Д Е Т С К А Г Р А Д И Н А „С Л А В Е Й Ч Е“
Гр.Кюстендил; ул. „Гладстон“ 17; тел.: 078 55 06 02; e-mail: info-1000061@edu.mon.bg

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ДГ „СЛАВЕЙЧЕ“, ГР.КЮСТЕНДИЛ

2025-2026 г.

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл.1.(1) ДГ „Славейче“ е юридическо лице със седалище гр.Кюстендил, Република България, с основен предмет на дейност образование и образователни услуги.
(2) ДГ обработва лични данни във връзка със своята дейност (образователна, възпитаваща, социализираща) и сама определя целите и средствата за обработването им.
Чл.2. (1) Настоящите ВП уреждат организацията на обработване и защита на личните данни на педагогическите специалисти, служителите, децата, посетителите, както и други физически лица, свързани с осъществяването на дейността на ДГ.
(2) Целта на настоящите ВП е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от ДГ регистри, за да се гарантира неприкосвеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.
(3) ВП се приемат с цел да регламентират:

- Създаване на процедури и механизми за гарантиране на неприкосвеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
- Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно, или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение, или разпространение, както и от всички други форми на обработване на лични данни);
- Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

(4) ВП се утвърждават, допълват, изменят и отменят от Директора на ДГ „Славейче“, гр.Кюстендил.

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

Чл.4. (1) ДГ „Славейче“ е администратор на лични данни по смисъла на чл.4, §7 от Регламент (ЕС) 2016/ 679.

(2) Според чл.4, §1 от Регламент (ЕС) 2016/ 679 „субект на лични данни“ е: идентифицирано физическо лице, или физическо лица, което може да бъде идентифицирано.

Чл.5. (1) Според чл.4, §1 на Регламент (ЕС) 2016/679 „лични данни“ са: всяка информация, свързана с идентифицираното 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) Според чл.4, пар.1 от Регламент (ЕС) 2016/679 „обработване“ е: 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, разпространение, или друг начин, по който данните стават достъпни, подреждане, или комбиниране, ограничаване, изтриване, или унищожаване.

(3) Личните данни се събират и обработват:

- За изпълнение на правомощията и присъщата дейност на ДГ, предоставени чрез ЗПУО е законодателството на Р България и ЕС;
- Въз основа на законови задължения, възложени чрез законодателството на Р България и ЕС (закони, наредби, инструкции, правилници, регламенти и др.);
- При сключване на договори, или подготовка за тяхното сключване;
- За защита на жизнено важни интереси на субекта на данните, или друго физическо лице;
- При липса на някое от горепосочените основания – единствено след съгласие на субекта на лични данни, дадено чрез подписана декларация за съгласие (по образец – *Приложение №1*);
- Когато обработването е необходимо за целите на легитимните интереси на администратора, или на трета страна, освен когато пред такива интереси преимущество имат интересите, или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

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

- ***Законосъобразност, добросъвестност и прозрачност –*** обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;
- ***Ограничение на целите –*** събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване на данни, несъвместими с тези цели;

- ***Свеждане на данните до минимум*** **–** данните да са подходящи, свързани с и ограничени до необходимото, във връзка с целите на обработването;
- ***Точност*** **–** поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване, или коригиране на неточни данни, при отчитане целите на обработването;
- ***Ограничение на съхранението*** **–** данните да се обработват за период с минимална продължителност, съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни, или исторически изследвания, стратегически цели, но при условие, че са приложени подходящи технически и организационни мерки;
- ***Цялостност и поверителност*** **–** обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически, или организационни мерки;
- ***Отчетност*** **–** администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(5) Събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин. Личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето, или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели. Личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват. Личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл.6. ДГ организира и предприема мерки за защита на личните данни от случайно, или незаконно унищожаване, от неправомерен достъп, от изменение, или разпространение, както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл.7. (1) ДГ прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

- Физическа защита;
- Персонална защита;
- Документална защита;
- Защита на автоматизирани информационни системи и/или мрежи.

Чл.8 (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на ДГ и/или нормалното му функциониране.

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

Чл.9. За всяка дейност по събиране на лични данни се поддържа регистър на дейностите в *Приложение №3* към настоящите ВП, където е посочено кой, за какви цели и на какво основание обработва личните данни.

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

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

(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 задължения.

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

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив в 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 архивните документи, съдържащи лични данни, имат единствено оторизираните със заповед лица.

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

Чл.13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на директора.

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

(3) Ръководството на ДГ трябва да уведоми длъжностното лице по защита на личните данни и Комисията за защита на личните данни до 72 часа от узнаването за неправомерния достъп.

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

Чл.15.(1) След постигане целта на обработване на личните данни, или преди прехвърлянето на контрола върху обработването на личните данни, съдържащи се в поддържаните от ДГ регистри, следва да бъдат унищожени, или прехвърлени на друг администратор на лични данни, съобразно изискванията на Закона за защита на личните данни (чл.25). При промени в структурата на ДГ, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след решение на Комисията за защита на лични данни.
(2) В случаите, когато се налага унищожаване на носител на лични данни, ДГ 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, в т.ч. презаписването на електронните средства, или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер.
(3) Унищожаването се осъществява от служителя, отговорен за архива на ДГ – ст.уч. Светла Мицова.
Чл.16.(1) Достъпът до данните от регистъра и разкриването на личните данни се осъществява при условията и по реда на ЗЗЛД и Регламент 2016/679 от:

- Физическите лица, за които се отнасят данните;
- Трето лице, ако е предвидено в нормативен акт;
- Обработващия личните данни.

(2) Достъп до лични данни може да бъде предоставен под формата на устна, или писмена справка, както и на преглед на данните от съответното физическо лице, или от изрично упълномощено от него друго лице.
(3) Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител, или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.
(4) Достъп на лица до лични данни се предоставя единствено ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление (*Приложение №2)*, респективно искане за достъп до информация и след тяхното легитимиране.
(5) Заявлението съдържа:

- Име, адрес и други необходими данни за идентифициране на съответното физическо лице;
- Описание на искането;
- Предпочитана форма за предоставяне на достъпа до личните данни;
- Подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Директорът разглежда заявлението за достъп и се произнася по него в 14-дневен срок.
(7) Директорът взема решение за предоставянето на пълен, или частичен достъп на заявителя, или мотивира отказ от предоставяне на достъп.
(8) Директорът писмено уведомява заявителя за решението си. Уведомяването е лично срещу подпис, или по пощата с обратна разписка.

Раздел II
МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.17.(1) ***Физическа защита*** в ДГ 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 ДГ 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, за 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 ДГ, 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 ДГ включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

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

(2) Основните мерки на персонална защита са:

- Познаване на нормативната уредба в областта на защита на личните данни;
- Познаване на политиката и ръководствата за защита на личните данни;
- Знания за опасностите за личните данни, обработвани от администратора;
- Съгласие за поемане на задължение за неразпространение на личните данни, изразено в декларация по образец *(Приложение №4).*

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

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

- Нормативната уредба в областта на защитата на лични данни;
- Политиката и ръководствата за защита на лични данни;
- Опасностите за личните данни, обработвани от администратора.

Чл.19. (1) Основните приложими *мерки за **документална защита*** на личните данни са:

- *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 ДГ;
- *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 ДГ. Начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;
- *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“;
- *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;
- *Процедури за унищожаване.* Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив и след изтичане на законовите срокове за тяхното съхранение не са необходими за нормалното функциониране на ДГ, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и др. подходящи за целта методи).

Чл.20. (1) ***Защитата на автоматизираните информационни системи и/или мрежи*** в ДГ 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:

- *Идентификация* чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на ДГ. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае“;
- *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;
- *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 направление ИКТ;

- Политиката по *създаване и поддържане на резервни копия за възстановяване* има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на ДГ;
- 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 др. носители на информация, еднократно записваеми носители и др.);
- *Персоналната защита на данните* е част от цялостната охрана на ДГ;
- *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на ДГ;
- Данните, които вече не са необходими за целите на ДГ и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване с шредер, постоянно заличаване от електронните средства).

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

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

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

(2) При необходимост от ремонт на компютърна техника, предоставянето ѝ на сервизна организация се извършва по възможност без устройствата, на които се съхраняват лични данни.

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

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице – ръководител на направление ИКТ.

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

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

Раздел III
ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл.25. Поддържаните регистри в ДГ са:

- Човешки ресурси;
- Деца;
- Родители;
- Проекти;
- Счетоводство и финансова отчетност;
- Контрагенти и доставчици;
- Архив

Чл.26. (1) Всички регистри са подробно описани в *Приложение №3* към правилата, което представлява Регистър на дейностите. В него е посочено кой работи с данните от всеки един регистър и какви мерки за защитата им се предприемат.

(2) Всяка година директорът издава заповед, с която определя кой отговаря за всеки отделен регистър.

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

- Ниско ниво на риска – когато загубата, или неправомерното обработване на личните данни от конкретен регистър не биха имали значителни последствия, застрашаващи живота на физическо лице, или кражба на самоличността му;
- Средно ниво на риска – когато загубата, или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на физическо лице;
- Високо ниво на риск – когато загубата, или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на група от физически лица;
- Изключително високо ниво на риск – когато загубата, или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, застрашаващи живота на физическо лице.

Чл.28. При „изключително високо ниво на риск“, констатирано при условията на предходния член, се извършва „оценка на въздействието“ спрямо критериите, залегнали в Регламент (ЕС) 2016/679.

Раздел IV
ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, РАБОТЕЩИ С ЛИЧНИ ДАННИ

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

- Да информира и съветва администратора, или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Общия регламент за защита на данните и на други разпоредби за защита на личните данни на равнище Съюз, или национално законодателство;
- Да наблюдава спазването на Общия регламент и на други разпоредби за защита на данни на равнище Съюз, или национално законодателство и на политиките на администратора, или обработващия лични данни, по отношение на защитата на лични данни;
- Да участва в повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване и съответните одити;

- При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
- Надлежно да отчита рисковете, свързани с операциите по обработване и да се съобразява с естеството, обхвата, контекста и целите на обработването;
- Да участва в заседания на ръководството, когато се обсъждат въпроси от областта на защитата на лични данни;
- Да дава становище (съвет, мнение) по всички въпроси, свързани със защитата на лични данни, да консултира администратора, или обработващия лични данни;
- Да си сътрудничи с надзорния орган;
- Да действа като точка за контакт с надзорния орган по въпроси, свързани с обработването и по целесъобразност да се консултира по всякакви други въпроси с надзорния орган.

(2) ДЛЗД има право:

- Да събира информация за определяне на дейностите по обработване;
- Да анализира и проверява изпълнението на дейностите по обработване;
- Да информира, съветва и отправя препоръки към администратора, или обработващия лични данни;
- Да получава информация и необходимата съдействие от страна на ръководни органи, от администратора/обработващия лични данни, от всички релевантни вътрешни структури, имащи отношение към операциите по обработване на лични данни.

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

Чл.30. Служителите на ДГ са длъжни:

- Да обработват лични данни законосъобразно, добросъвестно и прозрачно;
- Да използват личните данни, до които имат достъп, съобразно целите, за които се събират. Да не ги обработват допълнително по начин, несъвместим с тези цели;
- Да актуализират регистрите на личните данни (при необходимост);
- Да заличават, или коригират личните данни когато се установи, че са неточни, или непропорционални по отношение на целите, за които се обработват;
- 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;
- Да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;
- Незабавно да уведомят администратора на лични данни в случай, че установят изтичане на лични данни, независимо дали при извършване на своята работа, или при друго лице, което обработва лични данни.

Чл.31. (1) За неспазване на разпоредбите на настоящите Вътрешни правила служителите носят административна отговорност.

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

РАЗДЕЛ V
ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Всички педагогически специалисти и служители в ДГ „Славейче“ са длъжни срещу подпис да се запознаят с настоящите Вътрешни правила за защита на личните данни и да ги спазват;
§2. Вътрешните правила се издават на основание чл.23, ал.4 от ЗЗЛД и Регламент (ЕС) 2016/ 679;
§3. За всички неуредени в настоящите Вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, ЗЗЛД и действащото приложимо законодателство на Р България;
§4. Настоящите Вътрешни правила отменят действието на съществуващата до сега Инструкция за защита на личните данни;
§5. Вътрешните правила се утвърждават със заповед на директора на ДГ „Славейче“, гр.Кюстендил.