ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА АЙЗАЕМ.БГ ООД

ВЪВЕДЕНИЕ :

Настоящата Политика за поведение за защита на личните данни се приема на основание Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (по-нат. Регламента).

Политиката е приета и утвърдена от законния представител на дружеството администратор.

Администратор на лични данни е "АЙЗАЕМ.БГ" ООД, с ЕИК 203595295 по описа на ТР при АВ, със седалище и адрес на управление - гр.София, Столична община, ж.к. ХАДЖИ ДИМИТЪР, ул. ПАНАЙОТ ХИТОВ, бл. 118, вх. Д, ет. 1, ап. 123.

ГЛАВА ПЪРВА
Предмет

Чл.1. Тази политика урежда:

1. Принципите на добросъвестно и прозрачно обработване на лични данни от администратора;
2. Законните интереси на администратора при обработване на лични данни за целите на дейността като финансова институция;
3. Редът, лицата и операциите по събиране на лични данни;
4. Псевдонимизацията на личните данни;
5. Дейностите и отговорностите по информиране на обществото и субектите на данните;
6. Начина на упражняване на правата на субектите на данни;
7. Мерки и процедури за защита на данните и сигурността на обработването;
8. Процедури при нарушения на сигурността на лични данни;

Чл.2. (1) Тази политика цели осигуряване на най-висока степен на закрила на физическите лица във връзка с обработването на личните им данни, независимо от тяхното гражданство или местопребиваване относно кръга от дейности, извършвани по Закон за потребителския кредит.

(2) Правилата на политиката са съобразени с:

1. правният статут на финансовите институции;
2. определените в действащото законодателство основания за обработване на лични данни, свързани с финансовите дейности;
3. правните и фактически особености на дейностите на финансовите институции;
4. законовите задължения за предаване на обработваните лични данни на трети лица – публични органи.

ГЛАВА ВТОРА
РЕЖИМ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Раздел I.
Добросъвестно и прозрачно обработване на лични данни

Чл.3. Администраторът обработва лични данни при спазване на следните принципи:

1. законосъобразно, добросъвестно и по прозрачен начин обработване на данните;
2. обработване на ясно определен и ограничен обем от данни, пряко свързани с дейността по отпускане на потребителски кредити и на общите задължения по реда на облигационното, трудово, данъчно и осигурително законодателство;
3. мерки за осигуряване неприкосновеността на данните от неоправомощени по закон или договор трети лица;
4. точност и спазване на процедури за корекции на обработваните данни при грешки или непълнота;
5. придържане към определения в законодателството обем от обработвани данни, свързани със здравето на субектите;
6. съхранение на данните до определените в законодателството срокове и своевременно унищожаване на носителите на данни при спазване на правила за сигурност;
7. проследимост и механизъм за достъп до данните на субектите;
8. оценка на ниво на сигурност на личните данни и спазване на подходящи технически или организационни мерки за защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане на данните;
9. въвеждане на изисквания, обучение и контрол върху дейността на персонала, имащ функции по обработка на данни;
10. отчетност за спазване на принципите чрез прилагане на мерките и документите, предвидени в политиката;

Чл.4. (1) Администраторът обработва следните групи данни:

1. Данни за физическа идентичност на субектите – имена, ЕГН, подпис, адрес, телефон, месторождение, възраст, електронен адрес, документ за самоличност, образ;
2. Данни за социална и икономическа идентичност – имущество и доходи от трудова дейност или от друга дейност; работодатели; банкови сметки; договори за заем; кредитно досие;
3. Данни за здравословното състояние на лицата –данни относно здравословното състояние на служители и работници.

(2) Данните по ал.1 се обработват в един или повече от следните регистри:

1. Регистър на персонала относно данни на субектите по граждански и трудови договори;
2. Регистър на контрагентите;
3. Регистър на потребителите по договори за потребителски кредит.

Чл.5. (1) **Регистър на персонала** съдържа следните данни:

1. Данни за физическа идентичност на субектите – имена, ЕГН, адрес, телефон, месторождение, възраст, електронен адрес, документ за самоличност, саморъчен подпис;

2. Данни за социална и икономическа идентичност – трудовата дейност и образованието на субектите – стаж, предходни работодатели, образователни степени и институции, професионална квалификация, банкови сметки;
3. Данни за семейно положение – наличие на деца, сключен брак;
4. Данни за здравословното състояние на работници и служители и членове на семейството им.

(2) Данните по ал.1 се обработват на хартиен или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни.

(3) Данните се съхраняват на следните хартиени носители:

1. автобиография, мотивационно писмо, снимка, дипломи и други документи за доказване на професионална квалификация, трудов и граждански договори, длъжностна характеристика, допълнително споразумения към трудовия или граждански договор, актове за прекратяване на трудовото правоотношение, ведомости за изплатени възнаграждения, служебни бележки и удостоверения за трудов и осигурителен стаж и доходи, молби и заявления относно трудовото правоотношение (молби за ползване на отпуск, за напускане, за заместване, за трудоустрояване и други; декларации за получена трудова книжка, за удръжка от заплатата за допълнително пенсионно осигуряване; служебни бележки; протоколи за предадено материално оборудване и други, предвидени от Кодекс на труда и подзаконовите актове по прилагането му;

2. документ за медицински преглед при първоначално постъпване на работа и след преустановяване на трудовата дейност по трудово правоотношение за срок над 3 месеца по реда на Наредба № 4 от 11.05.1993 г. за документите, които са необходими за сключване на трудов договор; резултати от задължителни периодични медицински прегледи и изследвания по реда на Закона за здравословни и безопасни условия на труд и актовете по прилагането му; документи за медицинска екпертиза на работоспособността по смисъла на Наредба за медицинската експертиза.

(4) Част от изброените в ал.3 документи могат да бъдат създадени и обработвани в електронен вид.

(5) Данните по ал.1 се обработват със специализирани софтуерни програми за нуждите на начисляване и определяне на размера на трудови възнаграждения, определяне на размера на дължимите от осигурителя и осигурения осигуровки и данъци.

(6) Данните се обработват относно субекти, които са сключили трудов или граждански договор с търговеца на дребно за нуждите на дейността му. Забрането е копирането на документи за самоличност и съхранение на копия от тях на хартиен или електронен носител за субектите, наети по трудови или граждански правоотношения.

(7) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в трудовото, данъчното и осигурителното законодателство:

1. Национална агенция за приходите;
2. Национален осигурителен институт;
3. Изпълнителна агенция „Главна инспекция по труда“.

(8) Данните по ал.1 относно идентификация на лицата от персонала не се публикуват на интернет страница или в други рекламни или промоционални без изричното съгласие на субектите.

(9) Данните по ал.1 на хартиен носител или под формата на записи на електронни носители се унищожават по предвидения в закона и тази политика ред в следните срокове:

1. граждански договор, длъжностна характеристика, допълнителни споразумения към трудовия или граждански договор, декларации относно осигуряване, хонорар - сметки – десет години след прекратяване на трудовото или гражданско правоотношение;

2. трудов договор, заповеди за ползван неплатен отпуск над 30 работни дни годишно, заповеди за прекратяване на трудовото правоотношение, ведомости за изплатени възнаграждения, декларации и удостоверения относно социално осигуряване по трудови правоотношения (обр. УП-1, обр. УП-2, обр. УП-3 и обр. 30) – 50 години от прекратяване на трудовото правоотношение;

3. всички останалали документи и записи, описани в ал.3 – до три години след прекратяване на трудовото или гражданско правоотношение.

(10) По изключение посочените в ал.10, т.1 и т.3 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно-наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(11) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, дипломи и други документи за квалификация, документи от медицинската експертиза, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон - справка за валидни документи за самоличност и др.

(12) Данните от регистър персонал се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;

2. определени от него счетоводители или други лица, наети по трудови правоотношения, с възложени функции по управление на хора според длъжността;

3. обработващи данни извън структурата на администратора, с които има сключен договор – счетоводни кантори и дружества за определяне на дължими трудови възнаграждения и свързани с тях публични плащания, одитори, посредници за наемане на работа, адвокати и адвокатски дружества.

(13) За данните от регистър персонал се прилагат правилата по-долу относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

(14) Работодателят обработва данни при подбор на персонал относно автобиография на лицата, снимка и мотивационно писмо. Посочените документи се унищожават по реда на тази политика в срок до 30 дни от получаване на данните.

(15) Работодателят въвежда система за докладване на нарушения на обработката на лични данни на работници и наети субекти по граждански договор по реда на този кодекс.

(16) Работодателят въвежда системи за контрол на достъпа до помещенията на аптеките, работното време на персонала и трудовата дисциплина, които се съдържат в тази политика и в правилниците за вътрешен ред.

Чл.6. (1) **Регистър на контрагентите** съдържа следните данни за физическа идентичност на субектите – имена, ЕГН, адрес, телефон, факс, електронен и IP адрес, документ за самоличност, саморъчен подпис.

(2) Данните по ал.1 се обработват на хартиен или електронен носител, като за част от данните има само запис на електронен носител без съхранение на документи, съдържащи данни.

(3) Данните се съхраняват на следните хартиени носители:

1. сключени договори и допълнителни споразумения към тях; протоколи и приложения към договори; фактури, данъчни и кредитни известия;
2. уведомления, писма, документи за определяне на представители за нуждите на изпълнението на договорите, искови молби, заявления и други документи относно изпълнението на договорите.

(4) Част от изброените в ал.3 документи могат да бъдат създадени и обработвани в електронен вид.

(5) Част от данните по ал.1 се обработват със специализирани софтуерни програми за счетоводни записвания, водене на счетоводни сметки, ДДС дневници, определяне на дължими данъци.

(6) Данните се обработват относно субекти, които са сключили търговски и граждански сделки с търговеца на дребно за нуждите на дейността му.

(7) Данните се разкриват на законово основание на следните публични органи, въз основа на задължения в данъчното, осигурителното законодателство и административното законодателство:

1. Национална агенция за приходите;
2. Национален осигурителен институт;
3. Държавна агенция „Национална сигурност“ относно мерки за изпиране на пари и предотвратяване на тероризма;
4. Агенция „Митници“ и икономическа полиция;
5. БНБ.

(8) Лични данни, получени на основание сключените граждански и търговски сделки от аптеката, не се публикуват на интернет страница или в други рекламни или промоционални материали без изричното съгласие на субектите.

(9) Данните по ал.1 на хартиен носител или под формата на записи на електронен носител се унищожават по предвидения в закона и този кодекс ред в следните срокове:

1. търговски и граждански договори и документи относно сключването, изпълнението и прекратяването им – пет години след прекратяване на търговското или гражданско правоотношение;
2. всички останалали документи и записи, описани в ал.3 – до две години след прекратяване на търговското или гражданско правоотношение.

(10) По изключение посочените в ал.9, т.1 и т.2 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(11) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, декларации и молби. При необходимост

администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон - справка за валидни документи за самоличност от интернет страницата на МВР, справки относно регистрани в Търговски регистър, воден от Агенция по вписванията, адреси за кореспонденция с НАП, телефони, факс и електронни адреси и др.

(12) Данните от регистър контрагенти се обработват от следните лица, определени от администратора:

1. законни представители на администратора по смисъла на приложимия към статута на лицето закон;
2. определени от него счетоводители, юрисконсулти, мениджъри търговска дейност, търговски и финансови директори или други лица, наети по трудови правоотношения, с възложени функции по управление на хора според длъжността;
3. обработващи данни извън структура на администратора, с които има сключен договор – счетоводни кантори и дружества за определяне на дължими трудови възнаграждения и свързани с тях публични плащания, одитори, посредници за наемане на работа, адвокати и адвокатски дружества.

(13) За данните от регистър контрагенти на аптеката се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;
2. задължения на обработващите на данни по договор с администратора;
3. съгласие на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

(14) Забрането е копиране и съхранение на хартиен или електронен носител на документи за самоличност на лицата, представляващи контрагентите.

(15) Ползването на ЕГН на лицата, представляващи контрагентите, се заменя преимуществено с посочване на номер и дата на издаване на документи за самоличност на лицата в договорите и другата съпътстваща документация. Последното не се прилага за сключвани граждански договори с физически лица, за които данъчното законодателство изисква подаване на декларации с посочване на ЕГН.

Чл.7. (1) **Регистър на потребителите по договори за потребителски кредит** съдържа следните данни за :

- физическа идентичност на субектите – имена, адрес, телефон, електронен адрес, възраст, документ за самоличност, данни за банкови сметки и средства за електронно разплащане, саморъчен подпис;
- социална и икономическа идентичност – имущество и доходи от трудова дейност или от друга дейност; работодатели; банкови сметки; договори за заем; кредитно досие от регистър на ЦКР при БНБ.

(2) Данните по ал.1 се обработват на хартиен и на електронен носител, като за част от данните има само запис в автоматизирани системи.

(3) Данните се съхраняват на следните хартиени или електронни носители:

1. сключени договори за заем и допълнителни споразумения към тях; протоколи и приложения към договори;
2. искане за сключване на договор за заем;

3. въпросници относно идентификация и нуждите на клиента, продуктите, към които има интерес;

4. декларации за изрично съгласие за обработване на лични данни.

(4) Изброените в ал.3 документи могат се създават и обработват в електронен вид със специализиран софтуерен продукт за управление на договорите за заем – Приста Хард ЕООД.

(5) Програмите отговорят на изискванията за автоматизирано обработване на данни в тази политика и в закона.

(6) Данните се обработват относно субекти, които са клиенти на финансовата институция с оглед на дейността му за отпускане на потребителски заеми на физически лица.

(7) Данните не се разкриват регулярно на законово основание на публични органи или на други трети лица, освен в предвидените в закона случаи.

(8) Лични данни, получени на основание искане на клиентите за получаване на заем, не се публикуват на интернет страница или в други рекламни или промоционални без изричното съгласие на субектите.

(9) Данните по ал.1 на хартиен носител или под формата на записи в автоматизирани системи се унищожават по предвидения в закона и този кодекс ред в следните срокове:

1. договори за потребителски заем, заявките, приложенията и допълнителните споразумения към тях– 5 години от датата на изпълнение на договора, съответно приключване на всички съдебни производства по събиране на вземанията.;

2. всички останалали документи и записи, описани в ал.3 – до две години след прекратяване на търговското или гражданско правоотношение.

(10) По изключение посочените в ал.9, т.1 и т.2 срокове може да се удължат при наличие на образувани преди изтичане на срока на унищожаване на данните съдебни, административно - наказателни или административни производства и данните са необходими за провеждане на производствата. Администраторът определя само относими към характера на съответното производство данни, като останалите се унищожават.

(11) Точността и верността на данните се проверява от администратора чрез представени от субектите документи за самоличност, декларации и молби. При необходимост администраторът може да прави проверки до масиви от данни, които са публично достъпни по закон - справка за валидни документи за самоличност от интернет страницата на МВР и др.

(12) Данните от регистър **на потребителите по договори за потребителски кредит** се обработват от следните лица, определени от администратора:

1. законни представители на търговеца по смисъла на приложимия към статута на лицето закон;

2. определени от него търговски директор, мениджъри, консултанти продажби и административни сътрудници, счетоводители, инкасатори или други лица, наети по трудови правоотношения, с възложени функции по сключването и изпълнението на договори за потребителски кредит според длъжността;

3. обработващи данни извън структура на администратора, с които има сключен договор – софтуерни доставчици, дружества за събиране на задължения и адвокати.

(13) За данните от **регистър потребителите по договори за потребителски кредит** се прилагат правилата по-долу на кодекса относно:

1. права на субектите на данните;

2. задължения на обработващите на данни по договор с администратора;

3. съгласие на субектите;
4. технически и организационни мерки на защита на данните;
5. ред за унищожаване на данните;
6. жалби и извънсъдебно разрешаване на спорове.

(14) Забрането е копиране и съхранение на хартиен или електронен носител на документи за самоличност на клиентите на аптеката.
(15) Ползването на ЕГН на лицата, представляващи контрагентите, се заменя преимуществено с посочване на номер и дата на издаване на документи за самоличност на лицата в договорите и другата съпътстваща документация.
(16) Данните в регистър **потребителите по договори за потребителски кредит** за нуждите на дейността по отпускане на потребителски кредити се обработват само при изрично съгласие на субектите.
(17) Данните от регистъра се предават на БНБ за нуждите на водене на Централен кредитен регистър по Наредба № 22 на БНБ за водене на ЦКР (име, ЕГН, договор за заем – размер, вноски и задължения).

Чл.8. (1) Администраторът се придържа към принципа за минимално обработване на лични данни, като за регистрите по чл.4, ал.2, т.1 – 3, не се обработват данни извън посочените.
(2) За всеки от регистрите се посочва началната и крайната дата на водене на съответния регистър, както и наименованието и координатите за връзка на администратора, и когато е приложимо, на съвместните администратори и на длъжностното лице по защитата на данните.
(3) Данните относно водените регистри се съхраняват в писмена форма, включително в електронен формат.

Раздел II.
Законни интереси за обработка на лични данни, преследвани от администратора

Чл.9. (1) Всяко обработване на лични данни по реда на кодекса е в изпълнение на законни интереси на администратора.
(2) При отпадане на законния интерес от обработване на данните, администраторът спира дейностите от деня на отпадане на интереса. Счита се, че интересът е отпаднал в следните случаи:

1. вземане на решение за прекратяване дейността на търговеца, откриване на производство по ликвидация или несъстоятелност – всички регистри;
2. прекратяване на лицензията от БНБ за извършване на дейност като финансова институция.

(3) Администраторът временно преустановява водените регистри при спиране дейността на предприятието или поради неизпълнение на определените в ЗКИ изисквания.
(4) При спиране на обработването, администраторът определя със заповед лица, които отговарят за архивиране и спазване на сроковете за унищожаване на данните.

(5) При временно преустановяване обработването на данни, администраторът взема предвидените организационни и технически мерки за архивиране и съхранение на данните.

Чл.10. (1) Законните интереси и целите за обработване на данните са:

1. Регистър на персонала относно данни на субектите по граждански и трудови договори - нуждите на сключвани от администратора трудови и граждански договори на основание Кодекс на труда и подзаконовите актове по прилагането му, Закон за здравосвовни и безопасни условия на труд и подзакови актове по прилагането му, Закон за задълженията и договорите, Кодекс за социално осигуряване и подзаконови актове по прилагането му, Закон за данък върху доходите на физическите лица, Закон за корпоративноно подоходно облагане, Данъчно – осигурителен процесуален кодекс;
2. Регистър на контрагентите– нуждите на извършваните граждански и търговски сделки по смисъла на Закон за задълженията и договорите и Търговски закон, както и нуждите за водене на редовна счетоводна отчетност на сделките по Закон за счетоводството, Закон за ДДС, Закон за корпоративноно подоходно облагане, Данъчно – осигурителен процесуален кодекс;
3. Регистър на потребителите по договори за потребителски кредит – извършване на дейност като финансова институция по реда на Закон за кредитните институции и предоставяне по занятие на потребителски кредити на физически лица по Закон за потребителския кредит.

(2) Субектите нямат право спрямо данните от регистрите по чл.4, ал.2, т.1-3 да бъде преустановена обработката им или да бъдат унищожени (субектът да бъде забравен) предвид посочения обществен интерес в определените в посочените в съответните регистри срокове и правно основание преди изтичане на законовите срокове на съхранение на данните.

Чл.11. (1) Всяко предаване на лични данни от администратора на трети лица се основава на законен интерес, описан в настоящия кодекс или в действащото законодателство.
(2) Данните от регистрите по чл.4, ал.2 не се предават на трети държави или на международни организации.

Чл.12. (1) Обработването на данните може да бъде ограничено при оспорване на точността на личните данни от субекта на данните и тяхната точност или неточност не може да бъде проверена, личните данни трябва да бъдат запазени за доказателствени цели или по разпореждане на Комисията.
(2) Администраторът информира субекта на данните преди да премахне ограничаването на обработването, когато то е наложено при оспорване на точността им.
(3) В ползваните от администраторите автоматизирани регистри на личните данни ограничаването на обработването се осигурява чрез техническа забрана за корекции или промяна на въведените данни чрез последващи операции.
(4) Обработване на данните от различните регистри за цели, различни от тези, описани в кодекса, не се допуска, освен за изпълнението на задача от обществен интерес и предвидените в действащото законодателство изключения.

Чл.13. (1) Преди събиране на данните на субектите се предоставя информацията по чл.13 от Регламента.
(2) При дейностите по предоставяне на потребителски кредити на видно място в помещенията на офисите се поставя информация за вида на обработваните данни на законово основание, цели и описание, че данните се предават на трети лица – БНБ и други органи за контрол на финансовите институции.
(3) Потребителите на кредити предоставят изрично съгласие в писмена форма за обработка на данните им.

Раздел III .
Събиране на данните и псевдонимизация

Чл.14. (1) Събирането на данните е първоначално или последващо.
(2) Първоначалното събиране на данни се осъществява при извършване на съответната операция – преди сключване на трудово или гражданско правоотношение със субектите от персонала, преди сключване на търговска сделка с контрагенти, при искане за отпускане на потребителки кредит.
(3) При последващото събиране на данни се извършва обработка на нови видове данни при вече възникнали правоотношения.
(4) Администраторът следва да информира субекта за последващо събиране на данни съобразно изискванията на чл.13 от Регламента.

Чл.15. (1) Данните се събират пряко от субектите чрез предоставените от тях устно или в писмена форма данни.
(2) Информацията относно регистрите по чл.4, ал.2, т.3 се събира от субектите и по електронен път чрез електронна поща. В случай, че информацията се попълва и подава чрез готови бланки чрез интернет страницата на администратора или трето лице, подадените данни се съхраняват по реда на посочените в кодекса мерки на техническа защита.

Чл.16. (1) Данните се събират само от изрично определените от администратора служители и обработващи данни.
(2) Лицата са длъжни да ползват личните данни от регистрите по начин, така че да предотвратяват тяхното разпространение или узнаване от трети лица, които имат право на това.
(3) Лицата ползват само личните данни, до които имат право на законосъобразен достъп и когато са им необходими във връзка с изпълнението на конкретните служебни задължения, като спазват приетите технически и организационни мерки, включително и специално, ако данните се предават по електронен път, за защитата им от случайно или незаконно нарушение, незаконно разкриване или достъп, нерагламентирано изменение или разпространение, както и всички други форми на обработване на личните данни.
(4) Лицата са длъжни да събират, обработват и съхраняват личните данни в регистрите така, че да предотвратяват тяхното разпространение или узнаване от трети лица.
(5) Всички лични данни от регистрите, които стават достъпни на лицата или по повод на изпълнение на техните задължения са служебна тайна. Лицата нямат право да разпространяват под каквато и да е форма и пред когото и да е факти и сведения, които

представляват лични данни и са узнати от него при и по повод изпълнение на служебните задължения.
(6) Лицата нямат право, извън уреденото със законово основание или по изрично нареждане на администратора, да копират, преглеждат, изнасят на материални носители, включително електронни, да изпращат по електронен път или по друг начин лични данни, до които имат достъп при изпълнение на служебните си задължения.
(7) Администраторът предвижда изрична дисциплинарна отговорност за нарушение на трудовата дисциплина в трудовите договори, правилника за вътрешен трудов ред и/или длъжностните характеристики на служителите при нарушение на задълженията им по кодекса и актовете по прилагането му в предприятието на търговеца на дребно на лекарствени продукти.
(8) Личните данни от регистрите по чл.6, ал.2 се обработват само от определените лица, като нямат право да искат от други служители на администратора или сами да осъществяват достъп до регистър, за който не са определени задължения по обработка.

Чл.17. (1) Обработването на лични данни от обработващи се извършва при спазване на изискванията на Регламента и на Закона за защита на личните данни.
(2) Администраторът определя обхвата на данните и задълженията на обработващите в договор или друг акт, в който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора, както и останалата информация по чл.28, §3 от Регламента.
(3) В договора или друг акт изрично се определят данните от кои регистри по смисъла на този кодекс се обработват и се възлага спазването на всички правила на този кодекс, включително технически и организационни мерки при обработването.
(4) Обработващият няма право да изготвя и съхранява копия от носители, съдържащи обработените лични данни, след като оргиналите бъдат предадени на администратора.
(5) Обработващият няма право да дава информация или да предоставя достъп до обработваните данни на други обработващи или на трети лица без получаване на предварителното разрешение от страна на администратора.
(6) Всички лични данни от регистрите, които стават достъпни на обработващия при или по повод изпълнение на неговите задължения са служебна тайна.
(7) Обработващият не може да разпостранява под каквато и да форма и пред когото и да е факти, които представляват лични данни и са узнати от него при или по повод изпълнението на задължението му.
(8) Ако обработващ лични данни определи в нарушение на закона целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.
(9) Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването се изисква от правото на Европейския съюз или законодателството на Република България.

Чл.18. (1) Събирането на лични данни се подчинява на правилата за отчетност, съответно събиране само на данни и по начин, описан в регистрите по кодекса.

(2) Обработването на данни чрез въведените автоматизирани системи се извършва при спазване на изискванията на закона относно наличието на записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване.
(3) Записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно — идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни.
(4) Записите се съхраняват в определените в кодекса срокове.

ГЛАВА ТРЕТА
ИНФОРМАЦИЯ И ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ
Раздел I.
Информиране на обществеността и на субектите на данни

Чл.19. Екземпляр от настоящата политика се съхранява на хартиен носител във всички офиси на администратора.

Чл.20. (1) Администраторът предоставя на субектите за регистрите по чл.4, ал.2, т.1-3 данни относно обработването на лични данни, законовото основание и преследваните цели, вида на обработваните лични данни и правата на субектите в нарочно съобщение за обработване на лични данни, което се поставя на видно място в помещенията на администратора.
(2) Администраторите поставят съобщения в помещенията на офисите относно данните, които идентифицират администратора и координатите за връзка с него; координатите за връзка с длъжностното лице по защита на данните, когато е приложимо; правото да бъде подадена жалба до наблюдаващия орган и до комисията и техните координати за връзка.

Чл.21. При изтриване, коригиране или ограничаване на данните в регистрите субектите се уведомяват.

Раздел II.
Упражняване на правата на субектите на данни

Чл.22. (1) Правата на субектите на данни, определени в Регламента и в закона, са гарантирани от политиката. Администраторът приема мерки за навременно, пълно и ефективно приложение на правата на субектите.
(2) Правата на субектите се упражняват по следните начини :

1. предоставяне на информация по разбираем и навременен начин относно правата на субектите от администратора и определените от него длъжностни лица, натоварени с обработка на данните;
2. приемане на запитвания, заявления, възражения и жалби от администратора;
3. разглеждане на запитванията, заявленията, възраженията и жалбите в определените в закона и в Регламента срокове;
4. регистриране на подадените от субектите искания и други актове;
5. информиране на надзорния орган при необходимост.

(3) Субектите имат следните определени от Регламента права:

1. право на потвърждение и достъп до данните за субекта;
2. право на коригиране на данните;
3. право на изтриване на данните (право „да бъдеш забравен“);
4. право на ограничаване на обработването;
5. право на преносимост на данните;
6. право на възражение, включително относно решения при автоматизирано обработване на данните и профилиране;
7. право на обяснения при нарушения в режима на защита на данните;
8. право на жалба до наблюдаващия и до надзорния орган за нарушения на правилата за обработване на лични данни;
9. право на обезщетение и съдебна защита.

(4) Правата по ал.3, т.1 - 7 се упражняват с писмено заявление по образец (Приложение № 1) от субекта на данните или негов изрично упълномощен представител. Упълномощаването следва да бъде с нотариална заверка на подписите на субекта. При непълнолетни и лица с ограничена дееспособност, правата се упражняват със съдействието или чрез законните представители.

(5) Всяко лице, чийто данни се обработват има право да подава заявление относно данните, които се отнасят за него.

(6) Заявлението трябва да е в писмена форма и съдържа:

1. Име, адрес и други данни, които са необходими за да може администратора да го идентифицира. Информация относно актуален адрес и данни за контакт;
2. Предпочетената форма, в която лицето иска да му се предоставя достъп до личните данни или да му се предостави отговор относно заявеното право;
3. Подпис, дата на подаване на заявлението.

(7) Когато заявлението се подава по електронен път, то следва да бъде изпратено на електронен адрес: valentina_pancheva@abv.bg, който е предназначен за получаване на искания относно упражняването на правата на субектите на данни и относно обработването на лични данни.

(8) Правата не се разглеждат без заявление, попълнено по надлежния начин.

Чл.23. (1) Всяко заявление по чл.22, ал.4 се завежда в регистър, който представлява книга – тетрадка, в която се номерират и заверяват с подпис и печат отделните страници.

(2) В регистър на заявленията се определят:

1. Графа № и дата – заявлението се завежда със съответния номер, в зависимост от поредността на неговото постъпване и датата. Всяка заявление се вписва с входящ номер;
2. Графа „име и подпис на заявителя” – посочва се кое лице подава заявлението;
3. Графа „изпълнение на искането” – посочва се датата на уведомяването и се удостоверява факта на връчване на съответния акт. В графата има две колони в първата се вписва датата, на която лицето лично трябва да получи съответния акт и лицето се подписва. Във втората колона лицето получило вече уведомлението се подписва и се вписва датата.
4. Графа „отказ” – посочва се датата на неговото връчване и се удостоверява факта на самото връчване.

(3) Всяко заявление се подрежда в класьор.

(4) Заявленията се съхраняват една година, след което се унищожават.
(5) Достъп до заявленията имат администратора или определени от него длъжностни лица.
(6) Забранява се достъпа до заявленията от други лица, освен изброените в горната алинея.
(7) След като заявлението бъде разгледано, се уведомява субекта за предприетите действия или на коя дата да се яви, за да получи достъп до данните.
(8) Уведомлението се вписва и извежда в регистъра по описания по-горе начин.

Чл.24. (1) След завеждане на заявлението в регистъра се проверява неговота допустимост и законосъобразност съобразно Регламента и закона.
(2) Администраторът е длъжен да направи следното:

1. Да провери дали подаденото заявление отговаря на формалните законови изисквания.
2. Да провери дали подаденото заявление отговаря на материалните законови изисквания, дали лицето има основание и т.н.

(3) Посочените проверки се извършват в двадесетдневен срок от подаване на заявлението.
(4) Решението на администратора по подаденото заявление се издава в срок до 60 дни от датата на постъпване на заявлението.
(5) Решението се изпраща по посочените от субекта данни за контакт – писмо с обратна разписка, електронен адрес или факс.
(6) Решенията, с които не се удовлетворява искането на субекта, съдържат правни и фактически основания за това.
(7) При заявленията по чл.22, ал.3, т.1-4, субектът на данните може да упражни правата си и чрез комисията (непряко упражняване на права). Администраторът информира субекта на данните за възможността да упражни правата си чрез комисията в решението.

Чл.25. (1) Субектът има право да посочи всяка една от формата на **достъп** до личните данни:

1. Устна справка;
2. Писмена справка;
3. Да прегледа лично документите си;
4. Копие от документите, в които се съдържат лични данни (освен, ако документът не е предоставен от самия субект на администратора);
5. Предаване на електронен път.

(2) Субектът, на който е разрешен достъп до личните му данни, няма свободен достъп до документите. Извлеченията на данните и копията от тях се правят от администратора на лични данни.
(3) Когато е необхфодими изнасяне на документи от помещенията за съхранение това се прави от администратора на лични данни, след вписване в регистъра на датата и причината за това. За длъжностното лице възниква задължението да върне документите след приключване на текущата работа не по- късно от края на работния ден.
(4) Субектът, който иска достъп до чужди лични данни попълва заявление по образец за разрешаване на достъп. В него освен необходимото съдържание задължително се посочва и причината поради, която се иска достъпа до чужди лични данни. Формулировката е свободен текст като се посочва какви права се черпят от този достъп или какви задължения изпълнява.

(3) Субектът, до чиито данни се иска достъп, го разрешава писмено, като разрешението трябва да има следното съдържание: името на субекта, подпис и дата , поставени лично от субекта; лични данни, до които се дава достъп и имената на лицето, на което се дава достъп.
(4) Администраторът е длъжен да предостави достъп без съгласие на субекта в следните случаи:

1. личните данни са необходими за да бъде защитен живота и здравето на титуляра;
2. нужни са за целите на научни изследвания и статистически цели и се предоставят анонимно;
3. състоянието на титуляра не позволява той да даде писмено съгласие.

(5) Лицето, което иска достъп, доказва наличието на основанието като прилага към заявлението и болничен лист, смъртен акт, удостоверение за наследници и други доказателства.

Чл.26. (1) Достъпът до лични данни става след разрешение на законния представител на администратора или друго определено от него лице, съответно длъжностното лице по защита на данните.
(2) Оправомощеното лице преценява законосъобразността на поискания достъп и го разрешава и забранява.
(3) Документите съдържащи лични данни се предоставят лично или се изпращат в запечатан плик или папка по начин, който гарантира защитатат на личните данни в тях.

Чл.27. (1) Достъп до личните данни от регистрите имат всички държавни или обществени органи, които по силата на специален нормативен акт имат право на такъв достъп.
(2) Адмнитраторът е длъжен да осигури поискания от държавните органи достъп да лични данни в регистъра без писмено или устно разрешение от страна на техния титуляр.
(3) В случаите, когато по дела, водени от или срещу администратора, има назначена съдебна експертиза, достъп на съответното вещо лице се допуска само при представяне на изрично съдебно удостоверение, в което се посочва видът и естеството на личните данни, видът и естеството на документите, които съдържат.
(4) Администраторът предоставя пълен или ограничен достъп до личните данни, като в случай на ограничаване на достъпа се посочват правните или фактически основания по закон за това.
(5) В случай, че администраторът установи, че няма право да предостави поисканата информация, се съставя решение за отказ, което съдържа правни и фактически основания : кои данни; поради каква причина и на какво основание се отказват за предоставяне; органът и срока, в който трябва да се обжалва частта на отказа - жалба до наблюдаващия орган, до комисията или търсене на защита по съдебен ред.

Чл.28. (1) Правото на **коригиране** на данните се основава на представени от субекта доказателства за неточностите – декларации, удостоверения.
(2) В случаите, когато поправката се установява от публични регистри или се дължи на грешка в обработването от страна на администратора, не се изискват доказателства от субекта.
(3) Администраторът може да откаже коригиране на данните в регистрите по чл.4, ал.2, т.3 – 5, когато за това е необходимо съдействие на публичен орган, на когато данните са

предадени и това не е възможно или е необходимо специално административно или съдебно производство, което не е от компетентността на администратора.

Чл.29. (1) Субектът има право да иска **изтриване** на данните относно него на предвидените в Регламента и закона основания.
(2) Данните в регистрите не се изтриват, когато са обработени законосъобразно и е налице законово изискване за съхранението им до посочения срок на съхранение в закона или за нуждите на извършвани проверки от публични органи.
(3) В случаите по ал.2 субектът се уведомява, че данните му ще бъдат изтрити след изтичане на сроковете за съхранение на данни в съответния регистър, определени в политиката.
(4) Данните се изтриват по предвидения в политиката ред за унищожаване на носители на лични данни, като администраторът прави разумна проверка за всички материални и електронни носители на данни – досиета и папки, електронни записи, включително в автоматизирани системи за обработка на данни, електронна поща и други.

Чл.30. (1) Субектът има право на **ограничаване** на обработването на данните с изключение на данните, предоставени от субектите, относно изискванията на трудовото, данъчното и осигурителното законодателство.
(2) Преди отмяна на ограничението администраторът уведомява субекта по предвидения в кодекса начин за уведомяване на решения по заявления.
(3) В случай, че субектът желае запазване на личните му данни след изтичане на определените в регистрите срокове за съхранение трябва да посочи и представи доказателства за причината за това – съдебни или административни производства и други. Администраторът определя разумен срок за ограничение на обработването предвид посочените от субекта причини.

Чл.31. Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия – при предадени с електронни средства данни в ЦКР на БНБ, които не позволяват корекцията им. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Чл.32. (1) Относно регистрите по чл.4, ал.2, т.1 – 3 субектите имат право на **преносимост** на данните, ако те се обработват по автоматизиран начин и са структурирани във вид, който е широко ползван и пригоден за машинно четене.
(2) Преносимостта се извършва при ясно определяне в заявлението от страна на субекта кои данни ще бъдат обект на преносимост, точно идентифициране на получателя на данните и начина на предаване на данните, който да бъде съответен на организационните и технически мерки за защита на данните.
(3) Преносимостта се извършва, когато данните се обработнат по начин, позволяващ обособяване на данните на субекта от други данни, които не могат да бъдат пренесени.

Чл.33. (1) Субектите имат право на **възражения** при обработване на данните им в регистъра по чл.4, ал.2, т.1 -3 , когато данните се отнасят до извършване на директен маркетинг на субектите.
(2) Данните от регистрите по този кодекс не се ползват за профилиране на субектите.

Чл.34. (1) В случаите на нарушение на сигурността на данните, за които субектът не е уведомен от администратора на основание чл.34, §3 от Регламента, субектът има право на обяснение от администратора.
(2) В предоставеното обяснение администраторът посочва вида на нарушението на данните, обхвата на данните, наличните технически и организационна мерки на защита, взетите мерки за ограничение на последиците от нарушението и препоръки към субекта.

Чл.35. (1) Субектите имат право на жалба надзорния орган.
(2) Жалбата се подава в писмена форма и отговаря на изискванията за подаване на жалби по закон.
(3) В жалбата се описват обстоятелствата относно нарушението на регламента или закона и се прилагат доказателства за това.
(4) Жалбата до наблюдаващия орган не ограничава правото на съдебна защита на правата на субектите.
(5) Администраторът и препраща в срок от 14 дни получени жалби на комисията, когато са получени от него и са с адресат комисията. Администраторът има право да приложи становище по жалбата.
(6) Субектите имат право на обезщетения за нанесени вреди от нарушения при обработване на лични данни пред съда, компететен по смисъла на чл.79, §2 от Регламента. Приложимото право за определяне на обезщетение за нанесени вреди се определя от Регламент 864/2007 относно приложимото право към извъндоговорните задължения.

Раздел III.
Информирането и закрилата на децата и начина за получаване на съгласие от носещите родителска отговорност за детето

Чл.36. (1) Обработването на лични данни на деца се извършва при получаване на изрично съгласие на законните им представители според приложимото към личния статут материално право. За български граждани законните представители се определят от Закона за лицата и семейството и Семеен кодекс – родители, настойници или попечители.
(2) Съгласието за обработване на лични данни на деца на данни от регистрите по чл.4, ал.2, т.1-3 се предоставя изрично и предварително.
(3) Администраторът не обработва лични данни на деца за нуждите на маркетинговите дейности и не извършва профилиране на лични данни на деца.
(4) В случай, че се налага обработване на лични данни на деца, информацията се предоставя на прост и разбираем език, като при възможност и според етапа на развитие на детето се предоставя в писмена форма.
(5) При обработване на лични данни на деца се обръща специално внимание на идентиикацията на субектите. Ако лицата нямат издаден документ за самоличност, изисква се потвърждение от законен представител на детето.

ГЛАВА ЧЕТВЪРТА
МЕРКИ И ПРОЦЕДУРИ ЗА СИГУРНОСТ И ОТЧЕТНОСТ НА ДАННИТЕ.
Раздел I.
Технически и организационни мерки за защита на данните

Чл.37. (1) Администраторът определя технически и организационни мерки в съответствие с предварително извършена оценка на риска и резултатите от нея.
(2) Оценката на риска и мерките са в следните области:
1. физическа защита;
2. персонална защита;
3. защита на автоматизирани системи и електронни носители и обмен на данни.
(3) Оценката на риска се извършва преди започване обработването на данни. Резултатите от оценката на риска се степенуват като нисък, среден и висок риск за съхранението на данните.
(4) При съответната оценка на риска, администраторът приема една или повече от изброените минимални мерки на защита в политиката, след прилагането на които се извършва нова оценка на риска.
(5) Ако въпреки предприетите мерки, оценката на риска е висок риск за съхранението на данните, администраторът уведомява длъжностното лице по защита на данните, ако има назначено такова, което дава задължителни предписания и срок за изпълнението на мерките.
(6) Оценка на риска се извършва най – малко в срок до 12 месеца след всяка предходна оценка.
(7) Администраторът поддържа запис на хартиен или електронен носител на направените в хронологичен ред оценки на риска, които да бъдат представени при поискване на наблюдаващия и на надзорния орган.

Чл.38. (1) Администраторът приема в комбинация някои или всички от следните мерки за **физическа защита:**
1. Определяне на зони за контролиран достъп за обработка и съхранение на данни – помещенията на офисите или на други помещения;
2. Наличие на входна врата на аптеката и на вътрешни помещения, в които се съхраняват лични данни, със секретно заключване;
3. Предпазни решетки или ролетни щори на врати и прозорци;
4. В приемното помещение на офисите достъпът през работното време се контролира от мениджъри,консултанти или охранители;
5. В извънработното време достъпът в аптеката се контролира чрез сигнално охранителна система и сключен договор за охрана с лицензиран по закон изпълнител;
6. В помещенията на администратора личните данни се обработват само от определените лица от персонала;
7. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в помещения с ограничен достъп само за упълномощени лица, съответно в затворени шкафове в зоните на офисите, в които външни лица нямат

достъп (зад оформени витрини, паравани, прегради, врати и вътрешни преградни стени и други);

8. Помещенията, в които се обработват лични данни са оборудвани с заключващи се врати, затворени или заключващи се шкафове и/или каси, пожарогасителни средства.

9. Всички изисквания на противопожарната и аварийна безопасност съгласно действащото законодателство се спазват, като в помещенията се поддържат изправни пожарогасители и други противопожарни системи.

10. Въвежда се самостоятелен код на сигнално – охранителните системи за достъп до помещенията на отделните служители.

11. Лица, извън персонала на аптеката, нямат достъп до ключовете за помещенията и шкафовете или други защитени пространства.

(2) Мерките на допълнителна физическа защите се описват в Процедури за обработка на данните, които се одобряват от наблюдаващия орган и съдържат правила за визуален достъп до документи, съдържащи лични данни; място и време на обработката; правила за изпращане на данни по отдалечен път и т.н.

Чл.39. (1) Администраторът приема в комбинация някои или всички от следните мерки за **персонална защита:**

1. достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“;
2. всички служители са длъжни да спазват ограниченията за достъп до личните данни, и са персонално отговорни пред законния представител на администратора за нарушаването на принципите за обработка на личните данни.
3. лицата, обработващи лични данни при постъпване на работа се запознават с:

- нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане, а именно: Регламента, Закон за защита на личните данни и подзаконови актове по прилагането му, кодекса и указания на Комисията;

- рисковете за личните данни, обработвани от администратора;

- одобрените от наблюдаващия орган образци на документи по реда на кодекса.

4. най-малко веднъж годишно се провежда обучение, в която програма е включено запознаване с кодекса, както и с актовете по т.3.
5. най-малко веднъж годишно се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.
6. лицата, обработващи лични данни, задължително подписват допълнително споразумение, неразделна част от съдържанието на трудовото или гражданско правоотношение, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по реме на изпълнение на служебните им задължения. Споразумението се съхранява в кадровото досие на всеки служител.
7. споделяне на лични данни между служителите (като идентификатори, пароли за достъп и т.н.) е забранено, освен с оглед обективното разпределение на трудовите функции.

8. обработване на лични данни се извършва само в работно време в помещенията на администратора и/или в офиса на администратора на лични данни.

9. личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от оправомощени лица.

10. забранено е изнасяне от помещенията на администратора на носители на данни, изпращането им по електронен път или копиране на електронни носители извън непосредственото изпълнение на законовите изисквания за предаване на данни.

11. забранен е предоставяне на достъп до данни на трети лица, както и унищожаването на данни, за които срокът на съхранение не е изтекъл или няма законосъобразно нареждане от адмистратора или от субекта на данните.

(2) Периодичните обучения и тренировки по т.4 и т.5, както и споразумението по т.6, се документират чрез образци, утвърдени от наблюдаващия орган.

(3) Администраторът приема по образец правила за поведение на персонала относно съхранение на данните.

Чл.40. (1) Администраторът приема в комбинация някои или всички от следните мерки за **защита на автоматизирани системи и електронни носители и обмен на данни:**

1. автоматизирана обработка на данни се извършва с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др. (офис-пакети).
2. при електронната обработка се използват само лицензирани системни и приложни софтуерни продукти.
3. упълномощените служители за работа с данните задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти.
4. всеки упълномощен потребител на автоматизирани системи и машини има личен профил с определени нива на достъп, съобразни със неговите задължения и принципа „Необходимост да знае“.
5. идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола.
6. заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти.
7. в помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.
8. работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

9. забранено е използването на преносими носители на данни за лични нужди.

10. не се разрешава осъществяването на отдалечен достъп до данни от регистрите, освен при съхранение на данни на облачни сървъри, които прилагат ISO 27000 : 2017 и се намират на територията на ЕС .

11. за защита на данните е инсталирана антивирусна програма и се извършва седмична профилактика на софтуера и системните файлове.
12. администраторът на автоматизираните системи създава и поддържа базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. Същият следи за своевременно обновяване (update) на системния, технологичния (офис-пакети и др.), приложния и антивирусния софтуер.
13. за криптографска защита се използват стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП).

(2) В системите за автоматизирано обработване се водят записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване.
(3) Записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно — идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни.
(4) Предаването на данни по отдалечен електронен път се извършва само в криптирана връзка.
(5) Администраторът документира мерките за защита на автоматизирани системи и електронни носители и обмен на данни със следните документи по образец :
1. Опис на техническите средства – компютърни конфигурации и други устройства за приложение на автоматизираните системи;
2. Одитен лист за проверка на спазването на изискванията от персонала;
3. Процедури за достъп, контрол и смяна на пароли за достъп до автоматизирани системи и електронни носители на данни.

Чл.41. (1) При възникване и установяване на инцидент (природни бедствия, престъпни посегателства от трети лица) веднага се докладва на законния представител на администратора и в зависимост от обстоятелства, се уведомяват съответните институции. От компетентните органи се изисква включване в съответните протоколи и актове на бележка относно загуба или повреждане на носители на лични данни.
(2) С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно. Всички мерки за ограничаване на последствията от инцидента (възстановяване на документи и други) не трябва да водят до допълнителни рискове за обработката на данните и се съгласуват с длъжносното лице по защита на данните, ако е назначено такова.

(3) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, в дневника се описват последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на законния представител на администратора, като това се отразява в дневника по архивиране и възстановяване на данни.

(5) За инцидентите се уведомява наблюдаващия орган и длъжностното лице по защита на данните, ако има назначено такова. В случаи на нарушения на сигурността на личните данни се прилагат правилата на кодекса за уведомление на надзорния орган.
(6) Администраторът изпълнява предписанията на наблюдаващия орган, които са задължителни.
(7) Адмистраторът взема предварителни мерки за възстановяване на данните чрез :

1. съхранение на преписи от документи в електронен вид, когато е възможно;
2. въвеждане на настройки за периодично архивиране (бек ъп) на данните в автоматизирани системи за обработка;
3. регулярно архивиране на данни, които не се пряко необходими за изпълнение на дейността на администратора в нарочни помещения, които отговарят на изискванията за физическа защита по този кодекс.

Чл.42. (1) Всяко унищожаване на данни е контролирано и се извършва след изтичане на определените срокове за съхранение в съответвните регистри и при спазване на изискванията за предаване на данни на Национален архивен фонд или на други публични органи.
(2) За унищожаване на лични данни администраторът назначава комисия.
(3) Документите, съдържащи лични данни, се унищожават по начин, непозволяващ тяхното възстановяване, например чрез нарязване на специално устройство (шредер) или изгаряне.
(4) След унищожаването на документите комисията съставя протокол и го представя на администратора и на длъжностното лице по защита на данните.
(5) Предаването на трети лица на носители за унищожаване на документи или други носители на данни се извършва след поемане на задължения за спазване на изискванията на кодекса от третото лице.
(6) Данните на електронен носител се унищожават чрез съответните команди и проверка за наличие на временни или други копия в операционната система, както и на копия на външни носители – външни дискове, дискове, флаш памет и т.н.
(7) При унищожаване на данните се прави проверка в служебната електронна поща за изпратени по електронен път преписи и съобщенията се изтриват, като се изпраща съобщение до получателя да извърши същата операция.

Чл.43. (1) При изпълнение на изискванията на Регламента и на закона, администраторът определя длъжностно лице по защита на данните.
(2) Администраторът обявява на видно място в помещенията на офисите данните за контакт с длъжностното лице по защита на данните и на интернет страницата си, ако поддържа такава.
(3) Администраторът уведомява наблюдаващия орган за координатите на длъжностното лице по защита на данните.
(4) В допълнение на определените в Регламента и в закона задължения, длъжностното лице по защита на данните:

1. обучава персонала на администратора и проверява спазването на изискванията на политиката;
2. осъществява контакти с надзорния орган и спазва неговите предписания относно приложението на регламента;
3. съобщава на администратора за пропуски в режима на защита на личните данни;
4. съдейства на администратора за прилагане на политиката и на образците на документи.

Чл.44. (1) Администраторът възлага на всички обработващи данни задължения относно спазването на настоящия кодекс чрез нарочни договори. В договорите се уреждат още предмета и срока на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, задълженията и правата на администратора.
(2) При съгласие от администратора обработващия данни да прибави друг обработващ, този друг обработващ приема задължения за спазване на изискванията на кодекса.
(3) Обработващият данни приема с договора да спазва предписанията на наблюдаващия орган и да му предоставя необходимото съдействие за контрол относно спазването на кодекса.

Раздел II.
Уведомяването на надзорните органи за нарушения на сигурността на личните данни и съобщаването за такива нарушения на сигурността на личните данни на субектите на данни

Чл.45. (1) Всички лица от персонала на администратора, длъжностните лица по защита на данните и обработващите данни докладват всяко съмнително събитие или инцидент на законния представител на администратора.
(2) Администраторът разследва възможно най-бързо и в срок не по-дълъг от два работни дни всеки доклад за инцидент. При разследването се включват длъжностното лице по защита на данните и ръководителя на съответния офис.

Чл.46. Следните мерки и действия се вземат при инциденти:
1. При кражба на носители на лични данни или достъп на неоправомощени лица до зона с достъп до лични данни:
- Проверка на Опис на техническите средства за обработка на данните, за да се установи кое средство липсва;
- Проверка на основанието за липса на носител на информация – преместване в друго помещение, поправка и др.
- При неправомерно отнемане на носителя, уведомяване на органите на МВР в рамките на същия ден с изрично указване на вида и обхвата на личните данни, които се съдържат на носителя;
- Оценка на необходимостта от допълнителни мерки на защита – промяна на пароли за достъп, смяна на ключалки на помещения и шкафове и др.

2. При осъществен достъп извън персонала до договори за потребителски кредит, както и до регистри по чл.4, ал.2, т.1-2:
- Събиране на данни от персонала на офиса в рамките на същия ден;

- Проверка от доставчици на интернет и поддръжка на автоманични средства за обработка на данните, включително одит на системата;
- Обяснения от субектите на данни;
- Оценка на необходимостта от допълнителни мерки на защита – промяна на пароли за достъп, смяна на ключалки на помещения и шкафове и др.

3. При неправилно унищожаване и изхвърляне на публични места на носители на данни:

- Проверка как носителите са попаднали на публични места;
- Предприемане на мерки за предотвратяване на нови инциденти – дисциплинарни наказания, обучения и консултации на персонала.

4. При жалби от потребители, членове на персонала, контрагенти или други субекти на данни за нарушения на изискванията за защита на данните :

- Снемане на обяснения и информация от жалбоподателя;
- Разследване на обстоятелствата по подходящ начин и предприемане на пропорционални допълнителни мерки за възстановяване на данните и защитата им;
- Оценяване на нарушението според критериите за регистриране и уведомяване на надзорните органи.

5. Загуба на данни при изпращане на трети лица (БНБ и др.):

- Проверка на начина на изпращане на данните – електронно криптирано чрез подпис с КЕП; в затворен плик и т.н.;
- Анализ на възможните пропуски – предаване на КЕП на неоправомощетно лице, незапечатване на пощенски плик, ползване на прозрачен плик и т.н.;
- Уведомяване на получателя на данните (БНБ и др.) за възможни пробиви в сигурността на системата му за обработка на данни

Чл.47. (1) Всяко събитие, съдържащо опасност или нарушение на сигурността на данните се вписва в нарочен регистър на инциденти. В регистъра се описват фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него според одобрен от наблюдаващия орган образец на доклад за нарушение.

(2) Събитията се квалифицират в пет категории според обхвата им – незначителен риск (няма данни за достъп на трети лица до данните; данните не са напускали контролирана среда и не са предавани отдалечено; засегнати са по – малко от три лица), малък риск (данните са изгубени или има достъп на трети лица, но са защитени надлежно с криптиране и по друг начин, непозволяващ четенето им от третите лица; засегнати са до пет лица), среден риск (данните не са защитени с криптиране и са в отворен формат; засегнати до 20 лица; данните са относно здравословно състояние), висок (данните не са защитени за четене и възпроизвеждане; данните се отнасят до 1000 субекта; данните са относно здравословно състояние) и критичен риск (цялостен достъп до данните от даден регистър; засегнати над 1000 пациенти). При преценката на риска се взема предвид – дали данните са загубени или унищожени в контролирана среда (помещенията на офисите); загуба на договори на публично място; достъп на неоправомощено лице до данни относно кредитно досие на потребителите. При категориите среден, висок и критичен риск е необходимо да бъде изпратено уведомление до Комисията, както и да се уведомят субектите на данни.

(3) Длъжностното лице по защита на данните или администраторът оценяват вида на риска и последващите изисквания за уведомяване на Комисията, засегнатите субекти, органите на МВР, БНБ и застрахователни дружества.

Чл.48. (1) В случай на нарушение на сигурността на личните данни администраторът, без излишно забавяне, но не по-късно от 72 часа след като е разбрал за него, уведомява Комисията за нарушението на сигурността на личните данни, освен ако няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица (незначителен или малък риск). Когато уведомлението до комисията не е подадено в срок от 72 часа, то се придружава от причините за забавянето.
(2) Обработващият лични данни уведомява администратора без излишно забавяне, след като е установил нарушение на сигурността на лични данни.
(3) В уведомлението до Комисията се съдържа следното:

1. описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;
2. посочване на името и координатите за връзка на длъжностното лице по защита на данните, ако е назначено такова или на друга точка за контакт, от която може да се получи повече информация;
3. описание на евентуалните последици от нарушението на сигурността на личните данни;
4. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.
(5) Препис от уведомлението се изпраща и на наблюдаващия орган.

Чл.49. (1) Когато има вероятност нарушението на сигурността на личните данни да доведе до среден, висок или критичен риск за правата и свободите на физическите лица, администраторът без излишно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.
(2) В съобщението до субекта на данните, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и мерките, посочени в закона.
(3) Посоченото в ал. 1 съобщение до субекта на данните не се изисква, ако е изпълнено някое от следните условия:

1. администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;
2. администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани. Публичното съобщение се изпраща и до наблюдаващия орган за публикуване на специално създадена информационна интернет.

(5) Съобщението до субекта на данните може да бъде забавено, ограничено или пропуснато, при условията и на основанията, предвидени в закона.

Раздел III.
Отчетност на данните.

Чл.50. (1) Администраторът е длъжен да може да докаже спазването на определените в Регламента, закона и политиката принципи на обработване на данните.

(2) Принципът на отчетност се осигурява чрез документиране на всички основни обстоятелства относно обработването на данните съгласно Регламента.

(3) Наблюдаващият орган подпомага документирането на процеси и обстоятелства чрез одобряване на образци на документи (система).

(4) Администраторът поддържа и при поискване трябва да може да докаже и представи на Комисията и на наблюдаващия орган следните документи:

1. Списък с регистрите по чл.4, ал.2;
2. Оценка на риска за обработване на данните;
3. Договори с обработващи данни относно поемане на задълженията съобразно Регламента и закона;
4. Информация за субектите на данни;
5. Образци на заявления за упражняване на правата на субектите;
6. Процедури за обработка на данните;
7. Правила за поведение на персонала относно съхранение на данните;
8. Опис на техническите средства – компютърни конфигурации и други устройства за приложение на автоматизираните системи;
9. Одитен лист за проверка на спазването на изискванията от персонала;
10. Процедури за достъп, контрол и смяна на пароли за достъп до автоматизирани системи и електронни носители на данни
11. Регистър на нарушенията на сигурността на данните;
12. Договор за възлагане на функции на длъжностно лице по защита на данните;
13. Списъци с инструктаж на персонала и периодично обучение за обработка на лични данни;
14. Допълнителни споразумения към трудови и граждански договори на персонала с възложена дисциплинарна отговорност за неспазването им.

(5) Администраторът следва да съхранява посочената документация по начин, който позволява по всяко време проверка на отчетността, без да се нарушава непропорционално нормалната работа на аптеката и отпускането на лекарствени продукти на пациентите.

(6) При съответни мотиви за това, администраторът може да поиска да представи документацията в определен разумен срок, но не повече от три работни дни.

(7) Във всички случаи в помещенията на офисите се съхранява постоянно документация по ал.1, точки 1, 2, 4, 5, 6, 7, 10, 11 и 15.

ГЛАВА ПЕТА
ПРЕДАВАНЕ НА ДАННИ И ИЗВЪНСЪДЕБНО УРЕЖДАНЕ НА СПОРОВЕ.
Раздел I .
Предаването на лични данни на трети държави или международни организации

Чл.51. (1) Лични данни от регистрите по чл.4, ал.2, т.1 - 3, не се предават на трети държави или международни организации, освен при наличие на законово основание за това и задължително разпореждане на компетентен орган.
(2) Предаването на данните се извършва при спазване на изискванията на Регламента и на закона.
(3) Администраторът предава данни при цесия на вземания по договорите за кредит при изрично уведомяване на субектите и сключване на договори с цесионерите за гарантиране изпълнението на изикванията на защитата на лични данни.

Чл.52. (1) Лични данни от регистъра по чл.4, ал.2, т.3 могат да се предават на трети държави при спазване на изискванията на Регламента и на закона.
(2) Предаването на данни на трети лица от трети държави се извършва след информиране на субектите на данните за намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.
(3) В случай на липса на решение на Комисията по чл.45, §3 от Регламента, предаването на данните се извършва въз основа на договор за предаване на данни между администратора и третото лице, в който се съдържат стандантни клаузи за защита на данните, одобрени от Европейската комисия или Комисията, както и посочване на:

1. Целите на предаване на данните;
2. Категориите субекти на данните;
3. Сроковете за предаване и обработка на данните;
4. Приложими изисквания към получателя според неговата национална уредба;
5. Специални категории данни;
6. Данни за контакт на страните.

(4) Администраторът документира предаванията на основание на ал.3, включително датата и момента на предаване, информацията относно получаващия компетентен орган, обосновка на предаването и предадените лични данни.
(5) Администраторът информира Комисията за категориите предавания по ал. 3 и при поискване й предоставя достъп до документацията.

Раздел II.
Извънсъдебни производства и процедури за разрешаване на спорове между администраторите и субектите на данни по отношение на обработването

Чл.53. (1) Без да се засягат правата на субектите на данни по Регламента и закона за подаване на жалби и съдебна защита, споровете между субекти на данните и администраторите се уреждат на доброволна основа чрез преговори.

(2) Субектите на данни могат да отправят жалба относно засягане на правата им по Регламента, закона или кодекса, както и относно искане за обезщетение, до администратора.
(3) Жалбата е в писмен вид и трябва да съдържа:

1. трети имена на жалбоподателя и номер на документ за самоличност;
2. адрес за кореспонденция и електронен адрес;
3. име на представител;
4. изложение на обстоятелствата;
5. конкретно формулирано искане;
6. подпис.

(4) Жалбите се подават по поща с писмо с обратна разписка или куриер, по електронен път или факс.
(5) Към жалбата се прилагат доказателства, каквито субектът разполага, за доказване на твърденията му.
(6) За разглеждане на жалбата не се изисква такса или възнаграждение за наблюдаващия орган.
(7) Субектите на данни може да се представляват от нарочно упълномощено лице с изрично писмено пълномощно.

Чл.54. (1) В едноседмичен срок от получаване на жалбата администраторът изготвя становище по случая, като може да предложи на субектите извънсъдебно споразумение или да се обърнат към медиация.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящата политика е изработена и приета от „Айзаем.БГ“ ООД.
§2. Политиката влиза в сила и се прилага от 25.05.2018г.