Пенсионноосигурително дружество

„Топлина“ АД

Правилник за

защита и обработване на личните данни

на

ПОД „Топлина“ АД

НОЕМВРИ, 2019 г.

Съдържание:

Раздел I. Речник на термините

1. „***Лични данни***” са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („***субект на данни***“). Физическото лице, 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 лице;

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;

3. „***Регистър на лични данни***" е всяка структурирана съвкупност от лични данни, достъпът до които се осъществява, съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен, съгласно функционален или географски принцип;

4. „***Съгласие на субекта на данните***" („***информирано съгласие***”) 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;

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;

6. „***Администратор на лични данни***“ е физическо или юридическо лице, публичен орган, или друга структура, което само 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 Европейския съюз (ЕС) или правото на държава-членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

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

8. „***Получател***“ означава физическо или юридическо лице, публичен орган или друга структура, пред които 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 II. Предмет, цели и обхват на Правилника

Чл.1. Пенсионноосигурително дружество „Топлина“ АД (по-долу ПОД, ПОД „Топлина АД“ или дружеството) е учредено с решение на Общото събрание на акционерите на 24.01.2006 г. и е лицензирано под № 02-ПОД/17.08.2006 г. за извършване на дейност - допълнително пенсионно осигуряване от Комисията за финансов надзор на 17.08.2006 г. Дружеството е вписано в Търговския регистър при Агенция по вписванията с ЕИК 175137918. Седалището и адресът на управление са: гр.София 1360, Индустриална зона „Орион“, ул.„3020“, №34, ет.8. Предметът на дейност на дружеството е допълнително пенсионно осигуряване.

Чл.2. ПОД „Топлина“ АД е администратор на лични данни по смисъла на ЗЗЛД и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на лични данни на физическите лица и относно свободното движение на такива данни в Европейския съюз и страните от ЕИО (наричан по-долу „Регламента“ или „GDPR“, или Регламент 2016/679). Дружеството събира и обработва лични данни свързани с дейността му – допълнително пенсионно осигуряване, съгласно българското и европейското законодателство и международните стандарти по сигурността на информацията, както и съгласно вътрешните си правилници и правила, за да гарантира защитата на физическите лица във връзка с обработването на лични данни.

ПОД „Топлина“ АД е сертифицирано по ISO/IEC 27001:2013 относно управление сигурността на информацията.

Чл.3. „Правилник за защита и обработване на личните данни“ е част от цялостната дейност на дружеството по гарантиране на едно от основните права на физическите лица – защита на личните им данни. Правилникът точно и ясно дава информация за категориите лични данни, за целите и за правното основание за обработване, за какъв срок се съхраняват, информация за това дали личните данни ще бъдат предадени на трето лице и при какви условия и ред, а също и за получателите или категориите получатели на лични данни. Правилникът дава и изчерпателна информация относно правата, с които разполагат субектите на данни съгласно законодателството в сферата на защитата на лични данни и предвид новите положения съгласно Регламента.

Чл. 4. Персонален обхват - настоящият Правилник е предназначен за субектите на права - за служителите на ПОД „Топлина“ АД, вкл. осигурителните посредници, осигуряващите се в управляваните от дружеството фондове за допълнително пенсионно осигуряване, вкл. служебно разпределени или променили участието си от друг фонд в някои от управляваните от ПОД „Топлина“АД фондове за допълнително пенсионно осигуряване, пенсионери, наследници, пълномощници, попечители, настойници и други физически лица, които имат

правен интерес относно личните данни, които може да са събрани от дружеството, във връзка с пенсионноосигурителната му дейност (по-долу „служители“ и/или „осигуряващи се лица“).

Чл.5. Принципи и цели - определят се и основни принципи и правила, свързани с обработването на лични данни, правата на субектите на тези данни, задълженията и отговорността на дружеството, като администратор на данни, съответно на служителите му, в качеството им на обработващи данни, както и функциите на длъжностното лице по защита на личните данни.

Чл.6. Цели на обработване на информацията - спазване правата на физическите лица относно личните данни чрез система от технически, организационни и функционални мерки, засягащи сигурността на информацията. Правилникът гарантира, че служителите, осигурителните посредници и всички физически и юридически лица, работещи от името на дружеството и/или за негова сметка и обработват лични данни на субектите на правата, ще изпълняват стриктно разпоредбите на настоящия правилник, законите на Република България и правото на ЕС.

Основни цели:

1. Пенсионноосигурителна;
2. Охрана на зони и помещения;
3. Гарантиране на сигурността;
4. Встъпване и управление на взаимоотношения със служители и контрагенти;

Чл.7. Нарушаването на правилата по прилагането на този правилник, съответно нарушената защита на лични данни би представлявало сериозен риск за правата на носителите на субективните права, респективно за дружеството и неговите акционери.

Чл.8. Дружеството приема този Правилник, свежда го до знанието на всички свои служители, вкл. осигурителните посредници, провежда разяснителна кампания по прилагането му, качва го на интернет страницата си, с цел да подпомогне служителите по отношение на работата им, както и довежда основните положения от разпоредбите му на лицата по чл. 4, относно защитата на личните данни и техните права, включително чрез събиране на информирано съгласие (Раздел I, т.4.).

Раздел III. Принципи при обработването на лични данни

Чл.9. Принцип на законност - дружеството обработва лични данни (вж. Речник на термините, Раздел I, т.2) в съответствие със законодателството на Република България и Европейския съюз, както и в съответствие със своите вътрешни актове.

Чл.10. Правни основания (алтернативно или кумулирано):

1. Когато е необходимо да се спази законово задължение на ПОД относно събиране и обработване на лични данни;

2. Когато субектът на личните данни е дал информирано съгласие за една или повече цели, (вж. Раздел I, т.4) писмено или чрез електронен подпис или други технически способи, които гарантират изразената му воля;

3. Когато субектът на данните е странна по договор с ПОД, или са предприети стъпки за сключване да такъв договор, договори за изплащане на средства, договори с осигурителни посредници, трудови договори;

4. В изпълнение на задача от обществен интерес, в това число и обработване и предоставяне на информация на органите на държавната власт при поискване от дружеството (данъчно-осигурителен, трудов и финансов контрол);

5. Необходимо е да бъдат защитени жизненоважни интереси на лицето, субект на данните, неговите пълномощници, наследници, настойници и попечители или друго физическо лице;

6. За предоставяне на информация на съда и трети лица (юристи, адвокати, вещи лица и др.), в рамките на производство пред съд, съдебен арбитраж или помирителна комисия, съобразно изискванията на приложимите към производството процесуални и материални нормативни актове;

7. Защитата на личните данни за ненавършили 18 години деца е преимуществен приоритет на дружеството.

Чл.11. Законосъобразност на обработката на лични данни по отношение на осигурените лица във фондовете за допълнително пенсионно осигуряване на дружеството, доколкото дружеството обработва лични данни, свързани с дейността му като пенсионноосигурително дружество по допълнителното пенсионно осигуряване и в изпълнение на законовите си задължения, произтичащи от:

1. Кодекс за социално осигуряване, в това число и актовете на Комисията за финансов надзор по изпълнение на разпоредбите на КСО, Данъчно-осигурителен процесуален кодекс (ДОПК), актовете на Националната агенция за приходите (НАП), както и всички други законови и подзаконови нормативни актове, приложими към дейността на дружеството;

2. Надлежно попълнени и подадени документи от осигуреното лице:

а) Осигурителен договор;

б) Пенсионен договор;

в) Молба за изплащане на средства;

г) Заявление за промяна на участие във фонд за допълнително задължително пенсионно осигуряване, Заявление за прехвърляне на средства във фонд за допълнително доброволно пенсионно осигуряване, Искане за оттегляне на заявление за промяна на участие/за прехвърляне на средства;

д) Заявление за участие във фонд за допълнително задължително пенсионно осигуряване, Заявление за възобновяване на осигуряването във фонд за допълнително пенсионно осигуряване;

е) Заявление за достъп до лични данни;

ж) Други документи, свързани с упражняването на права от субектите съгласно КСО или друг законов/подзаконов нормативен акт;

3.Обработка на данни на субекта в изпълнение на законово задължение на дружеството, включително входящи и изходящи данни:

а) Данни, документи, информация в електронен или хартиен вид, постъпващи в дружеството от НОИ, НАП, друг орган на държавната власт или друго пенсионноосигурително дружество, във връзка с изпълнение на законови задължения;

б) Данни, документи и информация за осигуреното лице, които съответният фонд предоставя във връзка с изискванията на закона към НАП, НОИ, друг орган на държавната власт или друго пенсионноосигурително дружество.

4. Удостоверение за наследници, удостоверение за идентичност, пълномощни и др.

Чл.12. Законосъобразност на обработката на лични данни на служители и осигурителни посредници на ПОД „Топлина“ АД:

1. Относно служителите и ФЛ по договор за услуга:

Данни съгласно трудов договор, включително длъжностни характеристики и изискванията по Кодекс на труда, други според изискванията на данъчното и осигурителното право съгласно КСО и ДОПК, както и договорите за управление и договорите за услуга

2. Относно осигурителните посредници:

ПОД „Топлина“ АД събира лични данни на осигурителните посредници във връзка с осъществяването на дейността им, съгласно КСО и други приложими закони в осигурителното и данъчното право

Чл. 13. Принципи на добросъвестност, прозрачност и съразмерност на обработването на лични данни:

1. Принцип на добросъвестност – дружеството ще се ръководи от принципа на добросъвестността с оглед защитата и на личните данни, като основно право на физическите лица:

а) Чрез разяснителни кампании, семинари, обучения, инструкции, техническа и ръководна помощ;

б) Чрез въвеждане на вътрешна нормативна уредба и последващ контрол с цел опазването на личните данни.

2. Принцип на прозрачност – дружеството ще се ръководи от отвореността и прозрачността по отношение на защитата на личните данни, като основно право на физическите лица:

а) ПОД „Топлина“ АД ще информира лицата по Раздел II, чл. 4 своевременно, ясно, точно и коректно относно събираните им лични данни и тяхната обработка, включително и чрез публикуването на този Правилник в интернет страницата на дружеството;

б) Дружеството предоставя на физическото лице всякаква информация относно събраните за него на лични данни, както и за правните възможности за ограничаване събирането и обработката на данни.

3. Съразмерност на обработваните данни – дружеството обработва лични данни въз основа на легитимни цели и съгласно българското, европейското законодателство и вътрешната си уредба. ПОД „Топлина“ АД не събира, обработва и оперира по-нататък с лични данни, несъвместими с основната си дейност и този Правилник.

Чл. 14. Съотносимост с целите на обработката и свеждане до минимум на събираните данни - дружеството обработва лични данни, съотносими с целите по Раздел I, т.6. Събирането на данни е ограничено до необходимото с оглед постигане на целите.

Чл. 15. Точност и актуалност на данните - дружеството поддържа точни и актуални данните, с които разполага, като се има предвид спецификата на дейността, като:

1. Осигурява по подходящ начин възможност за корекция и изтриване на данните, ако е необходимо;

2. Поддържа точни и актуални данните за да изпълни коректно задълженията си към лицата по Раздел II, т.4.

Чл.16. Срокове на съхранение на лични данни - съхраняването на лични данни от ПОД „Топлина“ АД се извършва за сроковете, установени в действащото в страната законодателство, свързано с конкретния вид взаимоотношения и от регулаторните и надзорни органи:

1. Лични данни, за които липсва изрично законово или надзорно задължение за съхранение, ще бъдат изтривани, анонимизирани (необратимо заличаване на всички идентификационни данни на субекта, така че те да не могат да доведат последствие до неговата идентификация), псевдонимизирани (данните не могат да бъдат повече свързани със субекта на правото) или унищожени след постигане на целите, за които са събрани и са се обработвали, освен в случаите когато са необходими за висящо съдебно или административно производство или производство по разглеждане на жалба пред дружеството;
2. Ако за дадена дейност по обработка са приложими няколко нормативни изисквания относно сроковете за съхранение на данните, то срокът се определя от нормативният акт, поставящ изисквания за по-дълъг срок на съхранение. Също така срокът за

обработка на определени данни може да бъде, както намаляван – например по възражение на субекта на данните (ако е приложимо), така и увеличаван – например по указания на компетентни органи във връзка с осъществяваните от тях законосъобразни действия.

Чл.17. 1) Законови срокове за съхраняване на личните данни за осигурени лица – 50 (петдесет) години (съгл. чл.123и и следващи КСО) от датата на прекратяване на осигурителното правоотношение на оригиналите на хартиен и/или електронен документ (вж. примерно изброени в Раздел III, чл. 11) и поне 2 (две) години, когато субектът на правото е подал заявление за промяна на участие от пенсионен фонд, управляван от друго пенсионноосигурително дружество, в съответен фонд, управляван от ПОД „Топлина“ АД или е подало заявление за подновяване на осигуряването, но субектът на правото не е станал клиент на дружеството.

2) Законови срокове за съхраняване на личните данни на служители – не по кратък от 50 (петдесет) години за разплащателните ведомости и всички документи удостоверяващи осигурителен и трудов стаж, в това число и неплатени отпуски за срок по-дълъг от 30 (тридесет) дни и 5 (пет) години за останалите документи в трудовото досие от прекратяване на трудовото правоотношение, съгласно изискванията на Кодекс на труда, Данъчно-осигурителен процесуален кодекс, Закона за данъците върху доходите на физическите лица, Закона за счетоводството и Наредбата за трудовия стаж и трудовата книжка (напр. трудови досиета и документи, удостоверяващи изплатени възнаграждения).

3) Законови срокове за съхраняване на личните данни на осигурителните посредници – дружеството съхранява договорите с осигурителните посредници и свързаните с тях книжа – за целия срок на тяхното действие. Документи, удостоверяващи изплатени възнаграждения на осигурителния посредник се съхраняват не по-малко от 50 (петдесет) години от датата на прекратяване на съответното правоотношение съгл. ДОПК, ЗДДФЛ и Закона за счетоводството.

Чл.18. Поверителност, цялостност и наличност - в своята дейност дружеството обработва събраните лични данни в съответствие с принципите на поверителността, целостта и наличността. Дружеството прилага подходящи мерки срещу неразрешено, незаконосъобразно обработване на лични данни, в това число и срещу загуба, унищожаване или повреждане, като съблюдава изискванията на ISO/IEC 27001:2013 относно управление сигурността на информацията.

Раздел IV. Лични данни, обработвани от ПОД „Топлина“ АД

Чл.19. Лични данни според източника:

1. Лични данни, предоставени от субекта на правото (физическото лице) – данни, които субектът на данните предоставя чрез договор, заявление, във връзка с упражняване на пенсионноосигурителни права;

2. Лични данни на субекта на правото (физическо лице), предоставени от други източници – дружеството обработва данни за лицата, предоставени от държавни институции (НОИ, НАП, КФН и др.), както и от други пенсионноосигурителни дружества в предвидените от закона случаи.

Чл 20. 1) Лични данни според субекта:

1. Осигурителни посредници – дружеството обработва данни на осигурителните посредници-физически лица, осигурителни посредници-юридически лица, както и на физическите лица, упълномощени от осигурителни посредници – юридически лица при спазване на договорите, нормативната уредба и актовете на КФН;

2. Служители – дружеството обработва лични данни на своите служители при спазване на нормативната уредба и съгласно актовете на НАП и НОИ.

2) Като пенсионноосигурително дружество, осъществяващо допълнително пенсионно осигуряване ПОД „Топлина“ АД обработва данни на осигуряващите се лица, в това число и за бивши участници във фондовете на дружеството, съгласно нормативната уредба и актовете на КФН и НАП.

Чл.21. (1) Лични данни, които дружеството събира:

1. Идентификационни данни – три имена, ЕГН или ЛНЧ; данни от лична карта и снимка (копие на л.к., когато се изисква по закон); дата и място на раждане, в това число и за наследници, пълномощници и законни представители;

2. Информация за контакт – постоянен адрес или адрес за кореспонденция, телефонен номер, имейл адрес;

3. Финансова информация – индивидуална осигурителна партида – вноски, разпределена доходност, удържани такси, данъци, суми, за които е ползвано данъчно облекчение, суми, за които не е ползвано данъчно облекчение, източник на осигурителните вноски, изтеглени суми, прехвърлени суми, определена или получена пенсия, данни за банкова сметка при плащания по банков път, данни за свързани лица, заемащи висша държавна длъжност, гражданство, държава на постоянно пребиваване; професионална дейност крайни собственици на клиент ЮЛ, произход на средствата; данни за заплатите и осигуровките на служителите и осигурителните посредници;

4. Информация, свързана със законовите изисквания, съгласно Закона за мерките срещу изпирането на пари и Закона за мерките срещу финансирането на тероризма.

(2) Дружеството не обработва повторно данните за лицата и не предоставя на трети лица повторно обработена информация.

Чл.22. 1) Специална (чувствителна) информация и данни, които дружеството събира в предвидените от закона случаи:

1. Данни за здравословното състояние на служителите – събира се в предвидените от закона случаи;

2. Във връзка с нормативни изисквания при постъпване на работа/назначаване;

3. За целите на здравословните и безопасни условия на труд и трудовата медицина;

4. Във връзка с предвидените в КСО осигурителни случаи - временна или трайно намалена неработоспособност, майчинство (бащинство) и упражняването на съответните права;

5. Във връзка със закрилата при прекратяване на трудовото правоотношение.

2) Данни за здравословното състояние на осигурените лица – събират се в предвидените от закона случаи, предоставят се от осигурените лица, за да удостоверят трайно намалена работоспособност, във връзка с правото на изплащане на суми от фонд за допълнително пенсионно осигуряване (ТЕЛК, НЕЛК, ЛКК, други, ако са предвидени в нормативен акт).

Чл.23. 1) Информирано съгласие за обработване на лични данни на осигурени лица не се събира:

1. За сключване, администриране и изпълнение на договори за допълнително задължително пенсионно осигуряване, когато субектът на личните данни е страна по договора , освен в случаите когато се обработва чувствителна лична информация или лицето не е навършило 18 години;

2. За сключване, администриране и изпълнение на договори за допълнително доброволно пенсионно осигуряване, когато субектът на личните данни е страна по договора, освен в случаите когато се обработва чувствителна лична информация;

3. Събиране на дължими вземания, съдебни и помирителни процедури за защита на законни интереси на дружеството и/или осигурените лица/пенсионери;

4. За „таргетиране и реклама чрез персонализирана оферта“, „автоматично обработване и профилиране“, “повторно обработване на информация и предоставянето ѝ на трети лица“, защото дружеството не обработва такава информация;

5. Установяване и предотвратяване на опити за измами и спазване на законови задължения, като например, но не само данъчни, счетоводни, мерки срещу предотвратяване на изпирането на пари и други, тъй като това са законови задължения за дружеството;

2) Информирано съгласие се взема от служителите, осигурителните посредници, доколкото дружеството като администратор на лични данни може по силата на свое законово и/или договорно задължение да се сдобие с чувствителна за тези лица информация.

Раздел V. Информация, предоставяна от ПОД „Топлина“ АД при обработване на лични данни

Чл.24. 1) В случаите когато субект на лични данни ги предоставя на ПОД „Топлина“ АД, дружеството му предоставя информация относно:

1. Наименование на дружеството, ЕИК, адрес, телефон и e-mail за контакти;

2. Длъжностното лице по защита на личните данни и координати – телефон и/или e-mail;

3. Цели и правно основание за обработката на лични данни;

4. Получателите, на които данните на субекта могат да бъдат разкрити;

5. Информира субектите относно правото им да бъдат забравени, коригиране или изтриване на лични данни, както и правото на възражение;

6. Срокът за съхраняване на данните, съгласно предвиденото в българското и европейското право и в този правилник;

7. Възможността за подаване на жалба до Комисията за защита на личните данни.

2) В случаите, когато личните данни на субекта ги предоставя трето лице – орган на държавната власт или друго пенсионноосигурително дружество, ПОД „Топлина“ АД предоставя информация за източника на данните, както и какви данни обработва, освен ако субектът на данните вече разполага с тази информация.

Раздел VI. Права на субектите на лични данни

Чл.25. Право на достъп – субектът на данни има право да получи от дружеството потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

1. Целите на обработването; съответните категории лични данни; категориите получатели, пред които са или ще бъдат разкрити те, включително получатели в трети държави или международни организации;

2. Предвидения срок, за който ще се съхраняват личните данни, съществуването на право да се изиска от администратора коригиране или изтриване на лични данни, ограничаване на обработването им, да се направи възражение срещу такова обработване;

3. Правото на жалба до надзорен орган; информация за източника на данни, ако не са събрани от субекта на данните; Дружеството предоставя копие от личните данни, което не следва да се отъждествява с понятието „копие от документи”. Правото може да се упражнява по начин, незасягащ правата и свободите на други субекти на данни.

Чл.26. (1)Право на коригиране - субектът на данни има право да поиска от ПОД да коригира неточните лични данни, свързани с него. Като се имат предвид целите на обработването, субектът на данните има право да поиска и непълните лични данни да бъдат попълнени, включително чрез чрез допълване на декларираните от лицето обстоятелства и факти.

Чл.27. Право на изтриване (право „да бъдеш забравен“) - субектът на данни има правото да поиска от ПОД изтриване на свързаните с него лични данни без ненужно забавяне, като то има задължението да го извърши, когато е приложимо някое от посочените по-долу основания:

1. Личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

2. Субектът на данните оттегля своето съгласие, върху което се основава обработването на данните, и няма друго правно основание за обработването;

3. Субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество; Личните данни са били обработвани незаконосъобразно (съгл. чл. 21, § 1 и 2, Регламент 2016/679);

4. Личните данни трябва да бъдат изтрити с цел спазването на правно задължение, което се прилага спрямо дружеството в качеството му на администратор на лични данни;

5. Личните данни са били събрани във връзка с предлагането на услуги на информационното общество;

6. Правото на изтриване не се прилага, когато обработването е необходимо за спазване на правно задължение и за установяването, упражняването или защитата на правни претенции.

Чл.28. 1) Ограничаване обработването на лични данни - когато обработването е ограничено, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции, за защита на правата на друго физическо лице или поради важни основания от обществен интерес. Когато субект на данните е изискал ограничаване на обработването, дружеството го информира преди отмяната на ограничаването на обработването. Субектите на данни трябва да имат предвид, че при реализиране на правото на ограничаване на обработването, е възможно продукти и услуги, за които са използвани личните данни, да бъдат преустановени, а съответните правоотношения прекратени.

2) Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването. Дружеството съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Дружеството информира субекта на данните относно тези получатели, ако те поискат това.

3) Субектът на данните има право да изиска от дружеството ограничаване на обработването, когато е приложимо едно от следните основания:

1. Точността на личните данни се оспорва от субекта на данните, за срок, който позволявана дружеството да я провери;

2. Обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

3. Дружеството не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

4. Субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на дружеството имат преимущество пред интересите на субекта на данните.

Чл.29. Право на субектът на лични данни да оттегли даденото информирано съгласие -субектът на данните може да оттегли своето съгласие, върху което се основава обработването на данните, освен ако няма друго правно основание обработването да продължи.

Чл.30. Право на преносимост, когато:
1. Когато обработването е основано на съгласие или договорно задължение и се извършва по автоматизиран начин, субектът на данните 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 правото да прехвърли тези данни на друг администратор без възпрепятстване от дружеството;

2. Когато упражнява правото на преносимост на данните, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо. Упражняването на правото на преносимост, не засяга правото на изтриване (правото „да бъдеш забравен“) и не следва да влияе неблагоприятно върху правата и свободите на други лица. За всеки конкретен случай на преносимост на лични данни се прилага специфичното законодателство, което го урежда.

Чл.31. 1) Право на възражение – субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на легитимните интереси на дружеството, включително за профилиране, основаващо се на легитимен интерес. Дружеството 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.

Чл. 32. Право на субекта на данните да не бъде обект на решение, основаващо се единствено на автоматизирано обработване – субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен. Правото не се прилага, ако:

1. Решението е необходимо за сключването или изпълнението на договор между субектна данни и дружеството; или

2. Е разрешено от законодателството; или

3. Се основава на изричното съгласие на субекта на данни.

Към момента на приемане на този Правилник, в ПОД „Топлина“ АД не съществуват процеси на автоматизирано вземане на решения.

Чл.33. Право на жалба – субектите на данни имат право на подаване на жалба до дружество, а също и пред контролния орган в Република България - Комисията за защита на личните данни или по съдебен ред, както следва:

1) Жалба до дружеството:
ПОД „Топлина“ АД, гр. София 1360, Индустриална зона „Орион“, ул.„3020“, № 34, ет.8, уебсайт с форма за контакти: https://www.pod-toplina.bg/

2) Жалба до КЗЛД
Комисия за защита на личните данни, София 1592, бул.„Проф. Цветан Лазаров”№2, e-mail: kzld@cpdp.bg , уебсайт: https://www.cpdp.bg/

Чл.34. (изм. с Решение на УС от 11.11.2019 г.)

1) Съобщаване на субекта на данните за нарушение на сигурността на личните данни - дружеството предприема всички необходими технически и организационни мерки за защита на личните данни. Въпреки това, при евентуален случай на нарушение на сигурността им дружеството ще предприеме нужните действия по съобщаване на субекта на данните за нарушението, съобразно изискванията на приложимото законодателство.

2) Заявленията за упражняване на правата на лицата във връзка със защитата и обработването на личните им данни, както и жалбите до дружеството се подават лично в териториалните подразделения на дружеството, а субекта на данните се идентифицира с документ, удостоверяващ неговата самоличност пред служителя/осигурителния посредник на дружеството; от изрично упълномощено лице, чрез нотариално заверено пълномощно, а пълномощникът се идентифицира с документ, удостоверяващ неговата самоличност пред служителя/осигурителния посредник на дружеството; по пощата с нотариална заверка на подпис на лицето, субект на данните; както и по електронен път, по реда на Закон за електронния документ и електронните удостоверителни услуги (чрез електронен подпис).

3) Лицата, които се ползват от правото си за корекция на лични данни, с цел дружеството да осигури цялостност и документираност на извършваните промени, както и с цел да се защитят осигурените лица от неправомерни действия, както и предвид законоустановеността на пенсионноосигурителните правоотношения, представят пред дружеството документ, удостоверяващ промяната на личните данни, например съдебно решение, удостоверение за идентичност, акт за гражданско състояние, и други, от което да е видно, че има законово основание за съответната корекция на събраните от дружеството данни.

4) Приложените копия на документи по ал. 3 се заверяват като лицето, което подава документите изписва върху тях пълното си име съгласно личната си карта, дата, текст „Вярно

с оригинала“ и подпис. Ако документите са нотариално заверени – не се изисква повторна заверка от лицето. Не се изисква заверка на документите в случаите, когато подадените искания/заявления/жалби са подписани с електронни удостоверителни услуги.

5) Правилата по ал. 2-5 се прилагат аналогично и при упражняване и на останалите права по този правилник, ако исканите действия могат да доведат до неблагоприятни последици като нарушаване неприкосновеността на личните данни, възможност от измами или други действия, които биха накърнили законните права и интереси на субектите на данни – осигурени лица и пенсионери.

Раздел VII. Задължения на дружеството при изпълнение на правата, посочени в раздел VI

Чл.35. 1) ПОД „Топлина“ АД предоставя всякаква информация относно този Правилник и защитата на лични данни в писмена и устна форма на физическото лице, субект на данните, при поискване и след като лицето се идентифицира.

2) Дружеството не може да откаже съдействие, освен ако лицето не се идентифицира или лицето което се идентифицира не е субект на данните и не е надлежно упълномощено, или закон или друг нормативен акт постановяват законови изисквания относно оперирането с даден тип данни.

3) Дружеството се произнася с мотивирано решение по исканията, заявленията и жалбите, предвидени по този правилник в едномесечен срок. Този срок може да бъде удължен с още 30 дни, ако случаят представлява правна и фактическа сложност.

4) Анонимни сигнали и съмнения в самоличността на лицето - дружеството може да откаже да разглежда искания, заявления и жалби, ако те са анонимни или ако има основателни съмнения в самоличността на лицето.

Раздел VIII. Отговорност на администратора на лични данни

Чл.36. ПОД „Топлина“ АД обработва лични в съответствие със Закона за защита на личните данни, Регламент 2016/679 и цялото приложимо право, уреждащо защитата при обработка на лични данни.

Чл.37. 1) Интегриран подход - дружеството разработва и внедрява подходящи правила и осигурява технически средства в съответствие с предмета на дейност на дружеството, спецификите на работния процес и рисковете, които могат да окажат въздействие върху субектите на лични данни.

2) Система за управление на сигурността - внедрената „Система за управление сигурността на информацията“, сертифицирана по стандарта ISO/IEC 27001:2013, показва отговорността на дружеството пред субектите на лични данни и гарантира в максимална степен спазването на правата им.

Чл.38. Обработване на лични данни:

1. Обработващи лични данни са всички служители и осигурителни посредници на дружеството, които обработват лични данни при или по повод на изпълнение на служебните си или договорни задължения.

2. Обработващи лични данни, са и всички физически и юридически лица, въз основа на сключени договори за възлагане на услуги (например агенции за подбор и наемане на персонал), които извършват услуги, свързани с обработването на лични данни (съгл. Речник на термините т.2), като:

а) Информационни технологии и бази данни, използвани от дружеството;

б) Дигитализация, актуализация, организация на информацията;

в) Унищожаване на данни от хартиен носител;

г) Здравно осигуряване и трудова медицина и др.

Чл.39. Когато дружеството възлага обработването на лични данни на друго физическо или юридическо лице по договор за услуга, обработващият информацията следва да представи достатъчно гаранции за прилагането на достатъчно технически и организационни мерки в съответствие с ЗЗЛД и Регламент 2016/679, за да се гарантират правата на субектите на лични данни.

Чл.40. 1) Разрешение за обработване на лични данни - обработващите лични данни по договор за услуга (съвместно администриране на данни) следва да получат писмено общо или изрично писмено разрешение за обработката на лични данни. Когато разрешението е общо, обработващият личните данни е длъжен да уведоми дружеството при промяна в персоналния състав на обработващите лични данни. ПОД „Топлина“ АД си запазва правото да оспори всякакви промени, свързани с включването или замяната на лица, обработващи лични данни. Дейностите на обработващия данните се ограничават до „по-техническите“ аспекти на дадена операция, като например съхранение, извличане или изтриване на данни, ако това е технически и операционно възможно, с оглед на аспекта на конкретната услуга.

2) Обработващият лични данни оперира с тях въз основа на договор или друг правен акт, съгласно нормативната база. В договора се регламентират целта и естеството на личните данни, срокът на обработване, субектите, на които личните данни ще бъдат обработени, както и права и задължения за обработващия лични данни и ПОД „Топлина“ АД. Обработващият лични данни има следните задължения:

1. Обработва лични данни само след документирано писмено разрешение от дружеството;

2. Да е поел ангажимент за поверителност и конфиденциалност на данните по договор или да е задължен от закон или друг нормативен акт да спазва поверителността и конфиденциалността на данните;

3. Да предприема всички необходими мерки по защитата и съхраняването на личните данни като: криптиране на личните данни, данните на субекта да не съхраняват на мобилни устройства и обработването на данните да не се извършва на хард диска, а на определена директория в защитен файлов сървър;

4. Да подпомага дружеството при изпълнение на законовите му задължения;

5. Да заличи и върне на дружеството всички лични данни, след приключване на договора за услуга, освен ако нормативен акт не указва друго;

6. Да осигурява на дружеството пълен достъп до данните, включително да позволява и допринася за извършване на външни одити и одити от страна на дружеството;

7. Подпомага дружеството при изпълнение на задълженията възложени от чл. 32-36 от Регламент 2016/679, както и да уведоми дружеството, ако някое нареждане противоречи на Регламента;

8. Ако обработващият лични данни, на когото е възложено по договор или с нормативен акт обработването на лични данни от името на дружеството, и обработващият от своя страна има друг обработващ лични данни за извършване на специфични дейности по обработване, то за него важат същите правила, както и за обработващият данни на дружеството;

9. Обработващият лични данни отговаря по презумпция солидарно с ПОД „Топлина“ АД за свързаните с това обработваните лични данни;

10. По искане на дружеството или на КЗЛД, представители на дружеството и на обработващият лични данни от името на дружеството си сътрудничат с представители на КЗЛД при изпълнение на нейните правомощия.

Раздел IX. Сигурност на личните данни и нарушение на сигурността

Чл.41. Дружеството и обработващият лични данни осигуряват такива технически и организационни мерки, че да се осигури ниво за сигурност, в зависимост от рисковете с различна и вероятна тежест за правата и свободите на физическите лица.

Чл.42. Дружеството и обработващият лични данни от името на дружеството предприемат действия, гарантиращи че обработката на информацията ще се извършва по указания на дружеството, освен ако нормативен акт не предвижда друго.

Чл.43. При нарушение на сигурността, дружеството задейства наличните процедури за действие за справяне с нарушението и уведомява субектите на правата за нарушението. Ако нарушението е при обработващия лични данни той следва да уведоми незабавно ПОД “Топлина“ АД за нарушаване сигурността на данните.

Раздел X. Длъжностно лице по защита на личните данни

Чл.44. 1) ПОД „Топлина“ АД определя или назначава лице по защита на личните данни, публикува неговите данни за контакт в сайта си

2) Длъжностното лице може да изпълнява и други функции и задачи, стига те да не противоречат или да не водят до конфликт на интереси с дейността по защита на данните.

3) Дружеството осигурява на длъжностното лице по защита на личните данни техническа и организационна, обучителна, финансова и всякаква друга помощ, както и достъп до съответните регистри, лични данни и операции по обработване по повод изпълнение на задълженията на длъжностното лице.

Чл.45. 1) Обработващият лични данни и ПОД „Топлина“ АД правят необходимото, така че длъжностното лице да не получава указания във връзка с изпълнението на функциите си. Длъжностното лице по защита на личните данни не може да бъде освобождавано от длъжност, нито санкционирано от дружеството за изпълнението на своите функции. 2) Длъжностното лице по защита на личните данни участва по подходящ начин и своевременно при решаването на всички въпроси, свързани със сигурността на данните. 3) Длъжностното лице по защита на личните данни спазва изискванията на този правилник, включително изискванията за конфиденциалност и поверителност.

Чл.46. Функции на длъжностното лице:

1. Следи за съблюдаване спазването на нормативните изисквания относно защитата на личните данни при отговор на запитвания, молби и искания, свързани с личните данни на субектите.

2. Своевременно информира дружеството и служителите за задълженията им съгласно нормативната база, настоящият правилник и стандарта ISO 27001:2013 относно сигурността на информацията;

3. Следи за възлагане на отговорности, повишава осведомеността на служителите и осигурителните посредници, участва в обучителните процеси на персонала, участва в операциите по обработване и подпомага дружеството при извършване на съответните одити;

4. Сътрудничи си с КЗЛД, както и действа като лице за контакт на КЗЛД с дружеството по въпроси, свързани със ЗЗЛД и Регламент 2016/679;

5. При изпълнение и отчитане на своята дейност, длъжностното лице по защита на данните отчита рисковете, обхвата и целите на обработката на данни.

Заключителни разпоредби

Правилникът е приет с решение по Протокол № 186/21.05.2018 г. на Управителния съвет, одобрено от Надзорния съвет на ПОД „Топлина“ АД с решение по протокол № 172/ 25.05.2018 г. и влиза в сила от 25.05.2018 г., изм. с решение по Протокол № 206/11.11.2019 г. на Управителния съвет, одобрено от Надзорния съвет на ПОД „Топлина“ АД с решение по протокол № 193/14.11.2019 г.