

ИНСТРУКЦИЯ за мерките и средствата за защита на личните данни събрани, обработвани, съхранявани и предоставяни от ДП №162

1. Общи положения

Чл. 1. (1) ДП №162 „ВИХРОЛОНЧЕ“ е юридическо лице със седалище гр.София, Република България с основен предмет на дейност учебно – възпитателна дейност.
(2) ДП №162
обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им.

Чл. 2. (1) Настоящата инструкция урежда организацията на обработване и защитата на лични данни на преподавателите, служителите, обучаемите (деца), посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на детското заведение. Целта на настоящата инструкция е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от детското заведение регистри, за да се гарантира неприкосновеността на личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събраните и обработвани такива данни.
(3) Инструкцията се приема с цел да регламентира:

- 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 процес 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, слушайна 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) Инструкцията се утвърждава, допълва, изменя и отменя от Директора на детското заведение.

Чл. 3. Настоящата инструкция се прилага за обработването и съхранението на лични данни по смисъла на Регламент 679/2016 г.

Чл. 4. (1) Детското заведение е администратор на лични данни.

(2) Според Регламент 679/2016 „субект на лични данни“ е: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

Чл. 5. (1) (1) Според Регламент 679/2016 „лични данни“ са: 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, 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) Според Регламент 679/2016 „обработване“ е: всяка операция или свързана с нея операция, 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 комбинирание, ограничаване, изтриване или унищожаване

(3) Личните данни се събират и обработват:

- за изпълнение на правомощията и присъщата дейност на детското заведение, предоставени чрез Закона и училищното и предучилищно образование и законодателството на Република България и ЕС;
- въз основа на законови задължения, възложени чрез законодателството на Република България и ЕС /законали, 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 ;

администратора или на трета страна, освен когато пред таква интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни.

(4) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(5) Личните данни се обработват при спазване на следните принципи, въведени чрез Регламент 679/2016 г.: законосъобразност, добросъвестност, прозрачност, ограничаване на целите, свеждане на данните до минимум, точност, организиране на съхранението, цялостност, поверителност, отчетност. (6) събирането на лични данни трябва да бъде в рамките на необходимото. Информативта се събира по законен и обективен начин; личните данни не трябва да се използват за цели, различни от тези, за които са били събрани, 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; 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. Детското заведение организира и предприема мерки, за защита на личните данни от случайни или незаконно унищожаване, от неправомърен 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) Детското заведение прилага адекватна 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 автоматизираните информационни системи и/или мрежи;

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, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на детското заведение и/или нормативното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на детското заведение се извършва на хартиен, технически 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. За всяка дейност по събиране на лични данни се поддържа регистър на дейностите в Приложение № 1 към настоящата инструкция, където е определено кой, за какви цели и на какво основание обработва личните данни.

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

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на директора на детското заведение.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържаша лични данни. Всяко умислено 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, съдържаша лични данни, се извършва на хартиен носител в помещението, определено за архив, за спорове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(3) Съхраненето 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 системи и/или външни носители на информация. Архивиране на личните данни на технически носители 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 повреда 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 оторизирани длъжностни лица.

(5) Достъп до архивирани документи, съдържаша лични данни, имат единствено оторизирани 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, служителът, констатирачът, констатира това нарушение, докладва писмено за този инцидент на директори на детското заведение.

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

(3) Ръководство трябва да уведоми Комисията за защита на личните данни до 72 часа от узаването за неправомерна достъп.

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

Чл. 15. (1) След постигане целта на обработване на личните данни или преди превърлянето на контрола върху обработването личните данни, съдържани се в поддържащите от детското заведение регистри, следва да бъдат унищожени или превърляни на друг администратор на лични данни. При промени в стурктурата на детското заведение, налагани превърляне на лични данни. При промени в стурктурата на детското заведение, налагани превърляне 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, детското заведение прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване на 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, съдържани данни, се унищожават чрез нарязване или изгаряне.

(3) Унищожаване се осъществява от служителя, отговорен за архива на детското заведение.

Чл. 16. (1) Достъпът до данните от регистъра и разкриването на личните данни се осъществява:

- физическите лица, за които се отнасят данните;

- трето лице, ако е предвидено в нормативен акт;

- обработващи лични данни.

(2) Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(3) Физическото лице може да поиска копие от обработваните лични данни на предпоставан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(4) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление (Приложение № 3), респ. искане за достъп на информация, и след тяхното легитимиране.

(5) Заявлението съдържа:

1. името, адреса и други необходими данни за идентифициране на съответното физическо лице;

2. описание на искането;

3. предпочитана форма за предоставяне на достъпа до личните данни;

4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Директорът разглежда заявлението за достъп и се произнася по него в 14-дневен срок.

(7) Директорът взема решение за предоставяне на пълен или частичен достъп на заявителя или мотивира отказ за предоставяне на достъп.

(8) Директорът писмено уведомява заявителя за решението си. Уведомяването е лично срещу подпис или по пощата с обратна разписка.

II. Мерки по осигуряване на защита на личните данни

Чл. 17. (1) Физическа защита в детско заведение се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нередовен достъп и защита на сградите и помещениата, в които се обработват и съхраняват лични данни.

(2) Основните приложими мерки за физическа защита в детското заведение включват определяне на помещениата, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационни-информационните системи за обработване на лични данни, вкл. и определяне на организационна физическа защита.

Като мястена, в които се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служителите с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещениата се обособява непублична част, която е физически ограничена и достъпа само за служителите, на които е необходимо да имат достъп с оглед изпълнение на служебните им задължения.

Комуникационни-информационните системи, използвани за обработка на лични данни, се разполагат в помещенията, 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 ангажменти за поддръжката на нормалното функциониране на тези системи. Послелките нямат достъп до съхраняваните в електронен вид данни.

Организирана на физическа защита до помещенията, 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.

Като зони с ограничена достъп се определят всички помещения на територията на детското заведение, в които се събират, обработват и съхраняват лични данни.

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* в детското заведение включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожаропасителни 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. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

5. съгласие за поемане на задължение за неразпространение на личните данни; изразено в декларация по образец.

(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 със:

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. *Определение на регистрите, които ще се поддържат на хартиен носител*: на хартиен носител се съхраняват всички лични данни, които изискват потвърждение 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 детската градина;

2. *Определение на условията за обработка на лични данни*: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на детското заведение, 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. *Определение на срокове за съхранение*: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществява целта, за която са били събрани и/или изискванията на действащото законодателство.

5. *Процедури за унищожаване*: Документите, съдържани 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 детското заведение, се унищожават по подходящи 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 детското заведение включва набор от приложими технически и организационни мерки за

предотвратяване на нежелан 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, оценени с ниско ниво на въздействие, включват:

1. *Идентификация* чрез използване на пароли за липата, които имат достъп до мрежата и ресурсите на детското заведение. 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 натовадени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3. *Застава от ендуси*, 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 ръководител компютърен кабинет или от лице с въменени трюлови функции и технически познания.

4. Политиката по създаване и поддръжка на резервни копия за възстановяване регламентира - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на детското заведение.

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

6. *Персоналната защита на данните* е част от цялостната охрана на детското заведение.

7. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуклите на детското заведение.

8. Данните, които вече не са необходими и чийто срок за съхранение е изтекъл, се унищожават чрез *приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

9. По отношение на личните данни се прилагат и мерки, свързани с *криптозащита*

защита на данните чрез стандартните криптографски възможности на операционните системи, на програмите за управление на бази данни и на специализирания софтуер, с които се работи в детското заведение, когато това е необходимо.

(2) Криптирането се използва и за защита на личните данни, които се предават от СКМ по електронен път към НАЦ, НОИ и др. подобни учредения когато това се изисква.

III. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

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

(5) С цел повишаване сигурността на достъпа до информацията за длъжностните лица, 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 отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказуемост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставяването ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В детското заведение 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 осигуряване максималната им защита от неправомърен достъп, загубване, повреждане или унищожаване.

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

IV. Поддржани ретистри и тяхното управление

Чл. 25. Поддржките от детско заведение ретистри с лични данни са най-малко следните такива:

1. деца

2. Родители

3. Персонал

4 Други специалисти

5. Прониквателен и регистрационен режим

6. Видеонаблюдение

7. Контакти и партньори

8. „Кандидати за работа“

Чл. 26. (1) В ретистър „деца“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „деца“, обхващани в ДП в областта/района.

(2) Общо описание на ретистър „деца“

Ретистърът съдържа следните категории лични данни:

1. Физическата идентичност на лицето: име, ЕГН, адрес, акт за раждане, месторождение, телефони за връзка;
2. Семейна идентичност - родствени връзки;
3. лични данни, които се отнасят до здравето.

Нормативното основание е ЗПЛО и приложимото законодателство, свързано с предоставяването на образователни услуги.

(3) Технологично описание на ретистър „деца“:

> носители на данни:

На картисен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи помещения на операторите на лични данни, снабдени със заключващи механизми. Информацията от картисените носители за всяко дете, се записва в Ретистър на деца, които се обучават в детските градини на територията на съответната област или район; Ретистър на деца, които се обучават в специални детски градини за обучение и подкрепа на деца със сензорни увреждания и в центрове за специална образователна подкрепа на територията на съответната област/район;

Дневник на група/Дневник за дейности за подкрепа за личностно развитие;

Личен картон за ресурсно подпомагане със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите изолирани помещения

- На технически носители: Личните данни се въвеждат в специализирана Информационна система - НЕИСПЛО. Базата данни се намира на твърдия диск на изолирани компютри. - срок на съхранение: съгласно Нормативната на делата в институцията със срокове на съхранение;

(4) Определение на длъжностите:

Обработващи лични данни на ретистър „деца“ са: директор, зам.-директор, VII, ЗАС, РУ, учители, психолози, логопеди и сензорни терапевти.

Оператор на лични данни на ретистър „деца“ е целия педагогически персонал.

Длъжностите лица - обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1. поверителност - средно ниво;

2. пълнота - средно ниво;
 3. наличност - средно ниво;
 4. общо за релитър - средно ниво.
- (6) *Организационни мерки за физическа защита* - определени са помещениата, в които ще се обработват лични данни и са разположени комуникационни-информационните системи за обработване на лични данни, като физическа защита е организирана само за глужките с оглед изпълнение на глужбите им задължения (на база заключаване на системи). Достъп се предоставя само на глужките, на които той е необходим, за изпълнение на глужбите им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е организиран чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

Технически мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещениата с пожарогасителни средства. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддржане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддржане на информацията и на хартиен носител.

(7) Детското заведение предприема действия при защита на лични данни като съставя план за действие при различни случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от детската градина - предприемат се конкретни действия в зависимост от конкретната ситуация;
 2. защита от пожари - незабавно гасене със собствени средства / пожарогасители / и уведомяване на съответните органи;
 3. защита от наводнения - предприемат действия по организиране на разпространението, както и се изпомпва вода или зарежда със собствени подръчни средства.
- (8) Достъп до релитър „дети“ имат и държавните органи - МОН, РЗО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни на децата се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Норменклатурата на децата със сроковете за тяхното съхранение в институцията.

(10) След постигане на целите по предходната алинея личните данни на децата се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 27. (1) В релитър **„Родители“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настъпници и други категории, свързани с тях лица.

(2) Общо описание на релитър **„Родители“**

Релитърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, телефони за връзка и месторабота;
2. семейна идентичност - семейно положение и родствени връзки.
3. чувствителни данни/данни за здравословното състояние

4. Социална идентичност – образование, трудова дейност

Нормативното основание е ЗПЛО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на ретисър „Ролител“:

> носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни, снабдени със заключващи механизъм.

Информацията от хартиените носители се записва в личните дела на дщата:

Дневник на група със задължителни ревизити съгласно Наредба № 8 от 11.08.2016 г. за

информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите изолирани помещения.

- На технически носители: предвижда се електронен дневник на всяка група.
- Срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(4) Определение на длъжностите:

Обработващи лични данни на религиозни, психолози, логопеди и сензорни терапевти. УЧ, РУ, психолози, логопеди и сензорни терапевти.

Оператор на лични данни на религиозни, психолози, логопеди и сензорни терапевти. Длъжностните лица - обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на религиозни по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за религиозни - ниско ниво.

(6) *Организационни мерки за физическа защита* - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационни-информационните системи за обработване на лични данни, като физическа защита е ограничаване само за служители с отглед извършване на служебните им задължения (на база заключаване на системи). Достъп се предоставя само на служителите, на които той е необходим, за извършване на служебните им задължения. 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.

Технически мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на активирани програми, периодично архивиране на външен носител, както и чрез поддържане на инфраструктурата и на хартиен носител. (7) Делското задвижение предприема превантивни действия при защита на лични данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от институцията - предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно пасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3. защита от наводнения - предприемат действия по организиране на разпостранението, както и се изпомпва вода или зарежда със собствени поддръжни средства.

(8) Достъп до религиозни, родителски и държавните органи - МОН, РЛО, дирекции „Социално подпомагане“ за извършване на техните задължения, предвидени в съответните закони и подзаконни нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съди, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с извършването на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в институцията.

(10) След постигане целите по приходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 28. (1) В регистър „Персонал“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Общо описание на регистър „Персонал“

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕНН, адрес, данни от л.к., месторождение, телефони за връзка и банкови сметки;

2. психологическа идентичност - документи относно психическото здраве;

3. социална идентичност - образование и трудова дейност;

4. семейна идентичност - семейно положение и родствени връзки;

5. чувствителни лични данни - които се отнасят до здравето;

6. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване,

Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събраните данни в регистъра е свързано с :

1. Индивидуализиране на трудовете правоотношения;

2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действие законодателство;

3. Дейностите, свързани със сключаване, съществуване, изменение и прекратяване на трудовете правоотношения, изготвяне на договори, допълнителни споразумения, запоеди, документи, удостоверяващи трудова стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.

4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(2) Технологично описание на регистър „Персонал“:

> носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета). Папките се поддържат в шкафове, които са разположени в изолирани заклучващи помещения на операторите на лични данни, наблюдавани със заклучващи механизми.

- На технически носители: Личните данни се въвеждат в специализирана счетоводна програма: счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(3) Определения на дължкостите:

Обработващи лични данни на регистър „Персонал“ са: директор,

глав.счетоводител и ЗАС и касиер.

Оператор на лични данни на регистър „Персонал“ е директор.

(4) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(5) *Организационни мерки за физическа защита* - определени са помещениата, в които ще се обработват лични данни и са разположени комуникационни-информационните системи за обработване на лични данни, като физическа достъп е ограничен само за служителите извършване на служебните им задължения (на база заключаване на системи). Достъп се предоставя само на служителите, на които той е необходим, за извършване на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещениата с пожарогасителни средства. Трудовите досиата на персонала не се изнасят извън сградата на институцията. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на връшнен носители, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на вълности за заплати или платно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на институцията.

При въвеждане на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед осигуряване максималната им защита от неправомерен достъп, зареждане, повреждане или унищожаване.

(6) Деското заведение предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от деското заведение - предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3. защита от наводнения - предприемат действия по организиране на разпространението, както и се изпомпва вода или зарежда със собствени поръчни средства.

(7) Достъп до регистър „Лецонал“ имат и държавните органи - НАЦ, НОИ, МОН, РУО за извършване на техните задължения, предвидени в съответните закони и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с извършването на техните правомощия.

(8) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в институцията.

(9) След постигане целите по предходната агента личните данни се унищожават физически чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 29 . (1) В регистър „Други специалности“, се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Общо описание на регистър „Други специалности“

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, данни от л.к., месторождение, телефони за връзка и банкови сметки;

2. психологическа идентичност - документи относно психическото здраве;

3. социална идентичност - образование и трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки;

5. лични данни, които се отнасят до здравето;

6. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, ЗЗД, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събираните данни в регистъра е свързано с:

1. Индивидуализиране на трудовите или граждански правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключаване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, запоеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверение и др.
4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(10) Техническино описание на регистър „Други специалности“:

> носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трюлови досети) и каси с граждански договори. Папките и касиорите се подкрепят в шкафове, които са разположени в изолирани заклучващи помещения на операторите на лични данни, снадобени със заклучващи механизми.

- На технически носители: Личните данни се въвеждат в специализирана счетоводна програма: счетоводно, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно Нормативната на делата в институцията със срокове на съхранение;

(11) Определение на длъжностите:

Обработващи лични данни на регистър „Други специалности“ са: директор,

гл.счетоводител, ЗАС и касиер.

Оператор на лични данни на регистър „Други специалности“ е директора.

(12) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(13) *Organizational мерки за физическа защита* - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физически достъп е ограничен само за служителите с отгледено изпълнение на служебните им задължения (на база заклучващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещението с пожарогасителни средства. Трудовите условия и класиранските договори на персонала не се изнасят извън сградата на институцията.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на картисен носител. При изготвяне на вестимости за заплати или платно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на институцията.

При внедряване на нов програмен продукт за обработване на лични данни се провеждат възможностите на продукта с оглед осигуряване максимална им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(14) Детското заведение предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили формално-срещни, а именно:

1. защита при аварии, независещи от институцията - предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства/пожарогасители/ и уведомяване на съответните органи;

3. защита от наводнения - предприемат действия по организиране на разпространението, както и се изпомпва вода или зарежда със собствени поддръжни средства.

(15) Достъп до регистър „Други специалности“ имат и държавните органи - НАЦ, НОИ, МОН, РЛО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(16) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в институцията.

(17) След постигане целите по приходната линия личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 30 . (1) В регистър „Пропусквателен и регистрационен режим“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Категориите физически лица, за които се обработват лични данни, са посетителите на детското заведение.

(3) Обработваните лични данни на регистър „Пропусквателен и регистрационен режим“ са: Охранител, изпълняващ дейността по Организация на охранителната дейност и служителите от фирмата, която обслужва детското заведение извършващи монтаж и техническа поддръжка на системите.

(4) Оператор на лични данни на регистър „Пропусквателен и регистрационен режим“ е директора.

(8) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

(7) Източниците, от които се събират данните, са: от физически лица. Регистърът се попълва с данни от автоматично видеоанализиране (видеобраз) за движението на служителите и посетителите. Видеоанализирането се извършва чрез изградена система за видеоанализиране.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните и на лица, ако е предвидено в нормативен акт.

(5) Регистърът съдържа следните групи данни:
- физическа идентичност на лицето; видеобраз;

(4) Оператор на лични данни на регистър **„Видеоанализиране“** е директора.

(3) Обработващи лични данни на регистър **„Видеоанализиране“** са: служителите от фирмата, която обслужва детското заведение извършващи монтаж и техническа поддръжка на системите.

(2) Физическа идентичност – видеобраз на служителите, родители, ученици, контрагенти и други посетители на детското заведение.

Чл. 31 (1) В регистър **„Видеоанализиране“** се намират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

На технически носители не се предвижда.

Извънредна ситуация служителът се евакуира заедно с дневника.

„Инструкция за съхранение на документи на хартиен носител“; В случай на

На хартиен носител Дневник на хартиен носител се съхранява в съответствие с

инструкцията.

(9) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на

4. общо за регистъра - ниско ниво.

3. наличност - ниско ниво;

2. пълнота - ниско ниво;

1. поверителност - ниско ниво;

(8) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

(7) Източниците, от които се събират данните, са: от физически лица.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните и на лица, ако е предвидено в нормативен акт.

- физическа идентичност на лицето; трите имена на посетителя.

(5) Регистърът съдържа следните групи данни:

2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за ретисътра - ниско ниво.

(9) Данните в ретисътра се предоставят доброволно от лицата при влизането им в сградата на институцията.

Чл.32 (1) В ретисътра „Контрагентни и партньори“ се набират и съхраняват лични данни на лица, участващи в процеса на осъществяваната дейност на детското заведение.

(2) В ретисътра се съдържат данни от група

– Физическа иденитичност – име, адрес, телефон за връзка, електронен адрес за кореспонденция;

Образователна иденитичност – информация за дипломи и други документи за образование и допълнителна квалификация;

Трудова иденитичност – трудов стаж, предишни работодатели;

Друга информация предоставена от кандидатата за работа по свое усмотрение.

(3) Определение на длъжностите:

Обработващи лични данни на ретисътра „Контрагентни и партньори“ са: зам.директор АСД, гл. счетоводител и ЗАС.

(4) Оператор на лични данни на ретисътра „Контрагентни и партньори“ е директора, Нивото на въздействие на ретисътра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за ретисътра - ниско ниво.

(6) *Организационни мерки за физическа защита* - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с отглед изпитание на служебните им задължения.

В. Права и задължения на лицата, обработващи лични данни

Чл. 33. (1) В ретисътра „Кандидати за работа“ се набират и съхраняват лични данни на лица, кандидатстващи за работно място в детско заведение.

(2) Ретисътра съдържа следните категории лични данни:

Физическа иденитичност – име, адрес, телефон за връзка, електронен адрес за кореспонденция;

Образователна иденитичност – информация за дипломи и други документи за образование и допълнителна квалификация;

Трудова иденитичност – трудов стаж, предишни работодатели;

Друга информация предоставена от кандидатата за работа по свое усмотрение.

(3) Цел и основание за събиране на лични данни в регистър „кандидати за работа“ – потенциалният работодател да направи информирани подбор на персонал. Законно основание и цел на събраните лични данни е да се даде възможност на (4) Технологично описание на регистър „кандидати за работа“

Личните данни постъпват от кандидат за работа когато:

- На хартиен носител – когато кандидатът за работа подава документи на място в детското заведение;
 - На електронен носител – когато кандидатът за работа изпраща необходимите документи по електронна поща;
- Срок на съхранение:

- На хартиен носител – 3 календарни месеца;

- На електронен носител – 3 календарни месеца.

(5) Лъжкостности, които обработват и имат достъп до личните данни от регистър „кандидати за работа“

Директор.....

(6) Правила за обработка-Документите съдържат лични данни на кандидат за работа се комплетируют в досие на кандидата (в папка или джоб за документи). Всички досиета на кандидати, които не са утвърдени за назначаване, се комплетируют в обща папка с етикет „Кандидати за работа/Година“ и се предават за съхранение в архив.

(7) Ниво на въздействие на регистър „кандидати за работа“

Повреителност – ниско ниво

Лъжкостност – ниско ниво

Наличност – ниско ниво

Общо за регистъра – ниско ниво

(8) Организацията на работата, технически и мерки за защита на електронни данни- Има разпоредба утвърден Правилник за защита на личните данни. Лъжкостностите лица, които обработват лични данни на кандидат за работа, са подписали „Декларация за конфиденциалност“ и допълнение на Лъжкостността характеристика, и са преминали обучение за правилата за обработка на лични данни. Има назначено Лъжкостно лице за защита на личните данни, което контролира операторите на данни за правилното прилагане на мерките за защита и управлението на лични данни. Хартиен носител се съхранява в съответствие с „Инструкция за съхранение на документи на хартиен носител“. Електронните данни се съхраняват в съответствие с „Инструкция за техническо съответствие на информационната среда“

(9) Защита при извънредни ситуации- при извънредни ситуации се действат в съответствие с **Аварийен план** и **Противопожарни правила**. Взети са мерки за защита – осигурени са пожарогасителни средства. Служителите са преминали инструктаж.

В случай на регистриран неправилен достъп до личните данни на кандидатите за работа Лъжкостното лице за защита на личните данни предприема незабавни действия за предотвратяване на пробива в съответствие с „Инструкция за техническо съответствие на информационната среда“ и информира засегнатите лица в 3 дневен срок от констатирането на неправилен достъп в писмен вид чрез „Ведомление до субектите на данни за нарушение на сигурността на личните данни“

(10) Личните данни на кандидатите за работа не се предоставят на трети страни. След изтичане на срока за съхранение данните се унищожават в съответствие с вида на носителя. Поддържа се „**Бланка за унищожени лични данни**“.

Чл.34 (1) Лице по защита на личните данни е такава,което е в трудово-правни отношения с институцията или е в гражданско правоотношение със същата.
(2)Лицето наречено за краткост (длъжностно лице) по защита на личните данни има следните правомощия:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организацията процедура за обработка на личните данни, включваща време, място и ред при обработване, чрез регистрацията на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 35. Служителите на институцията са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
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 идентификация 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.

Чл. 36. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

(2) Ако в резултат на действията на 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 съответното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Преходни и заключителни разпоредби

§ 1. По смисъла на настоящата инструкция:

- **“Лични данни”** са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез едни или повече специфични признаци.
- **“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 институцията ДД.....
- **“Ниво на защита”** е степен на организация на обработката на личните данни в

зависимост от рисковете и вида им.

“Обработване на лични данни” е всяко действие или съвкупност от действия, които

- **“Обработван лични данни”** е лице, което обработва лични данни от името на администратора на лични данни, когато се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, закриване чрез предаване, разпространяване, актуализиране или комбиниране, блокиране, заличаване или унищожаване. Предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.
- **“Обработван лични данни”** е лице, което 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 на лични данни.
- **“Оценка на въздействие”** е процес за определяне нивата на въздействие върху администратора има достъп до лични данни и упражнява организиране по тяхната обработка съобразно нормативните актове, регламентиращи дейността на институцията.
- **“Поверителност”** е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- **“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.
- **“Съгласие на физическото лице”** е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недовъзмислено се съгласява, че да бъдат обработвани.
- **“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.
- **“Всички служители на институцията са длъжни да се запознаят с институцията и да я спазват.”**
- §3 За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Регламент 679/2016.
- §4. Инструкцията е утвърдена със Заповед №/.....2018г.

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долу подписаният/ата.....

ЕЛН:.....

Лична карта №....., издадена от..... на.....г.

ДЕКЛАРИРАМ:

Съгласен/а съм.....

да обработва личните ми данни, съгласно изискванията на Регламент 2016/679/ЕС Запознат/а съм с:

целта и средствата на обработка на личните данни;

доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;

правото ми на достъп и на копиране на събраните данни;

правото да оттегля съгласието си;

получателите или категориите получатели, на които могат да бъдат разкрити данните.

правото ми на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България.

ДЕКЛАРИРАМ, че ще уведомявам администратора на лични данни за всяка промяна в личните ми данни.

ДЕКЛАРИРАМ, че давам своето съгласие за обработване на лични данни свободно, съгласно волята си, и гарантирам верността на посочените

данни:.....

ДЕКЛАРАТОР:.....

гп./с.....

Дата:

ПРИЛОЖЕНИЕ № 1

**ДО ДИРЕКТОРА
НА
ГР.....
ЗАВЪЛЕНИЕ**

**за предоставяне на лични данни
от**

.....

име, презиме, фамилия
адрес: гр./с.

Упълномощено лице:
ул. № бл., вх., ет., ап., тел.

Адрес : гр. ул.
(име, презиме, фамилия)

Пълномощно №..... от (нотариално заверено, приложено към заявлението)

ОТНОСНО: Предоставяне на лични данни
(описание на искането)

УВАЖАЕМА Г-Н/Г-ЖО ДИРЕКТОР,

ВЪВ връзка

с

.....
1.
2.
с настоящото заявление се обръщам към Вас с оглед получаване на лични данни относно:

Предпочитам формата на предоставяната информация да бъде във вид на
(на дискета, CD, копиец, факс, електронна поща и др.)

Адрес за кореспонденция :
гр. ул. № бл., вх., ет., ап. тел.
Получател:
(име, презиме, фамилия)

С уважение:

Съгласие на родители за обработване лични данни на деца за образователни цели

Долу подписаният давам своето съгласие на снима/ки на детето на възраст да бъде използвана/ни за цели и включена в материалите на центъра, Училището/ ДТ.

Запознат съм, че личните данни ще се съхраняват по следния начин: , според законовите изисквания за защита на данните. Запознат/а съм с: целта и средствата на обработка на личните данни; доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им; правото ми на достъп и на копиране на събраните данни; правото да оттегля съгласието си; получателите или категориите получатели, на които могат да бъдат разкрити данните;

правото ми на възражения и жалби във връзка с обработването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България..

Декларирам, че ще уведомявам администратора на лични данни за всяка промяна в личните данни на детето. Запознат съм, че личните данни ще бъдат обработвани от так посочения администратор на лични данни, а именно: (посочват се имената и контактите на администратора). Запознат съм, че имам право да оттегля съгласието си за обработване на лични данни на детето частично или изцяло по всяко време, за което следва да уведомя администратора по следния начин: и на следните контакти: Запознат съм, че имам право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България. Декларирам, че давам своето съгласие за обработване на лични данни свободно, съгласно волята си, и гарантирам верността на посочените данни.

Дата: ДЕКЛАРАТОР:.....

гр./с.....

ПРИЛОЖЕНИЕ № 1

РЕЗИСТЪР

1. Името и координатите за връзка на:
- администратора и — когато това е приложимо — на всички съвместни администратори;
- на обработващия лични данни;
- на длъжностното лице по защита на данните.
2. Описание на регистъра.
3. Описание на дейността по събиране на лични данни.
4. Цели на събирането.
5. Законово основание.
6. Видове лични данни, които се събират.
7. Субекти на лични данни.
8. Получатели на лични данни.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава.
10. Гаранции за извършени прехвърляния на лични данни към трети държави или международни организации (ако е приложимо).
11. График със срокове на изтриване и основанието за срока, ако е възможно.
12. Локация на личните данни.
13. Общо описание на техническите и организационни мерки за сигурност.
14. Изисква ли се оценка на въздействието? Ако да — оценката.

ПРИЛОЖЕНИЕ № 1

ДЕКЛАРАЦИЯ

Долу подписания/ата
ЕПН: Лична карта №

издана от на г.

ДЕКЛАРАЦИЯ М:

Като обработващ лични данни нямам право да разпространявам информация за личните

данни, станали ми известни при изпълнение на служебните си задължения.

Запознат съм със законодателството във връзка със защитата на личните данни.

Нося отговорност за опазване на документите, съдържащи лични данни.

За неспазване на разпоредбите нося административна отговорност.

Дата: ДЕКЛАРАТОР:

(подпис)

г/с.....

ДЕКЛАРАЦИЯ

Администратор на лични данни:
Субект на лични данни:
Относно следните лични данни:, получени

В качеството си на администратор/обработващ/лични данни и извършвайки задълженията си съгласно Общия регламент за защита на данните декларирам, че ще използвам Вашите лични данни, описани по-горе, за следната цел: сключаване на договор/предоставяне на допълнителна подкрепа на детето/ученика; издаване на удостоверение за квалификация на кредит.....

Основание за обработването: *упражняване на публична власт на администратора на данни*
Декларирам, че личните Ви данни ще бъдат третиранни като строго поверителни и няма да бъдат споделяни.

Ще съхранявам Вашите лични данни не повече от закононо установения срок като данните ще бъдат съхранявани по следния начин:

Вашите права във връзка с настоящото събиране и обработване на лични данни са следните:

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни
- имате право да прекъснете личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна
- имате право да поискате да копирам без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на копиране или допълване на личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни

- имате право да поискате от администратора личните Ви данни да бъдат изтрети без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте отгегли своето съгласие; когато сте възрази срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрети с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

- Администраторът може да откаже да заличи личните данни по следните причини:
1. упражняване на правото на свобода на изразяването и правото на информация;
2. за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора ;

3. по причини от обществен интерес в областта на общественото здраве;
4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заначаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

- имате право да поискате администратора на личните Ви данни, да ограничи обработването на личните Ви данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани. Ако администраторът откаже да ограничи личните Ви данни, той следва да направи това само изрично и в писмен вид, като се мотивира за законосъобразната причина за този отказ.

- имате право да оттеглите Вашето съгласие за обработване на личните Ви данни по всяко

време с отделна молба, депозирана пред администратора ;

- имате право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република

България;

- при нужда Вашите лични данни ще бъдат използвани за нова цел, която не е обхваната от

настоящото известие за защита на данните, ще Ви се предостави ново известие за защита на данните, когато и където е необходимо, ще изискаме Вашето предварително съгласие за

новото обработване.

Данни за контакт на администратора:

Дата Подпис

СЪГЛАСИЕ

Долуподписаният с подписването на този формуляр

потвърждавам, че съм прочел това известие за защита на данните, като съм получил

разяснение на зададените от мен въпроси във връзка с текста и съм съгласен/а

..... да съхранява и обработва моите лични данни за посочените в

декларацията цели.

Съгласен съм и разбирам напълно описаното в настоящата декларация за поверителност и

ще се възползвам от предоставените ми права при необходимост.

Дата..... Подпис.....

ИНСТРУКЦИЯ ЗА СЪХРАНЕНИЕ НА ДОКУМЕНТИ НА ХАРТИЕН

НОСИТЕЛ

УТВЪРДИЛ:
/Директор/



Настоящата Инструкция регламентира правилата за съхранение и архивиране на документи на хартиен носител съдържаша лични данни. Ръководителът на организацията определя Заповед Помещенията, в които се съхраняват и/или архивират документи, съдържаша лични данни като изрично документи се класифицират по отношение на тяхното използване – дали ще бъдат използвани по време на текущата учебна година или са преминали в архив. Документите, съдържаша лични данни, които се използват в ежедневната практика се съхраняват при следните общи условия;

1. Определат се длъжностните лица, които оперират и имат достъп до документи;

2. Осигурява се ограничен достъп по подходящ начин;

3. Организира се периодична проверка на спазването на правилата за ползване и съхранение на документи, съдържаша лични данни;

4. При констатиране на отклонения в правилата за работа ръководителът на организацията предприема действия за предотвратяване на нередовните действия (заповеди, промени в организацията писмените правила за работа). Помещенията, определени за архив, трябва да отговарят на следните оптимални изисквания:

1. да са пожарообезопасени;

2. да бъдат сухи, леснопроветривии и изолирани от пряко действие на слънчевия лъчи;

3. през тях да не минават канализационни, топлопроводни и газоотоплителни пътища;

4. електрическата инсталация да е защитена; не се допуска използване на открити осветителни и отоплителни уреди;

5. пространствената подредба да осигурява лесен и удобен достъп до съхраняваните документи;

6. да е осигурено със средства за ограничаване на физическия достъп чрез надеждни заключващи системи и със средства за аварийен достъп.

Документите да се съхраняват в метални стелажки или метални шкафове. Два пъти годишно се извършва основно почистване на архивните помещения, съчетано с дезинфекция, дезинсекция и депатизация.

В общия план на организацията за управление при кризи се включва раздел за действията и по отношение на архива.

Поддръжката на документите в архивохранилищата се извършва по схема, изготвена по структурно-хронологичен принцип. Делата с общоадминистративен

Документите се поставят и съхраняват в твърди папки или в кутии. Твърдите папки и подвързаните токове се съхраняват във вертикално положение в помещенията, определени за архивохранилища, се съхраняват само документи. Достъп до архива имат само длъжностните лица, отговарящи за съхраняването и използването на документите от архива, и в тяхно присъствие - лица, оторизирани да извършват контрол по опазването и съхраняването на документите. Документите съдържат лични данни се използват от служителите съгласно вътрешните правила.

Изясняването на документи извън организациите за нуждите на специализирани държавни органи се извършва съобразно действащото законодателство и след писмено разрешение от ръководителя на организацията. За всяко изясняване и връщане на документи извън организациите се изготвя предавателно-приемателен протокол, в който се описват документите, определя се срокът за използване и се декларира ангажиментът за връщането им в архива. При установяване на липси и увреждания след връщането на документите в архива се съставя протокол и писмено се уведомява ръководителят на организацията. Длъжностното лице, отговарящо за архив, проверява състава и състоянието на документите преди и след използване.