ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ПЕНСИОННО-ОСИГУРИТЕЛНА КОМПАНИЯ „ДОВЕРИЕ“ АД

Раздел I.

ПРЕДМЕТ, ЦЕЛ И ОБХВАТ

1.1. Пенсионно-осигурителна компания „Доверие“ АД (Компанията) осъществява дейност по допълнително пенсионно осигуряване и е администратор на лични данни, съгласно Закона за защита на личните данни (ЗЗЛД). Компанията обработва лични данни, самостоятелно или чрез възлагане на обработващ данните, в съответствие със Системата за управление на сигурността на информацията ISO/IEC 27001:2013 и създадената вътрешна нормативна уредба за работа с лични данни, като осигурява и съблюдава за пълното спазване на изискванията на приложимото национално[1] и европейско[2] законодателство в сферата на защита на личните данни, както и на нормативната уредба в областта на допълнителното пенсионно осигуряване.

1.2. Настоящата Политика за защита на личните данни на Компанията (Политиката) определя основните принципи и правила, свързани с обработването на лични данни, правата на субектите на тези данни, задълженията и отговорността на Компанията, като администратор на данни, съответно на служителите й, в качеството им на обработващи данни, функциите на длъжностното лице по защита на личните данни. Политиката подлежи на актуализация и може да бъде променяна и допълвана периодично.

1.3. Политиката е част от цялостна система от вътрешни документи, технически и организационни мерки, които Компанията прилага с цел да гарантира, че нейните служители, осигурителни посредници и всички други физически и юридически лица, които, чрез възлагане, обработват лични данни, от името на Компанията, стриктно ще спазват изискванията на приложимото европейско и национално законодателство и на вътрешните правила, като, по този начин, ще гарантират спазване правата на физическите лица, свързани с техните лични данни.

1.4. Принципът за защитата на личните данни е един от десетте основни принципи на етично и бизнес поведение, към които Компанията се придържа. Този принцип е възприет в Политиката за съответствие и в Етичния кодекс на Компанията и неговото спазване е задължение и отговорност на всеки служител и се споделя от всички структурни звена и йерархични нива в Компанията. Настоящата Политика развива този принцип в конкретни правила и цели да подпомогне служителите в тяхната ежедневна работа с лични данни, така че да се избегне неговото нарушаване.

---

[1] Закон за защита на личните данни, обн., ДВ, бр. 1 от 4.01.2002 г., впоследствие изменян и допълван; Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, издадена от Комисията за защита на личните данни, обн., ДВ, бр. 14 от 12.02.2013 г.

[2] 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 (GDPR), в сила от 25.05.2018 г.

1.5. Нарушения в сигурността на личните данни биха могли да доведат до висок риск за правата на засегнатите физически лица и до значителни негативни последици, както за Компанията и нейните акционери, така и за нейните служители, нарушили изискванията на приложимата вътрешна и обща нормативна уредба. Поради това, всяко неспазване на тази Политика се третира като сериозно нарушение и действие, което уронва престижа и доброто име на Компанията, подкопава доверието в нея.

Раздел II.

ОПРЕДЕЛЕНИЯ

2.1. **„Лични данни”** са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“). Физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор, като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

2.2. **„Обработване на лични данни"** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни, чрез автоматични или други средства, като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване, чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

2.3. **„Регистър на лични данни"** е всеки структуриран набор от лични данни, достъпът до които се осъществява, съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен, съгласно функционален или географски принцип;

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

2.5. **„Нарушение на сигурността на лични данни“** означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

2.6. **„Администратор на лични данни“** е физическо или юридическо лице, публичен орган, агенция или друга структура, която, сама или съвместно с други, определя целите и средствата за обработването на лични данни. Когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Европейския съюз (ЕС) или в правото на държава членка;

2.7. „**Обработващ лични данни**" е физическо или юридическо лице, което обработва лични данни, от името на администратора на лични данни;

2.8. „**Получател“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни, в рамките на конкретно разследване, в съответствие с правото на ЕС или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните, съобразно целите на обработването.

Раздел III.

ПРИНЦИПИ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

3. Компанията обработва лични данни при спазване на следните принципи:

3.1. **Законосъобразност, добросъвестност и прозрачност**

Компанията обработва лични данни законосъобразно, добросъвестно и по прозрачен и ясен за субектите начин.

3.1.1. **Законосъобразност**

Всяко обработване на лични данни от Компанията (от нейните служители, осигурителни посредници и други обработващи от името на Компанията) се основава на валидно правно основание и се осъществява при спазване на общата и вътрешна нормативната уредба. Спрямо правните основания се прилага принципът на алтернативност, т.е. законосъобразно е обработването на данните, ако:

3.1.1.1.е необходимо за спазването на законово задължение, което се прилага спрямо дейността на Компанията;

3.1.1.2.субектът на данните е дал своето съгласие за обработване на личните му данни за една или повече конкретни цели по смисъла на Раздел II, т. 2.4, чрез предоставяне на Компанията на съответни писмени документи и/или чрез други действия и технически способи (включително по електронен път);

3.1.1.3.е необходимо за изпълнението на договор, по който субектът на данните е страна или за предприемане на стъпки, по искане на субекта на данните, преди сключването на такъв договор (това например са осигурителни и пенсионни договори, договори за разсрочено плащане на средства, трудови договори, договори с осигурителни посредници и др.);

3.1.1.4.е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данните или на друго физическо лице;

3.1.1.5.е необходимо за изпълнението на задача от обществен интерес или при изпълнението на действия по силата на законов или подзаконов нормативен акт (включително обработване, свързано с предоставяне на информация, изискана от орган на власт);

3.1.1.6.е необходимо за целите на легитимните интереси на Компанията или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

3.1.2. **Законосъобразност на обработването по отношение на осигурените лица във фондовете за допълнително пенсионно осигуряване (ФДПО), управлявани от Компанията:**

Компанията обработва лични данни на осигурените лица[3] във връзка с дейността по допълнително пенсионно осигуряване и в изпълнение на законовите си задължения,

[3] Понятието „осигурени лица“ включва осигурените лица, пенсионерите и техните наследници и законни представители.

на основание на:

3.1.2.1. Кодекса за социално осигуряване (КСО), актовете на Комисията за финансов надзор (КФН), Данъчно-осигурителния процесуален кодекс (ДОПК), актовете на Националната агенция за приходите (НАП) и всички други законови и подзаконови нормативни актове, приложими към нейната дейност;

3.1.2.2. Надлежно попълнени и подадени от осигурените лица документи, като например:

3.1.2.2.1. Заявление за достъп до лични данни;

3.1.2.2.2. Заявление за избор на фонд за допълнително пенсионно осигуряване (по образец, утвърден с наредба[4])

3.1.2.2.3. Заявление за промяна на участие / прехвърляне на средства / възобновяване на осигуряването във ФДПО (по образец, утвърден с наредба[5]);

3.1.2.2.4. Искане за оттегляне на заявление за промяна на участие (по образец, утвърден с наредбата по предходната точка);

3.1.2.2.5. Заявление за изплащане на средства;

3.1.2.2.6. Осигурителен договор;

3.1.2.2.7. Пенсионен договор;

3.1.2.2.8. Други образци на документи за упражняване на права по КСО, утвърдени от КФН, Националния осигурителен институт (НОИ), НАП или друг компетентен орган, или издадени въз основа на законов или подзаконов нормативен акт.

3.1.2.3. Документи, информация и данни за осигурени лица, постъпили от други пенсионноосигурителни дружества, НОИ, НАП или други държавни или общински органи, във връзка с дейността на Компанията и в изпълнение на нормативни изисквания;

3.1.2.4. Искане от орган на власт за предоставяне на лични данни, на осигурени лица, от Компанията, по силата на задължение, регламентирано в законов или подзаконов нормативен акт.

3.1.3. **Законосъобразност на обработването по отношение на служителите:**

Компанията обработва лични данни на своите служители, на основание на приложимото трудово, осигурително и данъчно законодателство, в качеството й на работодател (осигурител) и във връзка с дейността по сключването и изпълнението на трудовите договори, договорите за управление и договорите за услуги.

3.1.4. **Законосъобразност на обработването по отношение на осигурителните посредници[6]:**

Компанията обработва лични данни на осигурителни посредници – физически лица и на лица, упълномощени от посредници – юридически лица, на основание на приложимото осигурително и данъчно законодателство, в качеството й на възложител (осигурител) и във връзка с дейността по сключването и изпълнението на договорите с осигурителни посредници.

3.1.5. **Добросъвестност и прозрачност**

В изпълнение на принципа на прозрачност при обработването на лични данни, Компанията информира служителите си, осигурителните посредници и осигурените лица, по подходящ, ясен и разбираем начин, за дейността по събиране и обработване на личните им данни, от страна на Компанията и за техните права във връзка със защитата на личните им данни, включително чрез информация на интернет страницата си.

---

[4] Наредба № 33 от 19.09.2006 г. за индивидуалните заявления за участие във фонд за допълнително задължително пенсионно осигуряване и за възобновяване на осигуряването в универсален пенсионен фонд.

[5] Наредба № 3 от 24.09.2003 г. за реда и начина за промяна на участие и за прехвърляне на натрупаните средства на осигурено лице от един фонд за допълнително пенсионно осигуряване в друг съответен фонд, управляван от друго пенсионноосигурително дружество.

[6] Навсякъде в документа понятието „осигурителни посредници – физически лица“ включва и супервайзорите.

Компанията оказва съдействие на субектите на данни при упражняване на техните права. Служителите и осигурителните посредници на Компанията, в качеството им на обработващи лични данни, са информирани за правата на осигурените лица, като субекти на лични данни и се задължават да им предоставят информация, и да им оказват съдействие по реда на раздел VII.

3.2. **Ограничаване на целите**

Компанията обработва лични данни за конкретни, изрично указани в съответните нормативни актове, и/или договори и/или други документи, легитимни цели и не ги обработва по-нататък по начин, несъвместим с тези цели.

3.3. **Свеждане на данните до минимум**

Компанията обработва лични данни, които са подходящи, свързани със и ограничени до необходимото, с оглед целите, за които се обработват.

3.4. **Точност и актуалност**

Компанията събира и обработва точни лични данни и предприема всички разумни мерки, за да се гарантира своевременното коригиране или изтриване на неточни такива, като се имат предвид целите, за които те се обработват.

Компанията полага усилия да поддържа личните данни в актуален вид. В изпълнение на принципа за точност и актуалност на събраните данни и с цел да изпълни коректно задълженията си към осигурените лица, Компанията ги насърчава да я информират за промяна на техни лични данни и им оказва съдействие за актуализирането на данните им.

3.5. **Ограничение на съхранението**

Компанията съхранява личните данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от определения с нормативен акт, а ако такъв няма, за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.

След постигане целта на обработване на личните данни или след изтичане на определен в нормативен акт срок на съхранение Компанията, в качеството си на администратор, е длъжна да ги унищожи или прехвърли на друг администратор, като предварително уведоми за това Комисията за защита на личните данни (КЗЛД), ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

Компанията няма да унищожи лични данни и документи, ако те са необходими за висящо съдебно, административно производство или производство по разглеждане на жалба пред Компанията.

Компанията може да анонимизира лични данни, което е алтернатива на унищожаването им. Анонимиизрането представлява необратимо заличаване на всички лични и разпознаваеми елементи, които позволяват идентифицирането на субектите на данни. Не съществува нормативно изискване за унищожаване на анонимизирани данни, тъй като не представляват лични данни.

3.5.1. **Съхранение на лични данни на осигурените лица**

Съгласно изискванията на КСО[7] Компанията съхранява за срок не по-кратък от 50 години, считано от прекратяване на съответното осигурителното правоотношение, оригиналните документи на хартиен носител и електронните документи, като например:

3.5.1.1. заявления (за избор на пенсионен фонд, за промяна на участието, за възобновяване на осигуряването в универсален пенсионен фонд, за прехвърляне или изтегляне на средства и др.);

[7] Вж. чл. 123и прим, ал. 1 от КСО

3.5.1.2. договори (осигурителни, пенсионни и за разсрочено изплащане);

3.5.1.3. разпореждания и други свои актове за определяне размера на еднократни и периодични плащания, както и

3.5.1.4. другите документи, данни и информация, които са от значение за упражняване на правата на осигурените лица, пенсионерите или техните наследници.

Компанията съхранява, използва и унищожава документите и данните, свързани с дейността по допълнително пенсионно осигуряване, по ред, определен с наредба на КФН и при спазване изискванията на Регламент 2016/679, ЗЗЛД, КСО и изискванията на системата за сигурност на информацията ISO/IEC 27001:2013.

3.5.2. **Съхранение на лични данни на служителите**

Съгласно изискванията на Кодекса на труда, Данъчно-осигурителен процесуален кодекс (ДОПК), Закона за данъците върху доходите на физическите лица (ЗДДФЛ), Закона за счетоводството и Наредбата за трудовата книжка и трудовия стаж, Компанията съхранява за срок не по-кратък от 50 години, считано от прекратяването на съответното трудово правоотношение, на хартиен и/или електронен носител, трудовите досиета и документите, удостоверяващи изплатените възнаграждения на служителите.

3.5.3. **Съхранение на лични данни на осигурителни посредници**

Съгласно изискванията на КСО, Компанията съхранява договорите с осигурителните посредници и свързаните с тях документи за целия срок на тяхното действие на хартиен и/или електронен носител.

Съгласно изискванията на ДОПК, ЗДДФЛ и Закона за счетоводството, Компанията съхранява, за срок не по-кратък от 50 години, считано от прекратяването на съответното правоотношение, на хартиен и/или електронен носител, документите, удостоверяващи изплатените възнаграждения на осигурителните посредници

3.6. **Поверителност, цялостност и наличност**

Компанията обработва личните данни по начин, който гарантира подходящо ниво на тяхната поверителност, цялостност и наличност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу загуба, унищожаване или повреждане, като се прилагат подходящи технически и организационни мерки и при спазване на стандартите и изискванията за информационна сигурност на Системата за управление на сигурността на информацията ISO/IEC 27001:2013.

3.7. **Отчетност**

Компанията носи отговорност за спазването на принципите, изложени в този раздел и изисква тяхното спазване от своите служители, осигурителни посредници и всички физически и юридически лица, които обработват лични данни от името на Компанията и по нейно възлагане.

***Раздел* IV.**

ЛИЧНИ ДАННИ, КОИТО КОМПАНИЯТА ОБРАБОТВА

4. **Лични данни в зависимост от източника:**

4.1. **Лични данни, които са предоставени от субектите на данните**

Компанията обработва лични данни, които са предоставени от субекта на данните чрез заявление, договор или друг документ, по инициатива на лицето, с цел изпълнение от

страна на Компанията на дейност, поискана от субекта на данни или във връзка с упражняване на негови права.

4.2. **Лични данни, които не са предоставени от субектите на данни**

В предвидените от закона случаи и когато това е свързано с нормативни задължения на Компанията в качеството ѝ на пенсионноосигурително дружество, тя обработва лични данни на осигурени лица, които получава от съответните компетентни държавни органи – НАП, НОИ или от други пенсионноосигурителни дружества.

4.3. **Лични данни в зависимост от субекта на данните:**

4.3.1. В качеството си на пенсионноосигурително дружество, което осъществява дейност по допълнително пенсионно осигуряване, Компанията обработва данни на осигурени лица – настоящи или бивши участници, в управляваните от него фондове за допълнително пенсионно осигуряване, при спазване на нормативната уредба и актовете на КФН и НАП;

4.3.2. В качеството си на работодател, Компанията обработва лични данни на своите служители, при спазване на нормативната уредба и актовете на НАП и НОИ;

4.3.3. Компанията обработва лични данни на осигурителните посредници – физически лица, с които има сключен договор и на физически лица, упълномощени от осигурителни посредници – юридически лица, да осъществяват дейност по сключения от тях договор:

4.3.3.1. в качеството си на пенсионноосигурително дружество, от чието име и за чиято сметка осигурителните посредници – физически лица, както и физическите лица, упълномощени от осигурителни посредници – юридически лица, осъществяват дейност, при спазване на нормативната уредба и актовете на КФН;

4.3.3.2. в качеството си на възложител и осигурител по сключените договори с осигурителните посредници – физически лица, при спазване на нормативната уредба и актовете на НАП.

4.3.4. Компанията обработва лични данни на други лица, като лицата по договори за услуги, контрагенти и доставчици, при спазване на нормативната уредба и актовете на НАП и НОИ.

4.4. **Лични данни в зависимост от вида на данните (специални категории лични данни)**

4.4.1. Компанията не обработва специални категории лични данни, с изключение на:

4.4.1.1. **данни за здравословното състояние на своите служители:**

4.4.1.1.1. във връзка с изпълнение на законови изисквания при тяхното назначаване;

4.4.1.1.2. за целите на трудовата медицина и здравословните и безопасни условия на труд;

4.4.1.1.3. във връзка със закрилата при прекратяване на трудовото правоотношение;

4.4.1.1.4. във връзка с упражняване на правата им при временна неработоспособност;

4.4.1.1.5. във връзка с упражняване на правата им при трайно намалена работоспособност.

4.4.1.2. **данни за здравословното състояние на осигурени лица**, предоставени от тях в изпълнение на законовите изисквания за упражняване на права, удостоверяващи трайно намалената им работоспособност, във връзка с правото на изплащане на суми от фонд за допълнително пенсионно осигуряване.

Раздел V.

ИНФОРМАЦИЯ, ПРЕДОСТАВЯНА ОТ СТРАНА НА КОМПАНИЯТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

5.1. В случаите, когато Компанията получи лични данни от субект на данни, му предоставя информация за:

5.1.1. Данните, които идентифицират Компанията;

5.1.2. Координати за връзка с длъжностното лице по защита на личните данни;

5.1.3. Целите и правното основание за обработването на личните данни, когато това е приложимо;

5.1.4. Получателите или категориите получатели, на които могат да бъдат разкрити данните;

5.1.5. Информация дали предоставянето на лични данни е нормативно или договорно изискване, или е необходимо с цел сключване на договор или изпълнение на дейност от страна на Компанията, поискана от субекта на данни, както и евентуалните последствия ако тези данни не бъдат предоставени;

5.1.6. Информация за правото на достъп, коригиране, изтриване на лични данни или ограничаване на обработването им, както и за правото на възражение;

5.1.7 Срока, за който се съхраняват данните или критериите, които определят периода на съхранение;

5.1.8. Правото на жалба до Комисията за защита на личните данни (КЗЛД).

5.2. Когато личните данни не са получени от физическото лице, за което се отнасят, освен информацията, посочена в т. 5.1. по-горе, Компанията му предоставя и информация за съответните категории лични данни, които обработва и за техния източник, освен ако субектът вече разполага с тази информация.

5.3. Точки 5.1. до 5.2. от настоящия раздел не се прилагат в случаите, когато личните данни не идват от субекта на данните, но получаването или разкриването им е изрично разрешено от правото на ЕС или българското законодателство и в което се предвиждат подходящи мерки за защита на легитимните интереси на субекта на данните.

Раздел VI.
ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Съгласно Регламент 2016/679 и приложимото българско законодателство, субектите на лични данни имат следните права:

6.1.1. **Право на достъп**

Субектът на данните има право да получи, от Компанията , информация, дали Компанията обработва негови лични данни и ако ги обработва, той има право да получи достъп до тях и информация за:

6.1.1.1. целите на обработването;

6.1.1.2. съответните категории лични данни, които се обработват;

6.1.1.3. получателите или категориите получатели, пред които са или могат да бъдат разкрити неговите лични данни, по-специално получателите в трети държави или международни организации, ако има осъществявани такива трансфери на данни;

6.1.1.4. предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

6.1.1.5. съществуването на право да се изиска от Компанията коригиране или изтриване на негови лични данни или ограничаване на обработването им, или да се направи възражение срещу такова обработване, освен ако обработването не е в изпълнение на законово или договорно задължение;

6.1.1.6. правото на жалба до КЗЛД;

6.1.1.7. източника на личните данни, обработвани от Компанията, когато те не са събрани от субекта на данните;

6.1.1.8. съществуването на автоматизирано вземане на решения, включително профилирането, както и значението и предвидените последствия от това обработване за субекта на данните, ако се осъществява такова.

6.1.2. **Право на коригиране**

Субектът на данни има право да поиска от Компанията да коригира, без ненужно забавяне, негови лични данни, които са неточни или вече не са актуални, както и да ги допълни, когато данните са непълни.

6.1.3. **Право на изтриване (право да „бъдеш забравен“)**

Субектът на данни има правото да поиска от Компанията изтриване на негови лични данни, а Компанията има задължението да ги изтрие без ненужно забавяне, когато е приложимо някое от посочените по-долу основания:

6.1.3.1. личните данни повече не са необходими за целите, за които са били събрани или обработвани;

6.1.3.2. субектът на данните оттегля своето съгласие, въз основа на което се обработват неговите данни и няма друго правно основание за обработването им;

6.1.3.3. субектът на данните възразява срещу обработването съгласно член 21, параграф 1 от Регламент 2016/679 и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно член 21, параграф 2 от Регламент 2016/679;

6.1.3.4. личните данни са били обработвани незаконосъобразно.

6.1.3.5. Компанията прекратява обработването на личните данни в случаите на чл. 6.1.3.3.:

6.1.3.5.1. винаги, когато получи възражение по чл. 6.1.5.2. за целите на директния маркетинг;

6.1.3.5.2. при получено възражение по чл. 6.1.5.1., освен ако Компанията не докаже, че съществуват законови основания за обработването, които имат преимущество пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

6.1.3.6. Член 6.1.3. и 6.1.4. не се прилагат, когато:

6.1.3.6.1. не е изтекъл нормативно определен срок за задължително съхранение на данните;

6.1.3.6.2. обработването се извършва въз основа на договорно задължение по договор между Компанията и субекта на данните;

6.1.3.6.3. обработването е необходимо за установяването, упражняването или защитата на правни претенции на Компанията;

6.1.3.6.4. обработването е необходимо за спазването на нормативно задължение, което изисква или по естеството си предполага това обработване.

6.1.4. **Право на ограничаване на обработването**

6.1.4.1 Субектът на данните има право да изиска от Компанията ограничаване на обработването на своите лични данни, ако:

6.1.4.1.1 обработването е неправомерно, но субектът не желае личните му данни да бъдат изцяло изтрити, а вместо това изисква ограничаване на използването им;

6.1.4.1.2 Компанията не се нуждае повече от неговите лични данни за целите, за които същите са били обработвани, но субектът ги изисква за установяването, упражняването или защитата на правни претенции;

6.1.4.2 Данните, чието обработване е ограничено, съгласно чл. 6.1.4, се обработват само със съгласието на техния субект, с изключение на съхранението им или за установяването, упражняването или защитата на правни претенции, или за защита на правата на друго физическо лице, или поради важни основания от обществен интерес.

6.1.4.3 Когато субект на данните е изискал ограничаване на обработването, съгласно чл. 6.1.4., Компанията го информира преди отмяната на ограничаването на обработването.

6.1.4.4 При извършване на коригиране, изтриване или ограничаване на обработването на лични данни Компанията съобщава за всяко извършено действие на всеки получател, на когото личните данни са били предоставени, освен ако това е невъзможно или изисква несъразмерно големи усилия. ПОК "Доверие" АД информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

6.1.5. **Право на възражение**

6.1.5.1. Субектът на лични данни има право на възражение срещу обработването на лични данни, отнасящи се до него, ако обработването се извършва на основание изпълнение на задача от обществен интерес или на основание упражняване на официални правомощия, които са предоставени на Компанията, или обработването е било необходимо за целите на легитимните интереси на Компанията или на трета страна. Компанията прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

6.1.5.2. Когато Компанията обработва лични данни, за целите на директния маркетинг, техният субект има право по всяко време да направи възражение срещу обработването им за такъв вид маркетинг, включително срещу профилиране, доколкото то е свързано с директния маркетинг. В случай на постъпило възражение, Компанията прекратява обработването на личните данни за целите на директния маркетинг, насочен към този субект на лични данни.

6.1.5.3. В момента на първото осъществяване на контакт със субекта на данните Компанията изрично го уведомява за правото му на възражение, като уведомлението му се представя по ясен начин и отделно от всяка друга информация.

6.1.6. **Право на защита срещу автоматизирано обработване**

Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизираното обработване на лични данни, отнасящи се до него, включващо профилиране, което поражда правни последствия за него или го засяга, в значителна степен.

6.1.7. Компанията прилага вътрешни правила и процедури, които регламентират реда и условията за приемане, разглеждане и отговор, в едномесечен срок, на искания от физически лица – субекти на лични данни, свързани с упражняване на правата им по този раздел.

Раздел VII.

ЗАДЪЛЖЕНИЕ НА КОМПАНИЯТА ЗА СЪДЕЙСТВИЕ НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ ПРИ ОСЪЩЕСТВЯВАНЕ НА ПРАВАТА ИМ

7.1. Компанията е длъжна да предоставя на субектите, чиито лични данни обработва, информация за правата им по прозрачен и достъпен начин, в писмена или устна форма, или по друг начин, при поискване от тяхна страна и след като се идентифицират.

7.2. Компанията съдейства за упражняване правата на субектите, чиито лични данни обработва, посочени в раздел VI и не може да откаже да предприеме действия, освен ако не е в състояние да идентифицира самоличността на субекта, отправил искането.

7.3. Компанията предоставя на субекта на данни информация относно действията, предприети по негово искане, във връзка с упражняване на правата му, без ненужно забавяне и във всички случаи, в срок от 1 (един) месец от получаване на искането. При необходимост този срок може да бъде удължен с още 2 (два) месеца, като се вземе предвид сложността и/или броя на получените искания. Компанията информира субекта на данните за всяко такова удължаване в срок от 1 (един) месец от получаване на искането, като посочва и причините за забавянето.

7.4. Когато субектът на данни подава искане чрез електронни средства с квалифициран електронен подпис (КЕП) по реда на Закона за електронния подпис и електронните удостоверителни услуги, по възможност, информацията се предоставя по идентичен начин, освен ако субектът на данни е поискал друго. Правото на субекта да получи копие от информация(та) или достъп до личните си данни чрез отдалечена достъпна защитена система не трябва да засяга неблагоприятно правата и свободите на другите субекти, чиито данни се обработват от Компанията.

7.5. Ако Компанията не предприеме действия по искането на субекта на данни, тя го уведомява без забавяне, но най-късно в срок от 1 (един) месец от получаване на искането, за причините да не предприеме действия и за възможността за подаване на жалба до КЗЛД и търсене на защита по съдебен ред.

7.6. Информацията, предоставяна на субектите на данни по тяхно искане, както и всички действията на Компанията, свързани с упражняване на правата на субектите, са безплатни за тях. Когато исканията на субект на данни са явно неоснователни, прекомерни, или се повтарят твърде често, Компанията може:

7.6.1. да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията, или предприемането на исканите действия, или

7.6.2. да откаже да предприеме действия по искането.

7.7. Когато Компанията има основателни съмнения във връзка със самоличността на физическото лице, което подава искане с цел упражняване на правата си, тя може да поиска предоставянето на допълнителна информация и/или документи, необходими за потвърждаване на самоличността на субекта на данните.

Раздел VIII.

АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

8.1. **Отговорност на Компанията**

В качеството си на администратор на лични данни Компанията въвежда подходящи технически и организационни мерки, част от които е и настоящата Политика, с които гарантира и е в състояние да докаже, че обработва лични данни в съответствие с Регламент 2016/679 и приложимото национално законодателство, вземайки предвид естеството, обхвата, контекста и целите на обработването, както и потенциалните рискове с различна вероятност и тежест за правата и свободите на физическите лица – субекти на лични данни. Мерките се преразглеждат и при необходимост се актуализират.

8.2. **Защита на данните на етапа на проектирането и по подразбиране**

В Компанията е внедрена Система за управление сигурността на информацията, като Компанията е сертифицирана по ISO/ IEC 27001:2013, което е сериозна гаранция, че се осигурява адекватна защита на данните и на правата на субектите на данни.

Компанията въвежда към момента на разработването на нови бизнес модели/бизнес процеси/продукти/системи за работа, както и към момента на самото обработване, най-подходящите технически и организационни мерки за защита на личните данни, в това число и псевдонимизация, когато такъв подход е допустим.

8.3. **Обработващ лични данни**

8.3.1. Обработващи лични данни от името на Компанията, са всички **служители** и **осигурителни посредници** на Компанията, когато обработват лични данни при или по повод изпълнение на служебните си или договорни задължения.

8.3.2. По смисъла на тази Политика обработващи лични данни са и всички физически и юридически лица, които въз основа на сключени с Компанията договори за възлагане на услуги извършват някоя от дейностите, посочени в дефиницията за обработване на лични данни, съгласно раздел II, т. 2.2, като доставчици на следните, неизчерпателно изброени, услуги, свързани с:

8.3.2.1. информационни технологии, използвани от Компанията;

8.3.2.2. дигитализиране и друг вид техническо обработване на данните;

8.3.2.3. печатни дейности;

8.3.2.4. унищожаване на данни /на хартиен носител/;

8.3.2.5. здравно осигуряване и трудова медицина.

8.3.3. Когато възлага обработване на лични данни, Компанията използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на Регламент 2016/679, приложимото национално законодателство и да осигурява защита на правата на субектите на данни.

8.3.4. Обработващи лични данни от името на Компанията не включват и не възлагат обработване на друго лице, без предварителното, конкретно или общо, писмено разрешение на Компанията. В случай че Компанията предостави на обработващия лични данни общо писмено разрешение, обработващият се задължава да информира Компанията предварително за всякакви планирани промени за включване или замяна на лица, обработващи данни, като Компанията си запазва правото да оспори тези промени.

8.3.5. Обработването, извършвано от страна на обработващия лични данни, се урежда с договор или с друг правен акт, съгласно правото на ЕС или приложимото българско законодателство, в който се регламентират естеството и целта на обработването, срока на обработването, вида лични данни и категориите субекти на данни, както и задълженията и правата на обработващия и на Компанията, като за обработващия лични данни задължително се включват следните задължения:

8.3.5.1. да обработва личните данни само по документирано нареждане на Компанията, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато обработващият е длъжен да направи това по силата на правото на ЕС или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира Компанията за това правно изискване преди обработването, освен ако това право забранява такова информиране, с оглед важни основания от публичен интерес;

8.3.5.2. да гарантира, че лицата, оправомощени от него да обработват личните данни, във връзка с изпълнението на договора, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

8.3.5.3. да взема всички необходими мерки за сигурност при обработването;

8.3.5.4. да спазва условията, споменати по-горе, за включване на друг обработващ лични данни;

8.3.5.5. да подпомага Компанията чрез подходящи технически и организационни мерки, като взема предвид естеството на обработването, което му е възложено и доколкото е възможно, при изпълнението на задължението на Компанията да отговаря на отправени към нея искания, свързани с упражняване на нормативно предвидените права на субектите на данни;

8.3.5.6. да подпомага Компанията при изпълнението на задълженията, съгласно членове 32-36 от Регламент 2016/679, като отчита естеството на обработване, което му е възложено и информацията, до която му е осигурен достъп;

8.3.5.7. да заличава или връща на Компанията по неин избор всички лични данни след приключване на услугите по обработване, които са му възложени и да заличава/ унищожава съществуващите копия, освен ако правото на ЕС или правото на държава членка не изисква от него тяхното съхранение;

8.3.5.8. да осигурява достъп на Компанията до цялата информация, необходима за доказване изпълнението на задълженията, определени в настоящия член, и да позволява и допринася за извършването на одити, включително проверки, от страна на Компанията или друг одитор, оправомощен от него;

8.3.5.9. незабавно да уведомява Компанията, ако, според него, дадено нареждане нарушава Регламент 2016/ 679 или други разпоредби на ЕС или на националното законодателство относно защитата на лични данни.

8.3.6. Когато обработващ лични данни, на когото е възложено обработването на лични данни от името на Компанията чрез договор или друг правен акт, включва друг обработващ лични данни, за извършването на специфични дейности по обработване, на това друго лице се налагат същите задължения за защита на данните, като задълженията, предвидени в договора или акта, между Компанията и обработващия лични данни. Другият обработващ лични данни се задължава да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването, което той извършва, да отговаря на нормативните изисквания. При всички случаи, първоначалният обработващ данните носи пълна отговорност пред Компанията за изпълнението на задълженията на другия обработващ лични данни, на когото той е възложил извършването на специфични дейности по обработване.

8.3.7. Обработващите лични данни от името на Компанията, носят по презумпция солидарна отговорност за свързаните с това обработване процеси.

8.4. **Обработване, извършвано от името на Компанията, под ръководството на Компанията или на обработващ лични данни**

Обработващият лични данни и всяко лице, действащо под ръководството на или по възлагане от Компанията, или на обработващия лични данни, което има достъп до

личните данни, обработва тези данни само по указание на Компанията, освен ако обработването не се изисква от правото на ЕС или правото на държава членка.

8.5. **Сътрудничество с надзорния орган**

По искане на КЗЛД представители на Компанията и на обработващите лични данни, от името на Компанията, си сътрудничат с КЗЛД при изпълнението на нейните правомощия.

Раздел IX.

СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ И НАРУШЕНИЕ НА СИГУРНОСТТА

9.1. Компанията и обработващите лични данни от нейно име прилагат подходящи технически и организационни мерки за осигуряване ниво на сигурност, съобразено с рисковете с различна вероятност и тежест за правата и свободите на физическите лица.

9.2. Компанията и обработващите лични данни от нейно име предприемат действия, които да гарантират, че всяко физическо лице, действащо под ръководството на Компанията или на обработващия лични данни, от негово име, което има достъп до лични данни, обработва тези данни, само по указание на Компанията, освен ако от това лице се изисква да прави това по силата на правото на ЕС или правото на държава членка.

9.3. В случай на нарушение на сигурността на личните данни Компанията прилага утвърдена Процедура за действие при нарушение на сигурността на личните данни и за уведомление за нарушение;

9.4. Обработващият лични данни от името на Компанията уведомява Компанията, без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

Раздел X.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

10.1. Компанията определя длъжностно лице по защита на личните данни, публикува неговите данни за контакт на сайта на Компанията и ги съобщава на КЗЛД.

10.2. Компанията гарантира, че длъжностното лице по защита на данните участва по подходящ начин и своевременно при решаването на всички въпроси, свързани със защитата на личните данни.

10.3. Компанията и обработващите лични данни от нейно име подпомагат длъжностното лице по защита на данните, при изпълнението на посочените в т.10.8., функции, като осигуряват ресурсите, необходими за изпълнението на тези функции, осигуряват му достъп до съответните регистри, лични данни и операции по обработване. Компанията осигурява на длъжностното лице по защита на данните възможности, в това число и финансови, да развива и поддържа своите експертни знания.

10.4. Компанията и обработващият лични данни от нейно име правят необходимото, така че длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на функциите си. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от Компанията за изпълнението на своите функции. Длъжностното лице по защита на данните отчита своята дейност пред Управителния съвет на Компанията.

10.5. Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права.

10.6. Длъжностното лице по защита на данните спазва конфиденциалност и поверителност при изпълняване на своите функции, в съответствие с правото на ЕС или националното законодателство.

10.7. Длъжностното лице по защита на данните може да изпълнява и други функции и задължения. Компанията прави необходимото, така че тези допълнителни функции и задължения да не водят до конфликт на интереси с дейността му по защита на личните данни.

10.8. Основни функции и задължения на длъжностното лице по защита на данните са:

10.8.1. да информира и консултира Компанията или обработващите лични данни от нейно име, включително служителите, които извършват обработване, за техните задължения по силата на Регламент 2016/ 679 и на други разпоредби на европейското и национално законодателство, касаещи защитата на лични данни;

10.8.2. да съблюдава за спазването на Регламент 2016/ 679, на други разпоредби на европейското и национално законодателство и на вътрешните правила на Компанията или обработващия лични данни, от нейно име, по отношение на защитата на личните данни, включително да следи за възлагането на отговорности във връзка с обработването на лични данни, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване и съответните одити;

10.8.3. при поискване, да предоставя консултации по отношение на оценката на въздействието върху защитата на данните и съблюдава за извършването на оценката, съгласно чл. 35 от Регламент 2016/ 679;

10.8.4. да си сътрудничи с КЗЛД от името на Компанията;

10.8.5. да действа като точка за контакт за КЗЛД по въпроси, свързани с обработването, включително при предварителната консултация по смисъла на чл. 36 от Регламент 2016/ 679, както и по целесъобразност, се консултира, с КЗЛД по всякакви други въпроси.

10.9. При изпълнението на своите функции, длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

Настоящата Политика е приета от Управителния съвет на ПОК „Доверие“ АД, с решение по Протокол № 361 от 22.05.2018 г. и има действие от 25.05.2018 г.