ВЪТРЕШНИ ПРАВИЛА

за мерките за защита на личните данни
в “Дом за стари хора Попови ливади“ ЕООД

I. Общи положения

Чл. 1. (1) “Дом за стари хора Попови ливади” ЕООД, е юридическо лице със седалище гр. София, Р България с предмет на дейност „предоставяне на комплекс от услуги включително, хотелиерство и ресторантьорство, социални услуги, търговия и търговско представителство и посредничество, консултантски дейности, транспортни услуги, както и всякаква друга дейност, която не е забранена със закон“..

(2) “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД обработва лични данни във връзка със своята дейност и се основава на приложимото действащо законодателство в Европейския съюз и Република България.

Чл. 2. Настоящите правила уреждат организацията на обработване и защитата на лични данни на служителите, потребителите, посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД.

Чл. 3. (1) Като „обработване на лични данни“ се възприема всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 4. “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД е администратор на лични данни по смисъла на чл. 4, пар.7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламент за защита на личните данни).

Чл. 5. (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Принципите за защита на личните данни са:

1. *Принцип на ограничено и целесъобразно събиране* – събирането на лични данни трябва да бъде в рамките на необходимото за конкретни, изрично указани и легитимни цели. Информацията се събира по законен и обективен начин;
2. *Принцип на ограниченото използване, разкриване и съхраняване* – личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;
3. *Принцип на точност* – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;
4. *Принцип на сигурността и опазването* – личните данни трябва да се съхраняват и обработват 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.

Чл. 6. "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД организира и предприема мерки, за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване. Предприеманите мерки са съобразени с рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;

Чл. 8. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(2) Личните данни се съхраняват на хартиен и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД и/или нормалното му бизнес функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД се извършва на хартиен и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 9. Когато не е налице хипотезата на чл. 6, пар. 1, б. б), в), г) и д) от Регламент (ЕС) 2016/679, физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец.

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изричен акт на Ръководството на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив задължително се заключват.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд и Закона за защита на личните данни.

Чл. 12. С оглед защита на хартиените и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

II. Мерки по осигуряване на защита на личните данни

Чл. 18. *Физическа защита* в "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се създават, обработват и съхраняват лични данни.

Чл. 19. (1). Основните приложими *организационни мерки за физическа защита* в "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

(2) В случай че "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД оцени, че събирането, обработването и съхраняването на дадени лични данни има „средно" ниво на въздействие, към посочените мерки се включват и определяне на зоните с контролиран достъп и на използваните технически средства за физическа защита.

(3) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

(4) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(5) *Организацията на физическия достъп до помещения*, обработващи лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми, система за достъп до сградата и помещенията - магнитни карти и кодове за достъп) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(6) Като *зони с контролиран достъп* се определят всички помещения на "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД, в които се събират, обработват и съхраняват лични данни с определено ниво на въздействие по-високо от „ниско".

(7) *Използваните технически средства за физическа защита* на личните данни в "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае" с оглед изпълнението на работните им задължения.

(8) Всички записи и документи на хартиен носител, съдържащи лични данни, са в помещения с ограничен достъп, достъпен само от упълномощен персонал.

(9) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез нива на достъп и уникални потребителски идентификатори и пароли (буквено-цифрови с минимум 8 символа), а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Чл. 20. (1). Основните приложими *технически мерки за физическа защита* в "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД включват използване на чип-кари, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

(2) *Чип-картите* и свързаните с тях електронни устройства за заключване, като способ за физическа защита, се използват, за да осигурят защита на зоните, в които се съхраняват лични данни. Тези зони са достъпни само чрез чип-карти, предоставен единствено на оторизираните (с изрична заповед или в изпълнение на служебни задължения) за това лица.

(3) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки*, като последните са разположени в зони с ограничен (контролиран) достъп. Трудовите досиета се съхраняват в помещения с ограничен достъп.

(4) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: *ключалки* (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; шкафове и пожарогасителни средства.

(5) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 21. (1). Основните приложими *мерки за персонална защита* на личните данни, оценени с ниска степен на въздействие, са:

1. Задължение на служителите да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящата инструкция;
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от "ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ" ЕООД;
3. Забрана за споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на въздействие, се прилагат и:

1. Познаване на политиката и ръководствата за защита на личните данни;
2. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения и/или изисква подобно;

Чл. 22. (1). Основните приложими *мерки за документална защита* на личните данни, оценени с ниска степен на въздействие, са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител*: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на

действащото законодателство или пряко свързани с осъществяването на нормалната бизнес дейност на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД;

2. *Определяне на условията за обработване на лични данни*: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;
3. *Регламентиране на достъпа до регистрите*: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;
4. *Определяне на срокове за съхранение*: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.
5. *Процедури за унищожаване*: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

(2) За лични данни, оценени с по-висока степен на въздействие, се прилагат и мерки, свързани с:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;
2. *Правила за размножаване и разпространение*, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или по-висш държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение представлява нарушение на вътрешния ред в дружеството и подлежи на дисциплинарни санкции, включ. прекратяване на трудовите взаимоотношения.

Преходни и заключителни разпоредби

§ 1. По смисъла на настоящата инструкция:

- **„Лични данни“**означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентифика- ционен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице
- „**Администратор“** е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.

- „**Администратор на лични данни**” е “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД, ЕИК 208110080.
- „**Високо ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице.
- **„Външни мрежи“** са всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД.
- **„Вътрешни мрежи“** са всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД.
- „**Длъжностно лице**“ е служител, на когото е възложено да упражнява ръководство на процес в “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД, в нейните структурни и/или функционални единици, както и служител, който изпълнява работа на специалист във функционалните и обслужващите звена на “ДОМ ЗА СТАРИ ХОРА ПОПОВИ ЛИВАДИ” ЕООД.
- **„Документална защита на лични данни“** е система от организационни мерки при обработването на лични данни на хартиен носител.
- **„Защита на автоматизирани информационни системи и/или мрежи**“ е система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.
- „**Изключително високо ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица.
- „**Инцидент**” е непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни.
- „**Длъжностно лице по защита на личните данни**” е физическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.
- „**Наличност**” е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.
- „**Ниво на защита**” е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.
- „**Ниско ниво на въздействие**” е неправомерното обработване на лични данни, което би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.
- „**Носител на лични данни**” е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.
- „**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

- „**Обработващ лични данни**“ е физическо или юридическо лице, държавен орган или орган на местно самоуправление, който обработва лични данни от името на администратора на лични данни.
- „**Оператор на лични данни**” е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове.
- „**Оторизирано лице**“ е лице, което по силата на естеството на преките си служебни задължения и/или изричното оторизиране от Ръководството, има право за достъп до определена категория лични данни.
- **„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, цялостността или наличността на личните данни.
- **„Персонална защита на лични данни“** е система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
- „**Поверителност**” е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- „**Получател**“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, на когото се разкриват лични данни, независимо дали е трето лице или не. Органите, които могат да получават данни в рамките на конкретно проучване, не се смятат за получатели.
- „**Предоставяне на лични данни**“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.
- **„Регистър на лични данни**“ е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.
- „**Специфични признаци**“ са признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето.
- „**Средно ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица.
- „**Съгласие на физическото лице**“ означава 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

dompopovilivadi.bg
info@dompopovilivadi.bg

- „**Трето лице**“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.
- „**Физическа защита на лични данни“** е система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
- „**Цялостност**” е изискване, данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

§2. Настоящите вътрешни правила се приемат на основание Заповед на Управителя на „Дом за стари хора Попови ливади“ ЕООД и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламент за защита на личните данни), чл. 23, ал. 4 от Закона за защита на личните данни и Наредба № 1/30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни, издадена от Комисията за защита на личните данни.

§3. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и действащото приложимо законодателство на Р. България.