**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СЕЛСКО СТОПАНСТВО “ГЕО МИЛЕВ”**

**✉ гр. Мъглиж, ул. “Гео Милев” № 70, e-mail: pgssmg@abv.bg, www.pgssmg.com**

**☎ 04321 / 23 10 - Директор, 23 71 - канцелария**

**УТВЪРЖДАВАМ: /п/**

**заповед № 1282-240/28.05.2018 г.**

**ДИРЕКТОР: инж. Татяна Стоева**

# ВЪТРЕШНИ ПРАВИЛА

# ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, СЪГЛАСНО РЕГЛАМЕНТ (ЕС) 2016/679

# НА ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СЕЛСКО СТОПАНСТВО „ГЕО МИЛЕВ“, гр. МЪГЛИЖ

## РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

**Чл. 1** (1) Професионална гимназия по селско стопанство „Гео Милев", гр. Мъглиж, наричана за краткост ПГСС, е общинско неспециализирано професионално училище, чиято дейност се регламентира от Закона за предучилищното и училищното образование и Закона за професионалното образование и обучение.

(2) Изпълнявайки функциите на образователна институция ПГСС обработва лични данни на ученици, записани и кандидатствали в училището; на родителите на ученици; на служителите си, действащи и освободени; на кандидатите за работа; на всички други групи физически лица, с които ПГСС влиза в отношения при осъществяването на правомощията и дейността си, при което се явява администратор на лични данни.

(3) В случаите, в които ПГСС обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от ПГСС и трето лице, ПГСС има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

**Чл. 2.** (1) Настоящите Вътрешни правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД) и уреждат организацията на обработването и защитата на лични данни от ПГСС. Правилата се приемат с цел да регламентират:

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

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

3. Видовете регистри, които се водят в ПГСС, и тяхното описание.

4. Задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, и отговорността при неизпълнение на тези задължения;

(2) Настоящите Вътрешни правила са задължителни за всички категории служители в ПГСС, съобразно с възникваща при изпълнението на служебните им задължения необходимост от обработване на лични данни за регистрите на училището, включително по отношение на задължения на институцията за съхраняване, достъп и предаване на лични данни, възникнали със закон или подзаконов нормативен акт.

**Чл. 3.** (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"). „Физическо лице, което може да бъде идентифицирано“, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

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

(3) „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.

**Чл. 4.** (1) ПГСС е администратор на лични данни по смисъла на чл. 4, т. 7) от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни, при обработването им ПГСС спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

**Чл. 5.** (1) Принципите за защита на личните данни са:

1. ***Законосъобразност, добросъвестност и прозрачност*** - Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субектаите на данните;
2. ***Ограничение на целите*** – Личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели. По-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели, съгласно чл. 89, пар. 1 от Общия регламент относно защитата на данните (ЕС) 2016/679;
3. ***Свеждане на данните до минимум*** – Личните данни са подходящи, конкретни, ограничени до необходимото и свързани с целите, за които се обработват;
4. ***Точност*** – Личните данни са точни и където и доколкото е необходимо са поддържани в актуален вид. Предприемат се всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;
5. ***Ограничение на съхранението*** **–** Личните данни се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни. Личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящи технически и организационни мерки, с цел да бъдат гарантирани правата и свободите на субекта на данните;
6. ***Цялостност и поверителност*** **–** Личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;
7. ***Отчетност*** **–** ПГСС, в качеството си на администратор, носи отговорност и е в състояние да докаже спазването на горните принципи.

(2) Ако конкретната цел или цели, за които се обработват лични данни от ПГСС, не изискват или вече не изискват идентифициране на субекта на данните, ПГСС не е задължена да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

**Чл. 6.** ПГСС 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 на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

**Чл. 7.** ПГСС прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на информационни мрежи.

**Чл. 8.** (1) Личните данни се събират за конкретни, точно определени от законите цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощията и правните задължения на ПГСС и/или за нормалното й функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на ПГСС се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

**Чл. 9.** Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от ПГСС, подписват декларация за съгласие по образец (***Приложение № 1***).

**Чл. 10.** (1) Право на достъп до регистрите с лични данни имат само органите на ПГСС, съобразно възложените им от закона правомощия и оторизираните служители на ПГСС, както и обработващите 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.

(2) Оторизирането на служители /педагогически специалисти и непедагогически персонал/ се извършва на база длъжностна характеристика или чрез изрична заповед на директора на ПГСС.

(3) Педагогическите специалисти и непедагогическия персонал 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 по отношение на съответните служители.

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

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

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

(3) Документите на електронен носител се съхраняват на 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 с цел осигуряване на възможност 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.

(4) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица и органите на ПГСС, съобразно законовите им правомощия.

**Чл. 12.** (1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец, съгласно ***Приложение № 2***.

**Чл. 13.** (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от ПГСС регистри. Проверките се извършват от комисия, назначена от директора на ПГСС, която изготвя Доклад за резултатите от проверките.

(2) Докладите по ал. 1 трябва да включват преценка на необходимостта от обработка на личните данни или от унищожаването им. Докладите се адресират до длъжностното лице по защита на данните и до директора на ПГСС.

**Чл. 14.** (1) При регистриране на неправомерен достъп до регистрите с лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на директор на ПГСС и информира длъжностното лице по защита на данните.

(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.

(3) Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позвалява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

*Данни за уведомяване: Комисия за защита на личните данни*
*Седалище и адрес на управление: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2*
*Данни за кореспонденция: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2*
*Телефон: 02 915 3518*
*Имейл: kzld@government.bg, kzld@cpdp.bg*
*Уеб сайт: www.cpdp.bg*

**Чл. 15.** (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, ПГСС може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

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

**Чл. 16.** (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от ПГСС регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, ПГСС прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;
2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване или изгаряне.

(3) Унищожаването се осъществява от служители, определени със заповед на директора на ПГСС и след уведомяване на длъжностното лице по защита на данните

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3, съгласно образец, представляващ ***Приложение № 3***.

**Чл. 17.** (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, ПГСС съобщава чрез уведомление в 1-месечен срок от подаване на заявлението.

(3) Липсата на уведомление по ал. 2 се счита за отказ.

(4) Администраторът отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон.

(5) Информацията може да бъде предоставена в предпочитаната от заявителя формата:
1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(6) Действията на АЛД по разрешаване или отаз на достъп до лични данни се обжалват по реда на Глава VII от ЗЗЛД.

(7) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец съгласно ***Приложение № 4***, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(8) Третите страни получават достъп до лични данни, обработвани в ПГСС, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, РУО и др.).

## РАЗДЕЛ II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

**Чл. 18.** Конкретните технически и организационни мерки за защита на личните данни в ПГСС „Гео Милев“, сроковете за прилагането им и отговорните лица се регламентират ежегодно в допълнителна инструкция, неразделна част от настоящите Вътрешни правила.

**Чл. 19.** ***Физическата защита*** в ПГСС се осигурява чрез набор от приложими организационни и технически мерки за предотвратяване на нерегламентиран достъп до сградите, помещенията и устройствата, използвани за извършване дейности по обработване на лични данни.

(1) Основните ***организационни мерки за физическа защита*** в ПГСС включват:

1. определяне на помещенията, в които се обработват лични данни – всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват физически носители на лични данни /кабинет на директора, канцелария, стая на главния счетоводител, стая на счетоводството, кабинет на заместник

директора по учебната дейност, кабинет на заместник директора по учебно-производствената дейност, учителска стая, институционален архив, архив на счетоводството, административен архив/;

2. определяне на конкретни лица, отговарящи за воденето и достъпа до регистрите в институцията;

3. определяне на помещенията, в които са разположени елементи на комуникационно-информационни системи за обработване на лични данни – помещения с ограничен достъп, оборудвани с компютърна и комуникационна техника /кабинет на директора, канцелария, стая на главния счетоводител, стая на счетоводството, кабинет на заместник директора по учебната дейност, кабинет на заместник директора по учебно-производствената дейност/;

4. оторизация на физическия достъп - достъпът до помещения, елементи от комуникационно-информационни системи и регистри е физически ограничен и контролиран. Разрешение за достъп дава директора на ПГСС само на служители с оглед изпълнение на служебните им задължения и ако длъжностната им характеристика изисква това. Лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на заключващите системи, СОТ и компютърната техника получават от директора временно достъп до устройствата, като нямат достъп до съхраняваните лични данни.

(2) Основните ***технически мерки за физическа защита*** в ПГСС включват:

1. използване на шкафове и метални каси в помещенията за съхранение на физическите /хартиени и електронни/ носители на лични данни,

2. използване на секретни ключалки и заключващи механизми за ограничаване на достъпа, в работно време, до помещенията и сградите, в които се обработват лични данни или са разположени елементи от комуникационно-информационни системи;

3. използване на сигнално-охранителна техника за ограничаване на достъпа, в извънработно време, до помещенията и сградите, в които се обработват лични данни или са разположени елементи от комуникационно-информационни системи;

4. оборудване на сградите с пожароизвестителна система и на помещенията с пожарогасителни средства в съответствие с изискванията на съответната нормативна база;

5. използване на уникални потребителски идентификатори и пароли за достъп до компютри и сървъри, обработващи лични данни.

**Чл. 20.** (1). ***Мерките за персонална защита*** на личните данни, приложими в ПГСС – засягат всички служители на институцията и ангажимента им към осигуряване на защита на обработваните лични данни.

1. Задължение на служителите да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминат инструктаж и удостоверят това с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (***Приложение № 5***) /за всички служители на институцията/;

2. Деклариране на поемане на задължение за неразпространение на личните данни /за всички служители в институцията/.

3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.) между персонала и всякакви други лица, които са неоторизирани /за всички служители на институцията/;

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;

2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

**Чл. 21.** (1) ***Защитата на информационни системи, мрежи и уеббазирани платформи*** в ПГСС включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до обработваните лични данни.

1. В ПГСС всички работни станции са настроени в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секудни, като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.
2. Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.
3. Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.
4. С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от ПГСС период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).
5. 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.
6. При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.
7. В ПГСС се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.
8. На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от директора на ПГСС лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.
9. При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

(2) ***Публикуване на информация в Интернет*** – извършва се единствено след оторизация от директора на ПГСС, независимо под каква форма, на каква платформа и на какво основание;

(3) ***Използване на квалифициран електронен подпис (КЕП)*** – служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица

## РАЗДЕЛ III. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

**Чл. 22.** (1) В ПГСС се водят и съхраняват следните официални регистри и бази данни:

| № | Видове регистри | Видове лични данни | Начин на съхранение | Обработващ личните данни в регистъра | Място на съхранение на регистъра |
|---|---|---|---|---|---|
| | **Регистри за обучаемите** | | | | |
| 1 | Регистър на лицата, обучавани за придобиване на правоспособност за управление на МПС, категория Ткт | лични данни за лицето: имена, ЕГН, адрес, месторождение, паспортни данни; данни за притежаваното свидетелство за основно образование; резултати от преминатото обучение и положени изпити | Хартиен носител / електронен регистър | Николай Кънев | Кабинет на ръководителя на обучението |
| 2 | Регистър на лицата, придобили правоспособност за управление на МПС, категория Твк | лични данни за лицето: имена, ЕГН, адрес, месторождение, паспортни данни; данни за притежаваното свидетелство за основно образование; резултати от преминатото обучение и положени изпити | Хартиен носител / електронен регистър | Николай Кънев | Кабинет на ръководителя на обучението |
| 3 | Регистър на лицата, придобили правоспособност за управление на МПС, категория В | лични данни за лицето: имена, ЕГН, адрес, месторождение, паспортни данни; данни за притежаваното свидетелство за основно образование; резултати от преминатото обучение и положени изпити | Хартиен носител / електронен регистър | Николай Кънев | Кабинет на ръководителя на обучението |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Регистър на лицата, придобили правоспособност за работа със земеделска и горска техника | лични данни за лицето: имена, ЕГН, адрес, месторождение, паспортни данни; резултати от преминатото обучение и положени изпити | | Николай Кънев | Кабинет на ръководителя на обучението |
| 5 | Регистър на учениците с картотека на личните им картони и дневниците на класовете | лични данни за лицето: имена на ученика; ЕГН; адрес; паспортни данни; месторождение; данни за притежаваното свидетелство за основно образование; данни за образователния статус на ученика /форма на обучение, клас, специалност, професия, постигнати резултати от обучението, отсъствия, издадени документи за завършена степен на образование и квалификация/; здравен статус; данни за родителите – имена, адрес, образователен статус | Електронен регистър и хартиени носители | ЗАС, заместник-директорите, класните ръководители и преподавателите | Учителска стая, канцелории на заместник-директорите |
| 6 | Книга за вписване на подлежащите на задължително обучение ученици | лични данни за лицето: имена на ученика; ЕГН; месторождение; адрес; данни за свидетелството за основно образование; данни за родителите – имена, адрес | Хартиен носител | заместник-директорите, класните ръководители | Канцелария на ЗАС |

| | | | | | |
|---|---|---|---|---|---|
| 7 | Регистрационни книги за издадените документи за завършена степен на образование и професионална квалификация:<br>- Регистрационна книга за свидетелствата за основно образование;<br>- Регистрационна книга за дипломи;<br>- Регистрационна книга за удостоверения за завършен клас;<br>- Регистрационна книга за удостоверения за завършен гимназиален етап;<br>- Регистрационна книга за свидетелства за професионална квалификация;<br>- Регистрационна книга за дубликати на документи за завършена степен на образование и квалификация | лични данни за лицето: имена на ученика; ЕГН; месторождение; формата на обучение; изучавана специалност; данни за фабричния и регистрационен номер на издадения документ; подпис на лицето | Хартиен носител | Мария Желева – ЗАС, заместник-директорите | Канцелария на ЗАС |
| | **Регистри за служители** | | | | |
| 8 | Регистър на служителите в ПГСС с картотека на личните трудови и служебни досиета | лични данни за лицето: имена на служителя; заемана длъжност; ЕГН; адрес; паспортни данни; месторождение; копия на документи за образование и квалификация; документи, доказващи трудовата му дейност; финансова информация; медицински данни; данни относно гражданско-правния статус на лицата (като свидетелство за съдимост) | Електронен регистър и хартиен носител | Мария Желева – ЗАС, касиер, гл. счетоводител | Административен архив |

| | | | | | |
|---|---|---|---|---|---|
| 9 | Картотека с лични данни и документи на кандидати за обявени свободни позиции за преподаватели и служители | трите лични данни за лицето: имена на кандидата; ЕГН; адрес; паспортни данни; месторождение; копия на документи за образование и квалификация; документи, доказващи трудовата му дейност; финансова информация; медицински данни; данни относно гражданско-правния статус на лицата (като свидетелство за съдимост) | Хартиен носител | Мария Желева - ЗАС | Административен архив |
| | **Вътрешноведомствени регистри** | | | | |
| 10 | Регистър на инцидентите с лични данни по чл. 13, ал.2, т.4 от НМНТОМДВЗЛД | имена, ЕГН и адрес на длъжностното лице, установило инцидента;<br>лични данни – обект на инцидента | Хартиен носител | Длъжностно лице по ЗЛД | Канцелария на ЗАС |

## РАЗДЕЛ IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

**Чл. 23.** (1) Длъжностно лице по защита на данните се определя от директора на ПГСС.

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

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 с лични данни;
3. осъществява контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящите вътрешни правила;
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. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола;

10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

12. води регистър на дейностите по обработване на лични данни в ПГСС съласно образеца в Приложение № 6.

**Чл. 24.** Служителите на ПГСС 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 при необходимост регистрите на личните данни;

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.

**Чл. 25.** (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ПГСС или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

## РАЗДЕЛ V. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

**Чл. 26.** Всички служители на ПГСС са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

**Чл. 27.** (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни,.

(2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- **Приложение № 1** – *Декларация-съгласие за обработка на лични данни* (която се подписва, когато обработването не се извършва на друго основание, предвидено в чл. 6 от Регламент 2016/679);
- **Приложение № 2** – образец Протокол за задължителен инструктаж за запознаване с правилата за Противопожарна безопасност;
- **Приложение № 3 –** образец на Протокол за унищожаване на лични данни и носители на лични данни.
- **Приложение № 4** – Споразумение за обработка на данни;
- **Приложение № 5 -** Протокол за преминат нструктаж за приложимите в ПГСС правила и мерки за защита на личните данни;
- **Приложение № 6 –** Регистър на дейностите по обработка;

**Чл. 28.** Настоящите вътрешни правила влизат в сила от 28.05.2018 г.