ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ОБЛЕКЛО И ХРАНЕНЕ „РАЙНА КНЯГИНЯ" – СТАРА ЗАГОРА

гр. Стара Загора, кв. Три чучура - север
Директор: +359 42 652038; Зам.-директори: +359 42 624382; Счетоводство: +359 42 624282;
Канцелария: +359 42 631118 E-mail: info-2400165@edu.mon.bg http://www.pgohsz.com

УТВЪРЖДАВАМ :
ДИРЕКТОР:.....
/Зина Камбурова /

Съгласно Заповед № РД-10-735/18.05.2023 г.

ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
В ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ОБЛЕКЛО И ХРАНЕНЕ
„РАЙНА КНЯГИНЯ"– гр.СТАРА ЗАГОРА

I. Общи положения

Чл. 1. (1) ПГОХ «Райна Княгиня» е юридическо лице със седалище гр. Стара Загора, 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. Настоящищите правила уреждат организацията на обработване и защитата на лични данни на преподавателите, 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. (1)Правилата са разработени в съответствие с 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 личните данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защита на данните).

Чл. 5. Настоящите Правила уреждат:

1. Принципите, процедурите и механизмите за обработка на личните данни;
2. Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;
3. Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;
4. Лицата, които обработват лични данни и техните задължения;
5. Правилата да предаване на лични данни на трети лица в България и чужбина;
6. Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване в случай на инциденти, които случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
7. Технически ресурси, прилагани при обработка на лични данни.

Чл.6. (1) ПГОХ „Райна Княгиня“, гр. Стара Загора събира и обработва лични данни. необходими за осъществяване на своите права и задължения като работодател, доставчик на образователн и услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от гимназията, са групирани в регистри на дейностите по обработване, съдържащи правила за обработванена лични данни, отнасящи се до:

- работници и служители;
- изпълнители по граждански договори;
- кандидати за работа;
- доставчици на услуги;
- ученици и родители.

(2) Относно лицата, заети по трудови или граждански правоотношения в учебното заведение. и на кандидатите за работа, се събират следните лични данни:
а) Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон. данни по лична карта или паспортни данни;
б) Образование и професионална квалификация; данни, свързани с образование, трудов опит. професионална и лична квалификация и умения;
в) Здравни данни: здравословно състояние, здравни книжки, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;
г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт или електронно свидетелство за съдимост, с което работодателят да се снабди, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на учебното заведение като работодател.
(3) Относно физически лица, контрагенти на учебното заведение, се събират лични данни. които са необходими за изпълнението на законовите задължения на същото като доставчик на услуги, както следва:

- име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни.

(4) Относно физически лица, доставчици на услуги на учебното заведение, се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на учебното заведение от външни доставчици, както следва:

- име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.

(5) ПГОХ „Райна Княгиня“, гр. Стара Загора обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните права и задължения в областта на трудовото и осигурително законодателство.
(6) Относно физически лица, ученици и родители се съхраняват лични данни, необходими за учебно-възпитателния процес.

Чл.7. Целите на обработването на лични данни са:
(1) управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на учебното заведение в качеството му на работодател;
(2) администриране на отношенията с контрагенти на учебното заведение и предоставяне на услуги;
(3) сключване и изпълнение на договори с доставчици за предоставяне на услуги на учебното заведение.

Чл.8. Личните данни:
- ✓ се обработват законосъобразно и добросъвестно;
- ✓ се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели;
- ✓ допълнителното им обработване за исторически, статистически или научни цели е допустимо, при условие че администраторът осигури подходяща защита, като гарантира, че данните не се обработват за други цели;
- ✓ са съотносими, свързани с, и ненадхвърлящи целите, за които се обработват;
- ✓ са точни и при необходимост да се актуализират;
- ✓ се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- ✓ се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
- ✓ които ще се съхраняват за по-дълъг период за исторически, статистически или научни цели, се поддържат във вид, непозволяващ идентифицирането на физическите лица.

Чл.9. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:
(1) Субектът на данните е дал своето съгласие;
(2) Това е необходимо за изпълнение на нормативно установено задължение.
(3) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
(4) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
(5) Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;
(6) Обработването е необходимо за изпълнение на задача от обществен интерес;
(7) Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, трябва да са описани в приложимите известия по защита на данните.
(8) Всички служители в учебното заведение при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни в т. ч. лични данни, както и да не

разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения, като за тази цел подписват декларация по образец.
(9) Учебното заведение поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.

Чл.10. (1) Изразеното съгласие трябва да бъде свободно дадено, конкретно. информиранои недвумислено заявление. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси. Съгласието трябва да бъде дадено свободно.Такова съгласие е налично в случаите, когато субектът на данни има истински и свободен избор и е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.
(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието, то следва да се прекрати.
(3) Декларациите за съгласие се съхраняват от учебното заведение, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност. Съгласието остава едно от алтернативните условия за обработване на личните данни.
(4) Учебното заведение трябва да може да докаже неговото наличие.Субектът на данните следва да бъде информиран за последиците при отказ да даде съгласие за обработване на отделни категории лични данни.
(5) Съгласието може да бъде дадено онлайн. Това може да бъде осъществено чрез отбелязване на отметка в поле, избиране на технически настройки за услуги на информационното общество или друго заявление или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Мълчанието, предварително отметнатите полета или липсата на действие не представляват съгласие.

Чл.11. (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 (Приложение № 1).

Чл.12. 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.13. (1) ПГОХ «Райна Княгиня», гр. Стара Загора 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.14. (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 й 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.15. Физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец. /Приложение № 2,4 /. Съгласието трябва да бъде изрично, както по отношение на събраните данни, така и по отношение на целите, за които се събират. Съгласието за деца трябва да бъде дадено от родителя или попечителя на детето и да бъде проверено (дете – 16 години) Приложение № 3

Чл.16. (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. 17. (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.18. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл.19. (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.20. (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.21. (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. 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.22. (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 (Приложение № 4), 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.23. (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.24. (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.25. (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.26. (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.27. (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.

(5) 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.28. (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.29. (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.30. (1) Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

Чл.31. (1)Събирането, обработването, използването и съхраняването на информацията в системата на предучилищното и училищното образование се извършва чрез НЕИСПУО.

(2)Националната електронна информационна система за предучилищното и училищното образование се състои от електронни модули и интегрирани с тях регистри:

1. **модул "Институции"** съдържа информация, описана в приложение № 1 от Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование и Регистър на институциите в системата на предучилищното и училищното образование съгласно чл. 345, ал. 1 ЗПУО;
2. **модул "Документи за дейността на институцията"** съдържа електронни раздели съгласно приложение № 2 от Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование
3. **модул "Деца и ученици"** съдържа лични образователни дела на децата и учениците с информация, описана в приложение № 3 от Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование, и Регистър на документите за завършено основно образование, средно образование и/или придобита степен на професионална квалификация.

(3) Въвеждането и подаването на данни и документи в НЕИСПУО се извършва с квалифициран електронен подпис, издаден съгласно изискванията на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.) и на Закона за електронния документ и електронните удостоверителни услуги.

(4) Информацията, събирана от институциите, се обработва чрез НЕИСПУО и други информационни продукти, интегрирани с нея и обслужващи определени дейности или процеси в образованието.

(5) Информацията се събира, обработва и съхранява в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ, L 119, 4.05.2016 г.), Закона за защита на личните данни, Наредбата за обмена на документи в администрацията, приета с ПМС № 101 от 2008 г. и с Наредбата за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 2019 г.

(6) Ползването на информацията в НЕИСПУО се осъществява чрез служебен или публичен достъп. Видът и обхватът на информацията, достъпна чрез служебен или публичен достъп, се определя със заповед на министъра на образованието и науката.

1. Служебният достъп осигурява дейността на институциите, на МОН, на неговите административни структури, на Националния инспекторат по образованието (НИО) и на съответните първостепенни разпоредители с бюджет.
2. Публичният достъп осигурява информираност на гражданите, юридическите лица и държавните органи по отношение на системата на предучилищното и училищното образование и се осъществява чрез интернет страницата на МОН при спазване на Закона за защита на личните данни и Закона за достъп до обществена информация.

(7) Информацията в НЕИСПУО се събира, съхранява и ползва от длъжностни лица, определени със заповед на директора на институцията.

Чл.32. Информацията, необходима за издаване на документи за завършване, удостоверяване и признаване на професионално обучение на лицата, навършили 16 години, в институциите за професионално обучение се използва и съхранява по ред, определен с наредбата по чл. 17в, ал. 2 от Закона за професионалното образование и обучение (ЗПОО).

Чл.33. (1) Документите в системата на предучилищното и училищното образование се издават, водят и съхраняват в електронен и/или хартиен вид.

(2) Организирането, обработването, експертизата, съхраняването и използването на документите на хартиен носител се извършва при спазване на Закона за Националния архивен фонд и Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции, приета с ПМС № 41 от 2009 г.

(3) Съхраняването на документите в електронен формат се извършва съгласно Наредбата за обмена на документи в администрацията, приета с ПМС № 101 от 2008 г.

Чл. 34. Документите, издавани или водени от институциите, се създават, попълват и водят или издават на хартиен и/или електронен носител съгласно разпоредбите на Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование.

Чл.35. (1) Документите, които се попълват в електронен вид, се разпечатват с номерирани страници. Достоверността на отразената в документа информация се потвърждава на последната страница с подписите на длъжностното лице по чл. 39, т. 1 от Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование и на директора и се полага печатът на институцията.

(2) Дневниците с номенклатурен номер, посочени в приложение № 2 от Наредба №8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование, се приключват от директора и се подписват с електронен подпис в модул "Документи за дейността на институцията". Те се съхраняват във формат "pdf" съгласно сроковете, описани в приложението, и се разпечатват при необходимост.

IV. Поддържани регистри и тяхното управление

Чл.36. Поддържаните от ПГОХ «Райна Княгиня» регистри с лични данни са:

1. Ученици
2. Персонал
3. Родители
4. Пропускателен режим
5. Видеонаблюдение
6. Доставчици

Чл.37. (1) В регистър **„Ученици“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в гимназията при спазване на ЗПУО, ЗЗО, КСО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(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.
(3) Определяне на длъжностите:
1. Обработващи лични данни на регистър **„Ученици“** са: зам.-директор, ЗАС и класни ръководители.
2. Оператор на лични данни на регистър **„Ученици“** е целия педагогически персонал.
(4) 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.
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.
(7) ПГОХ «Райна Княгиня» 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 ПГОХ «Райна Княгиня» – 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.
(8) 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.
(9) 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 ПГОХ «Райна Княгиня».
(10) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

(11) Сроковете за съхранение са съгласно Номенклатурата на делата в ПГОХ «Райна Княгиня», гр. Стара Загора

Чл.38. (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 при спазване на ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(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.

(3) Сроковете за съхранение са съгласно Номенклатурата на делата в ПГОХ «Райна Княгиня», гр. Стара Загора

(4) Определяне на длъжностите:

1. Обработващи лични данни на регистър **„Родители“** са: ЗДУД; ЗДУПД; ЗАС и класни ръководители.
2. 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.

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.

(7) ПГОХ «Райна Княгиня», гр. Стара Загора 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 ПГОХ «Райна Княгиня» – 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.

(8) 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.
(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 ПГОХ «Райна Княгиня».
(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл.39. (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, като основание за това са: 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.
(2) 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.
Предназначението на събираните данни в регистъра е свързано с:
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.
(3) 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 технически носител: Личните данни се въвеждат в специализирана счетоводна програма „Рефлекс“: счетоводство, ТРЗ. Базата данни се намира на твърдия диск на изолирани компютри.
- Сроковете за съхранение са съгласно Номенклатурата на делата в ПГОХ «Райна Княгиня», гр. Стара Загора
(4) Определяне на длъжностите:
1. Обработващи лични данни на регистър **„Персонал“** са: зам .-директор , гл.счетоводител и счетоводител.

2. Оператор на лични данни на регистър **„Персонал“** 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 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.
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.
(7) ПГОХ «Райна Княгиня» 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 ПГОХ «Райна Княгиня» – 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.
(8) 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.
(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 ПГОХ «Райна Княгиня».
(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл.40. (1) В регистър „**Пропускателен режим**“ 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 „**Пропускателен режим**“
1. Регистърът съдържа следните групи данни - физическата идентичност: име по лична карта и адрес.
(3) Технологично описание на регистър „**Пропускателен режим**“: Данните се набират в писмена форма в дневник.
(4) Определяне на длъжностите:
1. Обработващ лични данни на регистър **„Пропускателен режим“** е охраната.
2. Оператор на лични данни на регистър **„Пропускателен режим** 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 помещенията, в които 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 **„Пропускателен режим“**: 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.41. (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**“:
1. Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградите на гимназията.
2. 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:
1. Оператори на лични данни на регистър **„Видеонаблюдение“** са зам .-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 1 месец. 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. 1, 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.

Чл.42. (1) В регистър „**Доставчици**" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за счетоводството. Категориите физически лица, за които се обработват лични данни, са доставчици, с които работи училището.
(1) Общо описание на регистър „**Доставчици:** "Регистърът съдържа следните групи данни - физическата идентичност: наименование,булстат, седалище и банкова сметка .
(2) Технологично описание на регистър „**Доставчици**": Данните се набират в писмена форма в първични счетоводни документи.
(3) Определяне на длъжностите:
1. Обработващ лични данни на регистър **„Доставчици"** е главен счетоводител.
2. Оператор на лични данни на регистър **„Доставчици"** 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 помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.
(6) ПГОХ „Райна Княгиня" 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 ПГОХ «Райна Княгиня» – 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.
(7) Достъп до регистър **„Доставчици“**: Категориите лица, на които личните данни могат да бъдат разкривани са физически лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт, на лица по силата на договор.
(8) Лични данни се съхраняват до осъществяване на целите, за които се обработват.
(9) След приключване на срока на съхранение, съгласно номенклатурата на делата в ПГОХ „Райна Княгиня“, гр. Стара Загора същите се унищожават физически, чрез изгаряне, след уведомяване на ДА.
(10) Източниците, от които се събират данните, са: от юридически и физически лица.
(11) Данните в регистъра се предоставят доброволно при съставяне на счетоводните документи.

V. Права и задължения на лицата, обработващи лични данни

Чл. 43. (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. 44. 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.45. (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. Обработващият данните трябва да

уведоми администратора без неоснователно забавяне, след като узнае за нарушаване на сигурността на личните данни.
(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.46. (1) Администраторът 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.

Чл.47. (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 настоящите правила:

- **„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 облекло и хранене “Райна Княгиня“ (физическо или юридическо лице, публичен орган,агенция или друга структура, която сама или съвместно с други определя целите исредствата за обработването на лични данни)
- „**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. Обработването също включва и трансфер на лични данни до трети лица.
- „**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.
- **ЗЗЛД** - Закон за защита на личните данни.
- **КЗЛД** - Комисия за защита на личните данни.
- **ОРЗД** - Регламент (ЕС) 2016/679 на Европейски я парламент ина Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива даннии за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

- **Длъжностно лице по защита на данните** - физическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД.
- **Лице, отговорно за личните данни** - лице, което е служител в учебното заведение или изпълнява функции по поръчение, на което са възложени задълженията във връзка със защитата и процесите по обработка на лични данни, уредени в тези Правила. Основните дейности на администратора или обработващия лични данни не се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни или в мащабно обработване на специалните категории данни ина лични данни, свързани с присъди и нарушения.
- **Известия по защита на данните** - отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който учебното заведение събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.
- **Псевдоминизиране** - заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними"), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.
- **«Специфични признаци»** са признаци,свързани с физическа, физиологична, или генетична, психическа, психологическа, икономическа, културна, социална друга идентичност на лицето.
- **«Съвместни администратори»** означава, че двама или повече администратори съвместно определят целите и средствата на обработването на лични данни. Физическото лице, за което се отнасят данните (субект на данни), може да упражнява своите права в областта на защитата на личните данни по отношение всеки и срещу всеки от администраторите.

§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. 1 ал.1, 2, 3 от Закона 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 и са утвърдени със Заповед № РД-10-735/18.05.2023 г.на директора на ПГОХ „Райна Княгиня", гр. Стара Загора и влизат в сила от деня на утвърждаването им.

ПРИЛОЖЕНИЕ № 1 към чл.11

Оценка на нивото на въздействие на регистър към дата 18.05.2023 г.

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	цялостност	наличност	общо за регистъра
Име на регистъра				
персонал	високо	високо	високо	високо
учащи	високо	високо	високо	високо
родители и настойници	високо	високо	високо	високо
доставчици	ниско	ниско	ниско	ниско
видеонаблюдение	средно	средно	средно	средно

ПРИЛОЖЕНИЕ №2

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долуподписаният_____,

ЕГН: _____

Лична карта № _____ издадена от _____ на _____ г.

ДЕКЛАРИРАМ:

Съгласен/а съм Професионална гимназия по облекло и хранене“Райна Княгиня“ гр. Стара Загора да обработва личните ми данни, съгласно изискванията на Закона за защита на личните данни и Общия Регламент / ЕС/ 2016 /679 за изпълнението на трудов договор, граждански договор или услуга/ вярното се подчертава/ .

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 на достъп и на коригиране на събраните данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.

ДЕКЛАРАТОР:

Дата:

гр. Стара Загора

ПРИЛОЖЕНИЕ №3

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долуподписаният_____,

родител/настойник на _____

от _____ клас на ПГОХ „Райна Княгиня“гр. Стара Загора

ДЕКЛАРИРАМ:

Съгласен/а съм Професионална гимназия по облекло и хранене“Райна Княгиня“ гр. Стара Загора да обработва личните данни на детето ми , съгласно изискванията на Закона за защита на личните данни и Общия Регламент / ЕС/ 2016 /679 за изпълнение да дейостите по обучение в дневна задочна ,смостоятелна форма на обучение форма

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 на достъп и на коригиране на събраните данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.

ДЕКЛАРАТОР:

Дата:
гр. Стара Загора

ПРИЛОЖЕНИЕ №4

ДО ДИРЕКТОРА
НА ПГОХ»Р.Княгиня»
ГР. СТАРА ЗАГОРА

ЗАЯВЛЕНИЕ
за предоставяне на лични данни

От _____
(име, презиме, фамилия)

Адрес : гр. _____, ул. “ _____” № __, бл__,вх.__, ет___, ап.___,
тел. _____

Упълномощено лице
_____
Адрес : гр. _____, ул. “ _____” № __, бл__,вх.__, ет___, ап.___
Пълномощно №_____от_____(нотариално заверено, приложено към заявлението)

Относно: Предоставяне на лични данни _____
(описание на искането)

_____
_____

Уважаема _____,

Във връзка с
_____
_____
(посочват се обстоятелствата, във връзка с които се иска информацията)

и на основание Закона за защита на личните данни (ЗЗЛД) с настоящото заявление се обръщам към Вас с оглед получаване на лични данни относно:
1. _____
2. _____
3. _____

Предпочитам формата на предоставената информация да бъде във вид на _____
(на дискета , CD , копие ,факс , електронна поща и др.)

Адрес за кореспонденция :
гр. _____, ул. “ _____” № __, бл__,вх.__, ет___, ап.___,
тел. _____
Получател_____

Дата: _____

С уважение:_____