ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ДРУЖЕСТВОТО

ОПРЕДЕЛЕНИЯ

В настоящата Политика се използват следните определения:

1. „Приложимо право" означава приложимото законодателство на Европейския съюз и Република България по отношение на защитата на личните данни;

2. „ОРЗД" означава Регламент (ЕС) № 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни и относно свободното движение на такива данни, и за отмяна на Директива 95/46/ЕО („Общ регламент за защита на данните");

3. „Лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;

4. „Обработване" е всяка операция или съвкупност от операции, извършвани с лични данни чрез автоматични или други средства, като събиране, записване, организиране, структуриране, съхранение, промяна, употреба, разкриване чрез предаване, разпространение или друг начин, чрез който данните стават достъпни;

5. „Профилиране" е 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;

6. „Регистър с лични данни" означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии;

7. „Администратор" означава физическо или юридическо лице, публичен орган или друга структура, която сама или съвместно с други определя целите и средствата за обработването на личните данни;

8. „Обработващ лични данни" означава физическо или юридическо лице, публичен орган или друга структура, която обработва лични данни от името на администратора;

9. „Съгласие на субекта на данни" означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

10. „Разкриващ лични данни" означава страната по този Договор, която предава лични данни на Получателя на лични данни;

11. „Получател на лични данни" означава страната, която получава личните данни от Разкриващия личните данни;

12. Термините „Субект на лични данни", „Нарушение на сигурността на личните данни", „Обработване", „Специални категории лични данни" и „Надзорен орган" имат същото значение като в ОРЗД и приложимото национално законодателство;

13. „Дружеството" означава ЗАД „Армеец" АД.

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата Политика за защита на личните данни определя правилата по отношение защита на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни, съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент.

Чл. 2. Настоящата Политика определя целите и средствата за защита на личните данни. Целта на Политиката по защита на физическите лица във връзка с обработване на личните им данни се осъществява чрез:

1. Установяване на ясни правила и координираност в дейността на служителите на Дружеството при събиране, записване, организиране, структуриране, съхраняване, промяна, употреба, разкриване чрез предаване, разгласяване на лични данни, ограничаване и изтриване на данни от водените в Дружеството регистри, за да се гарантира неприкосновеността на правата на субектите на данни при обработване на свързаните с тях лични данни;

2. Установяване на ясни правила при упражняване правата на субекта на данни по отношение на неговите данни;

3. Определяне на Длъжностното лице по защита на данните и регламентиране на неговите задължения;

4. Регламентиране достъпа на служителите до данните в съответния Регистър на дейностите по обработване;

5. Определяне Регистри на дейностите по обработване;

6. Регламентиране на принципи, които трябва да се спазват при управление на данните;

7. Определяне на необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни);

8. Определяне нивата на въздействие върху обработваните лични данни и съответното ниво на защита.

Чл. 3. Настоящите правила регламентират:

1. Принципите на дейността на Дружеството, в качеството му на администратор на лични данни, в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент, на Закона за защита на личните данни и на Наредба № 1 от 30.01.2013 г. за

минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни;

2. Механизмите, регламентиращи въвеждането и спазването на горните принципи;

3. Правата на субектите на данни. Процедури при осъществяване правата на субектите на лични данни;

4. Функциите на Дружеството в качеството му на администратор;

5. Отношенията на Дружеството с дружества, които по силата на договор се явяват също администратори или обработващи лични данни;

6. Процедурата по оценка на въздействието върху обработваните лични данни и определяне нивата на въздействие и защита на обработваните лични данни.

РАЗДЕЛ II
ПРИНЦИПИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Чл. 4. (1) Основните принципи на дейността по обработване на лични данни в Дружеството са:

1. Законосъобразно, добросъвестно и по прозрачен начин обработване на личните данни. За да бъде обработването законосъобразно и добросъвестно, личните данни следва да бъдат обработвани на конкретни законови основания, съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент или на правен акт на Република България, уреждащ материята, както следва:

а) на основание легитимен интерес на Дружеството;

б) на основание спазването на законово задължение, наложено на Дружеството, в качеството му на администратор на данни;

в) на основание изпълнение на договор, по който субектът на данни е страна или с оглед предприемане на стъпки по искане от субекта на данни преди встъпване в договорни отношения;

г) на основание изрично съгласие на субекта на данни.

Изпълнението на принципа прозрачност изисква всяка информация и комуникация във връзка с обработването на личните данни да бъде лесно достъпна и разбираема, и да се използват ясни и недвусмислени формулировки.

2. Ограничение на целите. Личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

3. Свеждане на данните до минимум. Събираните лични данни са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват.

4. Точност. Събраните и обработвани от Дружеството лични данни следва да са точни и при необходимост да бъдат поддържани в актуален вид, като за целта Дружеството предприема съответните мерки, за да се гарантира своевременното изтриване и коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

5. Ограничение на съхранението. Личните данни се съхраняват за период не по-дълъг от необходимото за целите, за които те се обработват. Данните могат да се съхраняват за дълги срокове единствено за статистически цели на Дружеството, при условие, че бъдат приложени съответните технически и организационни мерки, с цел да са гарантирани правата и свободите на субектите на данни.

6. Цялостност и поверителност. Личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни. За целта се прилагат подходящи технически и организационни мерки в Дружеството.

(2) Дружеството събира, обработва и съхранява личните данни на субектите на данни при:

1. гарантираност на неприкосновеността на личността и личния живот на субекта на данни при обработване на свързаните с тях лични данни;

2. законосъобразно и добросъвестно обработване на данните;

3. обработване на данни само от лица, чиито служебни задължения изискват обработване на конкретните данни на принципа „необходимост да се знае";

Мерките за защита на данните са функция от вида регистър, на който се поддържат и нивото им на чувствителност.

(3) С цел гарантиране ограничението на съхранение на данните, в Дружеството се създават и прилагат Вътрешен правилник за архивираната дейност.

Чл. 5. (1) Дружеството не обработва лични данни, които:

1. разкриват расов или етнически произход;

2. разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;

3. се отнасят до генетични и биометрични данни, които се обработват за целите единствено на идентифицирането на физическо лице;

4. се отнасят до сексуалния живот или сексуалната ориентация на физическото лице или до човешкия геном.

(2) Посочените в предходната алинея лични данни, Дружеството може да обработва само на законово уредените основания.

Чл. 6. Лични данни, отнасящи се до здравословното състояние, се обработват само по отношение на служителите, с оглед изпълнения на задълженията на Дружеството в областта на трудово-осигурителното законодателство, както и за клиенти, които ползват застрахователни продукти, изискващи предоставянето на подобна информация, при спазване изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и/или на правен акт на Република България, уреждащ материята.

Чл. 7. (1) Дружеството може да обработва лични данни самостоятелно или чрез трети лица, в качеството им на обработващи лични данни и съвместни администратори, на основание на сключен с тях договор. Съответните договори трябва много ясно и точно да определят какви лични данни ще се обработват, как, в какъв срок, с каква цел. При обработване на съвместни администратори трябва ясно да се определят съответните права и задължения на двете страни, както и техните отговорности.

(2) Обработването на личните данни на субектите на данни се осъществява при прилагане на професионална конфиденциалност. Това изискване е задължително във взаимоотношенията между служителите, между служители и клиенти, както и спрямо третите

лица, обработващи лични данни и съвместни администратори. В същата степен се изисква конфиденциалност и по отношение финансовото състояние на субектите на лични данни, както и извършваните от тях сделки.

(3) Независимо дали Дружеството обработва личните данни самостоятелно или чрез трети лица, в качеството им на обработващи лични данни и съвместни администратори, при обработването им винаги се прилагат принципите съгласно чл. 4 от настоящата Политика.

РАЗДЕЛ III
ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 8. (1) Правата на субектите на данни засягат всички лични данни на физическото лице, обработвани от Дружеството, както и всички субекти на данни, чиито данни се обработват от Дружеството.

(2) Основните права на субекта на данни по отношение на неговите данни, които правната рамка постановява и Дружеството спазва, са както следва:

1. Право на достъп;
2. Право на коригиране;
3. Право на изтриване (право „да бъдеш забравен");
4. Право на ограничаване на обработването;
5. Право на възражение;
6. Право да не бъдеш субект на автоматизирано вземане на решение;
7. Право на пренос на данни.

Чл. 9. (1) Правото на достъп на субекта на данни представлява правото да получи от Дружеството, в качеството му на администратор, потвърждение дали се обработват лични данни, свързани с него и ако това е така да получи достъп до личните си данни и следната информация:

а) цели на обработването;
б) съответните категории лични данни;
в) категории получатели, пред които са или ще бъдат разкрити личните данни;
г) предвидения срок, за който ще се съхраняват личните данни, а ако това е неприложимо, критериите, използвани за определяне на този срок;
д) съществуването на правото да се изиска от Дружеството коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данни, или да се направи възражение срещу такова обработване;
е) правото на жалба до надзорен орган;
ж) когато личните данни не се събират от субекта на данни, всякаква налична информация за техния източник;
з) съществуването на автоматизирано вземане на решение, включително профилиране, както и съществена информация относно използваната логика, както и значението, и предвидените последствия от това обработване за субекта на данни.

Чл. 10. Субектът на данни има право да поиска от Дружеството личните му данни да бъдат коригирани ако са неточни или непълни. Във всеки един случай, когато е налице грешка в обработваните от Дружеството данни, то е длъжно да уважи такова искане, като в тези случаи трябва да уведоми и останалите получатели, на които са разкрити тези данни, за да могат и те да отразят промяната.

Чл. 11. (1) Субектът на данни има право на изтриване (право „да бъдеш забравен") на данните му, ако:

а) данните вече не са необходими за първоначалната цел и не съществува нова законосъобразна цел;
б) законното основание за обработването е съгласие на субекта на данни и той оттегли това съгласие, и липсва друго правно основание за обработване;
в) субектът на данни възразява срещу обработването на данни и липсва друго правно основание за обработване;
г) личните данни са били обработвани незаконосъобразно;
д) личните данни трябва да бъдат изтрити с цел спазване на правно задължение, произтичащо от законодателство, което се прилага спрямо Дружеството;
е) личните данни са събрани във връзка с предлагане на услуги на информационното общество на субект на данни - дете.

(2) Правото на изтриване на данните на субекта на данни не следва да се прилага от Дружеството, доколкото обработването е необходимо:

а) за спазване от Дружеството на правно задължение, предвидено в законодателството, което изисква обработване на данните;
б) за установяването, упражняването или защитата на правни претенции.

Чл. 12. (1) Субектът на данни има право да изиска от Дружеството да ограничи обработването на данните му в следните случаи:

а) точността на личните данни се оспорва от субекта на данни за срока, който позволява да се извърши проверка на точността на личните данни;
б) когато обработването е неправомерно, но субектът на данни не желае личните му данни да бъдат изтрити, а изисква вместо това да се ограничи използването им;
в) когато Дружеството не се нуждае повече от личните данни за целите на обработването, но субектът на данни ги изисква за установяването, упражняването или за защитата на правни претенции;
г) субектът на данни е възразил срещу обработването и е в очакване на проверка от страна на Дружеството дали законните ни основания имат преимущество пред неговите интереси.

(2) Когато обработването на данни е ограничено съгласно условията на ал. 1, такива данни се обработват, с изключение на съхранението им, само със съгласието на субекта на данни или в случай на необходимост от установяването, упражняването или защитата на правни претенции или за защитата на правата на други физически лица или поради важни основания от обществен интерес.

(3) Когато субектът на данни е упражнил правата си за коригиране, изтриване или ограничаване на обработването и Дружеството съответно е коригирало записите, се задължава да съобщи за тези свои действия на всеки получател, на който личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия.

Чл.13. (1) Субектът на данни има право по всяко време на възражение срещу обработване на личните му данни, отнасящи се до него, което се основава на обработването, необходимо за целите на легитимния интерес на Дружеството. В този случай Дружеството може да не прекрати обработването на данните при наличие на законови основания за обработването им, които имат предимство пред интересите, правата и свободите на субекта на данни или за установяване, упражняване или защитата на правни претенции.

(2). Когато субектът на данни възрази срещу обработването на личните му данни за целите на директния маркетинг, Дружеството прекратява обработването им за тази цел.

Чл. 14. Субектът на данни има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включително профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга. Това правило не се прилага, ако решението е необходимо за сключване или изпълнение на договор между Дружеството и субекта на данни.

Чл. 15. (1). Субектът на данни има право да получи личните данни, които го засягат и които той е предоставил на Дружеството в структуриран, широко използван и пригоден за машинно четене формат и има право да прехвърли тези данни на друг администратор.

(2). Когато упражнява правото си на преносимост на данни, субектът на данни има право да получи пряко прехвърляне от страна на Дружеството към друг администратор, само ако това е технически осъществимо.

РАЗДЕЛ IV
ОЦЕНКА И НИВА НА ВЪЗДЕЙСТВИЕТО НА ЗАЩИТА НА ДАННИТЕ

Чл. 16. (1) За определяне на адекватното ниво на техническите и организационни мерки и допустимия вид защита, Дружеството извършва оценка на въздействието върху обработваните лични данни.

(2) Оценката на въздействието е процес на определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, целостността или наличността на личните данни.

(3) Във всеки един случай, когато има вероятност операциите по обработването на данни да доведат до висок риск за правата и свободите на физическите лица, Дружеството извършва оценка на въздействието на предвидените операции.

(4) Дружеството извършва оценка на въздействие за всички поддържани регистри.

(5) Оценката на въздействие съдържа най-малко следното:

а) системен опис на предвидените операции по обработване и целите на обработването;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни;

г) мерките, предвидени за справяне с рискове, мерките за сигурност и механизмите за осигуряване на защитата на личните данни.

Чл. 17. Принципите, при които се провежда процедурата по оценка на въздействието са целенасоченост, задълбоченост, всеобхватност и своевременност:

а) принципът за „целенасоченост“ се изразява в задължението на Дружеството да извърши процедурата по оценка по отношение на всеки воден регистър на лични данни;

б) принципът за „задълбоченост“ се изразява в задължението на Дружеството да отчете характера на обработваните лични данни, организирани в регистри;

в) принципът за „всеобхватност“ се изразява в задължението на Дружеството да извърши процедурата по обща оценка по отношение на всички водени от него регистри на лични данни;

г) принципът за „своевременност“ изисква от Дружеството незабавно да извършва процедура по оценка при всяка промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 18 (1) Критериите, съобразно които се извършва оценката на въздействието, са поверителност, цялостност и наличност в съответствие с формата на Приложение № 1 на Наредба №1/30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

(2) За целите на тези Вътрешни правила, се определят следните нива на въздействие:

а) Изключително високо ниво на въздействие - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

б) Високо ниво на въздействие - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

в) Средно ниво на въздействие - в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

г) Ниско ниво на въздействие - в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по предходната алинея, определя нивото на въздействие на съответния регистър.

(4) В зависимост от нивото на въздействие се определя и съответното ниво на защита.

(5) Нивото на защита на обработваните лични данни представлява съвкупността от технически и организационни мерки за

физическа, персонална, документална, информационна и/или друга защита, които Дружеството като администратор следва да прилага с цел защита на личните данни и на субектите на лични данни от неправомерно обработване на данни, както и с цел управление на въздействието върху обработваните лични данни, върху физическо лице или група физически лица.

(6) За целите на тази Политика се определят следните нива на защита на обработваните лични данни, които в зависимост от определените нива на въздействие на съответните регистри на лични данни, Дружеството, като администратор е задължено да прилага:

а) при ниско ниво на въздействие - ниско ниво на защита;

б) при средно ниво на въздействие - средно ниво на защита;

в) при високо ниво на въздействие - високо ниво на защита;

г) при изключително високо ниво на въздействие - изключително високо ниво на защита.

(7) Детайлно описание на нивата на защита като съвкупност от технически и организационни мерки, осигурени от Дружеството за всеки от поддържаните регистри, в съответствие с оценката на нивото на въздействие, следва да бъде представено в Инструкция за техническите и организационни мерки за защита на личните данни.

РАЗДЕЛ V
РЕГИСТРИ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Чл. 19. (1) В настоящия раздел са изброени примерните изисквания при обработката на лични данни в зависимост от вида носител, на който се поддържат регистрите и нивото на чувствителност на данните.

Чл. 20. (1) Дружеството, като администратор на лични данни, води следните регистри:

1. Регистър „Клиенти" по сключени от Дружеството застрахователни договори и образувани застрахователни преписки по щети. В него се обработват лични данни на клиенти на Дружеството, страни (или техни представители) и ползващи лица по застрахователни договори.

2. Регистър „Контрагенти" е предназначен за обработка на данни на други контрагенти на Дружеството (различни от Клиенти), свързани с дейността му.

3. Регистър „Управление на човешките ресурси", създаден с цел организиране дейността на Дружеството във връзка с управление на персонала. В него се обработват лични данни на служители на Дружеството и лични данни на кандидати за работа и стажанти.

4. Регистър „Видеонаблюдение", предназначен с оглед организацията на охранителния режим на Дружеството.

(2). Съгласно предвидения в закона ред и в зависимост от дейността на Дружеството, могат да бъдат създадени допълнително и други регистри.

(3) Личните данни в горните регистри се събират, обработват и съхраняват от съответните специалисти, участващи в процеса по администриране и обслужване на съответната дейност на Дружеството.

Чл. 21. В регистър „Клиенти" се водят и съхраняват следните групи лични данни за клиенти на Дружеството, техни представители (законни или по пълномощие), действителни собственици, трети лица, които без упълномощаване извършват сделка от тяхно име за чужда сметка, ползващи се лица и други лица, свързани по някакъв начин със застрахователния договор:

а) данни относно физическата идентичност на лицата по представен от лицето документ за самоличност - имена, ЕГН, номер на лична карта или друг документ за самоличност, по който физическо лице може да бъде идентифицирано, дата и година на издаване на документа, издател, адрес на физическото лице, телефони и др.;

б) данни относно икономическата идентичност на лицето - финансово състояние на лицето, когато това се налага с оглед вида на застраховката или за определяне рисковия профил на клиента от гледна точка на мерките срещу изпиране на пари и финансиране на тероризма;

в) данни относно здравословното състояние на лицето, дотолкова доколкото те са необходими за сключване и обслужване на застрахователния договор.

Чл. 22. (1) В регистър „Контрагенти" се обработват лични данни на контрагенти или лица, свързани с дейността на Дружеството. По сключени от Дружеството посреднически договори се водят и съхраняват лични данни за страните по договорите (юридически лица, физически лица), или техните представители - брокери и/или агенти по смисъла на Кодекса за застраховане. В същия регистър се обработват лични данни на лица по договори с външни доставчици на услуги, доверени лекари, външни експерти и други, които подпомагат извършване дейността на Дружеството. Същите се обработват само с оглед изпълнение на задълженията по договорите и за съответните срокове.

Чл. 23. (1) В регистър „Управление на човешките ресурси" се водят и съхраняват следните групи лични данни за служителите на Дружеството по трудов или граждански договор, лица с договори за управление:

а) данни относно физическата идентичност на лицата - по представен от лицето документ за самоличност - имена, ЕГН, номер на лична карта или друг документ за самоличност, по който физическото лице може да бъде идентифицирано, дата и година на издаване на документа, издател, адрес на физическото лице, месторождение, телефони и др;

б) данни относно образованието на физическото лице - вид на образованието, място, номер и дата на издаване на дипломата. Когато е необходимо се представят и данни относно допълнителна квалификация. Данните са необходими с оглед спазване нормативни или установени с щатното разписание изисквания за заемане, респективно за освобождаване на определени длъжности от лицата. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

в) данни относно трудовата дейност на физическото лице – упражнявана професия, трудова биография. Данните са от значение при избора на подходящо за съответната длъжност лице. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо;

г) други данни - лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, свързани с материална отговорност, като свидетелство за съдимост в случаите, изисквани от закона. Предоставят се на основание нормативно

задължение. Горната информация се съхранява в личните досиета на служителите.

(2) Дирекция „Човешки ресурси“ отговаря за операциите по правилното обработване на лични данни на служителите на Дружеството по трудов или граждански договор, лица с договори за управление, както и лични данни на кандидати за работа и стажанти.

Чл. 24. В Регистър „Видеонаблюдение” чрез видео камери се наблюдават визуални изображения на лица - посетители, клиенти, служители и трети лица по начин, който прави възможна по-нататъшната им идентификация. Дружеството уведомява физическите лица за извършеното видеонаблюдение чрез информационни табла, поставени на видно място и съдържащи информация, идентифицираща съответния администратор на лични данни, включително и информация за осъществяване на контакт с него.

Чл. 25. Минималните изисквания към регистрите, поддържани на хартиен носител, са:

а) Съхранение на носителите в заключващи се помещения, до които достъп нямат външни лица, а при необходимост и в шкафове със секретни ключалки.

б) При отпадане на основанието или постигане на целта на обработване и при изтичане на срока за съхранение, унищожаването на тези документи се извършва по начин, който предотвратява всякаква възможност за бъдещо разчитане на данните.

в) Лицата с пряк достъп до документи, съдържащи лични данни, са длъжни да уведомят незабавно прекия си ръководител, който от своя страна да съобщи на Длъжностното лице по защита на личните данни, в случай на установяване на неправомерен достъп или ползване на съответната информация, включваща лични данни, или на неправомерно проникване в помещение, в което тази информация се съхранява.

г) Мерките по предходните точки се спазват и от служителите, които по повод изпълнението на служебните си задължения са поискали предоставянето им от служителите, при които се поддържат първоначално събраните данни.

д) Длъжностното лице по защита на личните данни на Дружеството поддържа информация за сигналите и инцидентите по предходната алинея, анализира пропуските и предлага мерки за отстраняването им.

е) За архивиране на документите се спазват Вътрешните правила за архивиране на документите в Дружеството.

ж) Достъпът и предоставянето на данни от тези регистри се осъществяват по възможност без изнасяне на оригиналните носители извън помещенията, в които се съхраняват. Трудовите досиета на служителите не се изнасят извън сградата на Централно управление на Дружеството.

Регистри, поддържани на технически носител в електронен вид

Чл. 26. Данните, поддържани в електронните системи на Дружеството, съществуват на локален компютър или в мрежа, несвързана с обществената мрежа. Към тях се прилагат мерки, съответстващи на средно ниво на защита, като минимално изискване.

Чл. 27. Регистрите, спрямо които се прилага средно ниво на защита, са всички електронни масиви с клиентски данни и данни за други лица, свързани с услугите на Дружеството.

Чл. 28. Минималните изисквания към регистрите, съдържащи лични данни, спрямо които се поддържа средно ниво на защита, са:

1. Временните файлове, изпращани между служители по повод изпълнение на служебните им задължения и съдържащи лични данни, се изтриват след изпълнение на съответната задача или се изтриват личните данни в тях.

2. В случай на загуба на данни, това обстоятелство се съобщава на Комисията по защита на личните данни.

Чл. 29. Защитата на системите, използването на пароли, ограниченията за достъп и правилата за работа с тях, както и спецификацията на техническите ресурси, прилагани за обработка на данни, реда за съхраняване и унищожаване на информационните носители и реда за архивиране и възстановяване на данни в случай на загуба, са в съответствие с утвърдените вътрешни правила и инструкции на Дружеството.

РАЗДЕЛ VI
ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 30. (1) Поради естеството, обхвата и целите на операциите по обработване на данни, които изискват редовно и систематично мащабно наблюдение на субектите на данни, както и необходимостта от обработване на специални категории данни и в отговор на изискване на законодателството, в Дружеството се назначава Длъжностно лице по защита на личните данни, чиято цел е контрол на дейността и гарантиране, че Дружеството спазва задължението си по защита личните данни на субектите на данни.

(2) Назначаването на Длъжностното лице по защита на личните данни се извършва с Решение на Управителния съвет на Дружеството.

(3) Всички структурни звена в Дружеството са длъжни да оказват съдействие на Длъжностно лице по защита на личните данни и да изпълняват неговите предписания във връзка с обработването и защитата на личните данни.

(4) Субектите на данни могат да се обръщат към Длъжностното лице по защита на личните данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно законодателството.

Чл. 31. Изискванията към Длъжностното лице по защита на личните данни:

1. Длъжностното лице по защита на личните данни трябва да е независимо и да не получава никакви указания във връзка с изпълнение на задачите си, като не може да бъде освобождавано от длъжност или санкционирано от Дружеството или обработващ лични данни за изпълнението на своите задачи.

2. Длъжностното лице по защита на личните данни може да изпълнява и други задачи и задължения, стига това да не води до конфликт на интереси.

3. Длъжностното лице по защита на данните е длъжно да спазва секретността и поверителността на изпълняваните от него задачи в съответствие с законовите разпоредби.

Чл. 32. (1) Задължения на Длъжностното лице по защита на личните данни:

1. Да информира и съветва Дружеството, обработващите лични данни и служителите, които извършват обработване, за техните задължения, свързани със защитата на личните данни;

2. Да наблюдава спазването на законодателството във връзка със защитата на личните данни, на Политиката на Дружеството за защита на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване на данни;

3. При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните.

4. При нужда да дава предписания по организацията на водене на регистрите и правата за достъп на служители, съгласно предвидените мерки за гарантиране на адекватна защита;

5. Да си сътрудничи с надзорните органи в лицето на Комисията за защита на личните данни (КЗЛД) и да поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

6. Да подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите.

(2) Дружеството подпомага Длъжностното лице по защита на личните данни при изпълнение на посоченото в ал.1, като осигурява ресурсите, необходими за изпълнение на тези задачи, достъпа до личните данни и операциите по обработването, а така също поддържа неговите експертни знания.

РАЗДЕЛ VII
ПРОЦЕДУРА ЗА ДОСТЪП ДО ЛИЧНИ ДАННИ ОТ ТИТУЛЯРИТЕ НА ДАННИТЕ ИЛИ ТРЕТИ ЛИЦА, ПОДАВАНЕ НА ВЪЗРАЖЕНИЯ И ЖАЛБИ

Общи положения при разглеждане на искания, свързани с лични данни

Чл. 33. (1) Всички искания, свързани с лични данни се завеждат и регистрират в деловодството на Дружеството.

(2) Клиент може да подаде заявление за достъп до лични данни чрез всички канали за подаване на молби, жалби или възражения.

(3) Дружеството предприема действия по искане на физическо лице да упражни право по настоящия раздел, само ако е в състояние да идентифицира съответното лице. В случай че Дружеството има основателни опасения във връзка със самоличността на физическото лице, което подава искане по този раздел, Дружеството може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на лицето.

(4) Действията, които Дружеството предприема при и по повод упражняването на правата на клиентите, са безплатни. Когато искането на дадено лице е явно неоснователно или прекомерно (например поради своята повторяемост), Дружеството има право по свое усмотрение:

(а) да откаже да изпълни искането; или

(б) да изиска заплащането на разумна такса, определена на база на административните разходи, необходими за предоставяне на исканата информация или за предприемането на исканите действия.

(5) Дружеството се произнася в едномесечен срок от подаването на искането, като този срок може да бъде удължен с още един месец като се взема предвид сложността и броя на исканията. Дружеството информира съответното лице за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето.

(6) Отделът и/или Дирекцията, отговорна за обработката на конкретните база данни и обслужваща конкретните операции, касаещи искането на клиента, изготвя отговора до клиента и го съгласува с Длъжностното лице по защитата на данните. За взетото решение въз основа на подаденото искане се информира ръководителят на съответното структурно звено за предприемане на предписаните от Комисията по защита на личните данни мерки.

Достъп до лични данни от страна на лицето, за което се отнасят

Чл. 34. Всеки клиент на Дружеството може да подаде искане до Дружеството, с което да поиска упражняване на правата си, съгласно Раздел III от настоящата Политика.

Чл. 35. Ако данните, до които се иска достъп, представляват класифицирана информация, достъпът се отказва.

Достъп до лични данни от трети лица

Чл. 37. В случай, че трето лице иска достъп до данните на клиент на Дружеството, които не представляват тайна или класифицирана информация, исканите данни се предоставят само в случай, че едновременно са изпълнени следните условия:

1. съществува законен интерес на лицето, искащо данните;

2. не може да се направи извод, че интересите на титуляра на данните има преимущество спрямо интересите на лицето, искащо разкриването на данните;

3. получателят на данните попада в кръга от лица, за който титулярът на данните предварително е уведомен относно възможността за разкриване на негови данни или титулярът е уведомен за разкриването на неговите данни след постъпване на искането от третото лице;

4. лицето, за което се отнасят данните е дало своето изрично писмено съгласие.

Чл. 38. Ако исканите данни съдържат тайна или класифицирана информация, се спазват изискванията за забрана за разкриването им.

Искания за достъп от държавни органи

Чл. 38. (1) При постъпило искане от държавен орган за предоставяне на информация, която съдържа и лични данни, се спазва специалния нормативен акт, който регламентира реда за предоставяне на съответния вид информация.

(2) Когато в писмото, в което се съдържа искането на държавния орган, се съдържат лични данни, които индивидуализират определени клиенти, в отговора индивидуализиращата информация за клиента не се включва по-голям обем данни, освен ако такива се изискват от органа.

(3) При постъпило искане за предоставяне на конкретни лични данни, копие от писмото на съответния орган се предоставя и на Комисията по защита на личните данни в Дружеството, с оглед потвърждение на основанието по закон и предприемане на необходимите действия, съгласно Закона.

Подаване на възражения и жалби

Чл. 39. Физическо лице може да направи възражение или да отправи искане пред Дружеството относно:

1. обработването на личните му данни при наличие на законово основание за това. При преценка, че възражението е основателно, личните данни на съответното физическо лице не могат повече да бъдат обработвани;

2. обработването на личните му данни за целите на директния маркетинг, независимо от първоначално изразеното писмено съгласие;

3. уведомяване преди личните му данни да бъдат разкрити за пръв път на трети лица, независимо от първоначалното му писмено съгласие, като му бъде предоставена възможност да възрази срещу такова разкриване или използване. В случай, че без това разкриване или използване съществува пречка за изпълнение на задължения по застрахователен договор, договорът се прекратява, като клиентът се уведомява за това.

4. в случай, че лицето не е подало заявление по предходната точка, с което иска да бъде уведомявано преди всяко разкриване на негови данни, то също може да възрази срещу разкриването, като съответният застрахователен договор ще бъде прекратен.

Раздел VIII
ПРЕХВЪРЛЯНЕ, ПРОВЕРКА И СЪВМЕСТНО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ МЕЖДУ ЗАД „АРМЕЕЦ“ АД И ДРУГ АДМИНИСТРАТОР

Прехвърляне на данни от ЗАД „Армеец“ АД на друг администратор на лични данни по силата на договор

Чл. 40. (1) Предоставянето на клиентски данни от Дружеството на други администратори, включително от държави от ЕС, по силата на споразумение се извършва при спазване на условията и предвидените възможности, определени с настоящите Правила, като при липса на предварително уведомление за възможните категории получатели, задължително титулярът на данните се уведомява за предоставянето, непосредствено преди или след извършването му.

(2) Уведомлението по ал.1 съдържа следната информация:

1. категориите лични данни, които се предоставят;
2. получателят на данните;
3. целите на обработването.

(3) Като правило Дружеството се стреми да не изпраща лични данни на потребителите извън територията на Европейския съюз (ЕС) и Европейската икономическа зона (ЕИО). В определени случаи обаче е необходимо определени данни да бъдат изпратени до лица извън ЕС/ЕИО, при спазване на изискванията на приложимото законодателство и описаното в тази Политика за личните данни.

(4) В случай че се наложи лични данни на даден потребител да бъдат изпратени от Дружеството към държава извън ЕС или ЕИО, това ще бъде сторено при спазване на настоящата Политика и при наличие на някое от следните условия:

а) когато е налице решение на КЗЛД или на Европейската комисия, според което съответната държава осигурява адекватно ниво на защита на личните данни;

б) когато е сключено споразумение с организацията, към която се изпращат лични данни, съдържащо стандартните клаузи за защита на данните, одобрени от Европейската комисия с Решение № 2010/87/ЕС (https://www.cpdp.bg/userfiles/file/Transfers/BCR_Commission_decision_2010-87_Bg.pdf);

в) когато трансферът на данни е необходим, за да бъде изпълнен договор със съответния потребител;

г) когато е необходимо да се извърши трансфер на данни към организация в САЩ, трансферът се извършва доколкото съответната организация участва в Щита за неприкосновеност, приет с решение на Европейската комисия на 26.07.2016 година (https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection_en).

Получаване от страна на ЗАД „Армеец“ на данни от друг администратор

Чл. 41. При водене на преговори и сключване на договори за провеждане на съвместни кампании с други търговци, които предвиждат получаване от тях на лични данни на техни клиенти, от контрагента се изисква да гарантира спазване на ЗЗЛД при предоставяне на данните на Дружеството.

Чл. 42. В случай че в хода на съвместната кампания клиент изрази несъгласие с обработването на негови лични данни, когато клиентът не е страна по застрахователен и/или друг тип търговски договор, сключен със Дружеството, както и не се е съгласявал писмено за обработване на информация, отнасяща се до него, данните незабавно се унищожават на основание отпадане на целта на обработването.

РАЗДЕЛ IX
ПРАВИЛА ЗА ВПИСВАНЕ НА ЛИЧНИ ДАННИ В ЗАСТРАХОВАТЕЛНИ ДОГОВОРИ НА ДРУЖЕСТВОТО

Чл. 43. В застрахователните договори, по които Дружеството е страна, личните данни относно клиентите са в обем, който е достатъчен за индивидуализацията на клиента, освен ако от естеството на договора не следва друго.

Чл. 44. Задължително при съставяне на застрахователни договори, предлагани от Дружеството, се включва текст относно начина на обработване на личните данни на клиента и получаване на необходимите съгласия за обработване на лични данни, чието съдържание е съобразено с характера на продукта.

РАЗДЕЛ X
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 45. За неуредените в настоящата Политика въпроси се прилагат разпоредбите на действащото законодателство.

Чл. 46. Всяка промяна на нормативната уредба, която регламентира защитата на личните данни се прилага автоматично, без да е необходима изрична промяна на настоящата Политика.

Чл. 47. При противоречие между настоящата Политика и разпоредбите на ОРЗЛД, на ЗЗЛД и/или други актове по прилагането му, се прилагат нормите на действащата правна уредба.

Чл. 48. При необходимост Длъжностното лице по защита на личните данни дава методологически указания за прилагането на настоящата Политика.

Настоящата Политика е приета с Протокол № 68/04.05.2018 г. от Управителния съвет на Дружеството.