието на длъжностната характеристика на служителя за защита на данните.

Правен експерт заедно с ДЛЗЛД наблюдава и анализира законите за личните данни и промените в нормативната уредба, разработва изисквания за съответствие и подпомага бизнеса в постигането на целите си за лични данни.

ИТ мениджърът (Системен Администратор – СА или Служител по сигурността на автоматизирани информационни системи и мрежи – ССАИСМ) отговаря за:

- Осигуряване на всички системи, услуги и оборудване, използвани за съхранение на данни, да отговарят на приемливи стандарти за сигурност.
- Провеждане на редовни проверки и сканиране, за да се гарантира, че хардуерът и софтуерът за защита функционират правилно.
- Криптографската сигурност.

Мениджърът/Експертът по маркетинг отговаря за:

- Одобряване на всички декларации за защита на данните, прикрепени към съобщения, като имейли и писма.
- Обръщане към запитвания за защита на данните от журналисти или медии.
- Когато е необходимо, работата с ДЛЗЛД, за да се гарантира, че маркетинговите инициативи спазват принципите за защита на данните.

Мениджърът/Експертът по човешки ресурси отговаря за:

- Подобряване на информираността на служителите за защитата на личните данни на потребителите.
- Организиране на експертни познания за защита на личните данни и обучение за повишаване на информираността на служителите, работещи с лични данни.
- Защита на личните данни на служителите от край до край. Той гарантира, че личните данни на служителите се обработват въз основа на законните бизнес цели и необходимост на работодателя.

Мениджърът/Експертът по снабдяване отговаря за предаването на отговорностите за защита на личните данни на доставчиците и за повишаването на нивата на информираност на доставчиците за защита на личните данни, както и за понижаване на изискванията за лични данни към трети страни, които използват. МЕДИКЛИМ (Администраторът) си запазва правото да извършва одит на Системата за сигурност и защитата на личните данни на своите доставчици.

7. НАСОКИ ЗА СЪЗДАВАНЕ НА ВОДЕЩ НАДЗОРЕН ОРГАН

7.1. Необходимост от създаване на водещ надзорен орган

Определянето на водещ надзорен орган е от значение само ако МЕДИКЛИМ (Администратора) извършва трансгранично обработване на лични данни.
Трансграничен трансфер на лични данни се извършват, ако:

a) обработването на лични данни се извършва от дъщерни дружества на МЕДИКЛИМ (Администратора), които се намират в други държави-членки;

или

b) обработка на лични данни, която се извършва в едно предприятие на МЕДИКЛИМ (Администратора) в Европейския съюз, но съществено засяга или има вероятност да засегне съществено субектите на данни в повече от една държава-членка.

Ако МЕДИКЛИМ (Администратора) има само учреждения в една държава-членка и неговите преработвателни дейности засягат само субекти на данни в тази държава-членка, отколкото няма нужда да се създава водещ надзорен орган. Единственият компетентен орган ще бъде надзорният орган в страната, в която МЕДИКЛИМ (Администратора) е законно учредена.

7.2. ВОДЕЩ НАДЗОРЕН ОРГАН

7.2.1. Основен център за управление за Администратора на данни

Висшето ръководство на МЕДИКЛИМ (Администратора) идентифицира основния център за управление и защита на личните данни, така че да може да се определи водещият надзорен орган.

Ако МЕДИКЛИМ (Администраторът) е със седалище в държава-членка на ЕС и взема решения, свързани с трансгранични преработващи дейности на мястото на централната му администрация, ще има единствен водещ надзорен орган за дейностите по обработка на данните, извършвани от дружеството.

Ако МЕДИКЛИМ (Администраторът) има множество предприятия, които действат самостоятелно и вземат решения относно целите и средствата за обработка на лични данни, Висшето ръководство на МЕДИКЛИМ (Администратора) трябва да признае, че съществуват повече от един водещ надзорен орган.

7.2.2. Основно учреждение за обработващия данни

Когато МЕДИКЛИМ (Администратора) действа като **обработващ на данни**, основното предприятие е мястото на централната администрация. В случай, че мястото на централната администрация не се намира в ЕС, основното предприятие ще бъде учреждението в ЕС, където се извършват основните преработвателни дейности.

8. ОТГОВОР ПРИ ИНЦИДЕНТИ С НАРУШАВАНЕ НА ЛИЧНИ ДАННИ

Когато МЕДИКЛИМ (Администраторът) узнае за предполагаемо или действително нарушение на личните данни, ДЛЗЛД извършва вътрешно разследване и своевременно предприема подходящи мерки за отстраняване, в съответствие с политиката за нарушаване на данните.

Когато съществува риск за правата и свободите на субектите на данни, МЕДИКЛИМ (Администратора) уведомява съответните органи за защита на данните без неоснователно забавяне и, при възможност, в рамките на 72 часа.

9. ОДИТ И ОТЧЕТНОСТ

ДЛЗЛД и Вътрешните одитори контролират прилагането на тази политика.

Всеки служител, който нарушава тази Политика е обект на дисциплинарно наказание и служителят може да бъде обвързан с граждански или наказателни искове, ако неговото поведение нарушава законови или подзаконови актове.

10. ПРАВНИ КОНФЛИКТИ

Тази политика е предназначена да спазва законите и подзаконовите актове в мястото на установяване и в страните, в които МЕДИКЛИМ (Администратора) работи.

В случай на конфликт между тази Политика и приложимите закони и разпоредби, последните имат предимство.