

"ОКЕМА" ЕООД
ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ
НА ЛИЧНИТЕ ДАННИ

Версия 02 / 09.09.2024 г.

Утвърдил:

/Руди Тошев - Управител/

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

СЪДЪРЖАНИЕ

I. Въведение	3
1. Общ регламент за защита на личните данни (GDPR)	3
2. Обхват	3
3. Понятия	3
II. Декларация относно политиката по защита на личните данни	5
III. Задължения и роли по GDPR	5
IV. Принципи за защита на данните	6
V. Права на субектите на данни	10
VI. Съгласие	11
VII. Сигурност на данните	11
VIII. Разкриване на данни	12
IX. Съхраняване и унищожаване на данни	13
X. Трансфер на данни	13
XI. Регистър на дейностите по обработване по чл.30 от GDPR	14

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

I. Въведение

1. Общ регламент за защита на личните данни (GDPR)

EU GDPR 2016/679 (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) има пряко действие за държавите-членки, считано от 25.05.2018 г. Неговата цел е да модернизира и уеднакви политиките на държавите-членки на ЕС по отношение на начините за събиране и използване на лични данни, както и да осигури възможност за свободно движение на данни в рамките на цифровия единен пазар, както и да гарантира по-добра защита на неприкосновеността на личния живот.

2. Обхват

Материален обхват – GDPR се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (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 – GDPR се прилага 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 се намират 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 или сексуалната ориентация на физическо лице.

„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;

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

„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;

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

„Субект на данните“ - всяко живо физическо лице, което е предмет на личните данни обработвани 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“ – GDPR определя дете като всеки на възраст под 16 години, въпреки че посочената възраст може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че носителът на родителската отговорност за детето е дал 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, освен когато решенията относно целите и средствата за обработване на лични данни се вземат на друго място. По отношение на обработващия лични данни – седалището му в ЕС, или ако няма такова, мястото на установяване в ЕС, където се осъществяват основните дейности по обработването.

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.

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

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

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

II. Декларация относно политиката по защита на личните данни

1. Ръководството на “Окема” ЕООД, 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 “Окема” ЕООД събира и обработва съгласно GDPR.
2. В съответствие с GDPR към настоящата политика са описани и други релевантни документи, както и свързани процеси и процедури.
3. GDPR и настоящата 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 до всякакви други лични данни, които организацията събира от различни източници.
4. Отговорникът за защита на данните отговаря за преразглеждането на Регистъра на дейностите по обработване ежегодно в светлината на всякакви промени в дейностите на “Окема” ЕООД, както и всички допълнителни изисквания, оценки на въздействието върху защитата на данните и др. Този регистър трябва да бъде на разположение по искане на надзорния орган.
5. Тази политика се прилага за всички работници и служители/доброволци и ръководни и контролни органи на всички организационни нива), както и за всички партньори, външни изпълнители, доставчици на стоки и услуги на “Окема” ЕООД. Всяко нарушение на GDPR ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът своевременно ще се предостави за разглеждане на компетентните държавни органи.
6. Партньори и трети лица, които работят с или за “Окема” ЕООД, както и които имат или могат да имат достъп до личните данни, ще се очаква да се запознаят и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от “Окема” ЕООД, без предварително да е сключила договор Администратор - Обработващ, който налага на третата страна задължения, не по-малко обременяващи от тези, които “Окема” ЕООД е поел, и което дава право на “Окема” ЕООД да извършва проверки на спазването на наложените с договора задължения.

III. Задължения и роли по GDPR

1. “Окема” ЕООД е администратор на данни и/или обработващ данни съгласно GDPR.
2. Ръководството на “Окема” ЕООД е отговорно за разработване и насърчаване на добри практики в областта на обработване на лични данни в “Окема” ЕООД;
3. Длъжностното лице по защита на данните (ДЛЗД) (с роля и задължения, посочени в чл.37-39 от GDPR и длъжностната му характеристика), респ. Отговорникът по защита на данните (с роля и задължения, посочени в длъжностната му характеристика), трябва се отчита пред управителя на “Окема” ЕООД 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 ДЛЗД включва:

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

- разработване и внедряване на изискванията на GDPR както се изисква от настоящата политика;
- управление на сигурността и риска по отношение на съответствието с политиката.

4. ДЛЗД, което ръководството на Дружеството счита за подходящо, квалифицирано и опитно, може да бъде назначено, за да поеме отговорността за съответствието на “Окема” ЕООД с настоящата политика на ежедневна основа. ДЛЗД, респ. Отговорникът по защита на данните е пряко отговорен да гарантира, че както като цяло организацията на дейността на “Окема” ЕООД съответства на изискванията на GDPR.

5. ДЛЗД, респ. Отговорникът по защита на данните има специфични отговорности 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 “Окема” ЕООД, които обработват лични данни.

7. Политиката за обучение на “Окема” ЕООД определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на работниците/служителите на “Окема” ЕООД.

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 GDPR. Политиките и процедурите на “Окема” ЕООД имат за цел да гарантират спазването на тези принципи.

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

Законосъобразно – да идентифицира правно основание, преди да може да обработва лични данни („основания за обработване“).

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.

Прозрачно – GDPR включва правила относно предоставяне на подробна информация на субектите на данни. Те са подробни и конкретни, поставяйки акцента върху това, че уведомленията 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.

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;
- контактите на ДЛЗД, респ. Отговорникът по защита на данните;
- целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

- 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 право на възразение;
- 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 по чл.30 от GDPR.

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

- ДЛЗД/Отговорникът по защита на данните е отговорен да осигури “Окема” ЕООД да не събира информация, която не е строго необходима 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 уведомление за поверителност и да бъдат съгласувани с ДЛЗД, респ. Отговорника по защита на данните, или да е поет ангажимент по отношение на спазване на посоченото в Политиката за поверителност на Уебсайта.
- Длъжностното лице по защита на данните / отговорникът по защита на данните ще гарантира, че ежегодно всички способи за събиране на данни се преглеждат от него с помощта на вътрешен одит или външни експерти, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни.

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.

- Данните, които се съхраняват от администратора на данни, трябва да бъдат прегледани и актуализирани при необходимост.
- ДЛЗД, респ. 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 предава за обработване от “Окема” ЕООД са точни и актуални.
- От работниците/служителите, изпълнителите по граждански договори, клиентите, партньорите и др. трябва да се изисква, да уведомяват “Окема” ЕООД за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на “Окема” ЕООД е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

- ДЛЗД, респ. 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.
- ДЛЗД, респ. Отговорникът по защита на данните ежегодно прегледа сроковете на съхранение на всички лични данни, обработвани от “Окема” ЕООД, 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.
- ДЛЗД, респ. Отговорникът по защита на данните е отговорен за изпълнение на искания за корекция на данни в рамките на един месец. Този срок може да бъде удължен с още два месеца за сложни заявки. Ако “Окема” ЕООД реши да не се съобрази с искането, ДЛЗД / 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.

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 (минимизирани, криптирани, псевдонимизирани), 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 унищожени по указания в тази процедура ред.
- ДЛЗД / Отговорникът по защита на данните специално трябва писмено 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.

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

ДЛЗД / Отговорникът по защита на данните ще извърши оценка на риска и на въздействието, като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от “Окема” ЕООД.

При определянето на това доколко уместно е обработването, ДЛЗД / Отговорникът по защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. служители 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, ДЛЗД / Отговорникът 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;

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

- 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 “Окема” ЕООД.

При оценяването на подходящите организационни мерки ДЛЗД / Отговорникът по защита на данните ще вземе предвид следното:

- Нивата на подходящо обучение в “Окема” ЕООД;
- 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“¹ и „чист екран“;
- Съхраняване на хартия на базата данни в заключващи се 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

GDPR включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност изисква от администратора да докаже, че спазва останалите принципи в GDPR и изрично заявява, че това е негова отговорност.

¹ 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.

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

“Окема” ЕООД 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. Субекта на данни има следните права по отношение на обработването на негови лични данни:

- 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 поиска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
- Да поиска от администратора изтриване на лични данни (право „да бъдеш забравен“) при определените за това условия;
- 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 Комисията за защита на личните данни (КЗЛД) ако смята, че някоя от разпоредбите на GDPR 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, ако основанието за обработване е съгласие;
- 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. “Окема” ЕООД 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 за Процедурата за заявка за достъп до данни, която описва как “Окема” ЕООД ще гарантира, че отговора на искането на субекта на данни отговаря на изискванията на GDPR.
- Субектите на данни имат право да подават жалби до “Окема” ЕООД, свързани с обработването на личните им данни и обработването на техни искания в съответствие с Процедурата за жалби.

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

VI. Съгласие

1. Под „съгласие“ “Окема” ЕООД ще разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.
2. “Окема” ЕООД 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 него да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация не е 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 за дейностите по обработване чрез уведомление за поверителност или формуляр за съгласие.
4. За специални категории данни трябва да се получи изрично писмено съгласие на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.
5. Когато “Окема” ЕООД 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 14 години.

VII. Сигурност на данните

1. Всички работници/служители са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които “Окема” ЕООД държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако “Окема” ЕООД не е дал такива права на тази трета страна, като е сключил договор Администратор-Обработващ или става дума за държавен орган с посочена от закона компетентност да изисква такива данни.
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 Процедурата за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:
 - в стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или
 - ако са компютризирани - да са защитени с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация; 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 оторизираните работници/служители на “Окема” ЕООД. От всички работници/служители се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларации 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.

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

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, те трябва да бъдат унищожени в съответствие със създадена за това процедура.

5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедурата за съхраняване и унищожаване на данни. Записите на хартиен носител, които са достигнали крайната дата на съхранение, трябва да бъдат нарязани и унищожени като „поверителни отпадъци“. Данните върху твърдите дискове на неизползвани или бракувани персонални компютри и записващи носители трябва да бъдат изтрети или дисковете унищожени, съгласно изградените правила чрез изтриване или унищожаване на самите носители.

6. Обработването на лични данни „извън офиса“ представлява потенциално по-голям риск от загуба, кражба или нарушение на сигурността на личните данни. Работниците/служителите/изпълнителите по граждански договори трябва да бъдат специално упълномощен да обработва данните извън обекти на администратора.

VIII. Разкриване на данни

1. “Окема” ЕООД 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 работници/служители 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 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 ДЛЗД / Отговорника за защита на данните.

3. “Окема” ЕООД извършва ранна (преди първия достъп до данни!) проверка и подбор на всички доставчици на услуги, както и проверки на редовни интервали и документиране на всички външни сътрудничества. Това касае всички нови или променени сътрудничества, свързани със защита на данни с външни доставчици на услуги (физически или юридически лица, държавни служби, институции или други лица, които обработват лични данни по поръчка на дружеството). Терминът доставчик на услуга се използва като синоним на термина лице, обработващо лични данни.

4. Преди доставчиците на външни услуги да получат поръчка, или да бъдат сключени или променени договори с тях, те трябва да бъдат проверени от Отговорника за защита на данните, като предаването на данни от дружеството на външния доставчик на услуги не трябва да се случва преди проверката. За тази цел, всички отговорни лица, които имат правото да сключват договор с доставчици на услуги, трябва първо да докладват за своя проект на Отговорника за защита на данните. След преглед на нужните разпоредби съгласно закона за защита на данни и осъществяване на необходимите проверки на нивото на защита на данните при съответния

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

външен доставчик, Отговорникът за защита на данните препоръчва сключване на договора или отказ.

IX. Съхраняване и унищожаване на данните

1. “Окема” ЕООД 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. “Окема” ЕООД 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 Периодът на съхранение за всяка категория на лични данни, както и критериите, използвани за определяне на този период, включително всякакви законови задължения в тази връзка, са посочени в Процедурата за съхраняване и унищожаване на данните и графика към нея.

4. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност, 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 GDPR като „трети страни“) и Европейското икономическо пространство (ЕИП) (ЕС и Лихтенщайн, Норвегия и Исландия) са незаконни, освен ако няма подходящо 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 указаните 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.

Европейската комисия публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита. 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. Договорености при взаимоотношенията между ЕС и САЩ, регулиращи законосъобразния трансфер на лични данни

Ако администраторът желае да прехвърли лични данни от ЕС на трета страна в САЩ, той трябва да провери кой е адекватния способ за законосъобразен трансфер.

4. Задължителни фирмени правила

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

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

5. Стандартни договорни клаузи

“Окема” ЕООД може да приеме утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън ЕИП. Ако “Окема” ЕООД приема стандартните договорни клаузи, одобрени от съответния надзорен орган има автоматично признаване на адекватността.

6. Изключения

При липса на решение за адекватност, 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 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 дейностите по обработване по чл.30 от GDPR

1. “Окема” ЕООД е създава 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 GDPR. При инвентаризацията на данните в “Окема” ЕООД 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 във всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването;

ОКЕМА ЕООД	ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ Индекс 2.1.	Утвърдил: Руди Тошев Версия 02 / 09.09.2024 г.
------------	---	---

- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

2. “Окема” ЕООД е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. “Окема” ЕООД оценява нивото на риска за лицата, свързани с обработването на личните им данни. В предвидените от закона случаи се извършват оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от “Окема” ЕООД и във връзка с обработването, предприето от други организации от името на “Окема” ЕООД.

4. “Окема” ЕООД 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 “Окема” ЕООД следва да извърши оценка на въздействието на предвидените операции по обработване върху защитата на личните данни.

5. Когато в резултат на Оценката на въздействието е ясно, че “Окема” ЕООД 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 от страна на ДЛЗД, респ. Отговорника по защита на данните .

6. Ако ДЛЗД, респ. Отговорникът по защита на данните има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да предостави въпроса за решаване от КЗЛД.

7. ДЛЗД, респ. Отговорникът по защита на данните, прави ежегоден преглед на първоначално инвентаризирани данни, преразглежда вписаната информация в Регистъра по чл.30 в светлината на всякакви промени в дейностите на “Окема” ЕООД. Всички служители са задължени да информират Отговорника по защита на данните веднъж годишно за съществуващи операции по обработката, както и за промени в тези операции по обработка (включително нови).