УТВЪРДИЛ:.....
Юлия Пейчева – ВрИД Директор на
ДОМ ЗА СТАРИ ХОРА,гр.Казанлък

ВЪТРЕШНИ ПРАВИЛА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

В ДОМ ЗА СТАРИ ХОРА

Гр.Казанлък

2024 г.

ГЛАВА ПЪРВА
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Дом за стари хора е институция, предлагаща социални услуги (държавно делегирана дейност) със седалище гр.Казанлък, ул."Петьо Ганин" № 52.

(2) Социалната институция обработва лични данни във връзка със своята дейност и сама определя целите и средствата за обработването им.

Чл. 2. (1) Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на служителите, потребителите на социални услуги, посетителите, както и на други физически лица, свързани с осъществяването на дейността на Дома.

(2) Целта на настоящите вътрешни правила е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от Дом за стари хора, гр.Казанлък регистри, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.

(3) Вътрешните правила се приемат с цел да регламентират:

- Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

- Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

- Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

(4) Вътрешните правила се утвърждават, допълват, изменят и отменят от Директора на Дом за стари хора- гр.Казанлък.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни в Република България и Регламент (ЕС) 2016/679.

Чл. 4. (1) Дом за стари хора- гр.Казанлък е администратор на лични данни по смисъла на чл. 4, пар. 7 от Регламент (ЕС) 2016/679.

Чл. 5. (1) Личните данни се събират и обработват:

- за изпълнение на правомощията и присъщата дейност на дома, предоставени чрез Закона за социалните услуги, Наредба за качеството на социалните услуги и нормативната уредба на Република България и ЕС, регламентираща обществените отношения, свързани с предоставянето на социалните услуги;

- въз основа на законови задължения, възложени чрез законодателството на Република България и ЕС /закони, наредби, инструкции, правилници, регламенти и др./;

- при сключване на договори или подготовка за тяхното сключване;

- за защита на жизненоважни интереси на субекта на данните или на друго физическо лице;

- при липса на някое от горепосочените основания – единствено след съгласие на субекта на лични данни, дадено чрез подписана декларация за съгласие по образец. (Приложение № 2 и Приложение № 2а);

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

(2) Личните данни се обработват при спазване на следните принципи, въведени чрез Регламент 2016/679 г.:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

2. Ограничение на целите – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

3. Свеждане на данните до минимум – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;

4. Точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

5. Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6. Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(3) Събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин; 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.

(4) Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели; личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват; личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл. 6. Администраторът 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 със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) Дом за стари хора- Казанлък прилага защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита.
2. Персонална защита.
3. Документална защита.
4. Защита на автоматизирани информационни системи и/или мрежи.

Чл. 8. (1) Личните данни се събират за конкретни, точно определени 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, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на дома и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на дома се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразени с посочените в чл.7 ал.2 мерки за защита и нивото на въздействие на съответния регистър.

Чл. 9. За всяка дейност по обработка на лични данни се поддържа регистър на дейностите, по реда и при условията на Глава ТРЕТА от настоящите правила.

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 изрична заповед на Директора на Дом за стари хора – гр.Казанлък.

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 помещението, определено за архив, за срокове, съобразени с действащото законодателство, Вътрешни правила за дейността на учрежденския архив и Номенклатура на делата със срокове на съхраняване. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(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.

(4) Документите на електронен носител се съхраняват на специализирани компютърни конфигурации и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността и за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани със заповед лица.

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

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на директора на дома, който от своя страна незабавно уведомява длъжностното лице по защита на личните данни. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, последствията от него и мерките за отстраняването му.

Чл. 14. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, Дом за стари хора може да определи друго ниво на защита за регистъра.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

Чл. 15. (1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от дома регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни, съобразно изискванията на действащата нормативна уредба. При промени в структурата на институцията, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2) В случаите, когато се налага унищожаване на носител на лични данни, се прилагат необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер.

(3) Унищожаването се осъществява от членовете на Постоянно действаща експертна комисия, определени със Заповед на директора.

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3.

Чл. 16. (1) Достъпът до данните от регистъра и разкриването на личните данни се осъществява при условията и по реда на Закона за защита на личните данни и Регламент 2016/679 от:

- физическите лица, за които се отнасят данните;
- трето лице, ако е предвидено в нормативен акт;
- обработващия личните данни;

(2) Субектите на данни могат да реализират правата си по реда и при условията на чл. 32 и 33 от настоящите правила.

ГЛАВА ВТОРА
МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (1) Физическа защита в Дом за стари хора- гр.Казанлък се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими организационни мерки за физическа защита в дома 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, както следва:

А) Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на административния 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.

Б)Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, 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.

В)Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Г) Като зони с контролиран достъп се определят всички помещения на територията на дома, в които се събират, обработват и съхраняват лични данни.

Д) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(3) Основните приложими технически мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Чл. 18. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. съгласие за поемане на задължение за неразпространение на личните данни; изразено в декларация по образец. (Приложение 3).

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае".

(4) Лицата могат да започнат да обработват лични данни след запознаване с:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

Чл. 19. (1). Основните приложими мерки за документална защита на личните данни 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 дейност на Дом за стари хора- гр.Казанлък;

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 дейност на дома, 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. 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 институцията, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 20. (1) Защитата на автоматизираните информационни системи и/или мрежи в ДСХ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на дома. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае";

2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3. Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният софтуер се контролира, инсталира и поддържа от лицензирана фирма.

4. Създаване и поддържане на резервни копия за възстановяване - има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.

5. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.) ;

6. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на дома.

8. Данните, които вече не са необходими за целите на институцията и чиито срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване с шредер, постоянно заличаване от електронните средства).

Чл. 21. (1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

(2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 22. (1) Използваният хардуер за съхранение и обработване на лични данни трябва да отговаря на съвременните изисквания и възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва, по възможност, без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В институцията се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и ОРЗД за осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 24. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

ГЛАВА ТРЕТА
ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 25. Поддържаните регистри в Дом за стари хора са:

1.Персонал

2. Потребители на услуги

3. Видеонаблюдение

4. Счетоводство и финансова отчетност

5. Регистър на дейностите

Чл. 26. (1) Всички регистри са подробно описани в **Приложение № 1** към правилата, което представлява и Регистър на дейностите.

(2) Директорът определя със заповед служителя, който отговаря за всеки отделен регистър.

(3) Създаването на нови регистри и извършването на промени в тях е допустимо само с изрична заповед на Директора.

Чл.27. (1) За всеки регистър се оценява рискът по следния начин:

1. Ниско ниво на риска – когато загубата или неправомерното обработване на личните данни от конкретен регистър не биха имали значителни последствия, застрашаващи живота на физическо лице или кражба на самоличността му.

2. Средно ниво на риска - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на физическо лице.

3. Високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на група от физически лица.

4. Изключително високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, застрашаващи живота на физическо лице.

(2). При „изключително високо ниво на риск“, констатирано при условията на предходния член, се извършва „Оценка на въздействието“ спрямо критериите, залегнали в Регламент (ЕС) 2016/679.

Чл.28 Оценка на риска се прави на всеки три години или при промяна на обработваните данни и броя на засегнатите физически лица.

ГЛАВА ЧЕТВЪРТА
ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ.

Чл. 29. (1) Длъжностното лице по защита на данните е длъжно:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Общия регламент за защита на данните и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство;

б) да наблюдава спазването на Регламента и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни;

в) да участва в повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

г) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;

д) надлежно да отчита рисковете, свързани с операциите по обработване, като се съобразява с естеството, обхвата, контекста и целите на обработването;

е) да участва в заседания на ръководството, когато се обсъждат въпроси от областта на защитата на личните данни;

ж) да дава становище/съвет/мнение по всички въпроси, свързани със защитата на личните данни, да консултира администратора или обработващия лични данни;

з) да си сътрудничи с надзорния орган;

и) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, и по целесъобразност да се консултира по всякакви други въпроси с надзорния орган;

(2) ДЛЗД има право:

а) да събира информация за определяне на дейностите по обработване;

б) да анализира и проверява изпълнението на дейностите по обработване;

в) да информира, съветва и отправя препоръки към администратора или обработващия лични данни;

д) да получава информация и необходимото съдействие от страна на ръководните органи в предприятието, от администратора/обработващия лични данни, от всички релевантни отдели и вътрешни структури, имащи отношение към операциите по обработване на лични данни.

(3) При изпълнение на своите задачи ДЛЗД действа напълно независимо и свободно от указанията на администратора на лични данни.

Чл. 30. Служителите на учреждението са длъжни:

1. да обработват лични данни законосъобразно, добросъвестно и прозрачно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират регистрите на личните данни (при необходимост);

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;

7. незабавно да уведомяват администратора на лични данни в случай, че установят изтичане на лични данни, независимо дали при извършване на своята работа или при друго лице, което обработва лични данни.

(2) Служителите, на които е предоставен достъп до регистрите, съдържащи лични данни носят отговорност за опазването им.

Чл. 31. (1) За неспазването на разпоредбите на настоящите вътрешни правила служителите носят административна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

ГЛАВА ПЕТА
ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл.32 Субекти на данни са Правата на субектите на данни:

А)Информираност (във връзка с обработването на личните му данни от администратора);

Б) Достъп до собствените си лични данни;

В) Коригиране (ако данните са неточни) и допълване;

Г) Изтриване на личните данни (право „да бъдеш забравен“);

Д)Ограничаване на обработването от страна на администратора или обработващия лични данни;

Е) Преносимост на личните данни между отделните администратори;

Ж) Възражение спрямо обработването на негови лични данни;

З) Субектът на данни има право и 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;

И) Право на защита по административен или съдебен ред, в случай, че правата на субекта на данни са били нарушени.

Чл.33 (1) За да реализира, което и да е от правата си по чл.32, субектът на данни подава заявление / възражение до администратора (съгласно образците по Приложение № 4).

(2) Заявленията трябва да съдържат име на лицето и други данни, които го идентифицират – адрес и телефон за кореспонденция, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, основания за искането, подпис, дата; пълномощно (изрично и с нотариална заверка на подписа) – когато заявлението се подава от упълномощено лице.

(3) Възраженията трябва да съдържат име на лицето и други данни, които го идентифицират – адрес и телефон за кореспонденция, срещу какво се възразява, на какво основание и конкретни искания (ако такива са налични).пълномощно (изрично и с нотариална заверка на подписа) – когато възражението се подава от упълномощено лице.

(4) Заявленията/ възраженията до администратора се завеждат в специален регистър и се образува преписка.

Чл.34 Администраторът отговаря на искането на субекта на данни или го информира писмено за действията, предприети във връзка с неговото заявление, в срок до два месеца от получаване на искането. Срокът може да се удължи с още един месец, когато това се налага заради сложността или броя на исканията.

Чл.35. (1) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение.

(2) Отказът за предоставяне достъп може се обжалва от лицето пред посочения в решението орган и срок.

Чл.36 Актовете на администратора по чл.34 и решенията по чл.35 се съобщават писмено на заявителя лично срещу подпис или по пощата с обратна разписка.

Чл.37. При нарушаване на правата му по Регламент (ЕС) 2016/679 и по ЗЗЛД субектът на данни има право да сезира Комисията за защита на личните данни в срок 6 месеца от узнаване на нарушението, но не по-късно от две години от извършването му.

ГЛАВА ШЕСТА
ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички служители в Дом за стари хора гр.Казанлък са длъжни срещу подпис да се запознаят с настоящите вътрешните правила за защита на личните данни и да ги спазват.

§ 2.Вътрешните правила служат като основание за издаване на заповеди, разработване на инструкции и процедури, във връзка с изпълнението на ангажиментите на администратора по прилагане на разпоредбите на Регламент (ЕС) 2016/679 и действащото национално законодателство на Република България, относимо към защитата на личните данни.

§3. За всички неуредени в настоящите вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.