ВЪТРЕШНИ ПРАВИЛА
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ЗАСТРАХОВАТЕЛЕН БРОКЕР
„ЛайфТръст“ ЕООД

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите Вътрешни правила за защита на личните данни, наричани за краткост **„Правилата“**, определят правилата по отношение защитата на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни, съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския парламент.

Чл. 2. Настоящите Правила определят целите и средствата за защита на личните данни. Целта на Правилата по защитата на физическите лица във връзка с обработване на личните им данни се осъществява чрез:

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

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

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

4. Определяне Регистри на дейностите по обработване;

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

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

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

Чл. 3. Настоящите правила регламентират:

1. Принципите на дейността на „ЛайфТръст“ ЕООД в качеството му на администратор на лични данни, в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския парламент, на Закона за защита на личните данни и Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни;
2. Механизмите, регламентиращи въвеждането и спазването на горните принципи;
3. Правата на субектите на данни. Процедури при осъществяване правата на субектите на лични данни;
4. Функциите на „ЛайфТръст“ ЕООД в качеството му на администратор;
5. Отношенията на „ЛайфТръст“ ЕООД с дружества, които по силата на договор се явяват също администратори или обработващи лични данни;
6. Процедурата по оценка на въздействието върху обработваните лични данни и определяне нивата на въздействие и защита на обработваните лични данни.

РАЗДЕЛ II. ПРИНЦИПИ ПРИ ОБРАБОТВАНЕТО И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Чл. 4. (1) Брокерът събира и обработва личните данни при спазване на следните принципи:

1. законосъобразност, добросъвестност и прозрачност;

2. ограничение на целите – личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели. По-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели;

3. свеждане на данните до минимум – събират се само лични данни, ограничени до необходимото във връзка с целите, за които се обработват;

4. ограничение на съхранението – личните данни са 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; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящи технически и организационни мерки с цел да бъдат гарантирани правата и свободите на физическите лица, чиито данни се обработват;

5. цялостност и поверителност – личните данни са 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 и/или организационни мерки.

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

1. гарантираност на неприкосновеността на личността и личния живот на субекта на данни при обработване на свързаните с него лични данни;
2. законосъобразно и добросъвестно обработване на данните;
3. обработване на данни само от лица, чиито служебни задължения изискват обработване на конкретните данни на принципа „необходимост да се знае“.

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

Чл. 5. В случай че липсва изрично законово изискване, Брокерът не обработва лични данни, които:

1. разкриват расов или етнически произход;
2. разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;
3. се отнасят до генетични и биометрични данни, които се обработват за целите единствено на идентифицирането на физическо лице;
4. се отнасят до сексуалния живот или сексуалната ориентация на физическото лице или до човешкия геном.

Чл. 6. Брокерът събира и обработва лични данни, свързани със здравословното състояние, само по отношение на служителите му, с оглед изпълнението на техните трудови задължения, при спазване изискванията на трудово-осигурителното законодателство, както и за клиенти, които ползват застрахователни продукти, изискващи предоставянето на подобна информация, при спазване изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и/или на правен акт на Република България, уреждащ материята.

Чл. 7. Брокерът може да обработва лични данни самостоятелно или чрез трети лица, в качеството им на обработващи лични данни и съвместни

администратори, на основание на сключен с тях договор. Съответните договори трябва много ясно и точно да определят какви лични данни ще се обработват, как, в какъв срок, с каква цел. При обработване на съвместни администратори трябва ясно да се определят съответните права и задължения на двете страни, както и техните отговорности.

РАЗДЕЛ III. ВИДОВЕ РЕГИСТРИ

Чл. 8. Брокерът е администратор на лични данни и като такъв води следните регистри:
1. Регистър **„Служители и лица по граждански договори“** и
2. Регистър **„Клиенти“**.

Чл. 9. (1) В регистър **„Служители и лица по граждански договори“** се събират и съхраняват личните данни на служителите и изпълнителите по граждански договори при Брокера с цел:
1. Индивидуализиране на трудовите и граждански правоотношения;
2. Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив и др.;
3. Използване на събраните данни за съответните лица за служебни цели;
4. За всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения – за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);
5. За установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;
6. За водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица по трудови и граждански договори.
(2) В регистър „Служители и лица по граждански договори“ се съхраняват следните видове лични данни:
1. Лични данни в категория „Физическа идентичност“ на лицата, които се предоставят на основание нормативно задължение при сключването и изпълнението на договор – три имена, ЕГН, пол, постоянен адрес и месторождение за трудовите договори, а за гражданските – и номер на лична карта, дата и място на издаване, валидност, орган, който я е издал, телефони за връзка, електронна поща и др.;
2. Лични данни в категория „Социална идентичност“ на лицата, предоставяни на основание нормативно задължение и/или легитимен интерес, например:
2.1. вид и степен на образованието, място, номер и дата на издаване на дипломата и учебно заведение – данните са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата, както и при преценка и удостоверяване на компетентността на лицата, на които Брокерът възнамерява да възложи изпълнението на дейности по граждански или трудови договори. Предоставят се от служителите/изпълнителите при сключване на трудови или граждански договори с тях;
2.2. допълнителна квалификация – данните са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо. При необходимост данни за допълнителна квалификация се изискват и от лицата, на които Брокерът възнамерява да възложи изпълнението на дейности по граждански договори;
2.3. лични данни относно гражданскоправния статус на лицата, необходими за всички служители, назначавани по трудово правоотношение, включително за длъжностите, свързани с материална отговорност. Предоставят се на основание нормативно задължение;
2.4. данни от здравословното състояние на служителите, когато се налага обработване на болнични листове, документи във връзка с трудова злополука, трудоустрояване на работници и др.

Чл. 10. (1) В регистър **„Клиенти“** се събират и съхраняват личните данни на клиентите на Брокера с оглед:
1. Индивидуализиране на съответните контрагенти;
2. Изпълнение на нормативните изисквания на Закона за счетоводството и други относими нормативни актове;
3. Използване на събраните данни за съответните лица за служебни цели само и единствено след получаването на надлежно съгласие от лицата за обработване на техните лични данни за следните цели:
3.1. за всички дейности, свързани със съществуването, изменението и прекратяването на договорните правоотношения, както и със събиране на вземания, произтичащи от последните – за изготвяне на всякакви документи в тази връзка (договори, допълнителни споразумения, всякакви търговски, счетоводни и други документи);
3.2. за установяване на връзка с лицата по телефон, адрес и/или електронна поща, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им по сключените договори;
3.3. за водене на счетоводна отчетност.
(2) В регистър **„Клиенти“** се съхраняват следните видове лични данни относно категория „Физическа идентичност“ на лицата: имена и данни по лична карта (ЕГН, пол, номер на лична карта, дата и място на издаване, валидност, орган, който я е издал, постоянен адрес, телефони за връзка, електронна поща и др. Предоставят се на основание за сключването и изпълнението на договор.

Чл. 11. Регистрите се водят в следните форми:
1. Регистри, водени на хартиен носител, и
2. Регистри, водени на технически носител.

Чл. 12. (1) Писмената (документална) форма на организация и съхраняване на личните данни се състои в съхранение на данните в папки (кадрови досиета, досиета на изпълнители и клиенти) за всеки служител или нает по граждански договор лице, както и за всеки клиент, с когото е сключен договор.
(2) Минималните изисквания към регистрите, поддържани на хартиен носител, са:
1. Съхранение на носителите в заключващи се помещения, до които достъп нямат външни лица, а при необходимост и в шкафове със секретни ключалки;
2. При отпадане на основанието или постигане на целта на обработване и при изтичане на срока за съхранение унищожаването на тези документи се извършва по начин, който предотвратява всякаква възможност за бъдещо разчитане на данните.
3. Лицата с пряк достъп до документи, съдържащи лични данни, са длъжни да уведомят незабавно прекия си ръководител в случай на установяване на неправомерен достъп или ползване на съответната информация, включваща лични данни, или на неправомерно проникване в помещение, в което тази информация се съхранява.
4. Достъпът и предоставянето на данни от тези регистри се осъществяват по възможност без изнасяне на оригиналните носители извън помещенията, в които се съхраняват. Трудовите досиета на служителите не се изнасят извън офиса на Брокера.

РАЗДЕЛ IV. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 13. (1) Правата на субектите на данни засягат всички лични данни на физическото лице, обработвани от Брокера, както и всички субекти на данни, чиито данни се обработват от Дружеството.
(2) Основните права на субекта на данни по отношение на неговите данни, които правната рамка постановява и Дружеството спазва, са както следва:
1. Право на достъп;

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

Чл. 14. (1) Правото на достъп на Субекта на данни представлява правото да получи от Брокера, в качеството му на администратор, потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до личните си данни и следната информация:

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

Чл. 15. Субектът на данни има право да поиска от Брокера личните му данни да бъдат коригирани, ако са неточни или непълни. Във всеки един случай, когато е налице грешка в обработваните от Дружеството данни, то е длъжно да уважи такова искане, като в тези случаи трябва да уведоми и останалите получатели, на които са разкрити тези данни, за да могат и те да отразят промяната.

Чл. 16. (1) Субектът на данни има право на изтриване (право „да бъдеш забравен“) на данните му, ако:

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

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

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

Чл. 17. (1) Субектът на данни има право да изиска от Дружеството да ограничи обработването на данните му в следните случаи:

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

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

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

Чл. 18. (1) Субектът на данни има право по всяко време на възражение срещу обработване на личните му данни, отнасящи се до него, което се основава на обработването, необходимо за целите на легитимния интерес на Дружеството. В този случай Брокерът може да не прекрати обработването на данните при наличие на законови основания за обработването им, които имат предимство пред интересите, правата и свободите на субекта на данни или за установяване, упражняване или защитата на правни претенции.

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

Чл. 19. Субектът на данни има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включително профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга. Това правило не се прилага, ако решението е необходимо за сключване или изпълнението на договор между Дружеството и субекта на данни.

Чл. 20. (1) Субектът на данни има право право да получи личните данни, които го засягат и които той е представил на Дружеството, в структуриран, широко използван и пригоден за машинно четене формат и има право да прехвърли тези данни на друг администратор.

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

РАЗДЕЛ V. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА

Чл. 21. (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни. В случаите когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, Администраторът е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

(2) Заетите по трудови и граждански правоотношения, както и клиентите имат право на достъп до личните си данни, които се съхраняват при Брокера. За целта лицата подават писмено заявление до Брокера, в това число и по електронен път, по реда на Закона за електронния документ и електронния подпис.

(3) Заявлението съдържа име на лицето, адрес и други данни, които го идентифицират – три имена, ЕГН, длъжност и месторабота (когато е относимо), описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес за кореспонденция, а когато заявлението се подава от упълномощено лице – и нотариално заверено пълномощно. Заявлението се завежда в общия входящ регистър на Брокера.

(4) При получаване на заявление за достъп до собствени на заявителя лични данни, управителите на Брокера или упълномощено от тях лице разглежда заявлението за достъп. Срокът за разглеждане на заявлението и произнасяне по него е 1 месец от деня на подаване на искането. Администраторът

предприема необходимите мерки за предоставяне на информация, която се отнася до обработването на лични данни на заявителя в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства.
(5) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение, което отново се съобщава на заявителя по реда на предходното изречение.
(6) Администраторът предоставя на заявителя следната информация:
1. данните, които идентифицират Администратора и координатите за връзка с него;
2. целите на обработването, за което личните данни са предназначени, както и правното основание за тяхното обработване;
3. съответните категории лични данни на заявителя, които се обработват от Администратора;
4. получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави по смисъла на Регламента или международни организации, както и техните гаранции за защита;
5. когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
6. съществуването на право да се изиска от Администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със заявителя, както и правото да се направи възражение срещу такова обработване;
7. правото на жалба до Комисията за защита на личните данни;
8. когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник.
(7) Администраторът се задължава да съобщава за всяко 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. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.
Чл. 22. (1) В случай че трето лице иска достъп до данните на клиент на ЗЕАД „Булстрад Живот Виена Иншурънс Груп“, които не представляват тайна или класифицирана информация, исканите данни се предоставят само в случай че едновременно са изпълнени следните условия:
1. съществува законен интерес на лицето, искащо данните;
2. не може да се направи извод, че интересите на титуляря на данните има преимущество спрямо интересите на лицето, искащо разкриването на данните;
3. получателят на данните попада в кръга от лица, за който титулярят на данните предварително е уведомен относно възможността за разкриване на негови данни или титулярят е уведомен за разкриването на неговите данни след постъпване на искането от третото лице.
4. лицето, за което се отнасят данните, е дало своето изрично писмено съгласие.
(2) Ако исканите данни съдържат тайна или класифицирана информация, се спазват изискванията за забрана за разкриването им.
Чл. 23. (1) Предоставянето на лични данни в държава – членка на Европейския съюз, както и в друга държава – членка на Европейското икономическо пространство, се извършва при спазване на изискванията на действащото европейско и национално законодателство.
(2) Предоставяне на лични данни в трета държава извън тези по ал. 1 се допуска само ако тя осигурява адекватно ниво на защита на личните данни на своя територия.
Чл. 24. (1) Сроковете за съхраняване на личните данни по отношение на регистър „Служители и лица по граждански договори“ са следните:
1. Различните носители на счетоводна информация, съдържащи лични данни от регистър „Служители и лица по граждански договори“, се съхраняват в предвидените в Закона за счетоводството (ЗСч.) срокове, както следва:
1.1. ведомости за заплати и трудови досиета (документите във връзка с възникването, съществуването, изменението и прекратяването на трудовото правоотношение) – 50 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 12, ал. 1, т. 1 от ЗСч.);
1.2. счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции – 10 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 12, ал. 1, т. 2 от ЗСч.);
1.3. всички останали носители на счетоводна информация – 3 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 12, ал. 1, т. 3 от ЗСч.).
2. Видовете лични данни на служителите и на лицата по граждански договори, които не се съдържат в носителите на информация по предходната точка, се съхраняват за срок от 1 месец, считано от датата на отпадане на основанието за тяхното обработване, в т.ч. след изтичане на всички задължения по договора като евентуални съдебни претенции, гаранционна отговорност и др.
(2) В срок до 30 дни след изтичане на установените по-горе срокове личните данни се унищожават.
Чл. 25. Сроковете за съхраняване на личните данни по отношение на регистър „Клиенти“ са следните:
1. Различните носители на счетоводна и данъчна информация, съдържащи лични данни от регистър „Клиенти“ – на клиентите на Дружеството, с които е сключен договор, се съхраняват в предвидените в Закона за счетоводството (ЗСч.) и в Данъчно-осигурителния процесуален кодекс (ДОПК) срокове, както следва:
1.1. счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции – 10 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 12, ал. 1, т. 2 от ЗСч.);
1.2. всички останали носители на счетоводна информация, с изключение на ведомости за заплати и трудови досиета – 3 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят (чл. 12, ал. 1, т. 3 от ЗСч.);
1.3. документи за данъчно-осигурителен контрол – съхраняват се за срок до 5 г. след изтичане на давностния срок за погасяване на евентуални данъчни задължения на Дружеството за годината, през която договорът е прекратен/развален, считано от годината, през която съответният договор е прекратен/развален, и в случай че при прекратяването/разваляне на договора няма спорове относно неговото изпълнение.
2. Личните данни на клиентите, с които е сключен договор и които не се съдържат в носителите на информация по предходната точка, се съхраняват за срок от 30 дни, считано от датата на отпадане на основанието за тяхното обработване (от прекратяването на договора – предсрочно или на друго основание, предвидено в същия, в т.ч. след изтичане на давностните срокове и всички задължения по договора като евентуални съдебни претенции, гаранционна отговорност и др. Ако съответният клиент, в рамките на посочения срок, изрично поиска личните му данни да бъдат изтрити (забравени) или обработването им да бъде ограничено, то съхраняването на съответните данни ще бъде преустановено и същите ще бъдат унищожени при първа възможност след получаване на искане от клиента, освен ако не е налице изрично законово основание за продължаване обработването им.
Чл. 26. (1) В случай на нарушение на сигурността на личните данни Администраторът, без ненужно забавяне, но не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни Комисията за защита на личните данни (КЗЛД), освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Ако уведомлението до КЗЛД не е подадено в срок от 72 часа от нарушението, Администраторът трябва да съобщи и причините за забавянето.
(2) Уведомлението съдържа най-малко следната информация:
1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
2. посочване на името и координатите за връзка с управител на Брокера или на друга точка за контакт, от която може да се получи повече информация;

3. описание на евентуалните последици от нарушението на сигурността на личните данни;
4. описание на предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
(3) В случаите когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът без ненужно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни. Съобщението следва да бъде дадено на ясен и прост език, да дава информация за естеството на нарушението на сигурността на личните данни и да съдържа най-малко информация относно:
1. името и координатите за връзка на управител на Брокера или на друга точка за контакт, от която може да се получи повече информация;
2. евентуалните последици от нарушението на сигурността на личните данни;
3. предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
(4) Задължението на Администратора за уведомяване на субекта на личните данни по ал. 3 не се прилага, в случай че е налице едно от следните условия:
1. Администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
2. Администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
3. Това би довело до непропорционални усилия на Администратора. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.
Чл. 27. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването, като това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. Подобни мерки гарантират, че по подразбиране без намеса от страна на субекта неговите лични данни не са достъпни за неограничен брой физически лица.

РАЗДЕЛ VI. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО НА ЗАЩИТА НА ДАННИТЕ

Чл. 28. (1) Администраторът има задължение да извърши оценка на въздействието съгласно изискванията на Регламент 679/2016 ЕС, в случай че обработваните от него лични данни биха могли да породят висок риск за правата и свободите на физическите лица.
(2) Оценка на въздействие е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, целостта или наличността на личните данни.
(3) Оценката на въздействието се извършва периодично на всеки две години, а при промяна на характера на обработваните лични данни или броя на засегнатите физически лица, оценката на въздействието може да бъде извършвана и по-рано.
Чл. 29. (1) Оценката на въздействие съдържа най-малко следното:
1. системен опис на предвидените операции по обработване и целите на обработването;
2. оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
3. оценка на рисковете за правата и свободите на лицата, чиито данни се съхраняват;
4. мерките, предвидени за справяне с рискове, мерките за сигурност и механизмите за осигуряване на защитата на личните данни.
(2) За целите на настоящите Правила се определят следните нива на въздействие:
1. изключително високо ниво на въздействие;
2. високо ниво на въздействие;
3. средно ниво на въздействие;
4. ниско ниво на въздействие.
(3) Нивото на въздействие се определя по всеки критерий във всеки отделен регистър. Най-високото ниво на въздействие определя нивото на въздействие на съответния регистър на лични данни.
(4) За целите на настоящите Правила се определят следните нива на защита на обработваните лични данни, които в зависимост от определените нива на въздействие на съответните регистри на лични данни, Брокерът като администратор е задължен да прилага:
1. при ниско ниво на въздействие – ниско ниво на защита;
2. при средно ниво на въздействие – средно ниво на защита;
3. при високо ниво на въздействие – високо ниво на защита;
4. при изключително високо ниво на въздействие – изключително високо ниво на защита.
(5) Всяко ниво на защита на обработваните лични данни представлява съвкупността от технически и организационни мерки за физическа, персонална, документална, информационна и/или друга защита, които Брокерът като администратор следва да прилага с цел защита на личните данни и на субектите на лични данни от неправомерно обработване на данни, както и с цел управление на въздействието върху обработваните лични данни, върху физическо лице или група физически лица.

РАЗДЕЛ VII. ДЕФИНИЦИИ

Чл. 30. За целите на настоящите Правила понятията носят следния смисъл:
1. „Приложимо право“ означава приложимото законодателство на Европейския съюз и Република България по отношение на защитата на личните данни;
2. „ОРЗД“ означава Регламент (ЕС) № 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни и относно свободното движение на такива данни, и за отмяна на Директива 95 / 46 / ЕО („Общ регламент за защита на данните“);
3. „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;
4. „Обработване“ – всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства, като събиране, записване, организиране, структуриране, съхранение, промяна, употреба, разкриване чрез предаване, разпространение или друг начин, чрез който данните стават достъпни;
5. „Профилиране“ – всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;
6. „Регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии;

7. „Администратор“ означава физическо или юридическо лице, публичен орган или друга структура, която сама или съвместно с други определя целите и средствата за обработването на личните данни;
8. „Обработващ лични данни“ означава физическо или юридическо лице, публичен орган или друга структура, която обработва лични данни от името на Администратора;
9. „Съгласие на субекта на данни“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;
10. „Разкриващ лични данни“ означава страната по този Договор, която предава лични данни на Получателя на лични данни;
11. „Получател на лични данни“ означава страната, която получава личните данни от Разкриващия личните данни;
12. Термините **„Субект на лични данни“**, **„Нарушение на сигурността на личните данни“, „Обработване“**, **„Специални категории лични данни“** и **„Надзорен орган“** имат същото значение като в ОРЗД и приложимото национално законодателство.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите Вътрешни правила са в съответствие с Регламент (ЕС) № 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни и относно свободното движение на такива данни, и за отмяна на Директива 95/46/ЕО.
§2. Настоящите Вътрешни правила са утвърдени със Заповед на управителите на Застрахователен брокер „ЛайфТръст“ ЕООД №2/10.03.2022 г.
§3. Настоящите Вътрешни правила следва да бъдат предоставени на разположение на служителите на Застрахователен брокер „ЛайфТръст“ ЕООД, както и до назначените по граждански договор лица. За неизпълнение на задълженията по тези Правила и действащото към съответния момент национално и европейско законодателство за защита на личните данни, съответните лица носят дисциплинарна и имуществена отговорност.