



ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ ЕЗИЦИ “СИМЕОН РАДЕВ” -
2304 Перник, ул. ”Бл.Гебрев” 17; тел./факс: 076/ 67 01 40; 67 01 20

www.simeonradev.org; e-mail:gp4e@mail.bg

УТВЪРЖДАВАМ:
ДИРЕКТОР:
(Теменужка Крумова)



ВЪТРЕШНИ ПРАВИЛА
ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ
В ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ ЕЗИЦИ
„СИМЕОН РАДЕВ“

ГР. ПЕРНИК

СЪДЪРЖАНИЕ

I. Общи положения	3
II. Цели и обхват на правилата	3
III. Предназначение и видове регистри	4
IV. Достъп до лични данни	6
V. Достъп на трети лица до регистрите съдържащи лични данни	7
VI. Лица по защита на личните данни	8
VII. Мерки за защита при обработване на личните данни	9
VIII. Мерки за осигуряване на защита на личните данни при компютърна обработка	12
IX. Оценка на въздействието върху обработваните лични данни.....	12
X. Нива на въздействие	13
XI. Процедури за докладване и управление при инциденти	14
XII. Отговорност	14
Преходни и заключителни разпоредби.....	15
ПРИЛОЖЕНИЯ	17

**ВЪТРЕШНИ ПРАВИЛА
ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ
В ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ ЕЗИЦИ
„СИМЕОН РАДЕВ“**

ГЛАВА ПЪРВА

II. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер, архивиране и унищожаване на личните данни, както и мерките и средствата за тяхната защита.

(2) Настоящите правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник.**

(4) Администраторът предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

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

(6) Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на преподавателите, служителите, учениците, родителите и посетителите, както и на други физически лица, обработвани във връзка с осъществяването на дейността на училището.

ГЛАВА ВТОРА

II. ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

ЦЕЛИ

Чл. 2. Настоящите Правила имат за цел да регламентират:

(1) механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер, архивиране и унищожаване на личните данни;

(2) задълженията на Администратора, на лицата работещи с лични данни, на персонала на училището и длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;

(3) правилата за разпределение на личните данни и групирането им в регистри и Правилата за работа с личните данни;

(4) необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

(5) Обработването на личните данни на учениците до 14 години, когато са събрани със съгласие на субекта на данни, като съгласието се дава от единия родител/настойника на ученика.

Обхват

Чл. 3. Правилата са задължителни за всички лица имащи достъп до личните данни, обработвани от администратора.

ГЛАВА ТРЕТА

III. ПРЕДНАЗНАЧЕНИЕ И ВИДОВЕ РЕГИСТРИ

Набиране и съхраняване на лични данни

Чл. 4. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица. Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична Заповед на директора на училището, или сключен договор.

(2) В изпълнение на дейностите си училището поддържа регистър на дейностите по обработване на лични данни на основание чл. 30 от Общия регламент относно защитата на данните и регистри на лични данни, описани в приложение № 3, неразделна част настоящите вътрешни правила.

(3) Създаването на нови регистри, премахването на съществуващи и извършването на промени се извършва със заповед на Директора на Администратора на лични данни.

(4) Документите и преписките, по които работата е приключила, се архивират.

(5) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(6) 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 и съгласно Номенклатурата на делата със срокове за съхраняване, утвърдена от директора на дирекция „Централен държавен архив“.

(7) Унищожаването на ведомости за заплати, за които е изтекъл срокът по чл. 38, ал. 1, т. 1 от Данъчно-осигурителния процесуален кодекс (50 години) може да бъде извършено при наличието на всички законови основания и предпоставки.

(8) 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.

(9) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица, определени от директора на училището.

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

Форми на водене на регистъра

Чл. 5. (1) Формите на водене на регистрите биват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на училището и/или нормалното му функциониране.

1. Водене на регистър на хартиен носител:

1.1. Форма на организация и съхраняване на личните данни – писмена (документална);

1.2. Местонахождение на картотечния шкаф –

.....;

(2) Носител (форма) за предоставяне на данните от физическите лица – Личните данни от лицата се подават на администратора на лични данни и оправомощеното лице, назначено за обработването им – обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо;

1. Достъп до личните данни – такъв има само обработващият лични данни.

(3) Водене на регистър на технически носител:

1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на твърд диск, на изолиран компютър;

2. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове, както и длъжностното лице по защита на личните данни посредством делегирани му права и задължения от администратора на лични данни.

Групи данни в регистъра

Чл. 6. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:

1. физическата идентичност на лицата – имена, ЕГН, номер на документ за самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт, електронна поща;

2. семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;

3. образование и квалификация – вид на образованието, място, номер и дата на издаването на дипломата, допълнителна квалификация и др., основна и допълнителни квалификации;

4. трудова дейност – професионална биография, трудов и осигурителен стаж, педагогически стаж, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;

5. медицински данни – здраве статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;

6. други лични данни – парични обезщетения, статус на лицето (осъждано/неосъждано/реабилитирано) и други.

(2) Личните данни в регистрите се събират от администратора на лични данни на хартиен или електронен носител.

Задължения на лицето, отговарящо за водене и съхраняване на данните в регистрите

Чл. 7. (1) Задълженията на лицето/ата, отговарящо/и за водене и съхраняване на данните в регистрите (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

Периодично архивиране

Чл. 8. Архивиране на личните данни на технически носител се извършва периодично от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

Контрол при обработване на личните данни

Чл.9. Контролът върху дейностите по обработка на лични данни се осъществява от Директора на Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник.

Актуализация на лични данни

Чл.10. Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в образователната институция. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;
2. по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;
3. при установена грешка при обработката на личните данни.

ГЛАВА ЧЕТВЪРТА

IV. ДОСТЪП ДО ЛИЧНИ ДАННИ

ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл.11.(1) Всяко физическо лице има право на достъп до отнасящите се до него лични данни, обработвани от администратора.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се него.

(3) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Чл. 12. (1) Правото на достъп се осъществява с писмена молба до администратора на лични данни.

(2) Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Молбата по ал. 1 се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Чл. 13. (1) Молбата по чл. 12 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;
2. описание на искането;
4. предпочитана форма за предоставяне на достъп до личните данни;
5. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на молба от упълномощено лице към същото се прилага и пълномощно.

(3) При приемане на молбата, техническо лице извършва регистрация на същата в деловодната система на администратора.

Чл. 14. (1) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от молителя форма на предоставяне на информацията по чл. 11, ал. 3.

(3) Администраторът на лични данни предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;
2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Чл. 15. (1) Администраторът на лични данни или изрично оправомощено от него лице разглежда молбата по чл. 11 и се произнася в 14-дневен срок от неговото постъпване.

(2) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(3) С решението си администраторът предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето ѝ.

Чл. 16. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник** – администратори на базите данни, служителите на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни), както и служителите, за които служебните им функции налагат такъв достъп.

Чл. 17. Служителите в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник** с оторизиран достъп до лични данни са длъжни да обработват същите законосъобразно и добросъвестно, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги поддържат във вид, който им позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които се обработват.

V. ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 18.(1) Достъп до обработваните от администратора лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Не се изисква съгласие на лицето, ако обработването и трансфера на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания или при наличие на преимуществен обществен интерес. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на детската градина училището.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 14 - дневен срок от подаване на молбата, респ. искането.

ГЛАВА ПЕТА

ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

VI. ЛИЦАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19.(1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът определя лице по защита на личните данни.

(2) Лицето по защита на личните данни има следните правомощия:

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

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

3. да наблюдава спазването на политиките на администратора по отношение на защитата на личните данни;

4. да си сътрудничи с надзорния орган (КЗЛД) в качеството ѝ на надзорен орган на Република България по всички въпроси, предвидени в Общия регламент за защита на данните или произтичащи от други правни актове на Европейския съюз или от законодателството на Република България, или по въпроси, инициирани от надзорния орган;

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

6. да осъществява контрол по спазване на изискванията за защита на регистрите;

7. периодично информира персонала по въпросите на защитата на личните данни;

8. следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

(3) Длъжностното лице по защита на данните не получава никакви указания във връзка с изпълнение на дейностите по ал. 2 и действа независимо, като се отчита пряко пред директора на **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник**, който представлява администратора на лични данни

(4) Лицето по защита на личните данни не може да делегира своите пълномощия изцяло и/или частично на други лица.

(5) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката. В случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък администратора на лични данни. Настъпилото събитие поражда задължение за администратора на лични данни в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник**.

Чл. 20. (1) С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) Видове защита:

1. Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

2. Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

3. Документална защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

4. Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

5. Псевдонимизация чрез употребата на технически и организационни мерки.

6. Мерките на различните видове защита се определят съгласно приложение № 6 от настоящите Правила.

Чл. 20а. (1) Всяко лице желаещо да внесе документ съдържащ лични данни предоставя същия в „деловодството“ на **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник (канцелария ЗАТС)**. Лицето приемащо документа е задължено да запознае вносителя на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му, вносителят попълва съответна Декларация по образец, предоставена му от лицето приемащо документите за деклариране на предоставените лични данни и основанийето, на което те се предоставят и ще се ползват.

(2) Внесените документи с лични данни се докладват на Директора, който ги разпределя на лицата обработващи съответните лични данни.

(3) Лицата обработващи личните данни са задължени да предоставят личните данни в съответствие с разпореждането на Директора на Администратора.

(4) Лични данни се предоставят на трети лица само чрез Директора на Администратора.

(5) При предоставяне на личните данни за ползване то трети лица, те попълват декларация за задължението си да обработват личните данни съгласно Регламент 2016/679 и ЗЗЛД.

VII. МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 21. (1) Правилата за защита при обработване на лични данни регламентират технически мерки, които:

1. отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;
2. предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;
3. предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;
4. предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;
5. гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;
6. осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;
7. осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;
8. предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;
9. осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;
10. осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

Чл. 22. (1) Служителят/ите, обработващ/и лични данни, взема/т мерки за гарантиране на надеждност при обработването, като осъществява/т технически и организационни мерки за защита на личните данни.

(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:

1. неоторизирано четене, възпроизвеждане, промяна или премахване на носителя на данните;
2. неоторизирано въвеждане, промяна или заличаване на съхранени лични данни;
3. неоторизирано използване на системите за лични данни чрез средства за пренос на данни;
4. неоторизиран достъп до лични данни.

Чл. 23. Служителите на училището 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.

б. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 24. (1) За неспазването 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.

Чл. 25 (1). Основните приложими мерки за документална защита на личните данни са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител:* на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището;

2. *Определяне на условията за обработване на лични данни:* личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

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

4. *Определяне на срокове за съхранение:* личните данни се съхраняват в срок, посочен в Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

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 училището, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 26. (1) *Защитата на автоматизираните информационни системи и/или мрежи* в училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

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

2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3. *Защитата от вируси*, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от ръководител направление ИКТ;

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 училището;

5. Основни електронни *носители на информация са*: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, паметни ленти и други носители на информация, еднократно записваеми носители и др.);

6. *Персоналната защита на данните* е част от цялостната охрана на училището;

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 училището и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

VIII. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 27. (1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

(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. 28. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата и криптографска защита.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 29. (1) В училището се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

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

Чл. 30. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица.

ГЛАВА ШЕСТА

ОЦЕНКА И НИВА НА ВЪЗДЕЙСТВИЕ И ЗАЩИТА

IX. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 31. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

(2) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 32. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.

2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;

3. лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;

4. лични данни в широко мащабни регистри на лични данни;

5. данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

X. НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 33. Определят се следните нива на въздействие:

1. „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. „Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 34. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри съгласно приложение № 1.

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2, определя нивото на въздействие на съответния регистър.

Чл. 35. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 36. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) Нивата на защита са, както следва:

1. при ниско ниво на въздействие – ниско ниво на защита;

2. при средно ниво на въздействие – средно ниво на защита;

3. при високо ниво на въздействие – високо ниво на защита;

4. при изключително високо ниво на въздействие – изключително високо ниво на защита.

ГЛАВА СЕДМА

XI. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл. 37.(1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на лицето по защита на личните данни в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник.**

(2) За инцидентите се води регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(3) След анализ от лицето по защита на личните данни, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в регистър по архивиране и възстановяване на данни.

(5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

XII. ОТГОВОРНОСТ

Чл. 38. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание.

Чл. 39. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник**, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на администратора на лични данни на виновните лица се търси имуществена отговорност по Кодекса на труда или Закона за държавния служител.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. По смисъла на настоящите вътрешни правила:

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

- **„Администратор на лични данни по настоящите вътрешни правила е Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник (училището).**

- **Ниво на защита** е степен на организация на обработката на лични данни в зависимост от рисковете при обработката на съответния вид лични данни.

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

- **„Обработващ лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

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

- **„Поверителност“** е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване по нерегламентиран път.

- **„Предоставяне на лични данни“** са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

- **„Регистър с лични данни“** е 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;

- **„Съгласие на субекта на данните“** е всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

- **„Трета страна“** е физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

- **„Псевдонимизация“** означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързани 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.

§2. Всички служители на училището са длъжни срещу подпис да се запознаят с вътрешните правила и да ги спазват.

§3. Вътрешните правила се издава във връзка с Регламент (ЕС) 2016/679 от 27.04.2016 г. относно защитата на физически лица във връзка с обработването на лични данни и относно свободното движение на такива данни и на основание чл. 23, ал. 4 от Закона за защита на личните данни и Наредба № 1/30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни, издадена от Комисията за защита на личните данни (ДВ, бр. 43 от 25 май 2018 г., в сила от 25.05.2018 г.).

§4. За всички неуредени в настоящите вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679 от 27.04.2016 г. относно защитата на физически лица във връзка с обработването на лични данни и относно свободното движение на такива данни, Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и действащото приложимо законодателство на Р България.

§5. Вътрешните правила са утвърдени със Заповед № година.

ДО ДИРЕКТОРА НА
Гимназия с преподаване на чужди езици “Симеон
Радев” - гр. Перник

ЗАЯВЛЕНИЕ

за предоставяне на лични данни

От

(име, презиме, фамилия)

Адрес : гр. , ул. “” № .., бл.....,вх., ет.....,
ап....., тел.

Упълномощено лице:.....

(име, презиме, фамилия)

Адрес : гр. , ул. “” №, бл...,вх.,
ет....., ап

Пълномощно №..... от (нотариално заверено, приложено към
заявлението)

Относно: Предоставяне на лични данни

(описание на искането)

.....
.....

Уважаема,

Във връзка с

.....

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

и на основание чл. 29, ал.1 от Закона за защита на личните данни (ЗЗЛД) с настоящото
заявление се обръщам към Вас с оглед получаване на лични данни относно:

1.

2.

3.

Предпочитам формата на предоставената информация да бъде във вид на

.....

(на дискета , CD , копие , факс , електронна поща и др.)

Адрес за кореспонденция :

гр. , ул. “” №....., бл...,вх....., ет..., ап....., тел.

Получател:.....

(име, презиме, фамилия)

Дата:

С уважение:

ДЕКЛАРАЦИЯ

ФОРМА ЗА ИНФОРМИРАНО СЪГЛАСИЕ ОТ СЛУЖИТЕЛ			
GDPR	Идент. № FORM_05	Версия 0.1	Стр. 1 от 1
Администратор: ПГЧЕ “Симеон Радев” гр. Перник – директор Теменужка Крумова		ДЛЗД/Отговорник:	

Версия	Дата	Описание	Автор	Одобрил

Аз, долуподписан/ият/та,

.....

(трите имена на служителя)

съм съгласен да се обработват

(име на администратора, данни за идентификация)

личните ми данни за целите на

.....

(изрично уточнете целите, които се преследват с обработването на личните данни, както и точно описание на данните)

Информиран съм за:

- 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.

Съзнавам, че мога да оттегля моето съгласие по всяко време.

Разбирам, че оттеглянето на съгласието ми по-късно няма да засегне законосъобразността на обработването, основано да даденото сега съгласие.

Подпис на субекта на данни:.....

Дата:.....

Получено от: на.....

Контакт с Администратора на лични данни:		
Уебсайт: https://www.simeonradev.org/	Е-mail: gp4e@abv.bg	Телефон: 0879826280

**РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА
ОСНОВАНИЕ ЧЛ. 30 ОТ ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА
ДАННИТЕ**

Администратор на личните данни:

Гимназия с преподаване на чужди езици „Симеон Радев“, представляван от Теменужка Стефанова Крумова - Директор

(наименование)

Координати за връзка с администратора:

2304, гр. Перник, област Перник, ул. „Благой Гебрев“ №17,; e-mail: gp4e@mail.bg

(адрес, електронна поща)

Длъжностно лице по защита на данните:

Велин Венков Койчев – управител на „Дейта Протекшън“ООД – гр. София, ж.к. Лозенец,, ул. „Вежен“ №14, ап.10

(име, длъжност, контакти)

Открит на 12.11.2019г.

Дата	Регистър с лични данни	Цели на обработване	Правно основание	Категории субекти	Категории лични данни	Категории получатели	Срок за изтриване
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

ВИДОВЕ РЕГИСТРИ

1. Регистър „Ученици“ и „Родители“ - се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“ в процеса на тяхното обучение, възпитание и социализация. Регистърът включва книга за подлежащите на задължително образование – данни за ученици и родители.

1.1. Книга за подлежащите на задължително обучение данни за ученици в училището и родители е предназначена за водене на отчет на ученици от задължителната за обучение възраст в подготвителните групи и в класовете, и се попълва с данни, събрани за учениците по съответния ред. Книгата съдържа имена и ЕГН на ученици, година на раждане; пореден номер; учебна година; възраст на детето в години; клас и паралелка за съответната учебна година и възраст на детето; данни за дошлите или преместилите се в други училища; данни за родителя/настойника.

1.1.1. Регистърът се води от упълномощено лице със Заповед на директора.

1.1.2. Данните от регистъра се предоставят доброволно от лицата при записването им.

1.1.3. Книгата се съхранява в канцеларията на ЗАТС.

1.1.4. Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, заместник-директорите по учебната дейност (ЗДУД), заместник-директора административно-стопанската дейност (ЗДАСД), учителите при изпълнение на правомощията им по Кодекса на труда, Закон за предучилищното и училищно образование (ЗПУО) и длъжностна характеристика.

- Държавни органи надлежно легитимирани се с документи, издадени по законоустановения ред; длъжностното лице по защита на личните данни и лицата, обработващи личните данни по указания на Администратора.

1.2. В Книга за подлежащите на обучение данни за ученици в училището и родители, данните за „Родители“ се набират и съхраняват с цел индивидуализиране на физически лица, в качеството им на родители/ настойници /. Книгата съдържа следните групи данни:

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

Нормативното основание за обработване на данните е Законът за предучилищното и училищното образование (ЗПУО) и приложимото законодателство, свързано с предоставянето на образователни услуги.

1.3. Технологично описание на регистър „Ученици“ и „Родители“:

➤ Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки за входяща кореспонденция. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения. Информацията от хартиените носители се записва в Книга за подлежащите на задължително обучение деца в училището; Дневник за I – VII клас със задължителни реквизити съгласно Наредба № 8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в определените от Администратора помещения.

- На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ-Про. Базата данни се намира на твърдия диск на изолирани компютри.

- Съхранение в „облака“ – Електронен дневник -съдържа дневници за VIII - XII клас със задължителни реквизити съгласно Наредба № 8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование,(с възможност за генериране на ученически книжки и лични картони и тяхното архивиране на хартиен носител), с външен администратор – ШКОЛО ООД, който е администратор на лични данни и притежава сертификати за информационна сигурност.

- Срок на съхранение: съгласно Номенклатурата на делата в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник** със срокове на съхранение;

1.4. Определяне на длъжностите на служителите: Обработващи лични данни в регистър „Ученици“ и „Родители“ се определят от директора.

Достъп до регистър „Ученици“ и „Родители“ имат:

- Директорът, заместник-директорите по

-

- учебната дейност (ЗДУД), ръководител направление ИКТ, лицата, обработващи личните данни по указания на Администратора, учителите при изпълнение на правомощията им по Кодекса на труда, Закон за предучилищното и училищно образование (ЗПУО) и длъжностна характеристика;
- държавни органи, надлежно легитимирани се с документи, издадени по законоустановения ред;
- длъжностното лице по защита на личните данни
- лицата, за които се отнасят данните в регистъра, по тяхно изрично искане.

2. Регистър „Персонал“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори. Общо описание на регистър „Персонал“ съдържа следните групи данни:

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

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

2.1. В Регистър „Персонал“ се съдържа: заявление за кандидатстване за започване на работа, лични досиета на персонала, дневник на издадени трудови книжки, удостоверения за стаж, удостоверения за доходи, регистър на болнични листове, регистър за трудови злополуки и професионални заболявания.

2.2. Предназначението на събираните данни в регистъра е свързано с :

- 2.2.1. Индивидуализиране на трудовите правоотношения;
- 2.2.2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
- 2.2.3. 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.

2.3. Технологично описание на регистър „Персонал“:

➤ Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета). Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни.
- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма. Базата данни се намира на твърдия диск на изолирани компютри. Личните данни се въвеждат и в специализирана Информационна система за училищна администрация Админ-Про. Базата данни се намира на твърдия диск на изолирани компютри.
- Съхранение в „облака“ – Електронен дневник - съдържа дневници за VIII - XII клас със задължителни реквизити съгласно Наредба № 8 от 11 август 2016 г. за информацията и документите за системата на предучилищното и училищното образование,(с възможност за

генериране на ученически книжки и лични картони и тяхното архивиране на хартиен носител), с външен администратор – ШКОЛО ООД, който е администратор на лични данни и притежава сертификати за информационна сигурност.

2.4. Срок на съхранение: съгласно Номенклатурата на делата в **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник** със срокове на съхранение.

Определяне на длъжностите: Администратор на лични данни на регистър „Персонал“ е директорът на училището. Обработващи лични данни на регистър „Персонал“ са зам. директори, ЗАС, гл. счетоводител, касиер, домакин, ръководител направление ИКТ.

3. Регистър „Информация за институциите в системата на предучилищното и училищното образование“ (Списък образец № 1) - събирането, обработването, използването и съхраняването на информацията в системата на предучилищното и училищното образование се извършва чрез Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование (НЕИСПУО). Предназначен е да служи за установяване на съответствието на организацията на учебния процес с нормативната уредба според ЗПУО. Той обслужва информационно нуждите на МОН, РУО, НИО, общинската администрация и финансиращия орган. Списък – образец № 1, съдържа реквизитите, посочени в приложение № 1, към чл. 7, т. 1 на Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование

Към Списък - образец №1 се прилагат: документи за статута на училището в случаите, в които е настъпила промяна през предшестващия период; прилаганите в училището учебни планове; утвърдените учебни програми за преподаваните предмети от раздели А и Б на учебния план в общообразователните училища и раздели В и Г в професионалните училища; годишен план на училището; дневен режим на институцията.

3.1. Данните от Списък - образец № 1 се въвеждат на магнитен носител и се разпечатват на хартиен носител, който се заверява от директора на училището.

Със заповед на директора се определя мястото на съхранение на хартиения носител до завършване на учебната година.

Регистърът се съхранява в архива на училището със срок от пет години.

3.2. Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, ЗДУД, главният счетоводител, учителите - при изпълнение на правомощията им по Кодекса на труда, ЗПУО и длъжностна характеристика.
- Държавни органи надлежно легитимирани се с документи, издадени по законо установения ред; длъжностното лице по защита на личните данни и лицата, обработващи личните данни по указания на Администратора.

3.3. Книга „**Щатни разписания**“ се съдържа информация за щатните разписания на персонала в училището.

Данните от регистъра могат да бъдат предавани по електронен път.

4. Регистър „Контрагенти“ съдържа лични данни на лица, участващи в процеса на осъществяваната финансова дейност на **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник**. В регистъра се обработват лични данни на физически, нормативно регламентирани във връзка с извършването на дейности, както пряко свързани с основната дейност на **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник**, така и във връзка с допълнителни дейности- възлагане на обществени поръчки, изпълнение на текущи и аварийни ремонти и др.

- индивидуализиране на данни, свързани със сключване на договори;
- използване на събраните данни за съответните лица за служебни цели;
- за всички дейности, свързани с осъществяване на основната дейност- правораздаване; по възникване на служебни правоотношения в останалите случаи-изготвяне на документи на лицата (служебни бележки, справки, удостоверения и др.); за установяване на връзка с лицата по телефон, по електронен път за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им по сключени договори или поети ангажменти.

4.1. В регистъра се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, номер, дата и място на издаване на документи за самоличност, постоянен и настоящ адрес и др.;
- трудова дейност: месторабота и заемана длъжност, професионален опит.
- социално-икономическа идентичност: текущо финансово състояние, участие в сдружения .

4.2. Технологично описание на регистъра:

4.2.1. Носители на данни - данните в регистъра се обработват на хартиен и технически носител.

4.2.2 Технология на обработване- данните в регистъра се предоставят от съответните лица, с оглед изпълнение на нормативно регламентирани задължения, възложени от администратора, при покриване на критерии и изисквания за участие в обществени поръчки, при които основанието за обработване е посочено в нормативен акт.

4.3. Срок за съхранение на информацията: - договори и приемо-предавателни протоколи за изпълнение на обществени поръчки - постоянен/ съхраняват се в училището/ - служебни бележки и удостоверения за изплатени възнаграждения - 10г. след одитиране /финансова ревизия/ - договори за отдаване под наем - 5 години след приключване.

4.4. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения:

- Данните от регистъра се обработват от ЗДАСД, главният счетоводител, касиерът, домакинът, в чиито длъжностни характеристики е определено задължение за обработване на данните на външни лица - вещи представители на фирми, извършващи външни услуги и при спазване на принципа „Необходимост да се знае”. Право на достъп до регистъра имат само упълномощените лица. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

5. В регистър „**Видеонаблюдение**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Общо описание на регистър „**Видеонаблюдение**“:

- Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградата на училището.

Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз; технологично описание на регистър „**Видеонаблюдение**“: Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите в сградата на училището.

Данните от регистър „**Видеонаблюдение**“ се въвеждат на магнитен носител и се съхраняват в сроковете, установени в Правилата за информационна сигурност, след което се унищожават чрез трайно изтриване от носителя.

Определяне на длъжностите: Администратор на лични данни на регистър „**Видеонаблюдение**“ е директорът на училището.

Обработващи лични данни на регистър „**Видеонаблюдение**“ са лицата, определени със специална заповед на Директора, издадена в съответствие с Правилата за информационна сигурност, разработвани от МОН при организацията на НВО , ДЗИ, изпити на ученици от самостоятелна форма на обучение.

6. В регистър „**Пропускателен режим**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Общо описание на регистър „**Пропускателен режим**“:

- Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградата на училището.

Регистърът съдържа следните групи данни - физическата идентичност на лицето – установяване на самоличност на субекта на данни и снемане на данни от индивидуализиращия го съгласно законодателството документ – л.к. ЛНЧ и др.

Определяне на длъжностите: Администратор на лични данни на регистър „**Пропускателен режим**“ е директорът на училището.

Обработващи лични данни на регистър „**Пропускателен режим**“ са дежурните охранители.

ЗАПОВЕД

№/2020 г.

На основание чл. 258, ал. 1, чл. 259, ал.1 от Закона за предучилищното и училищното образование и във връзка с чл. 10 от Вътрешни правила за мерките за защита на личните данни, събирани, обработвани, съхранявани и предоставяни от **Гимназия с преподаване на чужди езици “Симеон Радев” - гр. Перник.**

НАРЕЖДАМ:

1. Право на достъп до регистрите с лични данни да имат само оторизираните длъжностни лица в училище, а именно:

- Целия педагогически персонал;
- ЗДУД;
- Ръководител направление ИКТ
- Касиер
- домакин;
- Главен счетоводител.
- ЗАС

2. Длъжностните лица 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.

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

С настоящата заповед да се запознаят всички педагогически специалисти и непедagogически персонал от училището.

Контролът по изпълнението на настоящата заповед ще се осъществява лично от директора.

ДИРЕКТОР:
(Теменужка Крумова)

ЗАПОВЕД

№/..... 2020 година

На основание чл. 258, ал. 1, чл. 259, ал. 1 от Закона за предучилищното и училищното образование и във връзка с Регламент (ЕС) 2016/679 от 27.04.2016 г. относно защитата на физически лица във връзка с обработването на лични данни и относно свободното движение на такива данни,

УТВЪРЖДАВАМ

**ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И
ЗАЩИТА НА ЛИЧНИ ДАННИ В ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ
ЕЗИЦИ „СИМЕОН РАДЕВ“ - ГР. ПЕРНИК**

С настоящата заповед да се запознаят всички педагогически специалисти и непедагогически персонал от училището.

Контролът по изпълнението на настоящата заповед ще осъществявам лично.

ДИРЕКТОР:
(Теменужка Крумова)