бул. "Захари Стоянов", жк Меден рудник, 8009 Бургас, office@codingburgas.bg, codingburgas.bg

УТВЪРЖДАВАМ:

ДИРЕКТОР Димитрина Тодорова

ВЪТРЕШНИ ПРАВИЛА 3.3.2

ЗА СИГУРНОСТ ПРИ АДМИНИСТРИРАНЕ НА ЛИЧНИ ДАННИ ОТ СЛУЖИТЕЛИ В ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО КОМПЮТЪРНО ПРОГРАМИРАНЕ И ИНОВАЦИИ

СЪДЪРЖАНИЕ

Програмата е създаден на основание Закон за изменение и допълнение на закона за защита на личните данни и е приета от Педагогическия съвет Протокол № РД-05-02/7.09.2018 г. и е утвърдена със Заповед № РД-10-41-4/ 11.07.2018 г. на директора на училището.

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Настоящите Вътрешни правила за сигурност при администриране на лични данни от служители в ПГКПИ, наричани по-нататък за краткост ”Правила”, уреждат организацията и реда за упражняване на контрол при обработването на лични данни от служителите на ПГКПИ по смисъла на Закона за защита на личните данни (ЗЗЛД), както и условията и реда за водене на регистри съгласно ЗЗЛД.

(2) Обработването на личните данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

(3) Достъп до определена информация във връзка с обработването на личните данни се осигурява само на упълномощени за това лица.

Чл.2. Правилата се приемат с цел да регламентират:

1. създаване на процедури и механизми за гарантиране неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица от неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
2. задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, и отговорността при неизпълнение на тези задължения;
3. необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване;
4. видовете регистри, които се водят в ПГКПИ и тяхното описание.

Чл.3. (1) В ПГКПИ в процеса на упражняване на дейността си обработва лични данни и е регистрирана като администратор налични данни (АЛД) по смисъла на чл.3, ал.2 от ЗЗЛД

(2) Всички действия спрямо постъпили в ПГКПИ документи и заявления в електронен вид или на хартия се извършват при стриктно спазване на изискванията за защита на личните данни съгласно ЗЗЛД и останалите съотносими нормативни актове, както и настоящите правила.

Чл.4. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Защитата на лични данни се осъществява въз основа на следните принципи за:

1. Законосъобразно и добросъвестно обработване;
2. Ограничено събиране, използване, разкриване и съхранение:

- Ограничено събиране - личните данни се събират за конкретни, точно определени нормативно цели и не може да се обработват допълнително по начин, несъвместим с тези цели; допълнителното им обработване за други цели, различни от целите, за които са събирани, е допустимо само при посочени в закона условия; личните данни трябва да бъдат съотносими, свързани с и не надхвърлящи целите, за които се обработват;
- Ограничено използване - личните данни не трябва да се използват за цели, различни от тези, за които са били събрани;

- Ограничено разкриване - служителите на ПГКПИ, които имат достъп до лични данни, са длъжни да не допускат разкриването и разпространението на свързана с тези данни информация извън предвидените в закона случаи;
- Ограничено съхранение - личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват, освен в предвидените в закона случаи;

3. Прецизност - личните данни трябва да са точни, пълни и актуални, доколкото това е необходимо за регламентираните цели на използването им;

4. Сигурност и опазване - личните данни са защитени с мерки за сигурност в съответствие с вида и рисковете при обработването им и се съхраняват според нормативно определени изисквания и срокове.

РАЗДЕЛ II. ВИДОВЕ РЕГИСТРИ В УЧИЛИЩЕ И ФОРМИ НА ВОДЕНЕТО ИМ

Чл.5. В ПГКПИ се водят и съхраняват всички задължителни официални регистри и бази данни съгласно утвърдена номенклатура на делата със срокове за съхранение.

Чл.б. Регистрите и базите данни по чл.5 се водят и поддържат на хартиен, респективно — електронен носител, от съответните длъжностни лица.

РАЗДЕЛ III. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 7. (1) Администраторът възлага обработването на лични данни на служители на училището (обработващи), съобразно спецификата на изпълняваните от тях служебни функции.

(2) Имащи достъп и обработващите лични данни са:

1. Директор
2. ЗДАСД
3. ЗДУД
4. Учители, класни ръководители, учители по вид спорт и възпитатели
5. Счетоводител, домакин, управител общежитие
6. Технически сътрудник
7. ЗАС/ТРЗ

(3) Достъп до личните данни има само обработващият лични данни и/или действащото под негово пряко или на администратора ръководство оправомощено лице. Възможността за предоставяне на достъп до личните данни на друго лице е ограничена и регламентирана в Раздел V на Правилата - Предоставяне на лични данни.

(4) Лицата по ал.2 имат оторизиран достъп само до тези регистри и бази данни, които са необходими за изпълняване на техните служебни задължения.

(5) Предоставянето, промяната или прекратяването на оторизиран достъп до бази данни в ПГКПИ се контролира от директора на училището .

Чл.8. (1) Директора на ПГКПИ осъществява контрол върху законосъобразното водене и поддържане на регистрите и базите данни.

(2) Обработването на лични данни от лицата по чл. 7, ал.2 става само по указание на администратора.

Чл.9. (1) Лицата подават личните си данни до АЛД чрез длъжностното лице, административен секретар определено за обработването им въз основа на длъжностна характеристика.

(2) Обработващият данните информира техния притежател относно необходимостта от набирането им и целите, за които ще бъдат използвани.

(3) Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез: - устно подаване на данните от лицето; - хартиен носител (писмени документи);

- електронен носител;
- технически носител;
- външни източници, в изпълнение на нормативни изисквания.

Чл.10. При въвеждане, промяна или предаване на лични данни в базите данни администраторът осигурява съхраняване на информация за:

1. времето (дата и час) на въвеждане, промяна или предаване на личните данни;
2. лицата, извършващи въвеждането, промяната или предаването на личните данни; 3. лицата, предоставили личните данни;
4. променените или предадени лични данни, които са били въведени.

Чл.11. (1) Личните данни, организирани върху хартиен носител се съхраняват в папки в определени шкафове в кабинетите на съответните служители, които в извънработно време се заключват.

(2) Личните данни върху технически носител се съхраняват в определени шкафове в кабинетите на съответните служители, които в извънработно време се заключват.

(3) Личните данни не се изнасят от сградата на училището , освен от обработващия лични данни, при служебна необходимост и разрешение от прекия му ръководител.

Чл.12. (1) В ПГКПИ се поддържат следните регистри:

Регистър „Персонал”.

Високо НИВО на защита.

Срок на съхранение — 50 год.

С регистъра имат право да работят:

Служба „Човешки ресурси” – ЗАС/ТРЗ, технически сътрудник

Финансов счетоводен отдел.

Нормативно основание — Кодекса на труда, Кодекс за социално осигуряване, Закон за Данъците върху Доходите на физическите лица.

Личните трудови и служебни досиета на служителите в ПГКПИ се обработват и съхраняват в кабинета на техн. сътрудник и ЗДАСД.

(2) Личното трудово или служебно досие представлява съвкупност от писмени документи, които отразяват в цялост професионалното развитие и поведение на отделния служител и включват всички документи във връзка със създаването, изменението, развитието и прекратяването на трудовото, респ. служебното правоотношение, длъжностната характеристика, както и изискуемите декларации по Кодекса на труда.

(3) Личните трудови и служебни досиета се съхраняват съгласно нормативно определените срокове.

(4) Електронните копия на личните трудови или служебни досиета се съхраняват на файлов сървър. Достъпът до тази информация е реализиран с различни нива на достъп, оторизацията е с единна система за управление на акаунти на съответните служители. Физическият достъп до сървъра е със система за контрол на достъпа.

Регистър „ Контрагенти”.

Финансово счетоводна дейност Високо ниво на защита.
Срок на съхранение — 50 год.
Нормативно основание — Кодекса на труда, Кодекс за социално осигуряване, Закон за данъците върху доходите на физическите лица, Търговски закон.
Данните се съхраняват на хартия, както и в компютрите. Същите се предават по електронен път, защитени чрез криптиране на файловете, с отделна програма

Регистър на пропускателния режим
Регистър на видеонаблюдението
Регистър на родителите
Регистър „ Ученици”
ВИСОКО НИВО на защита.
Срок на съхранение — 50 год.

С регистъра имат право да работят длъжностните лица — Операторите на лични данни.
Програмата, която се използва в ПГКПИ за регистър на учениците и базата данни „Админ Софт“ е лицензирана. Документите се подписват с електронен подпис, Smart Card и пин. Нормативно основание: ММС, МОН, ЗПУО и др.

Чл.13. (1) Информацията, която личното трудово или служебно досие съдържа, е конфиденциална и не може да бъде разгласявана без изричното писмено съгласие на работника или служителя.

(2)Личните трудови или служебни досиета имат следните нива на защита:

1. При начално ниво на защита (за лични данни, обработвани на хартиен носител) формата на организация и съхраняване на лични данни е писмена (документална);
   - личните трудови или служебни досиета за всеки служител или наето по граждански договор лице се съхраняват в папки, които се поставят в шкафове; шкафове се намират в работни помещения, предназначени за самостоятелна работа на обработващите лични данни;
   - служителите, работещи с личните трудови или служебни досиета, заключват същите след приключване на работа с тях и/или напускане на помещението като в този случай заключват самото помещение.
2. При средно ниво на защита (за лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър или в мрежа, несвързани с обществената мрежа) формата на организация и съхраняване на лични данни е въвеждането им на твърд диск, на отделни компютри, които са свързани с локална мрежа, но със защитен достъп на лични данни, който е непосредствен само от страна на обработващия лични данни.

Чл.14. (1) Личните данни, организирани и съхранявани в електронен вид, се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на Наредба N9 1 от 30.01.2001 3 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (НМНТОМДВЗЛД), издадена от Комисия за защита на личните данни.

(2) При работа с данните се използват съответните софтуерни продукти за обработка на същите, включително относно управлението на човешките ресурси, възнагражденията на

персонала, в това число основни и допълнителни възнаграждения, данъчни и други (вноски по заеми, запори и пр.) задължения, трудов стаж, присъствени и неприсъствени дни и други подобни. Софтуерните продукти за обработка са адаптирани към специфичните нужди на училището.

(3) Достъп до операционната система, съдържаща файловете за обработка на лични данни, имат само обработващите лични данни чрез персонална парола за отваряне на тези файлове, известна само на съответния служител, а в негово отсъствие - на прекия му ръководител или друг служител, изрично определен със заповед на изпълнителния директор на училището.

Чл. 15. (1) Компютрите се поставят в помещения за самостоятелна работа на операторите на лични данни, а когато не е налице организационно-техническа възможност за това, компютрите могат да бъдат поставени в общо помещение за работа на обработващия лични данни с изпълняващи други дейности.

(2) Местонахождението на сървъра е в помещение с постоянно видео наблюдение.

РАЗДЕЛ IV. МЕРКИ ЗА ГАРАНТИРАНЕ НИВОТО НА СИГУРНОСТ

Чл.16. (1) В ПГКПИ са предприети необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

(2) Мерките по ал. 1 включват следните средства за защита на личните данни:

1. програмно-апаратни:
   - разработване и прилагане на система за ограничаване на достъпа до лични данни; - защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители.
2. физически:
   - заключване на помещенията в извънработно време и регламентиране на достъпа до тях;
   - заключване в определените случаи на шкафовете за съхранение на информация, свързана с лични данни;
   - осигуряване на физическа охрана на сградите, в които се намират работни помещения, в които се съхраняват носители на лични ранни и са разположени компютърни и комуникационни средства, и/или осигуряване на СОТ в тези помещения;
3. организационни:
   - осигуряване на възможност за установяване самоличността на лицето, отговорно за сигурността
   - при мерки при средно ниво за сигурност;
   - разработване и прилагане на процедури за създаване на архивни копия и за възстановяване на данни - при мерки при средно ниво за сигурност;
   - разработване и прилагане на система за докладване, управляване и реагиране при инциденти.
4. нормативни:
   - спазване на законовите изисквания и прилагане на процедурите за защита на техническите и информационни ресурси от аварии, произшествия и бедствия (пожар, наводнение и др.);
   - осигуряване на ефективни механизми за контрол над спазването на вътрешните правила и съотносимите нормативни актове в ПГКПИ.

(3) Мерките по ал. 1 и 2 са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на вида на защитените данни.

Чл.17. Всички действия, които водят или могат да доведат до нерегламентирано изтриване, унищожаване или изменение на постъпили в училището лични данни в електронен вид или на хартиен носител са забранени.

Чл.18. (1) След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни в ПГКПИ:

1. ги унищожава, или
2. ги прехвърля на друг администратор, като предварително уведоми за това комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни КТИ ги съхранява само в предвидените в закон случаи.

Чл. 19. В ПГКПИ се извършва проверка на всички работни компютърни конфигурации съгласно чл.5, ал. 1, т. 10 от НМНТОМДВЗЛД на всеки шест месеца от компетентно длъжностно лице въз основа на заповед на главния секретар на КТИ , [Чл.20. (1) При възникнал инцидент (непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни)

Чл.20. (1) При възникнал инцидент (непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни) узналото за инцидента длъжностно лице докладва незабавно на прекия си ръководител, който е задължен да съобщи незабавно на директора на училището.

РАЗДЕЛ V. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ

Чл.21. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между звената в ПГКПИ обосновано искане и при уведомяване на съответния пряк ръководител.

Чл.22. (1) Достъп до личните данни и разкриването им се осъществява по реда и при условията на ЗЗЛД от страна на следните лица:

1. физическите лица, за които се отнасят данните;
2. изрично упълномощени с нотариално заверено пълномощно представители на лицата по т. 1 ;
3. трето лице, в случай, че е предвидено в нормативен акт;
4. обработващия личните данни.

(2) Достъпът се предоставя под формата на:

- устна или електронна справка,
- преглед на данните;
- предоставяне на копие от обработените данни.

(3) При поискване АЛД предоставя копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

Чл.23. (1) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от АЛД:

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;
3. информация за логиката на всяко автоматизирано обработване на лични данни, отнасящи се до него, поне в случаите на автоматизирани решения по чл. 346 от ЗЗЛД.

(2) При смърт на физическото лице правата му на достъп до личните данни и разкриването им се упражняват от неговите наследници.

(3) Информацията по ал. 1 може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(4) АЛД е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията по ал. 1.

(5) АЛД предоставя информацията по ал. 1 безплатно в електронен вид.

Чл.24. Физическото лице има право по всяко време ла поиска от АЛД да:

1. заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на този закон;
2. уведоми третите лица, на които са били разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с т. 1, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

Чл.25. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

(2) При не получаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

(3) Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.

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

Чл.26. (1) Правото на достъп и правата по чл.23 се осъществяват с писмено заявление/молба до АЛД, което може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронния подпис и съдържа:

1. име, адрес и други данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на информацията;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на заявление от упълномощено лице към заявлението се прилага и нотариално заверено пълномощно.

чл.27.

(1) Администраторът разглежда заявлението по чл.26, ал. 1 и се произнася в 14-дневен срок от постъпването му в училището.

(2) При заявленията за достъп АЛД разрешава пълен или частичен достъп на заявителя или мотивирано отказва извършването му.

(3) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в определените в чл.28, ал. 1, т. 1 и 2 от ЗЗЛД случаи, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(4) Администратора уведомява заявителя за решението си или отказа по ал.2 в съответния определен срок, лично срещу подпис или по пощата с обратна разписка.

(5) Липсата на уведомление по ал.4 се счита за отказ.

(6) Администратора на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

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

Чл.28. Действията на АЛД се обжалват по реда на Глава VII от ЗЗЛД.

РАЗДЕЛ VI. ПРАВА И ЗАДЬЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ В ПГКПИ

Чл.29. (1) Във връзка с обработването на лични данни служителите в училището имат права и задължения в съответствие с длъжностните си характеристики и са длъжни да спазват и изпълняват Вътрешните правила и съответните нормативни актове.

(2) За неспазване на нормативно установените си задължения във връзка с обработването на лични данни лицата по ал. 1 носят имуществена отговорност съгласно ЗЗЛД и дисциплинарна отговорност по Закона за държавния служител

РАЗДЕЛ VII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите правила са приети във връзка с чл.24, ал.4 от ЗЗЛД.
2. Контролът по изпълнение на настоящите Вътрешни правила се упражнява от Директора на ПГКПИ
3. Настоящите правила влизат в сила от деня на утвърждаването им със заповед на Директора на ПГКПИ
4. Изменението и допълнението на Правилата се извършва по реда за приемането им.
5. За неуредените с Правилата въпроси се прилагат ЗЗЛД и относимите нормативни актове
6. Оторизирани лица технология за достъп VPN, контролиран достъп с отдалечени сесии под контрола на лица имащи право да обработват лични данни.

Използване на комплексни пароли не по-къси от 8 знака, съдържащи букви, цифри или специални символи.

7. Съхранението и възтановяването на пароли се осъществява от оторизираните лица, обработващи личните данни с помощта на софтуер за управление на пароли.