Първо основно училище „Св. княз Борис I“
гр.Варна, р-н ”Вл. Варненчик” тел.052 510-313, тел.052 510-317
e-mail: osnovno_1@abv.bg www.1ou-varna.com

ВЪТРЕШНИ ПРАВИЛА И ПОЛИТИКИ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ

При изпълнение на дейностите, свързани със защита на личните данни следва да се спазват: Регламент (ЕС) 2016/279, Директива за защита на личните данни в полицейската и наказателната дейност /Директива (ЕС) 2016/680/, Конституция на РБ, Закон за защита на личните данни, Закон за електронните съобщения, Закон за мерките и действията по време на извънредно положение, Правилник за дейността на КЗЛД и нейната администрация, Наредба №1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни – отменена, считано от 25.05.2018г., Инструкция №1 от 21.12.2016г.за обстоятелствата , при които предприятията, предоставящи обществени електронни услуги, уведомяват потребителите за нарушения на сигурността на лични данни, формата и начина на уведомяването

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. I Основно училище „Свети княз Борис I“- Варна, като администратор на лични данни събира, обработва, съхранява и предоставя лични данни на служители, ученици, родители, посетители и други физически лица. Този документ съдържа политики и процедури, регламентиращи събирането и обработването на тази информация, която идентифицира всяко лице (лични данни).

Чл. 2. I Основно училище „Свети княз Борис I“- Варна е вписано като администратор на лични данни в публичния регистър на Комисията за защита на лични данни.

Раздел I. ЦЕЛИ, ОБХВАТ И ОСНОВНИ ПРИНЦИПИ НА ПОЛИТИКИТЕ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ

Чл.3. С настоящата политика се уреждат условията и реда за водене на регистри по ЗЗЛД, както и организацията и реда за упражняване на контрол при обработването на лични данни от служителите на I Основно училище „Св. княз Борис I“ - Варна.

Чл.4. Политиката е изготвена в съответствие с разпоредбите на Регламент (ЕС) 2016/279 на Европейския парламент и на Съвета от 27.04.2016г., Закона за защита на личните данни (ЗЗЛД) и Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и цели защита на интересите на учителите, служителите, родители, ученици, посетителите, както и на други физически лица на I Основно училище „Св. княз Борис I“ - Варна от незаконосъобразно и недобросъвестно обработване на личните им данни.

Чл.5. (1) Основен принципи при обработката на данните е, че те могат да се събират само за конкретни, изрични и легитимни цели, което означава, че няма да бъде приемливо първо да се събират данни и да се решава впоследствие как може да се използват.

(2) I Основно училище „Св. княз Борис I“ - Варна събира само минимално количество данни, необходими за изпълнение на конкретни, изрично указани и законни цели. Личните данни следва да са ограничени до необходимото във връзка с целите, за които се обработват.

Данните се съхраняват във формат, който не позволява лесно идентифициране на участващите, след като информацията вече не е необходима за първоначалната цел.

Чл. 6.Основните принципи при обработването на лични данни според Регламент (ЕС) 2016/279 на Европейския парламент и на Съвета от 27.04.2016г. са:

1. Принцип на точност - събраните данни трябва да бъдат точни и при необходимост да бъдат поддържани в актуален вид;
2. Принцип на ограничаване на съхранението - личните данни не трябва да се съхраняват за период по-дълъг от необходимото за целите, за които се обработват данните;
3. Принцип на цялостност и поверителност - въвеждат се технически и организационни мерки, които да гарантират необходимото ниво на сигурност на личните данни;
4. Принцип на отчетност - администраторът на лични данни може да демонстрира спазването на по-горните принципи.

Чл. 6. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстващи на целите, за които се обработват. В срок един месец от узнаването обработващият лични данни ги връща, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването или унищожаването се документира.

Чл. 7. (1) Първо основно училище „Св. княз Борис I“ - Варна, поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

(2) Първо основно училище „Св. княз Борис I“ - Варна спазва принципа за забрана на обработване на специални категории данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход; разкриване на политически възгледи, религиозни или философски убеждения; членство в политически партии или организации; сдружения с религиозни, философски, политически или синдикални цели; генетични данни, биометрични данни, лични данни, свързани с присъди и нарушения, данни за здравословното състояние на субекта, данни за сексуалната ориентация на субекта), като изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от ЗЗЛД.

Чл. 8. Законосъобразното обработване на данните включва наличието на следните елементи:

- Дадено валидно съгласие на субекта на данни.
- Когато обработването е необходимо за изпълнението на договор, по който субектът на данни е страна.
- Когато обработването е необходимо за спазване на законово задължение на администратора.
- Когато обработването е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данни;
- Когато обработването е необходимо за изпълнението на задача от обществени интерес;
- Когато обработването е необходимо за целите на легитимните интереси на администратора, освен когато преимущество пред тези интереси имат интересите или правата и основните свободи на субекта.

Чл. 9. (1) Съгласието на субекта на данни трябва да е свободно изразено, конкретно, информирано, недвусмислено, посредством изявление (декларация) или ясно потвърждаващо действие.

(2) Искането на съгласие за обработване се извършва задължително в момента на събиране на данните.

(3) Съгласието може да бъде оттеглено, като процесът на оттегляне е също толкова лесен, колкото процесът на предоставяне. След оттегляне на съгласието всяко последващо обработване на база на това съгласие трябва да се преустанови и данните следва да се изтрият или анонимизират.

(4) Ако обработването продължи на друга база (легитимни интереси), то субектът на данни трябва да знае за това - мълчаливо преминаване от една база на друга не е приемливо.

Раздел II ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 10. Субектът на данни се запознава със следните обстоятелства в момента на

предоставяне на данните си:

1. Кой обработва данните му;
2. Данни за контакт с администратора (длъжностно лице по защита на данните);
3. За какви цели ще се обработват данните и какво е законовото основание;
4. Ще бъдат ли предоставяни/обработвани данните от трети лица;
5. Какви са правата на субекта;
6. Как ще бъдат обработвани данните.

Чл. 11. Субектът на данни може да се информира за всички действия, извършвани във връзка с данните си и може да иска коригиране на неверни или неточни лични данни.

Чл. 12. Субектът на данни има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако е така да получи достъп до данните и информация относно целите на обработване, съответните категории лични данни, получателите, пред които са или ще бъдат разкрити личните данни и предвидения срок за тяхното съхранение.

Чл. 13. Субектът на данни има право да поиска от администратора да коригира неточните лични данни, свързани с него, както и да попълни непълните лични данни като се има предвид целите на обработването.

Чл. 14. Субектът на данни има право да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие личните данни, когато:

- Личните данни повече не са необходими за целите, за които са били събирани или обработвани;
- Субектът на данни оттегля своето съгласие и няма друго правно основание за обработването;
- Субектът на данни възразява срещу обработването на данни и няма законни основания за обработването, които да вземат преимущество;
- Личните данни са били обработвани незаконосъобразно;
- Личните данни трябва да бъдат изтрити с цел спазване на правно задължение съгласно европейското и национално законодателство;
- Личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

Чл. 15. Субектът на данни има право да поиска ограничаване на обработването в определени от закона случаи.

Чл. 16. Субектът на данни има право да получи данните си в структуриран, широко използван и пригоден за машинно четене формат (право на преносимост) и има правото да прехвърля тези данни на друг администратор, когато обработването е основано на съгласие или на договорно задължение или обработването се извършва по автоматизиран начин.

Чл. 17. Субектът на данни има право на възражение срещу обработването на лични данни и има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, което поражда правни последствия за субекта на данни или го засяга в значителна степен.

Чл. 18. Всички служители на I Основно училище „Св. княз Борис I“ - Варна при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни с родителите, служителите и учениците на училището, достъпни им при изпълнение на служебните задължения.

Чл. 19. I Основно училище „Св. княз Борис I“ - Варна поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.

Чл. 20. (1) В I Основно училище „Св. княз Борис I“ - Варна е определено длъжностно лице по защита на данните, което участва по подходящ начин и своевременно във всички въпроси, свързани с личните данни.

(2) Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните данни и с упражняването на техните права съгласно нормативните документи.

(3) Длъжностното лице по защита на данните е длъжно да спазва секретността или

поверителността на изпълняваните от него задачи в съответствие с европейското и национално законодателство.

РАЗДЕЛ III РЕГИСТРИ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Чл. 21. Поддържаните от I Основно училище „Св. княз Борис I“ - Варна регистри на дейностите по обработване на лични данни са, както следва:
1. „Ученици“
2. „Персонал“
3. „Родители“
4. „Видеонаблюдение“
5. „Пропускателен режим“

Нормативното основание е Закон за предучилищното и училищното образование и Наредбите към него за изпълнение на Закона, ЗЗЛД, КСО и приложимото законодателство, свързано с предоставянето на образователни услуги.

Чл. 22. (1) В регистър „Ученици“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в училището.

(2) Общо описание на регистър „Ученици“

Регистърът съдържа следните категории лични данни:
1. физическата идентичност на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка;
2. социална идентичност - образование;
3. лични данни, които се отнасят до здравето - здравно - профилактични карти на учениците, съдържащи данни относно текущия им здравен статус, предишни заболявания, хронични заболявания и др.

(3) Технологично описание на регистър „Ученици“:
1. 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 изолирани заключващи се помещения на операторите на лични данни. Информацията от хартиените носители за всеки ученик, се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст; Дневник за I -VII клас; Главна книга, които се съхраняват в същите изолирани помещения.
- На технически носител: Личните данни се въвеждат в специализирана информационна система за училищна администрация Админ Про, електронен дневник. Базата данни се намира на твърдия диск на изолирани компютри.
- срок на съхранение: съгласно Номенклатурата на делата в I Основно училище „Св. княз Борис I“ - Варна със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Ученици“ са: заместник - директори УД, ЗАС, секретар, класни ръководители и целия педагогически персонал. Длъжностните лица - обработващи лични данни и оператори на 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 - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще 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) I Основно училище „Св. княз Борис I“ - Варна 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 Първо основно училище „Св. княз Борис I“ - Варна - 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“, съд, следствие, прокуратура, ревизиращи органи, МВР, Община и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове, 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 I ОУ „Св. княз Борис I“ - Варна
(10) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, за което се изготвят актови протоколи за унищожаване.

Чл.23. (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, 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 - медицинско свидетелство;
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 и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в изолирани

заключващи се помещения на операторите на лични данни, снабдени със защитна сигнализация.
- На технически носител: Личните данни се въвеждат в специализирана програма 1111 ЕЛИТ-Личен състав и ТРЗ и Админ ПРО: счетоводство, ЗАС. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно Номенклатурата на делата в I Основно училище „Св. княз Борис I“ със срокове на съхранение.
(4) Определяне на длъжностите:
Обработващи лични данни на регистър „Персонал“ са: заместник - директори УВД, гл. счетоводител, ЗАС.
Оператор на лични данни на регистър „Персонал“ е ЗАС.
(5) 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.
(6) Организационни мерки за физическа защита - определени са помещенията, в които ще 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.
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 училището.
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.
(7) I Основно училище „Св. княз Борис I“ 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 Първо основно училище „Св. княз Борис I“ - 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 „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.
(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 I Основно училище „Св. княз Борис I“.
(10) След постигане целите по предходната алинея личните данни се унищожават физически, за което се изготвят актови протоколи за унищожаване.

Чл.24. (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, учители и служители в сградата на училището.
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 училището.
(4) Определяне на длъжностите:
Оператори на лични данни на регистър „Видеонаблюдение“ са заместник - директори УВД.
(5) 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.
(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 DVR за срок от 1 месец. 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.

Чл. 25. (1) В регистър „Пропускателен режим“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, които влизат в сградата на училището.
2) Общо описание на регистър „Пропускателен режим“:
Категориите физически лица, за които се обработват лични данни, са посетители и физически лица към външни изпълнители в сградите на училището.
Регистърът относно външните изпълнители съдържа следните групи данни:
1. физическата идентичност - имена.
2. дата и час на посещението;
3. име и ЕИК на фирмата, към която принадлежи посетителят (когато е приложимо).
4. цел на посещението;
5. внасяни в училището оборудване/материали, вид, брой.
6. подпис на портиер.
Регистърът относно посетителите съдържа следните групи данни:
1. физическа идентичност - име, фамилия;
2. дата и час на посещението;
3. при кого отива посетителят.
(3) Технологично описание на регистър „Пропускателен режим“: Регистърът се попълва на хартиен носител: Данните се набират в писмена (документална) форма от портиерите на училището.

(4) Определяне на длъжностите:
Обработващи лични данни на регистър „Пропускателен режим“ са заместник - директор УВД;
Оператори на лични данни на регистър „Пропускателен режим“ са портиери.
(5) 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.
(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) I Основно училище „Св. княз Борис I“ 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 Първо основно училище „Св. княз Борис I“ - 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.
(9) Достъп до регистър „Пропускателен режим“ имат и държавните органи - МВР, НАП, НОИ, МОН, РУО и други 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.
(10) 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 Първо основно училище „Св. княз Борис I“.
(11) След постигане целите по предходната алинея личните данни се унищожават физически, за което се изготвят актови протоколи за унищожаване.
(12) 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.

Чл. 26. (1) В регистър „Родители“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „родители“ на обучавани в училището ученици.

(2) Общо описание на регистър „Родители“
Регистърът съдържа следните категории лични данни:
1. физическата идентичност на лицето: имена, ЕГН, адрес, телефони за връзка

(3) Технологично описание на регистър „Родители“:
1. 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 изолирани заключващи се помещения на операторите на лични данни. Информацията от хартиените носители за всеки родител на ученик се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст; Дневник за I -VII клас, със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите изолирани помещения.
- срок на съхранение: съгласно Номенклатурата на делата в I Основно училище „Св. княз Борис I“ - Варна със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Родители“ са: заместник - директори УВД, класни ръководители и педагогически съветник. Длъжностните лица - обработващи лични данни и оператори на 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 - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще 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.

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) I Основно училище „Св. княз Борис I“ - Варна 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 I Основно училище „Св. княз Борис I“ - Варна - 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“, съд, следствие, прокуратура, ревизиращи органи, МВР, Община и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове, когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни на родителите 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 Първо основно училище „Св. княз Борис I“ - Варна

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

РАЗДЕЛ IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ И НА ДЛЪЖНОСТНОТО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл.27. Служителите на училището са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно и по прозрачен вид;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се обработват, и да не ги обработват по начин, несъвместим с тези цели;
3. да не обработват лични данни в по-голям обем от необходимия за постигането на определени цели;
4. да актуализират личните данни при установена необходимост;
5. да коригират личните данни при установена неточност;
6. да заличават лични данни, когато се установи че са непропорционални по отношение на

целите, за които се обработват;
7. 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;
8. да гарантират сигурността на личните данни, включително и като не изнасят и съхраняват такива извън специално определените за целта места – обект на технически и организационни мерки за защита;
9. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл.28. (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.

Чл.29. (1) Длъжностно лице по защита на личните данни има следните правомощия:
1. Информира и съветва администратора и обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 24 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и на други разпоредби за защита на данните на равнище ЕС или държава членка;
2. Наблюдава спазването на Регламент 2016/679 и на други разпоредби за защита на данни на равнище Съюз и държава членка и на политиките на администратора или обработващия данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване;
3. При поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценка съгласно чл. 35 от Регламента;
4. Сътрудничи с надзорния орган - КЗЛД;
5. Действа като точка за контакт на надзорния орган по въпроси, свързани с обработването.
6. Задължение на администратора и на обработващия лични данни е да гарантират участието на длъжностното лице по защита на данните по всички въпроси, свързани със защитата на личните данни.
7. При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработването, и се съобразява с естеството, обхвата, контекста и целите на обработката.
8. Играе ключова роля в насърчаването на културата по защита на данните в рамките на училището.
9. Длъжностното лице по защита на данните не поучава никакви указания във връзка с изпълнение на своите задачи и ги изпълнява независимо.
10. Длъжностното лице по защита на данните е обвързано със задължение да спазва конфиденциалност при изпълнение на неговите задачи.
11. Изпълнението на други задължения от длъжностното лице по защита на личните данни не следва да водят до конфликт на интереси.
12. Ролята на длъжностното лице в процеса на оценката на въздействие върху защитата на данните е помощна и консултативна.

РАЗДЕЛ V. ОТЧЕТНОСТ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 30. (1) Отчетността е задължение на администратора на лични данни и основен инструмент за доказване изпълнението на изискванията на Общия регламент за защита на личните данни.

(2) Отчетност представлява способността във всеки един момент администраторът на лични данни да удостовери и да докаже, че обработва личните данни законосъобразно, добросъвестно, прозрачно, за конкретни и пропорционални цели, с подходящо ниво на

сигурност и защита.

Чл. 31. Основните средства за спазване на принципа на отчетност са:

1. Поддържането на регистри на дейностите по обработване;
2. Определяне на длъжностно лице по защита на личните данни, когато такова се изисква;
3. Извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица;
4. Своевременно уведомяване на Комисията за защита на личните данни и субекта на данните при нарушения на сигурността;
5. Прилагане на доброволни механизми за сертифициране и/или спазването на кодекси на поведение.

РАЗДЕЛ VI. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 32. (1) Оценката на въздействието е важен инструмент за отчетност, който помага на администратора не само да спазват изискванията на Общия регламент за защита на личните данни, но и да демонстрира, че са взети подходящи мерки, за да се гарантира спазването на регламента.

(2) Оценката на въздействието е процес, предназначен, за да опише обработването на лични данни, да оцени необходимостта и пропорционалността на обработката и да спомогне за избора на най-подходящите технически и организационни мерки за защита.

(3) Оценката на въздействието може да се отнася до единична операция за обработване на данни или до многобройни повтарящи се или сходни операции.

Чл. 33. (1) Оценка на въздействието се изисква само когато обработването на лични данни има вероятност да доведе до висок риск за правата и свободите на физическите лица.

(2) Операции по обработване, които по правило пораждат висок риск, са например извършването на:

• автоматично вземане на решения, включително профилиране;

• мащабно обработване на данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация, както и данни за предишни осъждания на лицето;

• систематично мащабно наблюдение на публично достъпна зона.

Чл. 34. Оценка на въздействието може да бъде извършена от самия администратор, негов служител или от лице, външно за организацията, но отговорността за извършването ѝ остава на самия администратор. Администраторът задължително трябва да потърси съвет от служителя по защита на данните, когато такъв е определен, а взетите решения следва да бъдат документирани.

Чл. 35. (1) Общият регламент за защита на личните данни определя минималното съдържание на оценката на въздействието:

• системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

• оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

• оценка на рисковете за правата и свободите на субектите на данни,

• мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(2) Администраторът задължително провежда предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

Чл. 36. Ако администраторът установи нарушение на сигурността на личните данни, той следва да уведоми надзорния орган (КЗЛД) без ненужно забавяне и когато това е осъществимо

- не по - късно от 72 часа след като е разбрал за него.

(2) Уведомяване не е нужно, ако администраторът е в състояние да докаже, че няма вероятност нарушението да доведе до риск за правата и свободите на физическите лица.

Чл. 37. (1) Администраторът следва да уведоми субекта за всяко нарушение, което е вероятно да доведе до висок риск за правата и свободите на физическото лице.

(2) Уведомлението следва да съдържа информация за естеството на нарушението и препоръки за това как засегнатото препоръки за това как засегнатото лице да ограничи последиците от нарушението.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

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

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

§ 3. **„Регистър с лични данни“** 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.

§ 4. **„Администратор“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

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

§ 6. **„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. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 7. Всички служители на училището са длъжни срещу подпис да се запознаят с политиките и да ги спазват.

§ 8. Вътрешните правила и политиките се издават 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.

§ 9. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Регламент (ЕС) 2016/279 на Европейския парламент и на Съвета от 27.04.2016г., 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.