

**ПОЛИТИКА ЗА ПОВЕРИТЕЛНОСТ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
НА
"ПЕНСИОННО ОСИГУРИТЕЛНО ДРУЖЕСТВО - БЪДЕЩЕ" АД**

ИНФОРМАЦИОННА КАРТА

Дата на приемане на документа: Дата на влизане в сила:	04.09.2018 г. В сила от 01.10.2018 г.
Версия на документа: В сила от:	1.0
Структура/лице издател на документа	Длъжностно лице за „Защита на данните“/Раина Иванова/ Съгласувал: Функция за вътрешен контрол / Фросита Френкова Юрисконсулт: Ива Наумова
Срок на валидност на документа:	Безсрочен
Одобрено от/на:	Съвет на директорите/ 04.09.2018 г.

СЪДЪРЖАНИЕ:

Кои сме ние?

Какво представлява настоящия документ?

Определения

Принципи

За какви цели и на какви основания обработваме лични данни?

На кого предоставяме лични данни?

Задължения на трети лица, действащи като администратори или обработващи лични данни

Права на субектите на данни

Срокове за съхранение на личните данни

Сигурност и нарушение на сигурността

Кои сме ние?

„Пенсионно осигурително дружество – Бъдеще“ АД(наричано по-долу “Администратор” или “Дружеството” е дружество, извършващо дейност по допълнително пенсионно осигуряване по реда на Кодекса за социално осигуряване (КСО) въз основа на Лицензия №283-ПОД /30.07.2003 г., издадена от Комисията за финансов надзор. Дружеството е вписано в Търговския регистър при Агенция по вписванията с ЕИК131125704. Седалището и адресът на управление са: гр. София, ул. „Христо Белчев“ № 3, адрес за кореспонденция: гр. София, бул. „Христофор Колумб“ 43, интернет страница: www.budeshte.bg и телефон за контакт: 0700 14 250;E-mail: office@budeshte.bg.

При и за целите на осъществяване на основната си дейност, Дружеството събира, записва, организира, съхранява, използва, разкрива чрез предаване лични данни, което е известно като обработка на данни. Доколкото Дружеството решава как и защо се извършва обработката по смисъла на Общия регламент за защита на данните (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 (наричан по-нататък „ОРЗД“) то е администратор на лични данни.

Дружеството обработва лични данни при спазване на българското и общностното законодателство, вътрешните си документи и при спазване на международния стандарт за управление на сигурността на информацията ISO/IEC 27001:2013.

Съгласно законодателството за защита на данните, администраторите на лични данни трябва да са открити и да се отчитат пред отделните лица за това как данните се обработват. Дружеството е активно ангажирано да защитава неприкосновеността на личния живот на всички физически лица, чиито данни обработва и сме подготвили тази политика за поверителност, като част от мерките, които прилагаме за спазване на законовите ни задължения.

Какво представлява настоящия документ?

Настоящата политика има за цел да опише основните принципи и изисквания, приложими към предмета на дейност на дружеството, спазването на които гарантира защита на правата на физическите лица при обработка на лични данни.

Документът съдържа информация за категориите лични данни, за целите и основанията за тяхното обработване, срокът на съхранение и категориите получатели, на които могат да бъдат предавани лични данни на валидно законово основание.

Процедурите за упражняване на правата, с които разполагат субектите на данни, съгласно ОРЗД са предмет на самостоятелен документ - "Правила за упражняване правата на субектите на лични данни в ПОД- Бъдеще АД".

Политиката е предназначена за всички физически лица, чиито данни дружеството обработва в качеството си на администратор на лични данни, включително но неизчерпателно - членове на управителни и контролни органи, служители, кандидати за работа, осигурителни посредници - физически лица, лицата, които управляват и представляват осигурителни посредници-юридически лица, физически лица, упълномощени от осигурителни посредници - юридически лица, осигуряващите се в управляваните от Дружеството фондове за допълнително пенсионно осигуряване, служебно разпределени осигурени лица, осигурени лица, променили участието си от друг фонд в някой от фондовете, управлявани от Дружеството, пенсионери, наследници на пенсионери, пълномощници, законни представители на осигурени лица и други правоимащи, както и всички други физически лица, които влизат в контакт с Дружеството, включително като посетители на нашия корпоративен сайт, ползватели на мобилни приложения и/или други електронни услуги, и чиито лични данни се събират и обработват от Дружеството в хода на осъществяване на предмета му на дейност.

Определения

По смисъла на тази Политика:

1. **„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 ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държава членка.

2. **„Лични данни“** е всяка информация, въз основа на която може да бъде идентифицирано дадено физическо лице, 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, физиологическата, генетичната, психическата, умствената, икономическата, културната или социалната идентичност на това физическо лице;

3. **„Обработване на лични данни“** е 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.

4. „**Специални категории лични данни**“ означава лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице. Когато в настоящата политика се употребява терминът “специална категория лични данни” се има предвид само данни за здравословното състояние на физическото лице, доколкото Дружеството не обработва други видове данни от специална категория;

5. Термините “**обработващ лични данни**”, “**регистър с лични данни**”, “**съгласие на субекта на данните**”, “нарушение на сигурността на лични данни”, имат същото значение, което им е дадено за целите на ОРЗД;

6. „**Надзорен орган**“ означава Комисия за защита на личните данни, със седалище в гр. София, България

Принципи

Дружеството гарантира, че прилага необходимите мерки за защита на лични данни, включително гарантиране на сигурност и поверителност на обработваните лични данни, обработвано на лични данни е в степен, която е необходима и пропорционална на целите на обработката, както и че личните данни са:

а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели („ограничение на целите“);

в) подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) точни и ще бъдат поддържани в актуален вид с възможност за своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);

д) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни („ограничение на съхранението“);

е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

За какви цели и на какви основания обработваме лични данни?

ОРЗД изисква администраторите на лични данни да обработват лични данни само ако имат законно основание. В зависимост от категорията личните данни и причините за тяхната обработка, законното основание може да бъде различно. Обичайната причина, поради която обработваме личните Ви данни е да можем да изпълняваме нашите законови задължения.

Дружеството обработва лични данни на осигурените лица както и на други физически лица /например осигурителни посредници-физически лица или наследници на осигурени лица и т.н./ във връзка с дейността по допълнително пенсионно осигуряване в изпълнение на разпоредбите на КСО, ДОПК, съответните подзаконови актове, включително указанията и/или разпоредженията на Надзорния орган и други държавни институции (Комисия за финансов надзор(КФН), Национална агенция за приходите(НАП), Национален осигурителен институт(НОИ) и др.)

Основанията за обработване на Вашите лични данни са:

А) Сключване и изпълнение на договор, по който субектът на данни е страна или за предприемане на стъпки по искане на субекта на данните преди сключването на договор, включително в събрани данни в процедури за подбор на персонал, трудови правоотношения, договори за осигурително посредничество и други;

Предоставянето на лични данни за сключване на договор съгласие за обработване на Вашите лични данни не е необходимо за допълнително пенсионно осигуряване е задължително Ако Дружеството не може да обработва тези лични данни, няма да можем да Ви предоставим услугата по допълнително пенсионно осигуряване.

Б) Спазване на законово задължение, което се прилага спрямо Дружеството, включително предоставяне на информация на органите на властта, във връзка с осъществяване на данъчно-осигурителен, финансов, и други видове контрол, както и във връзка с разпоредбите за предотвратяване и разкриване на измами и пране на пари, избягване на конфликт на интереси, оценка на риска.

Дружеството обработва лични данни в изпълнение на законови задължения и когато обработва данни, определени съгласно Член 9 от ОРЗД като "специална категория лични данни" - данни за здравословното състояние, като обработването е необходимо за целите на изпълнение на задълженията и упражняването на специалните права на администратора по силата на трудовото право и правото в областта на социалната сигурност и закрила.

Дружеството е поднадзорно на КФН лице и дейността му подлежи на надзор и проверки в хода, на които също могат да бъдат обработвани лични данни.

В) За целите на легитимни интереси на Дружеството. Възможно е обработване на лични данни за гарантиране на сигурността на информационната система, включително при одитиране на дружеството за поддържане на международния стандарт за управление на сигурността на информацията ISO/IEC 27001:2013.

Г) С цел установяване, упражняване или защита на правни претенции, защита на права пред правораздавателни юрисдикции и органи за извънсъдебно разрешаване на спорове се обработват лични данни. В такива случаи дружеството може да използва адвокати, консултанти и други наети лица.

Д) Лични данни се обработват и в процеса на изготвяне на статистически и финансови анализи, необходими за да се формират нашите инвестиционни решения и актюерски анализ.

Е) В случай, че сте осигурено лице в управляваните от Дружеството фондове или сте подали заявление за упражняване на някое от правата по КСО и Наредба № 3 от 24.09.2003 г. и Наредба № 33 от 19.09.2006 г. на КФН, можем да Ви предоставим друга информация за продукти или услуги, които вие поискате от нас или които смятаме, че може да ви интересуват, когато сте се съгласили да се свържем с Вас за такива цели на електронния Ви адрес. Може също така да използваме Вашите данни, за да ви предоставим информация за услуги от нашите партньорски организации във връзка с програмата "Клубна карта", в случай, че сте предоставили изрично съгласие като сте станали част от програмата.

На кого предоставяме лични данни?

ПОД Бъдеще гарантира, че личните Ви данни ще бъдат обработвани само за целите и на основанията, посочени по-горе. Във връзка с изпълнение на тези цели, данните Ви могат да бъдат предоставяни на трети лица, действащи като администратори или обработващи лични данни, включително:

А) Държавни и други публични органи, други пенсионноосигурителни дружества, банки, служби по трудова медицина, доставчици на пощенски услуги;

Б) Одитори, адвокати, компании, на които е възложена определена дейност като поддръжка на IT-системи, поддръжка на архив и други.

Задължения на трети лица, действащи като администратори или обработващи лични данни

Ако сте страна по договор с „ПОД Бъдеще“ АД в качеството на администратор или обработващ лични данни, очакваме от Вас да спазвате разпоредбите за защита на личните данни и да сте привели дейността си в съответствие с изискванията на ОРЗД и националното законодателство.

ОРЗД изисква да се съобщава значителна допълнителна информация на субектите на данни за това как ще се използват техните данни и за техните права. Вашите уведомления към субектите на данни трябва да отговарят на тези изисквания.

Ако събирате лични данни от името на „ПОД Бъдеще“ АД, в качеството на обработващ лични данни (например: ако сте осигурителен посредник), трябва да гарантирате, че информацията за субекта на данни обхваща прехвърлянето на личните данни към ПОД Бъдеще АД и ползването им от нас. Може да поискаме да направите промени в Уведомление за поверителност или друг подобен документ, ако сметем, че текстът не обхваща тази или друг изискуема от ОРЗД информация.

Също така, трябва да сте сигурни, че притежавате подходящи процеси и технически решения, за да можете да спазвате правата на субектите на данни в съответствие ОРЗД, както и без забавяне да уведомявате Длъжностното лице по защита на данните на ПОД Бъдеще АД за всяко заявление получено директно от субект на данни, когато личните данни които са предметът на заявлението се държат от ПОД Бъдеще АД.

Необходимо е да осигурите прехвърлянето на лични данни да се извършват чрез прилагане на подходящи технически мерки за опазване на данни,. При групово прехвърляне на лични данни между нас или за редовно прехвърляне на данни, следва да се използват инструменти за сигурно прехвърляне на файлове.

Ако обработване лични данни в качеството на обработващ лични данни, за които ПОД Бъдеще АД е администратор, следва да осигурите възможност за проверки и одитиране на дейностите по обработка, включително чрез използване на въпросници и проверки и одити на място.

Всички Ваши служители които боравят с лични данни, трябва да са преминали обучение за обработване на лични данни в съответствие с правната рамка.

Дори когато обработвате лични данни на собствено основание и определяйки сами целта на обработка ще очакваме от Вас в хода на договорното си отношение с ПОД Бъдеще АД да ни уведомявате в случай на нарушение на сигурността, което може да засегне осигурени лица и пенсионери на управляваните от Дружеството пенсионни

фондове, наши служители или могат да бъдат свързани с Дружеството по начин, който сериозно да накърни репутацията му.

В хода на упражняване на правата на субектите, включително правото да се търси обезщетение и отговорност за причинени вреди всяка страна ще дължи на насрещната разумна подкрепа и съдействие

Лични данни не трябва да се държат по-дълго от времето необходимо за изпълнение на целта за която са получени. Щом завърши периодът на съхранение, трябва да заличите или анонимизирате данните по сигурен начин. Когато това е свързано с данни, обработвани по възлагане на ПОД Бъдеще АД трябва да се уверите, че действията Ви са в съответствие с изискванията за унищожаване на Дружеството, както и да сте в състояние да предоставите доказателства за унищожаването, съответно анонимизирането.

Дружеството ще има право да прекрати договор с обработващ лични данни, когато обработващият не отговаря на изискванията на съответствие с ОРЗД и изискванията на местното законодателство в областта на защита на данните.

Права на субектите на данни

Субектите на лични данни имат следните права:

- А) Право да получат информация на ясен и разбираем език кой, как и защо обработва данните им;
 - Б) Право на достъп до данните, свързани с него, които се обработват от администратора, включително копие на данните, които са в процес на обработване;
 - В) Право на коригиране на неточни данни, попълване на непълни лични данни, включително чрез декларация
 - Г) Право на изтриване (право "да бъдеш забравен")
 - Д) Право на ограничаване на обработването
 - Е) Право на преносимост на данните в структуриран, използван и пригоден за машинно четене формат, когато това е технически осъществимо
 - Ж) Право на възражение, включително срещу автоматизирано вземане на решение, включително профилиране;
- Към датата на изготвяне на този документ Дружеството не прилага процеси за автоматизирано вземане на решения.
- З) Право да оттегли съгласието си по всяко време, когато обработването се основава само на съгласие.
 - И) Право на жалба до дружеството и до надзорния орган - Комисия за защита на личните данни(КЗЛД), или по съдебен ред за обезщетение за претърпени материални и нематериални вреди.

Жалба до дружеството се подава на адреса за кореспонденция:
Гр. София, бул. „Христофор Колумб“ 43, E-mail: office@budeshte.bg.

Жалба до КЗЛД се подава на адрес:
Гр. София 1592, бул. "Проф. Цветан Лазаров" № 2, e-mail: kzld@cpdp.bg.

Редът и условията, при които могат да бъдат упражнени тези права са уредени в ОРЗД и в Правила за упражняване на правата на субектите на лични данни в ПОД Бъдеще АД, с които можете да се запознаете на официалната интернет страница на дружеството - www.budeshte.bg, както и в централния офис на дружеството на адрес -гр. София, бул. Христофор Колумб 43, ет.7.

Упражняването на правата е поставено в зависимост от определени обстоятелства като целта и основанието на обработка, и регламентираните срокове на съхранение, които могат да бъдат от значение за разглеждането на подадено искане.

Срокове за съхранение на личните данни

ПОД Бъдеще АД съхранява лични данни, във форма която позволява идентифициране на субекта на данните за период не по-дълъг от необходимото за целите, за които се обработват данните.

При определяне на срокове на съхранение на данните се взема предвид наличието на нормативно регламентиран срок или се извършва преценка за определяне на разумен срок на съхранение, която се документира.

„ПОД-Бъдеще“ АД съхранява лични данни на осигурените лица, пенсионери и други правоимащи по осигурителен, съотв. пенсионен договор, съобразно нормативно определените срокове, например:

А) Личните Ви данни ще бъдат съхранявани за срок от 50 години след прекратяване на осигурителното правоотношение с Дружеството на основание на чл. 123и¹ от Кодекса за социално осигуряване. Когато в дружеството е подадено заявление за промяна на участие, съответно – за прехвърляне на средства, заявлението и свързаните с него документи и съдържащите се в тях лични данни се съхраняват през целия период на съществуване на осигурителното правоотношение с осигуреното лице, а в случаите, когато заявлението е било анулирано или процедурата прекратена – за срок не по-малък от две години, на основание на Наредба № 3 от 24.09.2003 г. и Наредба № 33 от 19.09.2006 г. на Комисия за финансов надзор.

Б) Когато лични данни се обработват на основание сключен трудов договор, договор за възлагане на управлението или граждански договор с физическо лице, разплащателните ведомости и всички документи, удостоверяващи трудов и осигурителен стаж, включително документи за неплатени отпуски за срок по-дълъг от 30 дни се съхраняват 50 години,

съгласно Закона за счетоводството, Данъчно-осигурителния процесуален кодекс и Кодекса за социално осигуряване.

Данните не се обработват повторно за цели несъвместими с първоначалната цел.

Сигурност и нарушение на сигурността

Дружеството прилага подходящи технически и организационни мерки за гарантиране на сигурността на данните като взема предвид рисковете, свързани с обработването.

Системата за управление на информацията е сертифицирана по международно признатия стандарт ISO/IEC 27001.

Съгласно приетите политики и правила за управление на информационната сигурност се прилагат правила за физически и логически достъп до помещения и системи, политика за "чисто бюро" и "чист екран", съхранение и обмяна на данни само в защитена среда.

Всички служители на Дружеството, на които е възложено да обработват лични данни са задължени по закон да спазват конфиденциалност относно непубличната информация, свързана с дейността по допълнително пенсионно осигуряване, осигурените лица и пенсионерите.

Всички договори с други администратори и обработващи лични данни, подлежат на преглед и актуализация, когато и в случай, че е необходимо да се предвидят клаузи за защита на правата на субектите на лични данни.

Настоящата политика е приета на 04.09.2018 г. с Решение на Съвета на директорите на ПОД Бъдеще АД и влиза в сила на 01.10.2018 г. Политиката се преразглежда периодично и всяка промяна ще бъде оповестявана чрез официалната интернет страница на Дружеството - www.budeshte.bg.