МАТЕМАТИЧЕСКА ГИМНАЗИЯ „Д-Р ПЕТЪР БЕРОН“ - ВАРНА

УТВЪРДИЛ: .....

ДИРЕКТОР
/Елеонора Павлова/

ПОЛИТИКА
ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ
НА МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА

Чл. 1. Обхват на политиката и предназначение

1) Политиката на МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА за обработване и защита на лични данни е в съответствие с изискванията на Закона за защита на личните данни и чл. 9, ал.2, т.1 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

2) Видовете защита на личните данни са физическа, персонална, документална, техническа (защита на автоматизирани информационни системи и мрежи) и криптографска защита. Политиката на МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА за обработване и защита на лични данни е основна мярка в защитата на автоматизираните информационни системи и мрежи като въвежда система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

3) Освен първоначалната оценка на въздействието на обработваните регистри с лични данни и съответно нивото на защита, МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА извършва периодична оценка на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите лица и регистри.

4) Неразделна част от настоящата политика са Инструкцията по чл. 23, ал. 4 от Закона за защита на личните данни и чл. 19, т. 2 от Наредба № 1 (Приложение № 1), Оценка на нивото на въздействие на група от „2" регистъра (Приложение № 2) и Декларация по чл. 7, ал. 5 от Наредба № 1 (Приложение № 3).

Чл. 2. Цел на политиката.

Настоящата политика има за цел да регламентира:

1. минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита, прилагани от МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА;
2. осигуряването на адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване);

3. организационни мерки в МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА, прилагани спрямо лицата, обработващи лични данни и лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, осигуравящи спазването на нормативните изисквания и прилагането на тази Политика и Инструкцията;
4. оценка и нива на въздействие и определяне на ниво. на защита в дейността на МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА.

Чл. 3. Видове защита и мерки.

Видовете защита на личните данни и прилагането на система от мерки, съответстващи на различните видове защита, които осигуряват адекватно ниво на защита в поддържаните регистри с лични данни, както следва:

1) Физическа - въвеждане на система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
Основните организационни мерки на физическата защита са:
1. определяне на зоните с контролиран достъп;
2. определяне на помещенията, в които ще се обработват лични данни;
3. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
4. определяне на организацията на физическия достъп;
5. определяне на режима на посещения;
6. определяне на използваните технически средства за физическа защита;
7. определяне на екип за реагиране при нарушения.

Основните технически мерки на физическата защита са:
1. ключалки;
2. шкафове;
3. метални каси;
4. оборудване на зоните с контролиран достъп;
5. оборудване на помещенията;
6. устройства за контрол на физическия достъп;
7. охрана и/или система за сигурност;
8. средства за защита на периметъра;
9. пожарогасителни средства;
10. пожароизвестителни и пожарогасителни системи;
11. детектори за субстанции (метали, взривни вещества и др.).

2) Персонална - въвеждане на система от организационни мерки спрямо лицата, обработващи лични данни и лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, чрез указания, въведени от администратора, в Правилата за вътрешна организация и чрез определяне на правата и задължения в индивидуалните длъжностни характеристики.
Основните мерки на персоналната защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа "Необходимост да знае" и съответно са:
1. познаване на нормативната уредба в областта на защитата на личните данни;
2. знания за опасностите за личните данни, обработвани от администратора;
3. споделяне на критична информация между персонала (например

идентификатори, пароли за достъп и т.н.);
4. съгласие за поемане на задължение за неразпространение на личните данни;
5. обучение;
6. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3) Документална - въвеждане на система от организационни мерки при обработването на лични данни на хартиен носител.

Основните мерки на документалната защита са:

1. определяне на регистрите, които ще се поддържат на хартиен носител;
2. определяне на условията за обработване на лични данни;
3. регламентиране на достъпа до регистрите;
4. контрол на достъпа до регистрите;
5. определяне на срокове за съхранение;
6. правила за размножаване и разпространение;
7. процедури за унищожаване;
8. процедури за проверка и контрол на обработването;
9. съхраняване на документите в помещения за архиви с регулиран достъп.

4) Техническа — отнася се до защита на автоматизираните информационни системи и мрежи и представлява въвеждане на система от технически и организационни мерки за съхраняване и защита от незаконни форми на обработване на личните данни.

Основните мерки за защита на автоматизираните информационни системи и мрежи са:

1. политика за защита на личните данни, ръководства по защита и стандартни операционни процедури;
2. определяне на права, задължения и отговорности;
3. идентификация и автентификация;
4. управление на регистрите;
5. контроли на сесията;
6. външни връзки/свързване;
7. телекомуникации и отдалечен достъп;
8. наблюдение;
9. защита от вируси;
10. планиране на случайността/непредвидените случаи;
11. поддържане/експлоатация;
12. управление на конфигурацията;
13. копия/резервни копия за възстановяване;
14. носители на информация;
15. физическа среда/обкръжение;
16. персонална защита;
17. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;
18. определяне на срокове за съхранение на личните данни;
19. процедури за унищожаване/заличаване/изтриване на носители.

Чл. 4. Оценка и нива на въздействие. Определяне на ниво на защита.

1) За да определи адекватните техническите и организационните мерки за съответния вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. Оценка на въздействие се извършва за всички поддържани

регистри. Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

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.

3) При оценка на въздействието, се вземат предвид;

- личните аспектите, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение, която се основава на автоматизирано обработване и на чието основание се вземат мерки, които пораждат правни последици за лицето или го засягат в значителна степен;
- 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;
- лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;
- лични данни в широкомащабни регистри на лични данни;
- данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

4) След анализ на оценката на въздействие, администраторът определя нивото за въздействие за всеки един от водените регистри, което може да бъде:

- "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;
- "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;
- "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;
- "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.

5) На база оценката на нивото на въздействие, администраторът определя съответното ниво на защита, което представлява съвкупност от технически и организационни мерки за физическа, персонална, документална защита, техническа

(защита на автоматизираните информационни системи и мрежи) и криптографска защита на личните данни. Нивата на защита са, както следва:

- при ниско ниво на въздействие - ниско ниво на защита;
- при средно ниво на въздействие - средно ниво на защита;
- при високо ниво на въздействие - високо ниво на защита;
- при изключително високо ниво на въздействие - изключително високо ниво на защита.

6) След определяне на съответното ниво на защита, администраторът следва да осигури минималното ниво на технически и организационни мерки, отговарящи на определеното ниво и съответстващи на изискванията на нормативната уредба по отношение на видовете защита на личните данни - физическа, персонална, документална, техническа (защита на автоматизирани информационни системи и мрежи) и криптографска защита.

7) Оценката по чл. 4 се посочва в Приложение № 2.

Чл. 5. Организационни мерки спрямо обработващите лични данни.

1) Лицата, обработващи лични данни могат да започнат да обработват лични данни след:
   1. запознаване с нормативната уредба в областта на защитата на личните данни и настоящата Политика и Инструкцията;
   2. да познават опасностите при обработка на личните данни;
   3. да спазват различните нива на достъп, изградени в дейността на Администратора при обработка на лични данни;
   4. да не разпространяват и споделят данни, идентификатори, пароли и други с помежду си и пред трети лица.

2) Лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

3) Администраторът поддържа информация за изпълнение на следните задължения:
   1. наличие на декларации, удостоверяващи съгласие за поемане на задължение за неразпространение на личните данни;
   2. провеждане на обучение;
   3. провеждане на тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

4) Декларацията е със съдържание, съгласно Приложение № 3.

Допълнителни разпоредби

§ 1. Политиката е приета от Педагогически съвет на 27.09.2023 г.
§ 2. По смисъла на настоящата Политика:
- "Администратор на лични данни" е МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА.
- "Обработващ лични данни" са лицата, обработващи лични данни и лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични и

които работят по договор за МГ "Д-Р ПЕТЪР БЕРОН" ВАРНА.

- „Поверителност' е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- „Цялостност" е изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.
- „Наличност" е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.