Начално училище “П. Р. Славейков”– гр. Пловдив
Пловдив,4006, ул. „Славянска”82 тел:(032) 624 506,тел./факс:(032) 632 079,e-mail:nu_prslaveikov@abv.bg

УТВЪ
ДИМ
Дирек

ИНСТРУКЦИЯ

за събиране, обработване и защита на личните данни
в НУ „Петко Р. Славейков“, гр. Пловдив

I. Общи положения

Чл. 1. (1) НУ „П. Р. Славейков“, гр. Пловдив е юридическо лице със седалище град Пловдив, Република България с основен предмет на дейност образование и образователни услуги.

(2) Училището обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.

Чл. 2. Настоящата инструкция урежда организацията на обработване и защитата на лични данни на учителите, служителите, обучаемите (ученици), доставчиците, както и на други физически лица, свързани с осъществяването на нормалната дейност на училището.

Чл. 3. (1) Като „обработване на лични данни“ се възприема 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 друга форма на осигуряване на достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

(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. НУ „П. Р. Славейков“, гр. Пловдив е администратор на лични данни по смисъла на Закона за защита на личните данни и е вписана в регистъра на администраторите на лични данни и на водените от тях регистри на личните данни.

Чл. 5. (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 и умствената, икономическата, културната или социалната идентичност на това физическо лице;

(2) Принципи, свързани с обработването на лични данни:

1. Личните данни са:

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

б) събирани 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 („ограничение на

целите“);

в) подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат 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 („точност“);

д) съхранявани във форма, която да 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 съгласно член 89, параграф 1 от Регламент 16/679 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, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени във въпросния регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) обработвани 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 („цялостност и поверителност“);

2.Администраторът носи отговорност и е в състояние да докаже спазването на точка 1 („отчетност“).

(3) 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. 6. НУ „П. Р. Славейков“, гр. Пловдив 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) НУ „П. Р. Славейков“, гр. Пловдив, прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и/или мрежи;

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

(2) Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) 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;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на НУ „П. Р. Славейков“, гр. Пловдив в качеството ѝ на администратор на данни;

е) обработването е необходимо за целите на легитимните интереси на НУ „П. Р. Славейков“, гр. Пловдив 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.

(3) Когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на съгласието на субекта на данните или на правото на Съюза или правото на Република България, което представлява необходима и пропорционална мярка в едно демократично общество, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, се взема под внимание:

а) всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;

б) контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и НУ „П. Р. Славейков“, гр. Пловдив като администратор на лични данни;

в) естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно член 9 или се обработват лични данни, отнасящи се до присъди и нарушения, съгласно член 10 на Регламента;

г) възможните последствия от предвиденото по-нататъшно обработване за субектите на данните;

д) наличието на подходящи гаранции, които могат да включват криптиране или псевдонимизация.

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

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

Чл. 9. (1) Когато обработването на лични данни не произтича от нормативен акт или законово задължение или основание, е необходимо да се получи съгласие за обработването на данни от субекта чрез писмена декларация за съгласие по образец.

(Приложение № 2).

(2) Ако съгласието на субекта на данните е дадено в рамките на писмена декларация, която се отнася и до други въпроси, искането за съгласие се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като използва ясен и прост език. Никоя част от такава декларация, която представлява нарушение на Регламента не е обвързваща.

(3)Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това. Оттеглянето на съгласие е също толкова лесно, колкото и даването му.

(4) Когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор.

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 училището.

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

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

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

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив 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 личните 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 администраторът и обработващият личните данни в рамките на оторизацията от администратора или на преките му служебни задължения, произтичащи от длъжностната характеристика.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.

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

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, 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.

(3) В случай на нарушение на сигурността на личните данни директорът на НУ „П. Р. Славейков“, гр. Пловдив, в качеството си на администратор на лични данни, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни КЗЛД, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до КЗЛД съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(4) Обработващият лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни. В уведомлението се съдържа най-малко следното:

а) описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(5) Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

(6) Директорът на НУ „П. Р. Славейков“, гр. Пловдив в качеството си на администратор документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

(7) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, директорът на гимназията, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(8) В съобщението до субекта на данните на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват предприетите мерки.

(9) Съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

а) предприети са подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по- специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) впоследствие са взети мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

в) то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

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

Чл. 15.(1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от гимназията регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни (чл. 25). При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2) В случаите, когато се налага унищожаване на носител на лични данни, гимназията прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

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

II. Мерки по осигуряване на защита на личните данни

Чл. 16. (1) *Физическа защита* в НУ „П. Р. Славейков“, гр. Пловдив 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 училището 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 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 на 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 училището включват : използване на ключалки, шкафове, метални каси, използване на сигнално охранителна техника за охрана на помещенията, в които се съхраняват регистри лични данни с високо ниво както и оборудване на помещенията с пожарогасителни средства.

Чл. 17. (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. деклариране 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.

(5) При обработването на лични данни обработващият лични данни спазва инструкциите на администратора и вменените му с длъжностна характеристика или нормативен акт задължения.

Чл. 18. (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. 19. (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 оторизирано техническо лице.

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. 20. (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. 21. (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. 22. (1) В НУ „П. Р. Славейков“, гр. Пловдив 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. 23. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 24. Поддържаните от НУ „П. Р. Славейков“, гр. Пловдив регистри с лични данни са:

1. Ученици
2. Персонал
3. Родители
4. Доставчици
5. Видеонаблюдение

Чл. 26. (1) В регистър **„Ученици“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в гимназията.

(2) Общо описание на регистър „Ученици“

Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, данни от акта за раждане, месторождение, телефони за връзка ;
2. културна идентичност: интереси и хоби;
3. социална идентичност – произход, образование, среда, навици, свидетелство за завършено образование, резултати от НВО;
4. лични данни, които се отнасят до здравето – медицинска здравно-профилактична карта, имунизационен картон – медицинските документи се съхраняват от медицинската сестра и се връщат на ученика при напускане на училището.

Нормативното основание е Законът за предучилищно и училищно образование, подзаконовите нормативни документи и актове и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „Ученици“:

носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове в помещения на операторите на лични данни.
- На технически носител: Личните данни се въвеждат в специализирана информационна система за училищна администрация /НЕИСПУО/. Базата данни се намира на твърдия диск на изолирани компютри.
- срок на съхранение: съгласно Номенклатурата на делата в НУ „П. Р. Славейков“, гр. Пловдив със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър **„Ученици“** са: заместник-директор УД, ЗАС,

счетоводител, класни ръководители и педагогическия персонал.

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

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

1. поверителност – средно ниво;
2. цялостност – средно ниво;
3. наличност – средно ниво;
4. общо за регистъра – средно ниво.

(6) *Организационни мерки за физическа защита* – определени са помещенията, в които 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) НУ „П. Р. Славейков“, гр. Пловдив 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 НУ „П. Р. Славейков“, гр. Пловдив – 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 НУ „П. Р. Славейков“, гр. Пловдив .

(10) След постигане целите по предходната алинея личните данни на учениците се

унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 26. (1) В регистър „**Родители**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

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

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, телефони за връзка, електронна поща.

Нормативното основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на образователни услуги.

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

носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в помещения на обработващите лични данни.
- На технически носител: Личните данни се въвеждат в специализирана информационна система за училищна администрация НЕИСПУО. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно Номенклатурата на делата в НУ „П. Р. Славейков“, гр. Пловдив със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър **„Родители“** са: счетоводител, ЗАС, заместник-директор УД, класни ръководители и педагогическият персонал.

Длъжностните лица – обработващи 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 – високо ниво;
2. цялостност – високо ниво;
3. наличност – високо ниво;
4. общо за регистъра – високо ниво.

(6) *Организационни мерки за физическа защита* – определени са помещенията, в които 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, помещения със сигнално-охранителна техника, 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) НУ „П. Р. Славейков“, гр. Пловдив 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 НУ „П. Р. Славейков“, гр. Пловдив – 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 НУ „П. Р. Славейков“, гр. Пловдив

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

Чл. 27. (1) В регистър „**Персонал**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

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

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, данни от лична карта, месторождение, телефони за връзка, банкови сметки, електронна поща;
2. психологическа идентичност – документи относно психическото здраве;
3. социална идентичност - образование и трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки;
5. лични данни, които се отнасят до здравето;
6. други - лични данни относно гражданско-правния статус на лицата.

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

Предназначението на събираните данни в регистъра е свързано 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 се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в помещения на обработващите личните данни.
- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма : счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно Номенклатурата на делата в НУ „П. Р. Славейков“, гр. Пловдив със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър **„Персонал“** са: счетоводител, ЗАС.

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

1. поверителност – високо ниво;
2. цялостност – високо ниво;
3. наличност – високо ниво;
4. общо за регистъра – високо ниво.

(5) *Организационни мерки за физическа защита* – определени са помещенията, в които 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 и сигнално-охранителна техника.

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.

(6) НУ „П. Р. Славейков“, гр. Пловдив 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 НУ „П. Р. Славейков“, гр. Пловдив – 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 **„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.

(8) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в НУ „П. Р. Славейков“, гр. Пловдив.

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

Чл. 28. (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 и договори с контрагенти**“

Регистърът съдържа следните групи данни - физическата идентичност: наименование, булстат, седалище и банкова сметка .

(2) Технологично описание на регистър „**Доставчици и договори с контрагенти**“: Данните се набират в писмена форма в първични счетоводни документи.

(3) Определяне на длъжностите:

Обработващ лични данни на регистър **„Доставчици и договори с контрагенти“** е счетоводител.

(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) НУ „П. Р. Славейков“, гр. Пловдив 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 НУ „П. Р. Славейков“, гр. Пловдив – 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 НУ „П. Р. Славейков“, гр. Пловдив, 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.

Чл. 29. (1) В регистър „**Видеонаблюдение**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Общо описание на регистър „**Видеонаблюдение**“:

Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградите на НУ „П. Р. Славейков“, гр. Пловдив.

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 НУ „П. Р. Славейков“, гр. Пловдив, както и подстъпите към входовете на сградите.

(4) DVR-ите и мониторите за осъществяване на видеонаблюдението са разположени в обособени места на помещения с оторизиран достъп – кабинет на директора.

(5) Определяне на длъжностите:

Обработващи личните данни на регистър **„Видеонаблюдение**“ са заместник-директорите, педагогическият съветник и класни ръководители /при необходимост/.

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

1. поверителност – средно ниво;
2. цялостност – средно ниво;
3. наличност – средно ниво;
4. общо за регистъра – средно 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 до 30 дни. При необходимост записите могат да бъдат свалени на външен носител.

(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.

(10) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.

(11) На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 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.

V. Права и задължения на лицата, обработващи лични данни

Чл. 30. (1) Администратор на личните данни е Директорът на гимназията.

(2) администраторът 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) Администраторът на данни може да оторизира други лица – обработващи данни.

Чл. 32. Служителите на НУ „П. Р. Славейков", гр. Пловдив 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. 32. (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.

VI. Права на субекта на данни

Чл. 33. За осигуряване на правата на субекта на данни за прозрачна информация, комуникация и условия за упражняването на правата му:

1. Администраторът предприема необходимите мерки за предоставяне на всякаква информация, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства.

2. Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с негово искане, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането.

При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето.

Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

3. Ако администраторът не предприеме действия по искането на субекта на данни, администраторът уведомява субекта на данни без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.

4. Информацията и всяка комуникация и действия се предоставят безплатно.

5. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, НУ „П. Р. Славейков“, гр. Пловдив като администратор на лични данни може или:

а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или

б) да откаже да предприеме действия по искането. Администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

6. Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане по членове 15—21 на Регламента, администраторът може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

Чл. 44 (1) Когато лични данни, свързани с даден субект на данни, се събират от субекта на данните, в момента на получаване на личните данни администраторът предоставя на субекта на данните цялата посочена по-долу информация:

а) данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

б) координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

г) получателите или категориите получатели на личните данни, ако има такива;

д) когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация;

(2). Освен информацията, посочена в алинея 1, в момента на получаване на личните

данни администраторът предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

б) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;

в) съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

г) правото на жалба до надзорен орган;

д) дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

(3). Когато администраторът възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в алинея 2.

(4) Задълженията на горните алинеи на настоящия член не се прилагат, когато и доколкото субектът на данните вече разполага с информацията.

Чл. 45. (1). Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

а) целите на обработването;

б) съответните категории лични данни;

в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

е) правото на жалба до надзорен орган;

ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

(2). Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции във връзка с предаването.

(3). Администраторът предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна такса въз основа на административните разходи.

Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго.

(4). Правото на получаване на копие, посочено в алинея 3, не влияе неблагоприятно върху правата и свободите на други лица.

Чл. 46. Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез добавяне на декларация.

Чл. 47. (1).Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението

да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

в) субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването;

г) личните данни са били обработвани незаконосъобразно;

д) личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

(2). Когато администраторът е направил личните данни обществено достояние и е задължен съгласно алинея 1 да изтрие личните данни, той, като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

(3). Алинеи 1 и 2 не се прилагат, доколкото обработването е необходимо:

а) за упражняване на правото на свобода на изразяването и правото на информация;

б) за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на Република България, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

в) по причини от обществен интерес в областта на общественото здраве;

г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели; или

д) за установяването, упражняването или защитата на правни претенции.

Чл. 47. (1). Субектът на данните има право да изиска от администратора ограничаване на обработването, когато се прилага едно от следното:

а) точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на личните данни;

б) обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

в) НУ „П. Р. Славейков“, гр. Пловдив като администратор на лични данни не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

г) субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

(2). Когато обработването е ограничено съгласно алинея 1, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице или поради важни основания от обществен интерес

(3). Когато субект на данните е изискал ограничаване на обработването съгласно алинея 1, директорът на НУ „П. Р. Славейков“, гр. Пловдив в качеството си на администратор го информира преди отмяната на ограничаването на обработването.

Чл. 48. Администраторът съобщава за всяко извършено по искане на субекта на данни коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Чл. 49. (1). Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на НУ „П. Р. Славейков“, гр. Пловдив в структуриран, широко

използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от страна на училището, когато:

а) обработването е основано на съгласие в съответствие от субекта на данните или на договорно задължение;

б) обработването се извършва по автоматизиран начин.

(2). Когато упражнява правото си на преносимост на данните по алинея 1, субектът на данните има право да получи пряко прехвърляне на личните данни към друг, когато това е технически осъществимо.

(3). Упражняването на правото, посочено в алинея 1 от настоящия член не засяга член 17 от Регламента. Посоченото право не се отнася до обработването, необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

(4). Правото, посочено в алинея 1, не влияе неблагоприятно върху правата и свободите на други лица.

Чл. 50. (1). Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, включително профилиране. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

(2). Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни, отнасящо се до него за този вид маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг.

(3). Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.

(4). Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото по алинеи 1 и 2, което му се представя по ясен начин и отделно от всяка друга информация.

(5). В контекста на използването на услугите на информационното общество и независимо от Директива 2002/58/ЕО, субектът на данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

(6). Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1 на Регламента, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.

Преходни и заключителни разпоредби

§1. Извън определенията по чл. 4 от Регламент (ЕС) 2016/679, по смисъла на този инструкция:

1. „Общодостъпност“ е разкриване на лични данни или по друг начин осигуряване на достъп до тях от неограничен кръг от лица, без да са предприети мерки за осигуряване на отчетност;

2. „Мащабно“ е системното наблюдение и/или обработване на лични данни на неограничен кръг субекти на лични данни.

3. „Риск“ е функция от вероятността дадена заплаха да се превърне в потенциална уязвимост и резултатното въздействие от неблагоприятното събитие върху организацията.

4. „Уязвимост“ са слабости в процедурите за сигурност на системата, в процесите на разработване и изпълнение, във вътрешните контроли и т.н., които могат да бъдат инцидентно

или умишлено експлоатирани и това да доведе до нарушение на политиката на сигурност на системата.

§2. По смисъла на тази инструкция:

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 и умствената, икономическата, културната или социалната идентичност на това физическо лице;

2. „обработване“ 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 друга форма на осигуряване на достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

3. „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4. „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използване на лични данни за оценяване на някои лични аспекти, свързани с дадено физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

5. „псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

6. „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

7. „компетентен орган“ означава:

а) всеки публичен орган, който е компетентен за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване; или

б) всякакъв друг орган или образувание, който по силата на закон разполага с публична власт и публични правомощия за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване;

8. „администратор“ означава компетентният орган, който сам или съвместно с други органи определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Европейския съюз или правото на Република България, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Европейския съюз или в националното законодателство;

9. „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

10. „получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна

или не. Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Република България, не се считат за получатели; обработването на тези данни от тези публични органи отговаря на приложимите правила за защита на данните съгласно целите на обработването;

11. „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

12. „генетични данни“ означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация относно физиологията или здравето на това физическо лице и които са получени по-специално чрез анализ на биологична проба от въпросното физическо лице;

13. „биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

14. „данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

15. „надзорен орган“ означава независим публичен орган от държава членка на Европейския съюз, отговорен за наблюдението на прилагането на правилата за защита на личните данни, с които са въведени разпоредбите на Директива 2016/680 в съответното национално законодателство, с цел да се защитят основните права и свободи на физическите лица във връзка с обработването на лични данни и да се улесни свободното им движение в рамките на ЕС. За Република България надзорен орган е Комисията за защита на личните данни.

16. „международна организация“ означава организация и нейните подчинени органи, регламентирани от международното публично право, или друг орган, създаден чрез или въз основа на споразумение между две или повече държави.“

§3. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Закона за защита на личните данни и действащото приложимо законодателство на Р България.

Приложение №1

Д Е К Л А Р А Ц И Я

Подписаният/та……

(име, презиме и фамилия)

на длъжност…….. **..... в НУ „П. Р. Славейков“, гр. Пловдив,** в качеството си на обработващ лични данни на основание Инструкция за събиране обработка и мерки за защита на личните данни

Д Е К Л А Р И Р А М, ЧЕ :

1. Ще пазя в тайна личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения, няма да ги разпространявам и няма да ги използвам за други цели освен за прякото изпълнение на служебните ми задължения.
2. Запознат/а/ съм с нормативната уредба, политиката и ръководствата в областта на защита на личните данни, както и със съдържанието на Инструкция ……
3. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни нося дисциплинарна отговорност по Кодекса на труда, административно-наказателна отговорност по Закона за защита на личните данни и наказателна отговорност, ако деянието осъществява състава на чл. 284 и /или на чл. 319д от Наказателния кодекс.

Дата:…… **ДЕКЛАРАТОР:**……..

(подпис)

Приложение №2

ДЕКЛАРАЦИЯ

Долуподписаният/ата….....
ЕГН:.....Лична карта № ……..…. издадена от ……..……..
на.....г.

ДЕКЛАРИРАМ:

Съгласен/а съм НУ „П. Р. Славейков“, гр. Пловдив, да обработва личните ми данни, съгласно изискванията на Закона за защита на личните данни.

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.

Дата: ДЕКЛАРАТОР:
град Пловдив

Приложение №3

ДО
ДИРЕКТОРА
НА НУ „П. Р. СЛАВЕЙКОВ“
ГРАД ПЛОВДИВ

З А Я В Л Е Н И Е

Относно: достъп до лични данни

От .....

(Име, презиме и фамилия)

ЕГН: …..……, л. к. № ……..……..……., издадена на.....,

от ……., адрес .....,

телефон за контакт …….., e-mail ……

С настоящото заявявам, че желая да ми бъде предоставена информация относно личните ми данни, обработвани и съхранявани в НУ „П. Р. Славейков“, гр. Пловдив. Желая да получа исканата от мен информация в следната форма:

- преглед на информация;
- устна справка;
- писмена справка;
- копия на технически носител;
- по електронен път.

Дата: Подпис: ……

гр. Пловдив