„ЕМАМАР 2013” ЕООД

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Утвърдена на 14.05.2025 г.

Утвърдил: .....

/Управител/

Съдържание

1. ЦЕЛ, ПРИЛОЖИМО ПРАВО И ПРЕДМЕТЕН И СУБЕКТЕН ОБХВАТ 3

2. ОСНОВНИ ДЕФИНИЦИИ 3

3. ПРИНЦИПИ, ОТНАСЯЩИ СЕ ДО ОБРАБОТКАТА НА ЛИЧНИ ДАННИ 5

3.1. Законосъобразност, добросъвестност и прозрачност 5

3.2. Ограничение на предназначението 5

3.3. Необходимост, предназначение и минимизация 6

3.4. Точност и актуализация 6

3.5. Ограничение на сроковете за съхранение 6

3.6. Цялостност, поверителност, сигурност и контрол на достъпа 6

3.7. Отговорност и отчетност 6

4. ОРГАНИЗАЦИОННИ И ОПЕРАТИВНИ НАСОКИ 6

4.1. Уведомяване на субекта на данните за тяхното събиране и обработка 6

4.2. Информиран избор и съгласие на субекта 7

4.3. Събиране на лични данни 7

4.4. Използване, съхранение и унищожаване 7

4.5. Предоставяне на трети страни 8

4.6. Трансграничен трансфер на лични данни 8

4.7. Право на достъп на субекта на данни 8

4.8. Копиране на данни и предоставянето им на друг администратор 9

4.9. Правото „да бъдеш забравен" 9

5. ПРЕПОРЪКИ ЗА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ 10

5.1. Уведомяване на субектите на данни и трансгранично прехвърляне на данни 10

5.2. Получаване на съгласие от субекта 11

6. ОТГОВОРНИ ЛИЦА 13

7. НАСОКИ ЗА СЪЗДАВАНЕ НА ВОДЕЩ НАДЗОРЕН ОРГАН. ERROR! BOOKMARK NOT DEFINED.

7.1. Необходимост от създаване на Водещ надзорен орган ..... **Error! Bookmark not defined.**

7.2. Основно място на установяване и Водещ надзорен орган ..... **Error! Bookmark not defined.**

7.2.1. Основно място на установяване на Администратора на Данни.... ***Error! Bookmark not defined.***

7.2.2. Основно място на установяване на Обработващия данни ..... ***Error! Bookmark not defined.***

7.2.3. Основно място на установяване за Администратори и Обработващи данни извън ЕС ***Error! Bookmark not defined.***

8. УПРАВЛЕНИЕ НА РИСКА И ДЕЙСТВИЯ В ОТГОВОР НА НАРУШАВАНЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ 13

9. ОТГОВОРНОСТНА СЛУЖИТЕЛИТЕ 13

10. НЕСЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ЗАКОНОДАТЕЛСТВО 13

11. ВЛИЗАНЕ В СИЛА И АКТУАЛИЗИРАНЕ 13

1. Цел, приложимо право и предметен и субектен обхват

Тази политика за защита на личните данни е приета за **„ЕМАМАР 2013" ЕООД,** с ЕИК 206924415, със седалище и адрес на управление: Република България, община столична гр. София гр. София, р-н Кремиковци,кв.Враждебна,ул.38-ма,2 (наричано по-долу за краткост "**Дружеството**") и за Уеб сайта https://termomarket.bg//, и е приложима за всички лични данни, с които Дружеството оперира – събира, обработва, съхранява, предоставя достъп до и унищожававъв връзка с предлаганите услуги за посетители на сайта и клиенти от Дружеството.

Чрез приемането на тази политика Дружеството цели да приведе дейността си в съответствие с изискванията на Общия регламент за защита на личните данни - 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 и за отмяна на Директива 95/46 / ЕО (по-долу за краткост наричан „**Регламентът**"). Настоящата политика е изготвена в съответствие с насоките на Работната група по чл. 29, инструкциите на КЗЛД, действащия Закон за защита на личните данни и подзаконовите нормативни актове по прилагането му и проекта за Закон за изменение и допълнение на ЗЗЛД.

Тази политика определя основните принципи, чрез които Дружеството обработва личните данни в Съюза (по смисъла на чл. 1-3 вкл. на Регламента) на потребители, клиенти, доставчици, бизнес партньори, служители и други лица, и посочва отговорностите на обработващите лица по време на обработката на лични данни. Тя е приложима за Дружеството, неговите териториални поделения/клонове и свързаните с него лица по смисъла на Търговския закон и приложимите нормативни актове от правото на ЕС.

Настоящата политика е предназначена за всички служители и всички изпълнители, които работят от името на Дружеството.

2. Основни дефиниции

Следните определения на термините, използвани в този документ, са дефинирани в Преамбюла и в чл. 4 от Регламента:

- **Лични данни** означава 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, 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[1];

- **Чувствителни лични данни:** Личните данни, които по своята същност са особено чувствителни по отношение на основните права и свободи, заслужават специфична защита, тъй като контекстът на тяхната обработка може да създаде значителни рискове за основните права и свободи. Тези лични данни включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикати, генетични данни, биометрични данни, с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни, отнасящи се до пола на физическо лице, живот или сексуална ориентация;
- **Администратор на данни:**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 Съюза 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;[2]
- **Обработващият данни:**физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;[3]
- **Обработване:**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;
- **Псевдонимизация:**обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;
- **Трансгранично обработване:**а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятнода засегне съществено субекти на данни в повече от една държава членка**Надзорен орган:**независим публичен орган, създаден от държава членка съгласно член 51 на Регламента;[4]

---

[1]Такива лични данни са напр. имена, адрес, електронна поща, телефонен номер, IP адрес, ЕГН и специалните (чувствителни) лични данни съгласно дефиницията, дадена в следващата точка.

[2] За целите на настоящата политика, администратор на данни е „Комисията за защита на личните данни"

- **Водещ надзорен орган:** надзорният орган, който носи основната отговорност за извършването на трансгранична дейност по обработка на данни. Например когато субект на данни подаде жалба относно обработката на личните му данни, органът е отговорен, наред с другото, за получаването на уведомления за нарушаване на данните, за уведомяване за рискова обработка и има пълна власт по отношение на задълженията си, за да гарантира спазването на разпоредбите на Регламента;
- Всеки **местен надзорен орган** ще продължи да поддържа на своя собствена територия и ще наблюдава всички местни обработки на данни, които засягат субектите на данни или които се извършват от администратор, или обработващ от ЕС, или извън ЕС, когато обработването им е насочено към субекти на данни, пребиваващи на нейна територия. Техните задачи и правомощия включват провеждане на разследвания и прилагане на административни мерки и глоби, насърчаване на обществената информираност за рисковете, правилата, сигурността и правата във връзка с обработката на лични данни, както и достъпа до помещенията на администратора и обработващия , включително оборудване и средства за обработка на данни;

- **Основно място на установяване**означава: а) по отношение на администратор, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, 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 Съюза 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; б) по отношение на обработващ лични данни, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно Регламента;

- **Група от предприятия:**контролиращо предприятие и контролираните от него предприятия;

3. Принципи, отнасящи се до обработката на лични данни

Принципите за защита на данните очертават основните отговорности за организациите, обработващи лични данни. В член 5, параграф 2 от Регламента се посочва, че *администраторът е отговорен и е в състояние да докаже спазването на принципите – задължение за отчетност.*

3.1. Законосъобразност, добросъвестност и прозрачност

Личните данни трябва да бъдат обработвани законосъобразно, справедливо и по прозрачен начин по отношение на субекта на данните.

3.2. Ограничение напредназначението

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

3.3. Необходимост, предназначение и минимизация

Личните данни трябва да бъдат подходящи, уместни и ограничени до това, което е необходимо по отношение на целите, за които се обработват. Дружеството трябва да прилага анонимност или псевдонимация на личните данни, ако е възможно, за да намали рисковете за засегнатите субекти на данни.

3.4. Точност и актуализация

Личните данни трябва да бъдат точни и при необходимост, актуализирани; трябва да се предприемат разумни стъпки, за да се гарантира, че неточните лични данни, като се имат предвид целите, за които се обработват, се изтриват или коригират своевременно.

3.5. Ограничение на сроковете за съхранение

Личните данни трябва да се съхраняват не повече от времето, необходимо за целите, за които се обработват личните данни, когато се съхраняват във форма, която да позволява идентифицирането на субекта. Срокът за съхранение на лични данни, предоставени от участници в процедури по подбор на персонала, не може да бъде по-дълъг от три години.

3.6. Цялостност, поверителност, сигурност и контрол на достъпа

Личните данни трябва да бъдат съхранявани по начин, който да осигурява подходящо ниво на сигурност, вкл. защита срещу неразрешено или незаконосъобразно обработване или срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

3.7. Отговорност и отчетност

Администраторите на данни трябва да отговарят и да могат да докажат съответствие с принципите, изложени по-горе.

4. Организационни и оперативни насоки

За да се докаже съответствие с принципите за защита на данните, Дружеството трябва да изгради защита на данните в обема и според начините, предвидени в Регламента и другите актове от приложимото законодателство.Трябва да има необходимата защита на личните данни на етапа на проектирането (преди да започне обработката им) и по подразбиране (минимално количество данни, които се съхраняват за минимално необходимия срок).

4.1. Уведомяване на субекта на данните за тяхното събиране и обработка

Необходимо е субектът на лични данни да бъде уведомен за тяхното събиране и обработка, вкл., но не ограничено до, прозрачност по отношение на вида лични данни и степента на риск, за начина на събиране, използване, консултиране или обработване, както и информация за целите, за които тези данни се събират (пар. 39 от Преамбюла към Регламента). Всяка информация и комуникация по отношение на събирането на лични данни трябва да бъде лесно достъпна и разбираема за субекта. Този въпрос е по-

подробно разгледан в точка „Препоръки за обработката на лични данни" от настоящата политика.

4.2. Информиран избор и съгласие на субекта

Администраторът следва да може да докаже, че субектът е направил информиран избор за предоставяне на личните си данни, като е предоставил свободно дадено, конкретно, информирано и недвусмислено съгласие за обработването им. На децата се полага специална защита на личните данни. Този въпрос е по-подробно разгледан в точка „Препоръки за обработката на лични данни" от настоящата политика.

4.3. Събиране на лични данни

Дружеството трябва да се стреми да събира възможно най-малко лични данни – единствено тези, които са му действително необходими. Дружеството, в качеството си на работодател, може да копира документ за самоличност или свидетелство за управление на МПС или документ за пребиваване единствено, ако закон изисква това. Данни за съдимост се обработват само, ако закон изисква това [5].

Данни, които Дружеството събира, включват още:

- Информацията, предоставена от клиент или друго трето лице (имейл адрес, име, адрес за фактуриране, домашен адрес и т.н. – основно информация, която е необходима за доставка на продукт/услуга или за подобряване на потребителския опит с Дружеството. Запазва се предоставена информация за коментиране или за изпълнение на други дейности на уебсайта ..... Тази информация включва например име и имейл адрес на потребителя на сайта.

- Автоматично събрана информация за трето лице (информация, която автоматично се съхранява от "бисквитки" и други инструменти за сесии; информацията за вашата кошница, вашия IP адрес, историята на пазаруването (ако има такава) и др. с цел подобряване на потребителския опит.

- Информация от партньорите на Дружеството (с потвърждение, че имат правно основание да споделят тази информация с нас. Това е или информация, която клиентът е предоставил директно, или е събрана на други правни основания).

- Публично достъпна информация за трети лица.

Отговорност за събирането на данни, вкл. получавани от трети страни, носи управителят на „ЕМАМАР 2013" ЕООД.

4.4. Използване, съхранение и унищожаване

Обработването на личните данни трябва да бъде в съответствие с целите, за които първоначални са събрани личните данни. Възможно е обработване за други цели единствено, ако е налице някое от другите основания за законосъобразност на

[5] Според последните промени от 12.12.2017 г. в Наредба № 4 от 11.05.1993 г. за документите, които са необходими за сключване на трудов договор, свидетелство за съдимост за сключване на трудов договор се иска, само когато закон или нормативен акт изисква да бъде удостоверено съдебно минало.

обработването (различно от съгласие на субекта) – за изпълнение на договор със субекта, за спазване на законово задължение, за защита на жизненоважните интереси на субекта или за защита на легитимните (законово признатите) интереси на администратора или на трета страна.

Дружеството трябва да поддържа точността, целостта, поверителността и уместността на личните данни въз основа на целта на обработката и при осигуряване на възможност за корекцията им от субекта на данни. Трябва да се използват адекватни механизми за защита (технически и организационни), предназначени за защита на личните данни, за да се предотврати откраднването или злоупотребата с личните данни, и да се предотврати нарушаването на личните данни.Управителят на „ЕМАМР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

4.5. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[6], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този доставчик ще предостави мерки за сигурност, за да защити личните данни, които са адекватни на свързаните с тях рискове – напр. злоупотреба, неоторизиран достъп, неразрешено разкриване, унищожаване и др. и в съответствие с принципа, че защитата преминава заедно с данните. За целта, отговорното лице трябва да изисква съконтрахентът да осигури същото ниво на защита на данните – чрез съответствие с Регламента или чрез задължителни договорни клаузи за защита на личните данни.

Съконтрахентът трябва да обработва само лични данни, необходими му, за да изпълнява своите задължения към Дружеството или по нареждане на Дружеството, а не за други цели. Когато Дружеството обработва лични данни съвместно с независима трета страна, Дружеството трябва изрично да уточни своите съответни отговорности и третата страна в съответния договор или друг правно обвързващ документ.

4.6. Трансграничен трансфер на лични данни

Преди да се предадат лични данни извън ЕС и Европейското икономическо пространство (ЕИП), трябва да се използват адекватни предпазни мерки, включително подписването на споразумение за прехвърляне на данни, както се изисква от Европейския съюз, и при необходимост трябва да бъде получено разрешение от съответния орган за защита на данните. Лицето от трета страна, което получава личните данни, трябва да спазва принципите за обработка на лични данни, посочени в процедурата за трансгранично предаване на данни. Особено внимание се изисква при трансфер на лични данни към САЩ, доколкото за този вид е предвиден особен механизъм за защита на личните данни между ЕС и Швейцария и САЩ – TheEU-U.S. andSwiss – U.S. PrivacyShield[7].

4.7. Право на достъп на субекта на данни

[6]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[7]Механизмът е наличен на уебсайта на Европейската комисия, както и на уебсайта, създаден от правителството на САЩ за него - https://www.privacyshield.gov/welcome .

Когато действа от името на администратора на данни, управителят на „ЕМАМР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

4.8. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[8], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този е отговорен да предоставя на субектите на даннимеханизъм, който им позволява да имат разумен достъп до личните си данни, и трябва да им позволява да актуализират, коригират, изтриват или предават своите лични данни, ако е приложимо или се изисква по закон. Механизмът за достъп ще бъде допълнително описан в процедурата за заявка за достъп до субекта на данни.

4.9. Копиране на данни и предоставянето им на друг администратор

Субектите на данни имат право да получат при поискване копие от данните, които са ни предоставили в структуриран и машинно четим формат, и да предадат тези данни на друг администратор безплатно. Управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

4.10. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[9], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този е отговорен да гарантира, че тези искания се обработват в рамките на един месец и не засягат правата на лични данни на други лица.

4.11. Правото „да бъдеш забравен"

Правото на изтриване на данните (правото „да бъдещ забравен") включва възможността, когато субектът на данни не желае те да бъдат обработвани и не съществуват законови основания за съхранението им, да поиска заличаването им при наличие на едно от следните основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;
- субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

[8]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[9]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

- личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

Когато Дружеството действа като администратор на данни, управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

4.12. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[10], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този трябва да предприеме необходимите действия (включително технически мерки), за да информира третите лица, които използват или обработват тези данни, да се съобразят с искането.

5. Препоръки за обработката на лични данни

Личните данни трябва да се обработват само при изрично разрешение от управителя на Дружеството.

Дружеството трябва да реши дали да извърши оценката на въздействието върху защитата на данните за всяка дейност по обработка на данни, съгласно насоките за оценка на въздействието.

5.1. Уведомяване на субектите на данни и трансгранично прехвърляне на данни

По време на събирането или преди събирането на лични данни за всякакъв вид обработка, включително, но не само, извършване на подбор на персонал, продажба на продукти, услуги или маркетингови дейности (включително и за директен маркетинг), администраторът е отговорен 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 запазване, 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 Известие за поверителност.

Когато се споделят лични данни с трета страна, управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.2. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[11], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този трябва да гарантира, че субектите на данни са били уведомени за това чрез Известие за поверителност.

---

[10]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[11]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

Когато се прехвърлят лични данни на трета държава, в съответствие с Трансграничната политика за прехвърляне на данни, съобщението за поверителност трябва да отразява това и ясно да посочва къде и кои лични данни се прехвърлят.

5.3. Получаване на съгласие от субекта

Управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.4. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[12], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този отговаря за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласието си, и трябва да информира, и да гарантира, че тяхното съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време. Съгласието трябва да бъде:

• *свободно изразено* – да не е дадено под натиск или заплаха от неблагоприятни последици;

• *конкретно* – отделно съгласие за всяка конкретно определена цел, а когато е относимо - и за конкретна категория лични данни;

• *информирано* – дадено на основата на пълна, точна и лесно разбираема информация;

• *недвусмислено* – не се извлича или предполага на основата на други изявления или действия на лицето;

• *изрично изявление или ясно потвърждаващо действие* – мълчанието не може да се приеме за съгласие, както и предварително отметнатите квадратчета.

Когато събирането на лични данни е свързано с дете на възраст под 16 години, Управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.5. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[13], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този трябва да гарантира, че родителското съгласие е дадено преди събирането.

Когато се изисква да се оттегли даденото съгласие, както и да се проверят, коригират, изменят или унищожат записите с лични данни, управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

---

[12]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[13]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

5.6. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[14], който да обработва лични данни от негово име, управителят на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този трябва да гарантира, че тези изисквания се обработват в разумен срок.]също трябва Управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.7. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[15], който да обработва лични данни от негово име, управителя на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този да записва заявките и да води дневник за тях.

Личните данни трябва да се обработват само за целите, за които първоначално са били събрани. В случай, че Дружеството иска да обработва събраните лични данни за друга цел, Дружеството трябва да потърси съгласието на своите субекти на данни в ясен и кратък срок. Всяко такова искане трябва да включва първоначалната цел, за която са събрани данните, както и новата или допълнителната (ите) цел (и). Искането трябва да включва и причината за промяната на целта / целите.

Сега и в бъдеще, управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.8. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[16], който да обработва лични данни от негово име, управителя на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този трябва да гарантира, че методите за събиране са в съответствие със съответните закони, добри практики и стандарти.

Управителят на „ЕМАМАР 2013" ЕООД отговаря за спазването на изискванията, изброени в този раздел.

5.9. Предоставяне на трети страни

Когато Дружеството използва услугите на съконтрахент[17], който да обработва лични данни от негово име, управителя на „ЕМАМАР 2013" ЕООД трябва да гарантира, че този е отговорен за създаването и поддържането на регистър на известията за поверителност.

---

[14]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[15]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[16]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

[17]Това може да бъде доставчик, партньор, клиент и пр., с който Дружеството се намира в договорни или преддоговорни отношения.

6. Отговорни лица

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

7. Управление на риска и действия в отговор на нарушаване на защитата на личните данни

Когато Дружеството узнае за предполагаемо или действително нарушение на личните данни, мениджмънтът трябва да извърши вътрешно разследване и своевременно да предприеме подходящи мерки за отстраняване, в съответствие с политиката за нарушаване на данните. Когато съществува риск за правата и свободите на субектите на данни, Дружеството трябва да уведоми съответните органи за защита на данните без неоснователно забавяне и, когато е възможно - **в рамките на 72 часа**.

8. Отговорностна служителите

Всеки служител, който нарушава тази Политика, ще бъде обект на дисциплинарно действие и служителят може също да бъде обвързан с гражданска или наказателнаотговорност, ако неговото поведение нарушава закони или подзаконови актове.

Нарушението на настоящата Политика и на Регламента, ЗЗЛД и другите актове от приложимото законодателство се приемат за тежки нарушения на трудовата дисциплина (неизпълнение на други трудови задължения) и са основание за дисциплинарна отговорност по смисъла на чл. 187, т. 10 от Кодекса на труда.

9. Несъответствие с приложимото законодателство

Тази политика е предназначена да спазва законите и подзаконовите актове на мястото на установяване и на страните, в които Дружеството работи. В случай на конфликт между тази Политика и приложимите закони и подзаконови нормативни актове, последните имат предимство.

10. Влизане в сила и актуализиране

Този документ е валиден от датата на утвърждаването му.

Дружеството си запазва правото да преглежда периодично тази Политика за съответствие с приложимото законодателство и да внася промени в нея, ако това е необходимо, като уведоми за тях всички лица, за които тя се отнася.