УТВЪРЖДАВАМ :
МАРИЯ ГРАМОВА
ДИРЕКТОР

ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

В ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ХОТЕЛИЕРСТВО И ТУРИЗЪМ „ АКАДЕМИК НЕДЕЛЧО НЕДЕЛЧЕВ" - СЛИВЕН

I. Общи положения

Чл. 1. (1) ПГХТ „Акад. Н. Неделчев" - Сливен е юридическо лице със седалище гр. Сливен, Р България с основен предмет на дейност образование и образователни услуги.
(2) Гимназията обработва лични данни във връзка със своята дейност и сама определя целите и средствата за обработването им.
Чл. 2. Настоящите правила уреждат организацията на обработване и защитата на лични данни на учителите, служителите, обучаемите (ученици), посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на гимназията.
Чл. 3. (1) Като „обработване на лични данни" се възприема всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.
(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 4. Гимназията е администратор на лични данни по смисъла на чл.3 от Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година и на чл. 3, ал.1 от Закона за защита на личните данни и е вписана в регистъра на администраторите на лични данни и на водените от тях регистри на личните данни по чл.10, ал.1, т.2 от ЗЗЛД с уникален идентификационен номер 1307792.
Чл. 5. (1) „Лични данни" са всяка информация, отнасяща се до физическо и/или юридическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Принципите за защита на личните данни са:

1. Принцип на обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

- субектът на данните да е дал съгласието си за обработката на личните данни за една или повече конкретни цели.
- обработката е необходима за изпълнението на договор, по който съответното физическо лице е страна, или за да се предприемат стъпки по искане на субекта на данните преди сключването на договор.
- обработката е необходима за спазването на правно задължение, на което се подчинява администраторът.
- обработката е необходима, за да се защитят жизнените интереси на субекта на данните или на друго физическо лице.
- обработката е необходима за изпълнение на задача, изпълнявана в обществен интерес или при упражняване на публична власт, предоставена на администратора.
- обработването е необходимо за целите на легитимните интереси, преследвани от администратора или от трета страна, освен когато пред такива интереси преимуществено имат интереси или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете – не се прилага за обработването, което се извършва от публични органи при изпълнението на техните задачи.

2. *Принцип на ограничено събиране* – събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин;

3. *Принцип на ограниченото използване, разкриване и съхраняване* – личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;

4. *Принцип на прецизност* – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;

5. *Принцип на сигурността и опазването* – личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

В съответствие с чл. 11 ал. 3 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 6. Гимназията 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) ПГХТ 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 автоматизирани 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 гимназията и/или нормалното ѝ функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на училището 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. Физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец. Съгласието трябва **да бъде изрично**, както по отношение на събраните данни, така и по отношение на целите, за които се използва (член 7, определен в член 4 от Регламента). Съгласието за **деца** трябва да бъде дадено от **родителя или попечителя** на детето **и да бъде проверено** (член 8). (дете – 16 години) по образец.

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

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на гимназията.

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

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

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

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. 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 системи 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 ѝ 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 лица.

Чл. 12. С оглед защита на хартиените, електронните 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 прекия си ръководител, който от своя страна е длъжен, своевременно да информира училищното ръководство.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, 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 ѝ, гимназията може да определи друго ниво на защита за регистъра.

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 гимназията регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни (чл. 25). При промени в структурата на училището, 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, гимназията прилага 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.

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

Чл. 16. (1) Физическото лице, за което се отнасят данните има право на:

- Информираност
- Достъп до собствените си лични данни
- Коригиране (ако данните са неточни)
- Изтриване на личните данни (правото „да бъдеш забравен“)

Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление (по образец), респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, гимназията съобщава в 30-дневен срок от подаване на заявлението, респ. искането.

(3) Срокът по ал. 2 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(4) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;

3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.
(5) Изключение се допуска единствено за тези органи и/или институции, които извършват това въз основа на изискване на закона (напр. МОН, МВР, съд, прокуратура, НАП, НОИ и др.).

II. Мерки по осигуряване на защита на личните данни

Чл. 17. (1) ***Физическа защита*** в гимназията 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 гимназията 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.
Като *помещения, в които ще 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 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.
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.
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.
Като *зони с контролиран достъп* се определят всички помещения на територията на училището, 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 гимназията 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. 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;

(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. *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 училището;

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 училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

3. ***Регламентиране на достъпа до регистрите*:** достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;

4. ***Определяне на срокове за съхранение*:** личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.

5. ***Процедури за унищожаване:*** Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на гимназията, 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 гимназията 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, оценени с ниско ниво на въздействие, включват:

1. *Идентификация* чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. 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 ръководител компютърен кабинет.

4. Политиката по ***създаване и поддържане 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 гимназията.

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. ***Персоналната защита на данните*** е част от цялостната охрана на гимназията.

7. ***Личните данни в електронен вид се съхраняват*** съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.

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

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

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 отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, 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 без устройствата, на които се съхраняват лични данни.**

Чл. 23. (1) В гимназията 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 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.

IV. Поддържани регистри и тяхното управление

Чл. 25. (1) Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно

определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

(2) Поддържаните от ПГХТ регистри с лични данни са:

1. Персонал
2. Кандидати за работа
3. Ученици
4. Родители
5. Контрагенти
6. Заявление за упражняване на права
7. Посетители
8. Видеонаблюдение

(3) Право на достъп до регистрите с лични данни имат само служители на РУО - Сливен, съобразно възложените им от закона правомощия, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.
(4) Оторизирането на служители се извършва по силата на длъжностна характеристика или чрез изричен акт на директора на ПГХТ.
(5) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл.26. (1) В Регистър „Персонал" се обработват лични данни, свързани с педагогическия и непедагогически персонал на Професионална гимназия по хотелиерство и туризъм „Акад. Неделчо Неделчев" (Училището) . В качеството си на Администратор на лични данни, Училището е необходимо да обработва описаните по-долу категории с лични данни на педагогическия и непедагогическия персонал - учителите и служителите, работещи в Училището.

Категории лични данни и цели на обработването

- Физическа идентичност: име; ЕГН; адрес; данни от лична карта (без копия на документи за самоличност); телефон.
- Социална идентичност: образование; трудова дейност, професионална квалификация, правоспособност
- Семейна идентичност: семейно положение; родствени връзки.
- Икономическа идентичност: Сметки за превод на заплати
- Данни за здравословно състояние: Медицинско свидетелство при постъпване на работа, Болнични листове, Лекарски експертизи, Решения на ЛКК, ТЕЛК и НЕЛК, , здравна книжка
- Други: свидетелство за съдимост за лицата, за които същото се изисква – чл.215 и сл. от ЗПУО., информация **членство в професионална организация.**

<u>Физическа идентичност:</u>
Тези лични данни се обработват с цел на сключване на договор (трудов или граждански) с лицата както и с цел с цел да се провери законовото право на лицето да работи;

Социална идентичност:

- данни за придобитото образование на субекта на данни (вид на образованието, място, номер и дата на издаване на дипломата) са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата, както и за други свързани с управлението на човешките ресурси цели, като участие на служителите в програми за допълнително обучение/квалификация и професионално развитие;
- Трудова дейност - професионална биография. Данните са от значение при избора на подходящо за съответната длъжност лице, както и за други свързани с управлението на човешките ресурси цели, като участие на служителите в програми за допълнително обучение/квалификация и професионално развитие.
- Квалификация и правоспособност - Данните са от значение при избора на подходящо за съответната длъжност лице, ккакто и за преценка относно участие на служителите в програми за допълнително обучение/квалификация и професионално развитие

Семейна идентичност

Семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години). Данните са необходими при установяване правата на лицата за получаване на семейни добавки за деца до 18 години.

Икономическа идентичност :

номер на сметка за превод на заплати. С цел осъществяване на законово задължение да се заплаща престиран труд.

Чувствителни лични данни (специално защитени лични данни)

- Медицинско свидетелство за започване на работа. Данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, както и при необходимост на съобразяване на условията на труд със специфичното здравословно състояние на лицето и в случаите, в които това се изисква от действащото законодателство., документ от психодиспансер, че лицето не се води на отчет.
- Болнични листове и други медицински документи на служителя/работника, свързани с временна нетрудоспособност.
- Документ, че лицето не се води на отчет – нормативно изискване за заемане на определени длъжности с оглед видана извършената дейност.

Други данни

- Гражданско-правен статус на лицата, необходими за длъжностите, за заемането на които е поставено такова изискване.организация
- свидетелство за съдимост.
- Информация за участие в професионална

– **Основания за обработване**

Личните данни се предоставят на Администратора на лични данни (АЛД) от субекта на данни, за които те се отнасят във всички случаи, когато е необходимо. Когато не е налице хипотезата на чл.6, т.1, б”б” от Регламент 2016/ 679 (чл. 4, ал. 1, т. 1 от Закона за защита на личните данни), физическите лица, чиито лични данни се обработват от Училището, подписват декларация за съгласие по образец.

Законовите основания за обработване на данните са посочени в Кодекса на труда, Закона за счетоводството, Закон за облагане на доходите на физическите лица, Кодекс за социално осигуряване, Закон за предучилищно и училищно образование и др. и имат за цел: управлението на човешките ресурси и администрация, да се улеснят административните функции Лица, на които данните могат да бъдат разкривани на: субектите на данни, трети лица, по силата на договор; на лица, обработващи личните данни, на предвидени в закон държавни органи.

Технология на събиране и обработване

Личните данни в Регистър „Персонал" се набират при постъпване/възлагане на работа по трудово или гражданско правоотношение на дадено лице, Не се изисква и впоследствие прилага ксерокопие на документ за самоличност в личното трудово досие. В допълнение, някои лични данни се събират от други органи и публични регистри, в електронни и/или документи на хартиен носител, в качеството на работодател, чиито задачи включват разплащателни/ осигурителни функции и функциите на човешките ресурси, както е описано по-горе.

В случаите, когато Администраторът събира лични данни директно от служителите/ работниците, съгласно чл. 13 от Регламент 2016/679, то информира субекта на данни за необходимостта от обработване на лични данни, категориите лични данни и целите, за които ще бъдат използвани личните данни, получателите или категориите получатели, на които личните данни могат да бъдат разкрити, задължителния или доброволен характер на предоставянето на личните данни и последствията от тяхното непредоставяне, както и правата му по чл.15 -22 от Регламента.

Изготвеният договор, ако е на електронен носител се съхранява в отделен файл на компютър, като достъп до него имат само определени със заповед на директора лица. Достъп се предоставя на други служители, само ако е необходимо за определена цел, със специално упълномощаване от Директора.

След подписването на трудовия/гражданския договор в два екземпляра, единият екземпляр заедно с останалите носители на лични данни се подрежда в кадрово досие, което се поставя в картотечен шкаф със заключване, в заключващо се помещение, със строг контрол на достъпа., а другият екземпляр от трудовия/гражданския договор се връчва на постъпващия служител.

Личните данни на служителя се съхраняват и в електронен вид в Националната електронна информационна система за предучилищното и училищно образование / НЕИСПУО/ със защитен с парола достъп, достъпен само за определени със заповед на директора лица.. Достъп на други служители се предоставя със специално упълномощаване от Директора или упълномощено от него лице.

При необходимост от поправка или актуализиране на личните данни, лицето предоставя такива на директора на Училището или на упълномощени от него лица.

При гореописаните случаи, силно ограничен достъп до лични данни имат служители от счетоводството във връзка с изготвяне на разплащателни документи, за преводи на възнагражденията на лицата, наети по трудови и граждански правоотношения по банков път, както и във връзка със заплащането на данъчни и осигурителни задължения, подаване на декларации и други данни в тази връзка към компетентните органи и изпълнението на други нормативно определени задължения на работодателя.

Личните данни от Регистър „Персонал” се съхраняват на хартиен и технически носител в предвидените в нормативен акт срокове. След изтичане на установения срок те се

унищожават по заповед на директора на Училището като за изпълнението се съставя надлежен протокол.

Пренос на личните данните от Регистъра „Персонал" по електронен път се извършва при осигуряване на необходимото ниво на защита в съответствие с действащото законодателство с цел осъществяване на законовите задължения на Администратора на лични данни.

Администраторът / АЛД/ може да предоставя личните данни от Регистъра „Персонал" на лица- обработващи личните данни от името на Директора в съответствие с определените в Политиката за защита на личните данни цели и ред и при осигуряване на необходимата защита.

Администраторът на лични данни може да предоставя личните данни от Регистъра „Персонал" на трети лица - във връзка с изпълнение на нормативно определени задължения на администратора.

АЛД може да предоставя личните данни от Регистъра „Персонал" на субекта на данни или упълномощено от него лице - във връзка с подадено заявление за упражняване на права от субекта. Упълномощаването се доказва с пълномощно, по действащия към настоящият момент ЗЗЛД е необходимо нотариално заверено пълномощно, в проекта на ЗИДЗЗЛД, изготвен във връзка с Регламент 2016/679 не е предвидено изискване пълномощното да е нотариално заверено.

Защитата на личните данни в Регистър „Персонал" се осигурява чрез предвидените мерки в Политиката и процедурите , касаещи личните данни на Училището.

(2) 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.

(3) Общо описание на регистър „**Персонал**"

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, 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, 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 със :

1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия 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.

(4) Технологично описание на регистър **„Персонал":**

носители на данни:

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

- На електронен носител: Личните данни се въвеждат в специализирана счетоводна програма „Плюс Минус“: счетоводство, ЗУР . Личните данни се въвеждат и в Националната електронна информационна система за предучилищното и училищно образование / НЕИСПУО/ Базата данни се намира на твърдия диск на изолирани компютри;
- Срок на съхранение: съгласно Номенклатурата на делата в ПГХТ със срокове на съхранение;

(5) Определяне на длъжностите:
Лице за защита та личните данни в ПГХТ – старши учител
Обработващи лични данни на регистър **„Персонал“** са: зам.-директор , гл.счетоводител, счетоводител - касиер, ръководител направление ИКТ, технически сътрудник.
Оператор на лични данни на регистър **„Персонал“** са **зам.-директори, ръководител направление ИКТ, технически сътрудник**
(6) 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.
(7) *Организационни 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 физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи 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.
(8) Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.
Трудовите досиета на персонала не се изнасят извън сградата на училището.
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 хартиен носител.
При изготвяне на ведомости за заплати или щатно 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 гимназията.
При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните

данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.
(9) ПГХТ 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 ПГХТ – 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 ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
(10) Достъп до регистър **„Персонал“** имат и държавните органи – НАП, НОИ, МОН, РУО 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.
(11) 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 ПГХТ.
(12) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне, за което се изготвят актови протоколи за унищожаване.

Чл. 27. (1) В регистър **„Ученици“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в гимназията.
(2) **Общо описание на регистър „Ученици“**
Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. културна идентичност: интереси и хоби;
3. социална идентичност – образование;
4. семейна идентичност - родствени връзки;
5. лични данни, които се отнасят до здравето.

Нормативното основание е ЗПУО, ЗЗО, КСО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) **Технологично описание на регистър „Ученици“:**
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 защитна сигнализация. Разпечатка на личното образователно дело на ученика за дневна, задочна и самостоятелна форма на обучение, разпечатки на регистрационни книги за: издадените документи за завършена степен на образование и за придобита професионална квалификация, за издадени удостоверения, за издадените дубликати на удостоверения, за издадените дубликати на документи за завършена степен на образование и за придобита професионална квалификация, Книга за регистриране

на даренията в професионално училище 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 електронен носител: Личните данни се въвеждат в Националната електронна информационна система за предучилищното и училищно образование / НЕИСПУО/ . Базата данни се намира на твърдия диск на изолирани компютри. В електронен вид се попълват и съхраняват : личните образователни дела на учениците / 3-З/, дневници на паралелки / 3-87/, дневник за дейности за подкрепа на личностното развитие / 3-63.1/, регистрационни книги за издадените документи и дубликати на документи.
- След приключване на учебната година информацията за съответната учебна година се архивира както следва: В НЕИСПУО- се архивират документите с номенклатурен номер, за които има електронен раздел; в гимназията- документите , освободени от графичен дизайн;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър **„Ученици“** са: Зам.-директори, технически сътрудник, ръководител направление ИКТ, Светлана Минкова, педагогически съветник и класни ръководители.

Оператор на лични данни на регистър **„Ученици“** е целият педагогически персонал.

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 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.

(6) ***Организационни 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 физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи 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.

(7) Техническите 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 антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(8) ПГХТ 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 ПГХТ – 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 ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
(9) Достъп до регистър „Ученици“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ 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.
(10) Лични данни на учениците 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 ПГХТ.
(11) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 28. (1) **В Регистър „Кандидати за работа”** се обработват лични данни, свързани с лица кандидатстващи за работа като педагогически или непедагогически персонал в Професионална гимназия по хотелиерство и туризъм „Акад. Неделчо Неделчев”. (Училището). В качеството си на Администратор на лични данни, Училището е необходимо да обработва описаните по-долу категории с лични данни на кандидатите за работа.
Категории лични данни и цели на обработването

- Физическа идентичност: име; ЕГН; адрес; данни от лична карта (без копия на документи за самоличност); телефон.
- Социална идентичност: образование; трудова дейност., квалификация, правоспособност
- Данни за здравословно състояние-специално защитени данни: Медицинско свидетелство при постъпване на работа,
- Други: свидетелство за съдимост на лицата, (необходими за длъжностите, за които закон или друг нормативен акт изисква това (ЗПУО – чл.215 и следващите)

Физическа идентичност: Тези лични данни се обработват с цел да се провери законовото право на лицето да работи;
Социална идентичност:
Данни за придобитото образование на субекта на данни са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане;
Трудова дейност - професионална биография. Данните са от значение при избора на подходящо за съответната длъжност лице;
Калификация и правоспособност - Данните са от значение при избора на подходящо за съответната длъжност лице.
Специално защитени данни - Медицинско свидетелство за започване на работа.
Данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, както и при необходимост на съобразяване на условията на

труд със специфичното здравословно състояние на лицето и в случаите, в които това се изисква от действащото законодателство.,
Други данни - Гражданско-правен статус на лицата, необходими за длъжностите, за които се изисква такъв документ , напр. свидетелство за съдимост., във връзка с изискването, разписано в Закона за предучилищно и училищно образование(чл.215 и следващите)

Основания за обработване:
Личните данни се предоставят на Администратора на лични данни (АЛД) от субекта на данни, за който те се отнасят във всички случаи, когато е необходимо. Физическите лица, чиито лични данни се обработват от Училището декларарират съгласие за това.
Законовите основания за обработване на данните са посочени в Кодекса на труда, ЗЗД, ЗПУО и др. Нормативни актове се събират, за да се улеснят административните функции на АЛД. Лица, на които данните могат да бъдат разкривани на: субектите на данни, трети лица, на лица, обработващи личните данни; на предвидени в закон държавни органи.
Технология на събиране и обработване
Личните данни в Регистър „Кандидатите на работа" се набират при кандидастване за работа по трудово или гражданско правоотношение на дадено лице. Не се изисква и впоследствие прилага ксерокопие на документ за самоличност в личното трудово досие. В допълнение, някои лични данни се събират от други органи и публични регистри, в електронни и/или документи на хартиен носител.
В случаите, когато Училището събира лични данни директно от субектите на данни, съгласно чл. 13 от Регламент 2016/679, информира субекта на данни за необходимостта от обработване на лични данни, категориите лични данни и целите, за които ще бъдат използвани личните данни, получателите или категориите получатели, на които личните данни могат да бъдат разкрити, задължителния или доброволен характер на предоставянето на личните данни и последствията от тяхното непредоставяне, както и правата му по чл.15 -22 от Регламента.
Личните данни на кандидата се съхраняват на хартиен носител и са достъпни само за определени със заповед на директора лица. Достъп на други служители се предоставя със специално упълномощаване от Директора или упълномощено от него лице.
При необходимост от поправка или актуализиране на личните данни, лицето предоставя такива на директора на Директора на Училището или на упълномощени от него лица.
Личните данни от Регистър „Кандидати за работа" се съхраняват на хартиен и електронен носител за срок от 3 години. След изтичане на установения срок те се унищожават по заповед на директора на Училището, като за изпълнението се съставя надлежен протокол.
АЛД може да предоставя личните данни от Регистъра на лица - обработващи личните данни от името на Директора в съответствие с Политиката и правилата , касаещи личните данни при осигуряване на необходимата защита.
АЛД може да предоставя личните данни от Регистъра на трети лица - във връзка с изпълнение на нормативно определени задължения на администратора.
АЛД може да предоставя личните данни от Регистъра на субекта на данни или упълномощено от него лице - във връзка с подадено заявление за упражняване на права от субекта.
Защитата на личните данни в Регистъра се осигурява чрез предвидените мерки в Политиката и процедурите, касаещи личните данни на Училището.

Достъп до Регистър „Кандидати за работа” имат техническия сътрудник , заместник-директорите и лица определени със заповед на директора.

Чл. 29. (1) В регистър „**Родители**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

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

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, телефони за връзка и месторабота;
2. икономическа идентичност – финансово състояние;
3. социална идентичност – образование, трудова дейност;
4. семейна идентичност – семейно положение и родствени връзки.

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

(3) Технологично описание на регистър „**Родители**“:

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 защитна сигнализация. Информацията от хартиените носители се записва в електронния дневник на паралелката 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 електронен носител: Личните данни се въвеждат в електронния дневник на паралелката.
- Срок на съхранение: до завършване на ученика

(4) Определяне на длъжностите:

Обработващи лични данни на регистър **„Родители“** са: ЗДУД; ЗДУПД; ТС, ръководител направление ИКТ, Светлана Минкова и класни ръководители.

Оператор на лични данни на регистър **„Родители“** е целия педагогически персонал.

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 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.

(6) *Организационни 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 физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи 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.

(7) Техническите 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 антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.
(8) ПГХТ 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 ПГХТ – 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 ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
(9) Достъп до регистър „Родители“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ 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.
(10) Лични данни се съхраняват до осъществяване на целите, за които се обработват.
(11) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне, за което се изготвят протоколи за унищожаване.

Чл. 30. (1) **В Регистър „Контрагенти“ не се обработват специално защитени данни.**

- Физическа идентичност: име; ЕГН; адрес; телефон за връзка;
- Данните са необходими за идентификация на лицето, за необходимата кореспонденция с контрагента и за счетоводни цели.
- Срок на съхранение
- Данните в регистъра се съхраняват 5 години.

Основания за обработване:
Обикновено данните събирани от контрагентите се отнасят до юридическо лице и могат да включват информация, представляваща лични данни за съответното лице за контакт с това юридическо лице. В повечето случаи, търговският договор с контрагента е между АЛД и Контрагента. АЛД получава данните на Контрагента като част от управленските си задължения и обработва данните за цели, свързани с търговски взаимоотношенията и за данъчни и разплащателни нужди.
Лица, на които данните могат да бъдат разкривани: физическите лица, за които се отнасят данните; на трети лица по силата на договор; на лица, обработващи личните данни; на предвидени по закон държавни органи.
Технология на събиране и обработване:
Личните данни в регистър „Контрагенти” биват събрани със възникване на търговски отношенията по силата на договор между АЛД и Контрагента. Както е посочено по-горе, събраните данни могат да съдържат информация, във връзка със служители на контрагента, които изпълняват ролята на лице за контакт, както и информация, която е необходима за

администриране на взаимоотношенията с контрагента, включително и за извършване на плащания към него.
Личните данни, включват ограничено количество информация, необходима за връзка и управление на взаимоотношенията с представител на контрагента, тази информация се използва само за тези цели.
Личните данни, които са свързани с представители/служители на контрагента или контрагенти – физически лица биват съхранявани на защитен с парола електронен носител, достъпен за служители от Счетоводството, които са отговорни за управление на бизнес отношението. Достъп на други служители бива разрешаван само със специално разрешение дадено от директора на база принципа „Необходимост да знае".
Когато има необходимост от корекция или актуализация, лицето трябва да предаде на Директора или или упълномощен от него служител, който управлява бизнес взаимоотношението с контрагента коригираните или актуализирани данни.
В случаите посочени по-горе, служители на АЛД получават достъп до личните данни въз основа на принципа „Необходимост да знае"', във връзка със следното: подготвяне на платежни документи необходими за извършване на банкови преводи за заплащане на възнаграждения; заплащане на данъчни задължения; и изпълнение на други задължения установени със закон.
Личните данни, които се съхраняват в Регистър „Контрагенти" се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за управление на взаимоотношението с доставчика, колкото е необходимо за счетоводните нужди на Администратора на личните данни и/или за изпълнение на правни задължения на директора. Данните ще бъдат унищожени при изтичане на посочения период, съобразно утвърдените процедури за унищожаване.
Данните на хартиен носител свързани с контрагента се съхраняват след предприети технически и организационни мерки, в съответствие с принципите, посочени по-долу.
Електронното пренасяне на лични данни(ако се налага), се осъществява при осигуряване на адекватно ниво на защита в съответствие с приложимото законодателство, за да може АЛД да изпълнява законовите си задължения.
АЛД може да предоставя лични данни от Регистър „Контрагенти" на трети лица, в предвидените в закон случаи и при осигуряване на адекватно ниво на защита.
Защитата на личните данни в Регистър „Контрагенти" се осигурява чрез мерките и средствата, предприети от Училището чрез Политиката по защита на личните данни.

Достъп до Регистър „Контрагенти" има главен счетоводител на училището.

Чл. 31. В Регистър „Заявления за упражняване на права " се обработват лични данни на лица, търсещи информация, касаещи техни лични данни или на представлявани от тях лица.

Данни за физическа идентичност – име – собствено, бащино, фамилно; адрес; телефон за връзка; електронен адрес

Данните са необходими за идентификация на лицето, както и за изпълнение на задължения на АЛД, записани в закон.
Срокът за съхранение на данните е 1 година.

Основания за обработване

Личните данни от лицата се предоставят на администратора на лични данни, а основание

нормативно задължение – Регламент 2016/679, Закона за защита на личните данни.

Лица, на които данните могат да бъдат разкривани: субуктите на данни; обработващи личните данни; на предвидени по закон държавни органи

Технология на събиране и обработване

Информация за/от лицето, желаещо упражни правата си по чл.15 -22 от Регламент 2016/679 може да бъде събрана пряко от АЛД, като например по факс, имейл, или на хартиен носител, въведен с вх.№.

Личните данни в Регистъра се събират от АЛД директно от заявителя, респективно упълномощено лице.

Личните данни, които се съдържат в Регистъра „Заявления за упражняване на права" се съхраняват на хартиен, технически и/или електронен носител за времето основателно необходимо за целите, за които данните са били събрани, или за което е дадено съгласие от лицето, или е необходимо за изпълнение на правните задължения на Директора. Данните следва да бъдат унищожени при изтичане на съответния период за съхранението им.

Електронният пренос на личните данни, ако такъв се налага, се осъществява при осигуряване на защита, програма за защита на системата от външни лица, контрол на достъпа, актуализирана антивирусна защита, както и виртуална частна мрежа за дистанционен достъп, в съответствие с приложимото законодателство, за да може АЛД да изпълнява законните си задължения и за други нужди посочени в Политиката и процедурите на АЛД, както и в съответствие със законодателството приложимо към защита на личните данни.

АЛД може да предоставя лични данни от Регистъра на трети лица, за нуждите исканата информация и при осигуряване на нивото на защита.

Защитата на личните данни в Регистъра се осигурява чрез мерките, предвидени в Политиката и процедурите , касещи обработваните лични данни, на Училището.

Чл. 32. (1) В регистър „**Посетители**" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.
(2) Общо описание на регистър „**Посетители**"
Регистърът съдържа следните групи данни - физическата идентичност: име по лична карта и адрес.
(3) Технологично описание на регистър „**Посетители**": Данните се набират в писмена форма в дневник.
(4) Определяне на длъжностите:
Обработващ лични данни на регистър **„Посетители"** е охраната.
Оператор на лични данни на регистър **„Посетители"** е зам .-директор .
(5) 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.
(6) *Организационни мерки за физическа защита* – определени са позициите, където ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.
(7) Действия за защита при аварии, произшествия и бедствия: длъжностното лице изнася дневника при евакуация.
(8) Достъп до регистър **„Посетители“**: 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.
(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника).
(10) След приключване на дневника, същият се унищожава физически, чрез изгаряне.
(11) Източниците, от които се събират данните, са: от физическите лица.
(12) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.
(13) **На входовете на сградата се поставят информационни табла за уведомяване на гражданите за пропускателния режим в сградата и проверка съгласно чл. 30, ал. 1, т. 1, буква „а” и „б” от ЗЧОД, както и за използването на технически средства за наблюдение и контрол, съгласно чл. 30, ал. 2 и ал. 4 от ЗЧОД.**
Чл. 33. (1) В регистър „**Видеонаблюдение**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.
(2) Общо описание на регистър „**Видеонаблюдение**“:
Категориите физически лица, за които се обработват лични данни, са посетители, ученици, учители и служители в сградата на гимназията.
Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз.
(3) Технологично описание на регистър „**Видеонаблюдение**“: Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите в сградата на гимназията.
(4) Определяне на длъжностите:
Оператори на лични данни на регистър **„Видеонаблюдение**“ са заместник- директор и педагогическия персонал.
(5) 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.

(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 оглед изпълнение на служебните им задължения.
(7) 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.
(8) Лични данни се съхраняват в паметта на дивиара за срок от 14 дни. При необходимост записите могат да бъдат свалени на външен носител.

(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.
(10) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.
(11) **На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 131, т. 1, буква „а" и „б" от ЗЧОД и за използването на технически средства за наблюдение и контрол съгласно чл. 30, ал. 2 и ал. 4 от ЗЧОД.**

V. Права и задължения на лицата, обработващи лични данни
Чл. 34. (1) Лице по защита на личните данни е Директорът на гимназията.
(2) Лицето 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 организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация 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.
(3) Лицето по защита на личните данни може да делегира своите пълномощия изцяло и/или частично на други лица.
Чл. 35. Служителите на гимназията 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 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.
Чл.36 (1) Уведомяване на надзорния орган за нарушение на сигурността на личните данни. администраторът има задължение да уведомява надзорния орган за нарушение на данните в рамките на 72 часа след като е узнал за това (член 33).Обработващият данните

трябва да уведоми администратора без неоснователно забавяне, след като узнае за нарушаване на сигурността на ЛД.

(2) **Уведомлението трябва да съдържа най – малко следното:**

- Описание на естеството на нарушението на личните данни, включително, когато е възможно, категориите и приблизителния брой засегнати субекти на данни, както и категориите и приблизителния брой записи за лични данни;
- името и данните за контакт на служителя за защита на данните или на друго звено за контакт, където може да се получи повече информация;
- вероятните последици от нарушаването на личните данни;
- мерките, предприети или предложени да бъдат предприети от администратора за справяне с нарушаването на личните данни, включително, когато е уместно, мерки за смекчаване на евентуалните неблагоприятни последици.

Чл. 37. (1) Администратора на лични данни определя длъжностно лице по защита на данните

(2) Длъжностно лице по защита на данните има следните задължения:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

б) да наблюдава спазването на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

в) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 35 от Регламента ;

г) да си сътрудничи с надзорния орган;

д)да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в член 36 от Регламента, и по целесъобразност да се консултира по всякакви други въпроси.

(3) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

Настоящата заповед да се доведе до знанието на работещите в училището срещу подпис за сведение и изпълнение.

Чл. 38. (1) За неспазването на разпоредбите на настоящата инструкция 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.

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 един 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 Професионална гимназия по хотелиерство и туризъм „Акад. Н. Неделчев“ - Сливен

- „**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 могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

- „**Обработващ 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 има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на гимназията.

- **„Оценка на въздействие“** е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

- „**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, недвусмислено се съгласява, те 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.

§2. Всички служители на училището са длъжни срещу подпис да се запознаят с правилата и да ги спазват.
§3. Правилата се издават на основание чл. 23, ал. 4 от Закона за защита на личните данни и Наредба № 1/30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни, издадена от Комисията за защита на личните данни и Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни
§ 4. По отношение на обработването и защитата на личните данни всички вътрешни процедури от документооборота на Училището трябва да бъдат в съответствие с разпоредбите на Регламент 2016/679, ЗЗЛД и Вътрешните правила.