СРЕДНО УЧИЛИЩЕ “СВЕТИ КЛИМЕНТ ОХРИДСКИ”
ГРАД АКСАКОВО, ОБЛАСТ ВАРНА
ул. “Митко Палаузов” № 27ª; тел: 76-20-81; 76-32-81; e-mail: souaksakovo@abv.bg

УТВЪРЖДАВАМ:

МАРИЕЛА ПЕТРОВА
Директор на СУ „Свети Климент Охридски”

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА СУ „СВ. КЛИМЕНТ ОХРИДСКИ", ГР. АКСАКОВО

Тази вътрешни правила за защита на данните представят принципите и правните условия, които институцията трябва да спази, когато получава, обработва, предава или съхранява лични данни за целите на своята дейност, включително лични данни на ученици, доставчици и работници/служители и други физически лица. Правилата са в съответствие с изискванията на Общия Регламент за Защита на Данните (Регламент 2016/679) (GDPR).

1. ИНТЕРПРЕТАЦИЯ

1.1. ДЕФИНИЦИИ

Автоматизирано Вземане на Решения: когато дадено решение е взето изцяло на базата на Автоматизирано Обработване (включително профилиране), което води до правни последици или засяга значително физическото лице. GDPR забранява Автоматизираното Вземане на Решения (освен ако определени условия са на лице), но не и Автоматизираното Обработване.

Автоматизирано Обработване: всяка форма на автоматизирано обработване на Лични Данни, състоящо се в употребата на Лични Данни с цел оценка на личните аспекти на дадено физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението,_ местоположението или движенията. Профилирането е вид Автоматизирано Обработване.

Администратор: лицето или организацията, която определя кога, защо и как се обработват Лични Данни. Администраторът е отговорен за определяне на практики и политики в съответствие с GDPR.

Ние сме Администратор на всички Лични Данни, отнасящи се до нашия Персонал, както и на Лични Данни на учениците, родителите и други трети лица, използвани при изпълнение на дейностите като образователна институция.

Длъжностно лице по защита на данните (DPO): лицето или организацията, която следва да бъде определена в определени ситуации, регламентирани от GDPR. При липса на задължение за определяне на DPO, този термин означава Мениджър по Защита на Данните или друга длъжност, или екипа по сигурност на данни в организацията, който има отговорност за спазване на законодателството в областта на данните.

ЕИП: 28-те държави-членки на ЕС, както и Исландия, Лихтенщайн и Норвегия

Защита на данните на етапа на проектирането: въвеждане на подходящи технически или организационни мерки по ефективен начин, който да осигури съответствие с GDPR.

Известия по защита на данните: отделни известия, съдържащи информация, предоставяна на Субектите на Данни в момента, в който институцията събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на институцията), така и отнасящи се до обработване със специфична цел.

Изрично Съгласие: съгласие, което изисква много ясно и определено твърдение (не просто действие)

Име на Организацията: Средно училище „Свети Климент Охридски“ (СУ „Св. Климент Охридски“), гр. Аксаково, общ. Аксаково, обл. Варна, ул. „Митко Палаузов“ № 27а

Лични Данни: всяка информация, идентифицираща Субект на данни или информация, свързана със Субект на данни, който ние можем да идентифицираме (директно или индиректно) само чрез данните или в комбинация с други идентификатори, които притежаваме или до които имаме достъп. Личните Данни включват Чувствителни Лични Данни и Псевдоминизирани Лични Данни, но изключват Анонимизирани Лични Данни. Личните Данни могат да се отнасят до факти (например – име, e-mail адрес, местоположение или дата на раждане) или до мнение относно действията или поведението на Субекта на данни.

Нарушение на Защитата на Личните Данни: всяко действие или бездействие, което компрометира сигурността, конфиденциалността или целостта на данните, или на физическите, технически, административни или организационни защити, които ние или нашите изпълнители по договор използваме, за да ги защитим. Загубата, неоторизираният достъп, предоставяне или получаване на Лични Данни са примери за Нарушение на сигурността.

Обработване на Данни: всяка дейност, която е свързана с използването на Лични Данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на Лични Данни до трети лица.

Общият Регламент за Данните (GDPR): Общият Регламент за Данните ((ЕС) 2016/679). Личните Данни са обект на защитата, определена в GDPR.

Оценка на въздействието: механизми и мерки, използвани за идентифициране на риска, свързан с обработката на данните. Оценката на въздействието следва да бъде извършена за всички ключови системи или програми, свързани с Обработването на Лични Данни.

Персонал: всички работници и служители и ръководител, назначен по договор за управление и контрол

Псевдоминизиране: заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече изкуствени идентификатори (“псевдоними”) така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.

Субект на данни: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, и чиито Лични Данни ние обработваме.

Съгласие: всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на Субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на Лични Данни свързани с него.

Чувствителни Лични Данни: информация, разкриваща расовия или етнически произход, политическите мнения, религиозни и други подобни вярвания, членство в синдикални организации, физическото или умствено здравословно състояние, сексуален живот, сексуална ориентация, биометрични или генетични данни, както и Лични Данни отнасящи се до наказателни престъпления и присъди.

2. ВЪВЕДЕНИЕ

Тази политика по защита на данните оказва как ние, СУ „Св. Климент Охридски“ управляваме Личните Данни на учениците, родителите, доставчици, работници и служители, и други трети лица.

Тези вътрешни правила се прилагат спрямо всички Лични Данни, които обработваме, без значение от това на какъв носител са съхранени или дали са свързани с бивши и настоящи работници и служители, потребители на уебсайта ни или всеки друг Субект на Данни.

Тези вътрешни правила следва да се прилагат спрямо целия Персонал на Институцията. Всички работници и служители следва да прочетат, да се запознаят с и да спазват тази Политика, когато обработват лични данни от името на Институцията и да посетят обучение по нейните изисквания. Тези вътрешни правила оказват какви са нашите очаквания към Персонала да осигури спазване на законодателството от страна на Институцията. Всяко нарушение на тези вътрешни правила може да доведе до дисциплинарни санкции спрямо работника или служителя.

Тези правила са вътрешен документ и не могат да бъдат споделяни с трети лица, клиенти или регулаторни органи без предварително одобрение от представляващия Институцията.

3. ОБХВАТ

Ние оценяваме факта, че правилното и законосъобразно управление на Лични Данни ще осигури доверието в Институцията ни. Опазването на конфиденциалността и целостта на Личните Данни е ключова отговорност, към която ние се отнасяме изключително сериозно. Организацията може да подлежи на санкция в размер до 20 млн. евро или 4 % процента от световния оборот (което от двете е по-голямо и в зависимост от конкретното нарушение), ако не спази изискванията на GDPR.

Всички ръководни длъжностни лица в Институцията носят отговорност за спазването на тези правила от страна на Персонала и следва да въведат подходящи практики, процеси и обучение.

Длъжностното лице по Защита на Данните (DPO) е отговорно за контрола по прилагането на тези правила, както и, ако е приложимо, за разработване на свързани политики и други насоки. Тази позиция в момента заема Илко Божидаров Илиев – заместник-директор, административно-стопанска дейност, тел. 0884466736, e-mail souaksakovo@abv.bg

Моля, свържете се с DPO при всякакви въпроси относно приложението на тези правила или, ако имате опасения, че те не се прилагат коректно. Трябва задължително да се свържете с DPO в следните ситуации:

- Ако не сте сигурни за законовата база, на която може да разчитате при обработка на Лични Данни (*вижте Раздел 5.1 по-долу*)
- Ако трябва да разчитате на Съгласие и/или трябва да осигурите Изрично Съгласие
- Ако трябва да изготвите Известия по Защита на Данните (*вижте Раздел 5.3 по-долу*)
- Ако имате притеснение относно срока на съхранение на Лични Данни, които обработвате
- Ако не сте сигурни какви мерки за сигурност на данните следва да въведете, за да защитите Личните Данни
- Ако установите Нарушение на Защитата на Личните Данни
- Ако не сте сигурни на каква база може да извършите трансфер на Лични Данни извън ЕИП (*вижте Раздел 11 по-долу*)
- Ако имате нужда от съдействие в следствие на постъпила информация, че Субект на данни желае да упражни някое от правата си, съгласно GDPR (*вижте Раздел 12 по-долу*)
- Винаги, когато планирате да стартирате или да промените значително начина, по който извършвате определена операция по Обработване, която може да изисква Оценка на Въздействието (*вижте Раздел 13.5 по-долу*) или възнамерявате да използвате Лични Данни за цели, различни от тези, за които са били събрани
- Ако планирате да извършвате дейности по обработка на Лични Данни, базирани на Автоматизирано Обработване, включително Профилиране и Автоматизирано Вземане на Решения

- Ако имате нужда от съдействие относно спазване на приложимото законодателство спрямо дейности по директен маркетинг (*вижте Раздел 13.6 по-долу*)
- Ако имате нужда от съдействие във връзка с договори или в други области във връзка със споделяне на Лични Данни (особено с доставчици) (*вижте Раздел 13.7 по-долу*)]

4. ПРИНЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Ние се придържаме към принципите за защита на Личните Данни в GDPR, които изискват всички Лични Данни:

1. Да се обработват законосъобразно, добросъвестно и прозрачно
2. Да се събират само за конкретни, изрично оказани и легитимни цели
3. Да бъдат подходящи, свързани с и ограничени до стриктно необходимото за целите, за които се обработват
4. Да бъдат точни и при възможност поддържани в актуален вид
5. Да са съхранявани във формат, който да позволява идентифицирането на Субекта на данни за не по-дълъг срок от необходимия за целите на Обработването
6. Да са обработени по начин, който осигурява тяхната сигурност, използвайки технически и организационни мерки, които да ги предпазват от неоторизирано или незаконно Обработване и от случайна загуба, унищожаване или повреждане
7. Да не се трансферират до друга страна извън ЕИП без необходимите предпазни мерки
8. Да се предоставят на Субектите на Данни, на които да се даде възможност да упражнят правата си спрямо техните Лични Данни.

Ние следва да можем да демонстрираме, че спазваме принципите, описани по-горе.

5. ЗАКОНОСЪОБРАЗНОСТ, ДОБРОСЪВЕСТНОСТ, ПРОЗРАЧНОСТ

5.1. ЗАКОНОСЪОБРАЗНОСТ И ДОБРОСЪВЕСТНОСТ

Личните Данни трябва да се обработват законосъобразно, добросъвестно и по прозрачен начин спрямо Субекта на данни.

GDPR ограничава кръга на нашите действия с Лични Данни до тези, за които е на лице законосъобразна база. Тези ограничения не целят да предотвратят Обработването, а да гарантират, че обработваме Лични Данни добросъвестно и без негативни последствия за Субекта на данни.

GDPR регламентира законосъобразните бази за обработка, някои от които са изброени по-долу:

1. Субектът на данните е дал своето Съгласие
2. Обработването е необходимо във връзка с изпълнението на договор със Субекта на данните
3. Обработването е необходимо, за да изпълним нашите законови задължения
4. Обработването е необходимо, за да се защитят жизненоважните интереси на Субекта на данните
5. Обработването е необходимо за целите на легитимните ни интереси, освен когато пред интересите ни преимущество имат интересите или основните права и свободи на Субекта на Данни. Целите, за които обработваме Лични Данни на това основание трябва да са описани в приложимите Известия по Защита на Данните.

5.2. СЪГЛАСИЕ

Администраторите на данни могат да обработват Лични Данни единствено в случаите, в които поне една от законовите бази в GDPR е налице, което включва и Съгласие.

Субектът на данни е съгласен с Обработването, ако го изрази ясно – чрез изявление или позитивен акт. Съгласието изисква положително действие –предварително отметнати полета за съгласие или бездействие не представляват валидно съгласие. Ако Съгласието за Обработка на Лични Данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието с другите въпроси.

Субектите на данни трябва да могат лесно да оттеглят Съгласието си за Обработване по всяко време и оттеглянето трябва да бъде уважено своевременно. Съгласието трябва да се изиска отново, ако възнамерявате да обработвате Лични Данни на ново, различно основание, за което Субектът не е дал Съгласие първоначално.

В случаите, когато не можем да разчитаме на друга законова база за Обработване, Изрично Съгласие е обикновено необходимо при обработка на Чувствителни Лични Данни, при Автоматизирано Вземане на Решения и за трансфер на данни извън ЕИП.

Винаги когато разчитате на Съгласие трябва да го документирате и да пазите съвестна отчетност, за да може Институцията да демонстрира спазването на изискванията за Съгласие.

5.3. ПРОЗРАЧНОСТ СПРЯМО СУБЕКТА НА ДАННИ

GDPR изисква от всички Администратори да предоставят детайлна, конкретна информация до Субектите на данни, в зависимост от това дали данните са получени от тях директно или от друг източник. Тази информация трябва да бъде предоставена чрез подходящи Известия по Защита на Данните, които трябва да са лесно достъпни и да използват ясен език, без излишна правна терминология, така че Субектите на данни да могат лесно да ги разберат.

Винаги когато събираме Лични Данни директно от Субекта, включително с цел администриране на трудови правоотношения, трябва да им предоставим информацията, изисквана от GDPR.

Информацията следва да включва: данни за контакт с Администратора и DPO, как и защо ще използваме, обработваме, предоставяме, защитим и съхраним Личните Данни. Ние имаме задължение да предоставим информацията в момента на получаване на Личните Данни от Субекта.

6. ОГРАНИЧЕНИЕ НА ЦЕЛИТЕ

Всички Лични Данни трябва да се съберат само за конкретни и легитимни цели, и не трябва да се обработват по-начин, който не е съвместим с тези цели.

Нямате право да използвате Лични Данни за нови, различни и несъвместими с първоначалните цели, освен ако Субектът не предостави последващо Съгласие за новите цели.

7. МИНИМИЗИРАНЕ НА ДАННИТЕ

Личните Данни следва да бъдат подходящи, свързани с и ограничени до стриктно необходимото за целите, за които се обработват.

Вие имате право да Обработвате Лични Данни, само когато това е свързано с изпълнение на служебните Ви задължения. Не бива да събирате Лични Данни, които не са необходими.

Вие имате ангажимент да осигурите навременното изтриване/унищожаване или анонимизиране, в съответствие с насоките на Институцията, на всички Лични Данни, които вече не са необходими за конкретните цели.

8. ТОЧНОСТ

Личните Данни следва да бъдат точни и при възможност поддържани в актуален вид. При установяване на неточност, данните следва да се коригират или изтрият без забавяне.

Вие следва да се уверите, че Личните Данни, които съхраняваме, са точни, пълни, актуализирани и ограничени до целите, за които са събрани. Вие трябва да проверявате точността на всички Лични Данни в момента на тяхното събиране и на регулярни интервали след това. Вие трябва да вземете всички разумни мерки за унищожаването или корекцията на всички неточни или неактуални Лични Данни.

9. ОГРАНИЧАВАНЕ НА СЪХРАНЕНИЕТО

Личните Данни не бива да се съхраняват във формат, който позволява идентифицирането на Субекта за по-дълго време от необходимото за целите, за които са събрани.

Институцията разработва правила и политики относно съхранението на Лични Данни, които да осигурят изтриване на Данните, за които вече не съществува легитимна цел за Обработване, освен ако друг закон не ни задължава да запазим данните за определен минимален срок.

Ние ще вземем всички разумни мерки за унищожаване и изтриване от нашите системи на всички Лични Данни, от които вече нямаме нужда, в съответствие с правилата и политиките ни по съхранение – това може да включва и ангажимент да изискате от трети страни да изтрият тези Лични Данни.

Ние следва да се уверим, че Субектите на Данни са информирани (чрез съответните Известия по Защита на Данните) за какъв период техните Лични Данни ще се съхраняват и как се определя този период.

10. СИГУРНОСТ, ЦЯЛОСТ И КОНФИДЕНЦИАЛНОСТ

10.1. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Личните Данни следва да бъдат защитени с необходимите технически и организационни мерки срещу неоторизирано и незаконно Обработване, и срещу случайна загуба, унищожаване или увреждане.

Ние ще разработим, въведем и поддържаме подходящи мерки за защита, съобразени с дейността на нашата Институция, нашите ресурси, количеството и вида Лични Данни, които Обработваме. Ние ще извършваме редовна оценка на ефективността на тези мерки. Субектът на данни също носи отговорност за защитата на Личните Данни, които съхраняваме и следва да е особено внимателен, когато осигурявате защитата на Чувствителни Лични Данни от загуба и неоторизиран достъп, употреба или предоставяне.

Субектът на данни трябва да следва всички процедури и технологични мерки, които сме въвели, с цел опазване сигурността на Личните Данни от момента на тяхното събиране до момента на тяхното унищожаване. Може да трансферираме лични данни до изпълнители по договори, само ако те се съгласят да спазват нашите политики и процедури и да осигурят необходимите мерки за защита, които ние изискаме.

Ние трябва да осигурим сигурността на данните като защитите тяхната конфиденциалност, цялост и достъпност, дефинирани както следва:

- Конфиденциалност означава, че само хората, които следва да знаят и са оторизирани да използват Личните Данни, имат достъп до тях
- Цялост означава, че Личните Данни са точни и подходящи за употреба за целите, за които се Обработват
- Достъпност означава, че оторизираните потребители имат осигурен достъп до Личните Данни за оторизирани цели.

Субектът на данна трябва да спазва и да не възпрепятства действието на административните, физически и технически защити, които сме въвели.

10.2. ДОКЛАДВАНЕ НА НАРУШЕНИЕ НА ЗАЩИТАТА НА ДАННИТЕ

GDPR изисква от Администраторите да докладват Нарушенията на Защита на Данните пред регулаторния орган и, в някои ситуации, Субекта на данни.

Ние сме въвели процедури за идентифициране на подобни нарушения и ще уведомим регулатора, и Субекта на данни, ако е необходимо, в предвидените от GDPR случаи.

Ако имате информация за Нарушение на Защитата на Данните или подозирате, че такова е настъпило, не правете опит да го разследвате сами. Веднага се свържете с лицето, определено за целта - DPO. Вие трябва да съхраните всички доказателства за потенциалното нарушение.

11. ОГРАНИЧАВАНЕ НА ПРЕДАВАНЕТО

GDPR ограничава трансферите на данни до странни извън ЕИП с цел да гарантира пред Субектите, че нивото на защита, гарантирано от GDPR, не е компрометирано.

Ние можем да извършваме трансфер на Лични Данни извън ЕИП, само ако едно от следните условия е налице:

1. Европейската Комисия е издала решение, потвърждаващо, че страната, към която се извършва трансфера осигурява адекватно ниво на защита на правата и свободите на Субектите на данни
2. Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм
3. Субектът на данни е дал своето Изрично Съгласие за трансфера, след като е информиран за възможните рискове, или
4. Трансферът е необходим за една от целите, изброени в GDPR, включително изпълнението на договор със Субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на Субекта на данни в случаите, когато той е физически или

юридически неспособен да даде съгласие, и в някои ограничени случаи – за защита на легитимните ни интереси.

12. ПРАВА НА СУБЕКТИТЕ НА ДАННИ И ИСКАНИЯ ЗА ДОСТЪП ДО ДАННИТЕ

Субектите на данни имат права що се отнася до това как управляме техните Лични Данни, включително право да:

1. Оттеглят Съгласието си за Обработване по всяко време
2. Получат определена информациа за дейностите по Обработване на Администратора
3. Изискат достът до Личните им Данни, които Обработваме
4. Възразят срещу наша употреба на Личните им Данни за целите на директния маркетинг
5. Изискат от нас да изтрием Личните им Данни, ако същите не са вече необходими за целите, за които са събрани или да поправим неточни данни, или да допълним непълни данни
6. Ограничим Обработването в определени ситуации
7. Оспорят Обработване, което е извършено на база защита на нашите легитимни интереси или обществения интерес
8. Изискат копие на договора, въз основа на който Личните им Данни са трансферирани до държава извън ЕИП
9. Възразят срещу решение, взето изцяло на база на Автоматизирано Обработване, включително профилиране
10. Бъдат уведомени за Нарушение на Защита на Данните, което е вероятно да доведе до висок риск за техните права и свободи
11. Подадат жалба до регулаторния орган
12. В някои случаи, да получат или да поискат техните Лични Данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене

Ние трябва да удостоверим самоличността на лицето, което изисква да упражни някое от правата по-горе (не позволяваме на трети лица да ни убедят да предоставим Лични Данни без предварителна оторизация).

Ние трябва незабавно да препратим всяко искане за достъп до Лични Данни, което получим до нашия DPO.

13. ОТЧЕТНОСТ

13.1. Администраторът следва да въведе необходимите технически и организационни мерки по ефективен начин, за да осигури спазване на принципите на защита на данните. Администраторът е отговорен за спазването на тези принципи и трябва да може да докаже тяхното спазване.

Институцията трябва да има необходимите ресурси и контролни механизми, за да осигури спазването на изискванията на GDPR, включително:

- Определяне на DPO с подходяща квалификация и поемане на ръководна отговорност за сигурността на данните
- Въвеждане на защита на данните на етапа на проектиране, когато Обработва Лични Данни и извършва Оценка на Въздействието, когато Обработването представлява висок риск за правата и свободите на Субектите на Данни.
- Интегриране на защита на данните във вътрешната си документация.
- Осигуряване на регулярно обучение на Персонала по въпросите на защита на данните, като например: права на Субектите на Данни, Съгласие, законова база, Оценка на Въздействието и Нарушение на Защитата на Данни. Организацията следва да води регистър за посещаемостта на тези обучения от страна на Персонала.
- Регулярно тестване на мерките за осигуряване на защита и периодичен одит с цел оценка на ефективността и нивото на спазване.

13.2. РЕГИСТРИ

GDPR изисква от нас да водим пълна и точна документална отчетност на дейностите ни по Обработване.

Ние трябва да поддържаме точни и актуални регистри, отразяващи нашето Обработване, включително регистър на получените Съгласия и процедури по получаване на Съгласията.

Като минимум, тези регистри трябва да включват името и контактната информация на Администратора и DPO (ако е определен такъв), ясно описание на вида Лични Данни, Субекти на Данни, операции по Обработване, цели на Обработване, трети лица, получатели на Лични Данни, местосъхранение на Лични Данни, трансфери на Лични Данни, срок на съхранение на Лични Данни и описание на мерките за защита.

13.3. ОБУЧЕНИЕ И ОДИТ

Ние сме длъжни да осигурим адекватно обучение на нашия Персонал, което да им помогне да спазят изискванията на GDPR. Също така трябва регулярно да тестваме системите и процесите си.

Ние трябва да участваме във всички задължителни обучения по защита на данните и да преглеждаме регулярно системите и процесите, които са във наш контрол.

13.4. ЗАЩИТА НА ДАННИТЕ НА ЕТАПА НА ПРОЕКТИРАНЕ И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Ние имаме задължение да въведем мерки за Защита на Данните на Етапа на Проектиране, когато Обработваме Лични Данни, чрез въвеждане на подходящи технически и организационни мерки.

Ние трябва да преценим какво ниво на Защита на Данните на Етапа на Проектиране е подходящо за всички програми/системи/процеси, които управляваме, като имаме предвид следното:

1. Използваната технология
2. Разходите по внедряване
3. Вида, обхвата, контекста и целите на Обработването, и
4. Рисковете (от различна степен на вероятност и сериозност) за правата и свободите на Субектите, които произлизат от Обработването

Администраторът също трябва да извърши Оценка на Въздействието за високорискови дейности по Обработване.

Ние следва да извършим Оценка на Въздействието при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с Обработване на Лични Данни, включително:

1. Първоначалното въвеждане на нови технологии или прехода към нови технологии
2. Автоматизирано Обработване, включително профилиране или Автоматизиране Вземане на Решения
3. Обработване на Чувствителни Лични Данни в голям мащаб
4. Мащабно, систематично наблюдение на публично обществена зона

Оценката на Въздействието следва да съдържа:

1. Описание на Обработването, неговите цели и легитимните цели на Администратора, ако е необходимо;
2. Оценка на необходимостта и пропорционалността на Обработването спрямо неговата цел
3. Оценка на риска за лицата и мерките за управление на риска, които са взети

13.5. АВТОМАТИЗИРАНО ОБРАБОТВАНЕ (ВКЛЮЧИТЕЛНО ПРОФИЛИРАНЕ) И АВТОМАТИЗИРАНО ВЗЕМАНЕ НА РЕШЕНИЯ

Общо казано, Автоматизирано Вземане на Решения е забранено, когато решението има правни последици за Субекта на данни, освен ако:

1. Субектът на данни не е дал Изрично Съгласие
2. Обработването е позволено по закон, или
3. Обработването е необходимо за изпълнение или сключване на договор.

Ако определени видове Чувствителни Лични Данни се обработват, то тогава основания 2) и 3) не са приложими, но тези Чувствителни Лични Данни могат да бъдат Обработвани, когато това е необходимо (освен, ако могат да бъдат използвани други мерки, които навлизат в по-малка степен в личното пространство на лицето) за целите на съществен обществен интерес – като например превенция на измами.

Ако дадено решение е основано изцяло на база на Автоматизирано Обработване (включително профилиране), тогава Субектите на Данните трябва да бъдат уведомени за правото да възразят срещу това Обработване при първата комуникация с тях. Вниманието на Субектите трябва да бъде изрично насочено към това тяхно право.

Също така, ние трябва да информираме Субекта относно логиката, използвана при вземането на автоматизирани решения или профилиране, значимостта и вероятните последици и да дадем на Субектите правото да изискат човешка интервенция, изразят тяхната позиция или да оспорят решението.

Оценка на Въздействието следва да се извърши, винаги когато се предприема Автоматизирано Обработване (включително профилиране) или Автоматизирано Вземане на Решения.

13.6. СПОДЕЛЯНЕ НА ЛИЧНИ ДАННИ

Общо казано, на нашата Организация не е позволено да споделяме Лични Данни с трети лица, освен ако не са налице подходящи защити и договорни взаимоотношения.

Служител на Администратора може да споделя Лични Данни, които ние Обработваме, с друг служител в инсттитуцията, ако изпълняването на професионалните задължения на получателя изисква достъп до данните.

Служител на Администратора може да споделя Лични Данни, които контролираме, с трети лица, ако следните условия са изпълнени:

1. Те следва да знаят тази информация с цел да изпълнят услуга по договор
2. Споделянето на Лични Данни е в съответствие с Изявление по Защита на Данните, което е предоставено на Субекта, и, ако е необходимо, Съгласието на Субекта е предоставено
3. Третата страна се е съгласила да спази необходимите стандарти за сигурност на данните, политика и процедури
4. Трансферът е в съответствие с приложимите ограничения за трансфер до страни извън ЕИП, и
5. Е на лице, надлежно сключен, договор за Обработване с третотолице, който отговаря на изискванията на GDPR.

14. ПРОМЕНИ НА ТЕЗИ ВЪТРЕШНИ ПРАВИЛА

Ние си запазваме правото да променяме тези Вътрешни Правила по всяко време и без предупреждение.

Тези Вътрешни Правила не вземат превес над никое приложимо законодателство.
Настоящите правила са приети със заповед № РД-09-1363/15.05.2018 г. на директора на СУ „Св. Климент Охридски“, гр. Аксаково и влизат в сила от 25.05.2018 г.

15. ПОТВЪРЖДЕНИЕ НА ПОЛУЧАВАНЕ И ПРЕГЛЕД

Аз, [ИМЕ НА СЛУЖИТЕЛ], потвърждавам, че на [ДАТА] получих и прочетох копие от Вътрешните Правила по Защита на Данните на [ИМЕ НА ОРГАНИЗАЦИЯТА], от дата [ДАТА НА ТЕКУЩАТА ВЕРСИЯ] и разбирам, че съм отговорен за спазването на тези правила. Тези Вътрешни Правила не променят и не са част от условията по трудовия ми договор.

Подпис .....

Име .....

Дата .....