СРЕДНО УЧИЛИЩЕ „СВЕТИ КЛИМЕНТ ОХРИДСКИ”
6362 С. СТАМБОЛОВО, ОБЩ. СТАМБОЛОВО, ОБЛ. ХАСКОВО
тел.0879406488 e-mail: kl.ohridski.stambolovo@abv.bg

УТВЪРДИЛ:.....
ДИРЕКТОР: АТАНАСКА ХРИСТОЗОВА

ВЪТРЕШНИ ПРАВИЛА

ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ

НА

СРЕДНО УЧИЛИЩЕ

„СВ. КЛИМЕНТ ОХРИДСКИ”

като администратор на лични данни (АЛД)

СТАМБОЛОВО 2022 г.

СРЕДНО УЧИЛИЩЕ „СВЕТИ КЛИМЕНТ ОХРИДСКИ”
6362 С. СТАМБОЛОВО, ОБЩ. СТАМБОЛОВО, ОБЛ. ХАСКОВО
тел.0879406488 e-mail: kl.ohridski.stambolovo@abv.bg

СЪДЪРЖАНИЕ

СРЕДНО УЧИЛИЩЕ „СВЕТИ КЛИМЕНТ ОХРИДСКИ”
6362 С. СТАМБОЛОВО, ОБЩ. СТАМБОЛОВО, ОБЛ. ХАСКОВО
тел.0879406488 e-mail: kl.ohridski.stambolovo@abv.bg

ВЪВЕДЕНИЕ

Ръководството на СУ „Св. Климент Охридски“ разбира, оценява и подкрепя всички усилияи мерки, насочени към осигуряване сигурността на личните данни и ***защитата на правата, свободите и интересите*** *на физическите лица, чиито данни обработваме.*

СУ „Св. Климент Охридски“ приема, че опазването на конфиденциалността и целостта на обработваните от нас лични данни е ключова ***отговорност****, към която ние се отнасяме сериозно и ангажирано. Споделяме разбирането, че правилното и законосъобразно управление на лични данни осигурява желаното* ***доверие*** *в СУ „Св. Климент Охридски“ от страна на служители, деца, ученици, родители и общественост, поради което,*

със съставянето и утвърждаването на настоящите Правила, ръководството на

СУ „Св. Климент Охридски“

ДЕКЛАРИРА, че

- *се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на правата и свободите на физическите лица, чиито лични данни събира и обработва;*
- *ще прилага стриктно и в пълнота всички принципи за защита на личните данни, регламентирани в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България*
- *ще прилага настоящите Правила и изразените чрез тях политики при осъществяване на всички процеси по обработването на лични данни , включително тези, които се извършват относно лични данни на служители, ученици, родители, партньори и всякакви други лични данни, които събира от различни източници и обработва;*
- *ще положи всички необходими действия и усилия да запознае с настоящите Правила всички служители, родители, както и трети лица, които имат или биха могли да имат достъп до обработваните от институцията лични данни, като регламентира по надлежен начин изискването да се съобразят с прилагането на регламентираното в настоящия документ;*
- *ще разглежда всяко нарушение на ОРЗД като тежко нарушение на трудовата дисциплина, а в случай на наличие на данни или предположение за извършено престъпление, въпросът ще се отнася за разглеждане към съответните компетентни държавни органи;*
- *ще преразглежда Правилата най-малко веднъж годишно в светлината на всякакви промени в дейността си като администратор, както и всички допълнително възникнали изисквания, вкл. в следствие на нови оценки на въздействието върху защитата на данните.*

ДЕФИНИЦИИ

използвани съкращения и изрази

За целите на настоящите Правила, използваните съкращения и изрази имат следното значение:

• ***ОРЗД*** *(Общ регламент за защита на данните)* или ***„Регламент(а)”*** - Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);

• ***ЗЗЛД*** – Закон за защита на личните данни;

• ***КЗЛД*** – Комисия за защита на личните данни;

• ***„Лични данни"*** - 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;

• ***„Специални категории лични данни“*** – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация;

• ***„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;

• ***„Администратор"*** - всяко 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 ЕС 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;

• ***„Обработващ”*** лични данни – физическо или юридическо лице, публичен орган, агенция или друга организация, която обработва лични данни, предоставени от администратор на данни, от името на администратора, за постигане на възложените от администратора цели;

• ***„Субект на данни”*** – физическо лице, чиито лични данни са обект на обработване и което е идентифицирано или може да бъде идентифицирано чрез обработваните лични данни;

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

• ***„Длъжностно лице по защита на данните”*** или ***ДЛЗД*** – физическо лице, юридическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД;

• ***„Лице с достъп до лични данни“*** - всяко лице, действащо под ръководството на администратора или на обработващия, което има достъп до обработваните лични данни. Лицето може обработва данните само по указание на администратора/обработващия, освен ако в закон е предвидено друго;

• ***„Регистър с лични данни“*** - всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

• ***„Носител на лични данни“*** - физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

• ***„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, така и конкретно отнесени към обработването на лични данни със специфична цел.

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

• ***„Получател"*** - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, 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;

• ***„Основно място на установяване “*** – седалището на администратора в ЕС ще бъде мястото,

в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център. Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи.

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

• ***„Профилиране"*** - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

• ***„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.

• ***„Псевдонимизиране”*** – заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече 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.

• ***„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.

Глава ПЪРВА
ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) ***СУ „Св. Климент Охридски“***, наричано по-долу „Училището”, „Институцията“ или „Администратор(а)“ (АЛД), е самостоятелно юридическо лице - институция в системата на предучилищното и училищното образование, в която се обучават, възпитават и социализират деца и ученици.

(2) ***СУ „Св. Климент Охридски“***е с Единен идентификационен код /ЕИК/: **000893181** и със седалище в с. Стамболово и адрес на управление: Република България, област Хасково, Община Хасково, село Стамболово.

(3) ***СУ „Св. Климент Охридски“*** обработва лични данни във връзка със своята дейност и самостоятелно определя целите и средствата за обработването им. В този случай институцията действа като администратор на лични данни по смисъла на ОРЗД.

(4) В определени случаи, ***СУ „Св. Климент Охридски“*** може да обработва лични данни за цели, определени самостоятелно от трето лице или за цели, който са определени съвместно от ***СУ „Св. Климент Охридски“*** и трето лице. В тези хипотези, ***СУ „Св. Климент Охридски“*** би имала положението и статута или на обработващ лични данни (*ако целите са определени от лицето, което е възложило обработването*) или на съвместен администратор/ съадминистратор.

Чл.2. (1) Настоящите Вътрешни правила за обработване и защита на лични данни, наричани по-долу и „Правила(та)” определят реда, по който ***СУ „Св. Климент Охридски“*** обработва лични данни за целите на своята дейност, както и правилата за осигуряване защита на субектите на тези данни, във връзка с тяхното обработване.

(2) „Обработването” на лични данни по ал.1 включва всяка операция или съвкупност от операции извършвана с лични данни или набор от лични данни, в т.ч. събиране, записване, организиране, структуриране, съхраняване, адаптиране или променяне, извличане, консултиране, използване, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване, унищожаване или обработване по друг начин на лични данни.

(3) „Обработването” на лични данни по ал.2 се състои и в осигуряване на достъп до определена информация на лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл.3. Вътрешните правила на ***СУ „Св. Климент Охридски“*** за обработване и защита на лични данни са изготвени на основание, в съответствие и в изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (*в частност на основание чл.24, пар.1 от Регламента*), както и приложимото законодателство на Република България.

Чл.4. (1) Целта на настоящия документ е установяването на ясни правила при събиране,

организиране, съхраняване и предоставяне на лични данни, обработвани от ***СУ „Св. Климент Охридски“***, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентират техните права и процедурите за упражняването им.

(2) Тези Правила уреждат:

1. Принципите, процедурите и механизмите за обработка на личните данни;

2. Основанията за обработване на личните данни;

3. Правата на субектите на лични данни;

4. Процедурите за администриране на искания от субектите на данни за упражняване на техните права;

5. Лицата, които обработват лични данни, и техните задължения;

6. Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;

7. Процедурите и правилата, свързани с документиране и отчетност на обработването на лични данни;

8. Правилата за предаване на лични данни на трети лица в България и чужбина;

9. Процедурите по съхраняване и унищожаване, изтриване или заличаване на лични данни;

10. Процедурите за действия в случай на нарушения в сигурността;

(3) Настоящите Вътрешни правила имат и функцията на Политика по защита на данните, като указват начина, по който ***СУ „Св. Климент Охридски“*** управлява законосъобразно и с изискуемата грижа личните данни на работници и служители, ученици, родители, членове на Обществения съвет и други лица.

Чл.5. (1) Тези Правила се прилагат спрямо всички лични данни, които обработваме, без значение от това какъв е техния източник и на какъв носител са съхранени.

(2) Правилата следва да се прилагат от и спрямо всички служители на институцията. Всички работници и служители следва да прочетат, да се запознаят с и да спазват съдържащите се в правилата политики при обработване на лични данни от името на институцията. Всяко нарушение на тези вътрешни правила е основание за налагане на дисциплинарни санкции спрямо работника или служителя, който го е допуснал.

Глава ВТОРА

ПРИНЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Раздел I

Основни принципи при обработване на лични данни

Чл.6. (1) Като администратор на лични данни, ***СУ „Св. Климент Охридски“***, в процеса на обработване спазва принципите за законосъобразно обработване и защита на личните данни.

(2) Цялостният процес по обработване и защита на личните данни е подчинен и се извършва в съответствие с принципите за защита на данните, регламентирани в член 5 от Общия регламент относно защитата на данните (ЕС) 2016/679, законодателството на Европейския съюз и на Република България.

(3) Настоящите Правила, както и всички Политики и Процедури за защита на личните данни, разработени и внедрени от ***СУ „Св. Климент Охридски“*** имат за цел да гарантират спазването на тези принципи.

(4) **Принципите** за защита на личните данни, на които ***СУ „Св. Климент Охридски“*** подчинява дейността по обработване на данните, са:

1. Законосъобразност, добросъвестност и прозрачност;
2. Ограничение на целите;
3. Свеждане на данните до минимум;
4. Точност;
5. Ограничение на съхранението;
6. Цялостност и поверителност;
7. Отчетност.

Раздел II

Законосъобразност, добросъвестност и прозрачност

Чл.7. ***СУ „Св. Климент Охридски“*** обработва лични данни само при наличие на законно основание, при полагане на дължимата грижа и при надлежно информиране на субекта на данни.

Чл.8. (1) С цел осигуряване на **законосъобразност**, преди обработването на лични данни задължително се идентифицира законно основание за обработване на данните.

(2) **Законосъобразно** е обработването на лични данни, което се основава на наличието на поне едно от следните условия:

1. обработването е **в изпълнение на законово задължение**, което е предвидено в нормативен акт и се прилага спрямо ***СУ „Св. Климент Охридски“***;
2. обработването е необходимо **за изпълнението на договор**, по който субекта на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
3. обработването е необходимо, за да се защитят **жизненоважни интереси на**

субекта на данните или на друго физическо лице;

4. обработването е необходимо за изпълнение на задача от **обществен интерес**;
5. обработването е необходимо за целите на **легитимните интереси** на ***СУ „Св. Климент Охридски“*** или на трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. В тези случаи целите на обработването се изписват изчерпателно в известието до субекта на данни.
6. обработването се извършва въз основа на изричното **съгласие** на субекта на данни.

(3) За да е законосъобразно, обработването на лични данни следва да е в съответствие и с цялото законодателство на ЕС и на Република България, а не само на законодателството, регламентиращо защитата на личните данни.

Чл.9. (1) ***СУ „Св. Климент Охридски“*** няма да изисква съгласие от физически лица, чиито данни обработва, в случаите, когато за законосъобразното обработване на данните е налице друго годно основание.

(2) В случаите, когато изисква съгласие, институцията ще приема предоставянето му като годно основание за законосъобразно обработване на лични данни, когато са налице следните предпоставки:

1. Съгласието е изразено ясно, недвусмислено и конкретно, в разбираема и лесно достъпна форма, на ясен и прост език;
2. Съгласието е дадено чрез изявление или ясно утвърдителен акт (потвърждаващо действие), с който да се даде съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път;
3. Съгласието да е дадено информирано. За да бъде съгласието информирано, ***СУ „Св. Климент Охридски“*** за всеки конкретен случай ще предоставя на субекта на данни най-малко следната информация:

- данни за администратора;
- целта на всяка форма на обработване на данни;
- вида лични данни, които ще се събират и обработват;
- наличието на възможност за оттегляне на съгласието;
- дали данните ще се обработват за вземане на решение на база автоматично обработване / профилиране;
- дали данните ще се предават на трети лица и информация за свързаните с това рискове, ако не е налице решение за адекватно ниво на защита;
- какви са последиците при отказ да даване на съгласие.

4. Съгласието е дадено при наличие на действителен свободен избор на субекта да даде съгласието си, да откаже даването на съгласие или да оттегли вече даденото съгласие. Мълчаливото съгласие, предварително отметнатите полета във формуляр или декларация, и други, правят съгласието невалидно.
5. Даденото съгласие се отнася за всички операции по обработване на данните.

(3) ***СУ „Св. Климент Охридски“*** разбира и приема като "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да се приема като валидно основание

за обработване на лични данни.

(4) Образователната институция осигурява възможност за лесно оттегляне на даденото съгласие по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие преди оттеглянето му.

(4) ***СУ „Св. Климент Охридски“*** няма да изисква даване на съгласие за обработване на лични данни като условие за предоставяне на услуга или изпълнение на договор, когато данните, за обработване на които се иска съгласие, не са необходими за изпълнението на договора или предоставянето на услугата.

(5) Когато е необходимо като основание за обработване, в повечето случаи съгласието за обработка на лични и специални категории лични данни ще се получава рутинно от ***СУ „Св. Климент Охридски“***, като се използват стандартни документи за съгласие.

(6) Ако е необходимо, за нуждите на по-доброто администриране и по-добрата и пълна отчетност, ***СУ „Св. Климент Охридски“*** може да води и съхранява отделен Регистър на съгласията, в който ще отбелязва субекта на данни предоставил съгласието, за кои данни е дал съгласие, на коя дата е дадено съгласието, дата на оттегляне на съгласието, ако такова е постъпило от субекта. Към регистъра ще се съхраняват архиви с дадените съгласия.

Чл.10. (1) ***СУ „Св. Климент Охридски“*** обработва личните данни при съблюдаване на **принципа за добросъвестност**.

(2) Обработването е **добросъвестно**, когато не засяга неоправдано по неблагоприятен начин правата и свободите на физическите лица, субекти на данни, както и когато при обработването не се накърняват морала и добрите нрави.

(3) Когато лични данни са предоставени на ***СУ „Св. Климент Охридски“*** от субекта на данни, без правно основание или в противоречие с принципите по чл. 5 от Регламента, институцията ги връща незабавно или ги изтрива, или унищожава в срок от един месец от узнаването.

Чл.11. (1) ***СУ „Св. Климент Охридски“*** обработва лични данни при спазване на **принципа за прозрачност**, като предоставя детайлна и конкретна информация на субектите на данни.

(2) Прилагането на принципа за прозрачност се гарантира от регламентираните в настоящите правила процедури за реализиране от субектите на данни на предоставените им **право на информация** и **право на достъп**.

(3) Информацията по ал.1 се предоставя чрез подходящи Информационни съобщения (*Известия за поверителност*) или Декларация за поверителност (*Уведомление за поверително третиране на личните данни*), по ред и начин, регламентирани в настоящите Правила.

Раздел III
Ограничение на целите

Чл.12. (1) ***СУ „Св. Климент Охридски“*** събира лични данни на физически лица за конкретни, точно и ясно определени цели, и не може да ги обработва допълнително по начин, несъвместим с тези цели.

(2) По-нататъшно обработване на личните данни за целите на архивирането в

обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

Чл.13. (1) Целите, за които ***СУ „Св. Климент Охридски“*** на обработва лични данни са:

1. управление на човешките ресурси, в т.ч. набиране и подбор на персонал, сключване, изпълнение и прекратяване на трудови и граждански договори с физически лица, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на ***СУ „Св. Климент Охридски“*** за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на институцията в качеството ѝ на работодател по трудови договори или възложител по граждански договори;

2. изпълнение на основната си дейност като образователна институция – осъществяване на образователния процес и свързани с това други задължения;

(2) ***СУ „Св. Климент Охридски“*** не използва наличните лични данни за нови цели, различни и несъвместими с първоначалните цели, освен ако субекта на данни не предостави последващо съгласие за това.

(3) Ако конкретната(ите) цел или цели, за които се обработват лични данни от ***СУ „Св. Климент Охридски“,*** не изискват или вече не изискват идентифициране на субекта на

данните, институцията не е задължена да поддържа, да се сдобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на ОРЗД.

Раздел IV
Свеждане на данните до минимум

Чл.14. (1) Личните данни, които се събират и обработват следва да са подходящи, адекватни, релевантни, **свързани с и ограничени до необходимото** във връзка с целите на обработването.

(2) ***СУ „Св. Климент Охридски“*** не събира информация от физическите лица – субекти на данни, която не е строго необходима за целта, за която тя е получена и се обработва.

(3) Към датата на утвърждаване на настоящите Правила, ***СУ „Св. Климент Охридски“*** инвентаризира и актуализира всички използвани бланки, формуляри и други документи, в които се попълват лични данни, по начин, осигуряващ събирането и обработването само на минимално необходимата за целите на обработването информация.

(4) Длъжностното лице по защита на данните (ДЛЗД) се задължава да одитира ежегодно всички способи за събиране на данни, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни с оглед на целите, за постигане на които се събират и обработват.

(5) ***СУ „Св. Климент Охридски“*** осигурява навременното връщане или изтриване/унищожаване на всички лични данни, които вече не са необходими за конкретните цели.

Раздел V
Точност

Чл.15. (1) ***СУ „Св. Климент Охридски“*** поддържа събраните лични данни точни, пълни и

в актуален вид, във всеки един момент.

(2) Точността, пълнотата и актуалността на данните се проверява в момента на тяхното събиране, както и на регулярни интервали след това, но не по-малко веднъж годишно.

(3) ***СУ „Св. Климент Охридски“*** предприема всички разумни мерки за унищожаването или корекцията на всички неточни или неактуални лични данни.

Чл.16. (1) За осигуряване и гарантиране точността и актуалността на данните, които ***СУ „Св. Климент Охридски“*** обработва като администратор, ще се прилагат следните мерки:

1. не се допуска съхраняване на данни, в случаите, когато има вероятност да не са точни.
2. лицата, които са натоварени с функции по събиране и обработване на лични данни са обучени в значението на събирането на точни данни и поддържането им в актуализиран вид.
3. въвежда се задължение на субекта на данни да декларира, че данните, които предава на ***СУ „Св. Климент Охридски“*** са точни и актуални. При изготвянето на формуляри и бланки, се включва изявление на субекта, че съдържащите се в документа данни са точни, верни и актуални към датата на подаване.
4. въвежда се изискване към всички субекти на данни да уведомяват ***СУ „Св. Климент Охридски“*** за всякакви промени в обстоятелствата, които изискват актуализиране на записите на лични данни.
5. прилагат се подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени този обем и други относими фактори.
6. прилага се извършване на корекция на данни въз основа на искане за реализиране на правото на корекция;
7. надлежно и своевременно се информира всяка трета страна предоставила неточни или остарели лични данни, че информацията е неточна или остаряла, поради което не следва да се обработва и да се използва за вземане на решения относно лицата;
8. надлежно и своевременно се информират съответните получатели на лични данни, когато това е приложимо, и се препраща всяка корекция на лични данни, когато това е приложимо и необходимо.

Раздел VI
Ограничение на съхранението

Чл.17. (1) ***СУ „Св. Климент Охридски“*** обработва лични данни само за период с конкретно определена продължителност съгласно целите, за които данните се обработват.

(2) Образователната институция **не** съхранява данните във формат, който да позволява идентифициране на субекта на данни за по-дълго време от необходимото за целите, за които данните са събрани.

(3) Съхраняване за по-дълги срокове е допустимо единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки.

Чл.18. (1) С настоящите правила, ***СУ „Св. Климент Охридски“*** въвежда правила и

политики относно съхранението на лични данни, които да осигурят и гарантират изтриване/унищожаване на данните, за които вече не съществува легитимна цел за обработване, освен в закон не е предвидено задължение за запазване и съхраняване на данните за определен минимален срок.

(2) Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин, позволяващ да се защити самоличността на субекта на данните в случай на нарушение на данните.

Раздел VII
Цялостност и поверителност

Чл.19. (1) ***СУ „Св. Климент Охридски“*** обработва личните данни по начин, който гарантира подходящо ниво на сигурност, като се прилагат съответните технически и организационни мерки за това.

(2) Изискването за **цялостност** се постига чрез такова обработване и съхраняване на данните, че същите да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване, както и да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

(3) Изискването за **поверителност** (*конфиденциалност*) се постига чрез предприемане на мерки за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

(4) Изискването за **наличност** се постига чрез осигуряване на непрекъсната възможност за обработване на личните данни от оторизираните за това лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

Чл.20. Образователната институция ще следва всички процедури и технологични мерки, които се въвеждат с настоящите Вътрешни правила или други нарочни процедури или инструкции, с цел опазване сигурността на личните данни от момента на тяхното събиране до момента на тяхното унищожаване.

Раздел VIII
Отчетност

Чл.21. (1) Принципът за отчетност цели да гарантира, че обработването на личните данни се осъществява по осъзнат, прозрачен, надлежно документиран и следователно, лесно проследим и доказуем начин.

(2) С настоящите правила, ***СУ „Св. Климент Охридски“*** обезпечава прилагането на разпоредбите на ОРЗД, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност при обработването на лични данни.

(3) Институцията е отговорна за спазването на принципите за защита на личните данни и ги прилага по начин, който осигурява по всяко време възможност за доказване на тяхното спазване.

Чл.22. (1) ***СУ „Св. Климент Охридски“*** осигурява доказване спазването на принципите,

чрез изпълнение на конкретни действия и задължения, в т.ч.:

1. създаване, утвърждаване и прилагане на настоящите вътрешни правила;

2. прилагане на утвърдените и въведени с настоящите правила политики и процедури, както и чрез реализиране на съответните контролни механизми;

3. водене на предвидения в чл.30 от ОРЗД вътрешен регистър относно действията по обработване на лични данни;

4. регламентиране на отношенията свързани с обработването на лични данни с писмен акт и извършване на обработването само съобразно вписаното в договор/споразумение или съобразно документираните нареждания на администратора;

(2) Възможността за доказване спазването на принципите за защита на данните се обезпечава и чрез инвентаризация на цялата вътрешна документация и интегриране в нея на конкретни процедури и политики от настоящите правила, както и чрез инвентаризация и актуализиране на всички договори с външни за институцията партньори, доставчици и други трети лица.

(3) Възможността за доказване спазването на принципите се реализира и чрез преглед и актуализация на правното основание за предаване (*трансфер*) на данни към външни получатели, когато и ако това е приложимо.

Глава ТРЕТА
КАТЕГОРИИ ЛИЧНИ ДАННИ И КАТЕГОРИИ СУБЕКТИ НА ДАННИ

Раздел I
Категории субекти на данни

Чл.23. (1) ***СУ „Св. Климент Охридски“*** събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател и образователна институция, при съблюдаване изискванията на приложимото законодателство.

(2) Личните данни, обработвани от институцията като администратор на данни се отнасят до следните категории субекти на данни:

1. кандидати за работа;

2. работници / служители и изпълнители по граждански договори;

3. деца, ученици и родители;

4. други категории субекти, когато възникнат предпоставки за обработване на техни лични данни.

Раздел II
Категории лични данни

Чл.24. (1) Относно **лицата, кандидатстващи за работа в институцията** се събират следните лични данни:

1. Идентификация:

- трите имена;
- адрес за кореспонденция;

- телефон;
- електронен адрес;

2. Данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

3. В случаите, когато това е свързано с изискване за заемане на съответната длъжност, институцията изисква предоставянето на данни за здравословно състояние, медицински свидетелства, ТЕЛК решения, документи, удостоверяващи психическата пригодност.

4. Други данни, когато това е необходимо във връзка с длъжността, за която лицето кандидатства, напр. свидетелство за съдимост, данни от свидетелство за управление на МПС.

(2) Първоначалното събиране на лични данни от кандидатите за работа се извършва въз основа на депозирана от субекта на данни автобиография. При обработване на лични данни от автобиографии, ***СУ „Св. Климент Охридски“*** прилага следните правила:

1. Автобиографиите се представят от кандидатите за работа по един от следните начини:

- на хартиен носител - лично в деловодството на институцията или чрез пощенска пратка на адреса на институцията
- в електронен формат - чрез имейл на електронния адрес на институцията;

2. Данните от автобиографиите се обработват единствено във връзка с кандидатстването на физическото лице за работа в институцията и за оценка и подбор на кандидата;

3. Представените автобиографии и данните съдържащи се в тях не могат да се предоставят на трети лица;

4. Данните от автобиографиите се съхраняват до приключване на подбора за вакантното работно място, след което се унищожават по съответния ред;

(3) Образователната институция **не съхранява** данните на кандидатите за работа след приключване на процедурата по подбор.

(4) Когато в процедура по подбор, институцията е изискала да се представят оригинали или нотариално заверени копия на документи, удостоверяващи физическа и психическа годност на кандидата, образованието, необходимата квалификационна степен и стаж за заеманата длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от окончателното приключване на процедурата по подбор да получи обратно представените документи. Институцията връща документите, по начина, по който са подадени.

Чл.25. (1) Относно **лицата, заети по трудови или граждански правоотношения в институцията** се събират следните лични данни:

1. Идентификация:

- трите имена;
- ЕГН/ЛНЧ;
- постоянен и настоящ адрес;
- телефонен номер;
- данни по лична карта или паспортни данни;

2. Образование и професионална квалификация: данни, свързани с образование,

професионален опит, професионална и лична квалификация и умения, включително данни от свидетелство за управление на МПС;

3. Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

4. Данни за банкови сметки, които се обработват във връзка с изплащане на възнаграждения и обезщетения, в изпълнение на сключения трудов договор и нормативни разпоредби на трудовото и осигурителното законодателство;

5. Други данни: институцията изисква свидетелство за съдимост, само в случай, че за заемането на определена длъжност, в нормативен акт е предвидено изискване, свързано с липсата на осъдителни присъди или когато изрично се изисква представянето му съгласно нормативен акт.

(2) Лицето, натоварено с функции по обработване на личните данни на работниците / служителите може да копира документ за самоличност, свидетелство за управление на моторно превозно средство, документ за пребиваване на работник или служител, само ако това е изискване, предвидено в нормативен акт.

(3) Образователната институция обработва чувствителни данни (*напр. данни за здравословното състояние или данни за съдебното минало*) на работниците и служителите, само доколкото това е необходимо за изпълнение на специфичните й права и задължения на работодател в областта на трудовото и осигурително законодателство.

Чл.26. (1) Относно **деца, ученици и родители** се събират лични данни, които са необходими за изпълнението на основната дейност и свързаните с това законови задължения на образователната институция, както следва:

1. Трите имена;
2. Единен граждански номер;
3. Гражданство;
4. Месторождение;
5. Данни от лична карта (на ученици над 14 години);
6. Адрес;
7. Електронен адрес (имейл);
8. Телефонен номер;
9. Данни за образованието на ученика;
10. Пол;
11. Данни за родители – имена, телефонен номер, адрес, месторабота и други;
12. Информация за присъствия и отсъствия;
13. Данни за успеха и оценяването на ученика;
14. Информация за полагане на изпити (НВО, ДЗИ, олимпиади, състезания, конкурси и други);
15. Информация за издаване на дипломи, удостоверения, свидетелства, ученически книжки и ученически лични карти;
16. Информация за здравно осигуряване (за ученици на възраст над 18 г.);
17. Информация, необходима за предоставяне на стипендии;
18. Информация във връзка със социално подпомагане;

(2) ***СУ „Св. Климент Охридски“*** обработва и следните специални категории по-чувствителни данни за учениците:

1. Информация за здравословното състояние на учениците – вкл. здравно-профилактични карти, заболявания, наличие на трайни увреждания, имунизации, данни за

личен лекар и т.н.;

2. Информация за специални образователни потребности (когато е приложимо);

3. Фото и видео-материали, вкл. снимки на учениците за техни досиета или документи.

Глава ЧЕТВЪРТА

ПРАВА НА СУБЕКТИТЕ НА ДАННИ. ПРОЦЕДУРИ ПО РЕАЛИЗИРАНЕ НА ПРАВАТА И АДМИНИСТРИРАНЕ ИСКАНИЯТА НА СУБЕКТИТЕ.

Раздел I

Видове права на субектите на данни

Чл.27. Субектите на данни имат следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

- **право на информация**;
- **право на достъп**;
- **право на коригиране** или допълване на неточни или непълни лични данни;
- **право на изтриване** („право да бъдеш забравен“);
- **право на ограничаване** на обработването;
- **право на преносимост** на данните;
- **право на възражение**;
- **право да не бъде обект на изцяло автоматизирано решение**, включващо профилиране;
- **право на жалба**;
- **право на административна и съдебна защита**;
- **право на обезщетение**.

Раздел II

Процедура за осигуряване на прозрачност.

Чл.28. (1) В изпълнение на задълженията си по ОРЗД, ***СУ „Св. Климент Охридски“***, във всеки случай на събиране и обработване на лични данни, предоставя детайлна и конкретна информация на субектите на данни.

(2) В изпълнение на предходната алинея, ***СУ „Св. Климент Охридски“*** изготвя Известия (уведомления, политики) за поверителност, до които предоставя лесен достъп на субектите на данни при всяка точка за контакт с тях.

(3) Информацията в известията се предоставя на ясен и разбираем език.

(4) За всяка категория субекти на данни ***СУ „Св. Климент Охридски“*** изготвя конкретно Известие за поверителност на данните, до което субектите получават достъп чрез

връчване (*когато е възможно*) или по подходящ начин при съответната точка за контакт с тях.

Чл.29. Чрез Известията за поверителност, ***СУ „Св. Климент Охридски“*** предоставя на субектите на данни най-малко следната информация:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;
- данни за контакт с Длъжностното лице за защита на личните данни (ДЛЗД);
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- категориите лични данни;
- периода, за който ще се съхраняват личните данни;
- указание до субекта на данни за правата му по ОРЗД, вкл. следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- информация за правото на жалба до надзорен орган;
- получателите или категориите получатели на лични данни, където това е приложимо;
- информация за намерението (ако такова намерение съществува) или ангажимента на администратора да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква друга информация, необходима да се гарантира добросъвестно обработване.

Чл.30. При предоставяне на информацията, ***СУ „Св. Климент Охридски“*** спазва следните изисквания на ОРЗД:

- при събирането на лични данни **от субекта на данни**, ***СУ „Св. Климент Охридски“*** предоставя на субекта посочената в настоящите Правила информация **вмомента** на получаване на данните.
- при събирането на лични данни от източник, **различен от** субекта на данните, ***СУ „Св. Климент Охридски“*** предоставя на субекта посочената информация в срок до един месец от получаване на личните данни;
- в случаите, когато данните се използват за комуникация със субекта на данни, институцията съобщава информацията най-късно при осъществяване на първия контакт с него;
- в случаите, когато личните данни се разкриват на друг получател, ***СУ „Св. Климент Охридски“*** съобщава информацията най-късно при разкриването наличните данни за първи път;
- институцията не предоставя на субекта информацията по чл.34 от Правилата, ако той вече разполага с нея, както и в случай, че предоставянето се окаже невъзможно или би довело до прекомерно усилие;
- ***СУ „Св. Климент Охридски“*** няма задължение да предостави тази информация, в случай че получаването или разкриването на лични данни е изрично регламентирано от националното законодателство;
- ***СУ „Св. Климент Охридски“*** няма задължение да предостави тази информация, ако личните данни **трябва да останат поверителни** при спазване на задължение

за професионална тайна, регламентирано от националното законодателство, включително законово задължение за тайна;

- институцията предоставя на субекта на данните всяка допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване;
- цялата информация, се предоставя на субекта на данни на хартиен носител или чрез съответните означения и табели, а в случаите, когато се използва електронен формат, информацията ще се предоставя на субектите във формат, който да е лесен и подходящ за машинно разчитане.

Раздел III

Реализиране на правата и администриране на исканията на субектите на данни. Управление на исканията на субектите.

Чл.31. ***СУ „Св. Климент Охридски“*** осигурява всички необходими условия, които да гарантират упражняването на правата на субектите на данни.

Чл.32. (1) Всяко лице има право да иска **достъп до своите лични данни**, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, както и да се информира за целите на това обработване, за категориите обработвани данни, за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

(2) Ако субектът на данни получи потвърждение, че негови лични данни се обработват от институцията, той може да поиска осигуряване на достъп до данните, както и да отправи следните други искания:

1. да поиска копие от своите лични данни;

2. да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;

3. да иска коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;

4. да изиска изтриване на лични данни (право „да бъдеш забравен");

5. да иска ограничаване на обработването на лични данни, като в този случай данните ще продължат да бъдат само съхранявани, но не и обработвани;

6. да направи възражение срещу обработване на негови лични данни;

7. да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг;

8. да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на ОРЗД е нарушена;

9. да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане;

10. да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;

11. да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

Чл.33. (1) Субектите на данни, които желаят да упражнят някое от правата си, подават писмено искане до директора на ***СУ „Св. Климент Охридски“*** или определеното Длъжностно лице по защита на данните.

(2) Искането се подава лично или чрез лице, упълномощено изрично с пълномощно с нотариална заверка на подписа.

(3) Искането може да се подаде писмено по адреса на институцията или по електронен път на официалния електронен адрес.

Чл.34 (1) Исканията на субектите на данни следва да съдържат:

1. име на субекта на данни и други данни, които го идентифицират;
2. описание на искането;
3. предпочитаната форма за предоставяне на достъп до данните, когато се иска достъп;
4. адрес за кореспонденция;
5. дата;
6. приложено нотариално заверено пълномощно, когато искането не е подадено лично от субекта на данни.

(2) При поискване от страна на субектите, институцията им съдейства административно за подаване на искане, включително чрез предоставяне на примерни образци на исканията.

Чл.35. (1) При получаване на искане от субект на данни за упражняване на някое от неговите права, ДЛЗД прилага следната процедура:

1. завежда всяко подадено искане в Регистър на исканията на субектите на данни;
2. извършва проверка на самоличността на заявителя;
3. извършва проверка на основателността на искането;
4. разглежда искането в срок от 30 дни от датата на получаването му;
5. отговаря на исканията с писмо с обратна разписка или в електронен формат на посочения от субекта електронен адрес, като документира действията си.

(2) Ако искането е получено от директора или друг служител, същият незабавно уведомява ДЛЗД и му препраща искането.

Чл.36. (1) **Правото на достъп** се осъществява чрез искане отправено до институцията по реда, установен в настоящите Правила.

(2) Достъп до данните, по избор на субекта, се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или негов пълномощник с изрично пълномощно;
4. предоставяне на копие от исканата информация на хартиен носител или в електронен формат (*когато това е технически възможно*).

(3) При подаване на искане за осигуряване на достъп, институцията разглежда искането и при липса на основателност отказва достъпа, а при наличие на основателност, се разпорежда да се осигури искания от лицето достъп в предпочитаната от заявителя форма.

(4) Решението се съобщава писмено на заявителя лично срещу подпис, по пощата с обратна разписка или по електронен път.

(5) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган

и срок.

(6) Идентифицирането (търсенето) на личните данни се извършва във всички хранилища на данни и във всички архиви (хартиени и електронни), папки на електронната поща (и техни архиви).

(7) При предаване на копие от информацията, ДЛЗД извършва обработване на данните, с което отстранява всяка евентуална информация идентифицираща трети лица.

Чл.37. (1) При упражняване **правото на преносимост**, субектът на данни има право да получи личните данни, които той е представил на институцията, в структуриран, широко използван и пригоден за машинно четене формат, както и правото да прехвърли тези данни на друг администратор без възпрепятстване от ***СУ „Св. Климент Охридски“***, когато:

1. обработването е основано на съгласието на субекта на данни или на договорно задължение;

2. обработването се извършва по автоматизиран начин.

(2) Когато субектът упражнява правото си на преносимост на данните по ал.1, то той има право да получи пряко прехвърляне на личните данни към посочен от него друг администратор, когато това е технически осъществимо.

(3) ***СУ „Св. Климент Охридски“***, като администратор, гарантира, че е осигурила подходящото ниво на сигурност при предаване на данните и че са предприети подходящи мерки за ограничаване на риска.

(4) Ако действия по предаване на данните не бъдат предприети в срок от един месец от получаване на искането или предаването бъде отказано, ***СУ „Св. Климент Охридски“*** уведомява заявителя, като излага причините, поради които отказва или не предприема действията по предаване. Субекта се уведомява за правото му на жалба пред КЗЛД.

Чл.38. (1) При отправяне на **искане за коригиране, изтриване, ограничаване или при възражение** по отношение на обработваните лични данни, ДЛЗД извършва детайлна преценка за всеки конкретен случай за основателността на правото на субекта и наличието на други законови изисквания за неговото удовлетворяване.

(2) След приключване на проверката от ДЛЗД по предходната алинея, ***СУ „Св. Климент Охридски“***:

1. премахва личните данни от системите и прекратява операциите по обработката им, без ненужно забавяне, ако искането за изтриване е подадено от субекта на данните;

2. съобщава за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били разкрити;

3. информира субекта на данните относно тези получатели, ако субектът на данните поиска това, и документира това съобщение;

4. взема подходящи мерки, без ненужно забавяне, в случай че:

- субектът на данни е подал искане, с което възразява срещу обработването на личните данни изцяло или частично;
- отпаднало е основанието за обработка по законово задължение;
- данните са били незаконно обработвани.

Чл.39. (1) Субектът на данни има **право да поиска коригиране** на личните си данни като

отправи искане за това.

(2) В искането си субектът е длъжен да посочи конкретните данни, които иска да бъдат коригирани.

(3) ***СУ „Св. Климент Охридски“*** има задължение да коригира данните в срок от 30дни, като този срок може, при необходимост, да бъде удължен с до два месеца.

(4) Ако действия по коригиране на данните не бъдат предприети в срок от един месец от получаване на искането или коригирането бъде отказано, ***СУ „Св. Климент Охридски“*** уведомява заявителя, като излага причините, поради които отказва или не предприема действията по коригиране. Субекта се уведомява за правото му на жалба пред КЗЛД.

Чл.40. (1) Субектът на данни има право да отправи **възражение срещу обработването** на личните му данни.

(2) След получаване на искането по ал.1, ***СУ „Св. Климент Охридски“*** прекратяванезабавно обработването на личните данни на субекта, освен ако не съществуват законови основания обработването да продължи и когато тези основания имат предимство пред интересите, правата и свободите на субекта, вкл. когато обработването е необходимо за установяването, упражняването или защитата на правни претенции, за защита на правата на друго лице или поради важни причини от обществен интерес.

(3) Ако възражението не бъде уважено, ***СУ „Св. Климент Охридски“*** уведомява заявителя, като излага причините, поради които отказва и го уведомява за правото му на жалба пред КЗЛД.

Чл.41. (1) Субектът на данни има право да поиска **изтриване** на обработваните лични данни (*реализиране на правото „да бъдеш забравен”*).

(2) Искане по ал.1 може да бъде отправено, когато:

1. личните данни повече не са необходими за целите, за които са били събрани;

2. субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

3. субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;

4. личните данни са били обработвани незаконосъобразно;

5. личните данни трябва да бъдат изтрити с цел спазването на правно задължение на администратора;

(3) ***СУ „Св. Климент Охридски“*** може да откаже изтриване на личните данни, когато обработването е необходимо:

1. за упражняване на правото на свобода на изразяването и правото на информация;

2. за спазване на правно задължение на администратора, което изисква обработване или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора;

3. по причини от обществен интерес в областта на общественото здраве;

4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;

5. за установяването, упражняването или защитата на правни претенции на

администратора.

(4) Субектът на данни е длъжен да посочи конкретните данни, които иска да бъдат изтрити.

(5) Ако действия по изтриване / заличаване на данните не бъдат предприети или искането бъде отхвърлено, ***СУ „Св. Климент Охридски“*** уведомява заявителя, като излага причините, поради които отказва или не предприема действията по изтриване. Субекта се уведомява за правото му на жалба пред КЗЛД.

Чл.42. (1) Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повтаряемост, Длъжностното лице по защита на данните:

- отправя мотивиран отказ до субекта на данни и не предприема действия по изпълнение на искането;

или

- предлага на директора на институцията да определи и наложи разумна такса, съответстваща на административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия.

(2) Преди извършването на действия по искането и отправяне отговор до субекта на данни, ДЛЗД преценява дали в правото на ЕС или националното законодателство не са налице ограничения за упражняване на правата на субекта на данни, имащи за цел да гарантират:

- националната сигурност и отбраната;
- обществената сигурност;
- предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;
- важни цели от широк обществен интерес;
- важен икономически или финансов интерес на ЕС или на държава-членка, паричните, бюджетните и данъчните въпроси;
- общественото здраве и социалната сигурност;
- защитата на независимостта на съдебната власт и съдебните производства;
- предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;
- функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите;
- защитата на субекта на данните или на правата и свободите на други лица;
- изпълнението по гражданско-правни искове.

Глава ПЕТА
ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТВАНЕТО И СЪХРАНЕНИЕТО НА ЛИЧНИ ДАННИ И/ИЛИ ИМАЩИ ДОСТЪП ДО ДАННИТЕ

Раздел I
Лица, управляващи процесите по обработване на лични данни

Чл.43. (1) Като администратор на лични данни, ***СУ „Св. Климент Охридски“*** се представлява от директора на образователната институция.

(2) Ръководството на институцията е отговорно за разработване и насърчаване използването на добри практики в сферата на защитата на личните данни.

Чл.44. (1) Директорът на ***СУ „Св. Климент Охридски“*** определя с писмен акт Длъжностно лице по защита на данните (ДЛЗД).

(2) За ДЛЗД може да бъде определено физическо или юридическо лице, което притежава познания в областта на защитата на данните - законодателство и практическо приложение.

(3) Определеното Длъжностно лице по защита на данните подпомага директора и останалите служители при реализиране на дейностите по обработване на данните и тяхната защита.

Чл.45. (1) Длъжностното лице по защита на данните има следните правомощия и задължения:

1. информира и съветва директора и служителите, които извършват обработване на лични данни, за техните задължения по силата на ОРЗД и на други разпоредби за защитата на данни на равнище Съюз или държава членка;
2. наблюдава спазването ОРЗД и на други разпоредби за защитата на данни на равнище Съюз или държава членка, както и разпоредбите на настоящите Правила, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;
3. сътрудничи си с надзорния орган, когато е изрично оправомощен за това от директора;
4. действа като точка за контакт за надзорния орган по въпроси, свързани с обработването и по целесъобразност се консултира по всякакви други въпроси;
5. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите;
6. определя ред за съхраняване и унищожаване на информационни носители;
7. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
8. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;
9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;
10. изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

11. унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;

12. води регистър на дейностите по обработване на лични данни в ***СУ „Св. Климент Охридски“***.

(2) ДЛЗД е задължен да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка.

(3) ДЛЗД може да изпълнява и други задачи и задължения.

(4) При изпълнение на възложените по предходната алинея функции и правомощия, ДЛЗД действа като независим подпомагащ вътрешен орган и се отчита пряко пред Директора на институцията.

(5) Всички служители са длъжни да оказват съдействие на ДЛЗД при изпълнение на функциите му.

Раздел II

Лица, извършващи дейности по обработване на лични данни и/или имащи достъп до лични данни

Чл.46. (1) Достъп до личните данни, обработвани и съхранявани от ***СУ „Св. Климент Охридски“*** имат само служителите, на които такъв достъп е разрешен и необходим за изпълнение на служебните им задължения, както и за изпълнение на бизнес цели, при стриктно спазване на принципа „*Необходимост да знае*”.

(2) Оторизирането за достъп или извършване на дейности по събиране, обработване, съхранение и защита на личните данни се осъществява с нарочна заповед на директора или чрез формулираните в длъжностната характеристика конкретни трудови функции и задължения.

(3) Възможността за достъп до личните данни на други служители на институцията се ограничава до случаите, когато на тях е предоставен такъв с изрично разрешение, в което се посочват личните данни и целите, за които се предоставя достъпът, както и времето, за което той се предоставя.

Чл.47. (1) Служителите на ***СУ „Св. Климент Охридски“*** са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират при необходимост регистрите на личните данни;

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

6. да подпишат Декларация-Приложение №1 (за служители обработващи данни).

(2) Задълженията по предходната алинея се прилагат за всички длъжности в институцията, свързани с обработването на лични данни и/или имащи достъп до данните.

Чл.48. Работниците и служителите нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл.49. (1) Всяко нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните работници и служители.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ***СУ „Св. Климент Охридски“*** или за трето лице, от служителя може да се потърси имуществена отговорност по реда на общото гражданско законодателство.

Глава ШЕСТА
ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ МЕРКИ ЗА ОСИГУРЯВАНЕ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Раздел I
Общи положения

Чл.50. (1) ***СУ „Св. Климент Охридски“*** организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от изменение, от неправомерен достъп до данните или тяхното разпространение, както и от други незаконни форми на обработване на лични данни.

(2) Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл.51. (1) ***СУ „Св. Климент Охридски“*** прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и мрежи.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на институцията и/или нормалното й функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на ***СУ „Св. Климент Охридски“*** се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл.52. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, институцията може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят от ДЛЗД веднъж на 2 години или при промяна на характера на обработваните лични данни, както и по изрично нареждане на директора на институцията.

Раздел II

Физическа защита

Чл.53. Физическата защита в ***СУ „Св. Климент Охридски“*** се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл.54. (1) Основните **организационни мерки за физическа защита** включват:

1. определяне на помещенията, в които ще се обработват лични данни;

2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,

3. определяне на организацията на физическия достъп;

(2) Като **„помещения, в които се обработват лични данни”**, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. **Достъпът до тях е физически ограничен и контролиран** - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни.

(3) Когато в помещенията по ал.2 имат достъп външни лица, в помещенията **се обособяват „непублична“ и „публична” част**. В непубличната се извършват дейностите по обработване на лични данни и тя е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения. В достъпната публична част не се извършват дейности по обработване и не се съхраняват данни, независимо от техния носител.

(4) Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.

(5) Зони с контролиран достъп са всички помещения на територията на институцията, в които се събират, обработват и съхраняват лични данни.

Чл.55. (1) Използваните **технически средства за физическа защита** на личните данни в ***СУ „Св. Климент Охридски“*** са съобразени с действащото законодателство и нивото на въздействие на тези данни.

(2) Организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп, чрез заключващи системи и механизми, до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(3) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са разположени в помещения с ограничен достъп само за упълномощен персонал.

(4) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители,

включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Чл.56. (1) Основните **технически мерки за физическа защита** в ***СУ „Св. Климент Охридски“*** включват:

1. използване на сигнално-охранителна техника;
2. използване на ключалки и заключващи механизми;
3. заключващи се шкафове, метални каси;
4. оборудване на помещенията с пожароизвестителни и пожарогасителни средства;
5. Използване на видеонаблюдение.

(2) Документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

(3) Оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва:

- сигнално-охранителна техника;
- ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица;
- заключваеми шкафове и каси;
- пожарогасителни средства.

(4) Пожароизвестителните и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Раздел III
Персонална защита

Чл.57. (1) Основните **мерки за персонална защита** на личните данни, приложими в ***СУ „Св. Климент Охридски“***, са:

1. задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец;
2. запознаване на персонала с опасностите за личните данни, обработвани от институцията;
3. забрана за споделяне на критична информация (*идентификатори, пароли за достъп и др.п.*.) между персонала и всякакви други лица, които са неоторизирани;
4. деклариране на съгласие от служителите за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, освен мерките по ал. 1, могат да се прилагат и следните допълнителни мерки::

1. провеждане на специализирани обучения за работа и опазване на лични данни, в

случай че спецификата на служебните задължения изисква подобно;

2. организиране и провеждане на тренинги на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква това.

Чл.58. (1) ***СУ „Св. Климент Охридски“*** провежда политика по обучения на персонала с цел информираност относно установените от законодателството и тези Правила процедури и персоналните задължения на всеки служител, свързани със защитата на личните данни.

(2) Образователната институция създава условия за непрекъснато поддържане осведомеността на служителите относно вече въведените и новоприети изисквания за защита на данните, както и съответните на това нови мерки, въведени от ***СУ „Св. Климент Охридски“***

(3) В изпълнение на предходните алинеи, директорът, подпомаган от ДЛЗД, разработва конкретни програми за обучение, информираност и поддържане на осведомеността.

(4) Всяко проведено обучение се документира, като ДЛЗД следи за съставянето на Списък с присъствалите на съответните обучения.

Чл.59. (1) Длъжностното лице по защита на данните предприема действия за организиране и осъществяване на непрекъснат контрол за прилагане на следните персонални мерки за защита:

- проследяване и отчитане на броя, предмета, интензитета и нивото на преминато подходящо обучение от служителите;
- въвеждане и прилагане на мерки, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- включването на клаузи за защитата на данните в трудовите договори;
- включване на текстове регламентиращи конкретни правомощия, задължения и отговорности относно защитата на данните в длъжностните характеристики на служителите;
- идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- контрол на физическия достъп на служителите до електронни и хартиено базирани записи;
- въвеждане и прилагане на политика за „чисто работно място“, която изисква при напускане на работното място, цялата работна документация да е премахната или прибрана в подходящи за това и с ограничен достъп места - специални шкафове, заключени помещения, унищожаване на вече ненужни документи и т.н.;
- ограничаване на използването на служебните портативни и/или мобилни електронни устройства извън работното място;
- ограничаване на използването от служителите на лични портативни и/или мобилни устройства на работното място;
- приемане и прилагане на ясни правила за създаване и ползване на пароли от служителите;

(2) Посочените в предходната алинея контроли са систематизирани въз основа на

идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди от служителите обработващи данните или имащи достъп до тях.

Раздел IV

Документална защита

Чл.60. Основните **мерки за документална защита** на личните данни, прилагани от ***СУ „Св. Климент Охридски“***, включват:

1. **Определяне на регистрите, които ще се поддържат на хартиен носител** - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на институцията, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. **Определяне на условията за обработване на лични данни** - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на дружесвото, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. **Регламентиране на достъпа до регистрите с лични данни** – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа „*Необходимост да знае*”;
4. **Определяне на срокове за съхранение** - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство или в тези Правила срок.
5. **Прилагане на процедури за унищожаване** - Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на институцията или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин, при спазване на правилата, установени в Глава Осма, Раздел Трети на този документ.

Чл.61. (1) Въвеждат се и се прилагат правила за размножаване и разпространение, според които се разрешава копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган.

(2) Копия на документите се предоставят само на лица, на които са необходими във връзка с извършване на възложена работа в посочените в ал.1 случаи.

(3) Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки и санкции, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Раздел V

Защита на автоматизираните системи и мрежи

Чл.62. (1) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи.

(2) На лицата, изпълняващи дейности по техническа поддръжка функционирането на системите, не се разрешава достъп до съхраняваните в електронен вид данни.

Чл.63. (1) Защитата на автоматизираните информационни системи и/или мрежи в ***СУ „Св. Климент Охридски“*** **включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.**

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

1. **Идентификация** и **автентификация** чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на институцията. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае”;
2. **Управление на регистрите**, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;
3. **Управление на мрежи и/или свързване;**
4. **Защитата от зловреден софтуер;**
5. Прилагане на **политика по създаване и поддържане на резервни копия за възстановяване.**

Чл.64. Управлението на мрежите и свързването включва:

1. **Дефиниране на обхвата** на вътрешните мрежи:

- вътрешни мрежи са всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на ***СУ „Св. Климент Охридски“***.
- външни мрежи са всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на институцията.

2. **Регламентиране на достъпа** до вътрешната мрежа:

- достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от директора други лица.
- минималното изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

3. **Администриране на достъпа** до вътрешната мрежа:

- отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация.
- в отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки,

връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

4. **Контрол на достъпа** до вътрешната мрежа:

- отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация.
- оправомощените лица са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (*физически и/или отдалечен*) достъп до мрежите на институцията, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

Чл.65. Защитата от зловреден софтуер включва:

1. използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от ръководството на ***СУ „Св. Климент Охридски“*** лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на оторизирания от ръководството ИТ специалист.

2. използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от ръководството на ***СУ „Св. Климент Охридски“*** лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

3. активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

4. забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от ръководството на ***СУ „Св. Климент Охридски“*** лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (*чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация*). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

Чл.66. Политиката по създаване и поддържане на резервни копия за възстановяване се свежда до определяне на:

1. основната цел на архивирането - предотвратяване загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на институцията;
2. начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител;
3. отговорността за архивиране - на лицето, обработващо личните данни;
4. срок на архивиране, който следва да е съобразен с действащото законодателство и регламентираното в тези Правила;
5. съхраняването на архива, което следва да се реализира в друго, специално определено за целта физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

6. основните електронни носители на информация:

- вътрешни твърди дискове (*част от компютърна и/или сториджсистема*),
- еднократно и/или многократно презаписваеми външни носители (*външни твърди дискове, флаш-памет, многократно презаписваеми карти, памети ленти и други носители на информация, както и еднократно записваеми носители и др.*)

Чл.67. (1) ***СУ „Св. Климент Охридски“*** прилага и следните допълнителни мерки:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на институцията:

- Отдалечен достъп до вътрешни мрежи на институцията не се предвижда. По изключение, и след изричната оторизация от ръководството, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни;
- На персонала на институцията може да бъде предоставен интернет достъп (*отдалечен достъп*) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (*вкл. сайтове, файлове, услуги и др.*) се определя по преценка и предложение на преките ръководители, съгласувано с оторизираните от ръководството на институцията лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от ръководството и след становище на ДЛЗД.
- Отдалеченият достъп чрез интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ръководството, както и в случаите на заплаха за сигурността на данните.

2. Публикуването на служебна информация в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от ръководството на институцията или от нарочно упълномощен за това служител.

(2) Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на ***СУ „Св. Климент Охридски“,*** включват:

- Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на институцията от външни и вътрешни атаки (*Vulnerability test*), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.
- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на институцията, ако същите биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове.
- Забрана за използване на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако то представлява престъпление – и по предвидения за санкциониране на това деяние ред.

(3) Мерките, свързани със създаване на физическа среда (*обкръжение*), включват физически контрол на достъпа (*сигнално-охранителна техника, ключалки, метални решетки и други приложими способи*), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Раздел VI

Мерки за защита на личните данни при компютърна обработка

Чл.68. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) ***СУ „Св. Климент Охридски“*** прилага адекватни мерки за технически и административен контрол (*ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секунди*), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от системния администратор период, но не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (*вкл. и чрез изтриване на акаунта*).

(6) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (*log*) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (*например влизане в нетипично време, неизключване на работна станция след изтичане на работното време и др.*), системният администратор незабавно уведомява Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл.69. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на

сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл.70. (1) В ***СУ „Св. Климент Охридски“*** се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от ръководството на институцията лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл.71. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

Глава СЕДМА
ОТЧЕТНОСТ. ДОКУМЕНТИРАНЕ НА ОБРАБОТВАНЕТО. ВОДЕНЕ НА РЕГИСТРИ.

Раздел I
Общи положения

Чл.72. (1) ***СУ „Св. Климент Охридски“*** прилага принципа за отчетност при обработването на личните данни, като документира дейностите по обработване.

(2) Документацията се изготвя така, че да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

Чл.73. В изпълнение на задължението си да води необходимата документация, ***СУ „Св. Климент Охридски“*** изготвя:

1. Настоящите Вътрешни правила за обработване и защита на лични данни..;
2. Други вътрешни документи, съдържащи правила, процедури и политики свързани с обработването на лични данни;
3. Регистър на дейностите по обработване.

Раздел II
Регистри

Чл.74. (1) ***СУ „Св. Климент Охридски“*** поддържа:

1. Регистър на дейностите по обработване на лични данни по чл.30, пар.1 от ОРЗД;
2. Регистър на съгласията на субектите на данни (*ако бъде взето решение за воденето на такъв*);
3. Регистър на исканията на субектите на данни (*ако бъде взето решение за воденето на такъв*);
4. Регистър на нарушенията на сигурността;

5. Регистър на видео-наблюденията.

(2) Регистрите се водят и поддържат в писмен вид (*вкл. електронен*).

(3) При поискване от надзорния орган, ***СУ „Св. Климент Охридски“*** осигурява достъп до регистрите.

Чл.75. (1) Като администратор на лични данни, ***СУ „Св. Климент Охридски“*** изпълнява вмененото му от чл.30, ал.1 от ОРЗД задължение да води и поддържа Регистър на дейностите по обработване, за които отговаря.

(2) Регистърът по чл.30, пар.1съдържа:

1. данни идентифициращи администратора – име и координати и данни за длъжностното лице по защита на данните (ако такова е определено);

2. целите на обработването;

3. описание на категориите субекти на данни;

4. описание на категориите лични данни;

5. категории получатели, пред които са или ще бъдат разкрити личните данни, вкл. получатели в трети държави или международни организации, когато е приложимо;

6. предаването на личните данни на трета държава или международна организация, в случай на предаване на данни, посочено в чл.49, пар.1, когато е приложимо;

7. предвидените срокове за изтриване на различните категории данни, когато това посочване е възможно;

8. общо описание на техническите и организационни мерки за сигурност, когато е възможно.

Чл.76. ***СУ „Св. Климент Охридски“*** може да поддържа и следните регистри с лични данни:

1. Регистър „Работници/служители и лица по граждански договори”;

2. Регистър „Кандидати за работа”;

3. Регистър „Деца, ученици и родители”;

Раздел III

Форма и водене на регистрите. Контрол.

Чл.77. (1) Формата на водене на регистрите е писмена (*документална*).

(2) Регистрите се водят на хартиен и на електронен носител.

(3) При водене на регистрите на хартиен носител, същите се съхраняват в папки (досиета, дела, класьори).

(4) Папките се подреждат и съхраняват в картотечни шкафове, които са оборудване със заключващи механизми.

(5) Картотечните шкафове се помещават в помещения за самостоятелна работа на служителите, на които е възложено обработването на съответните регистри и данни.

(6) Достъпът до регистрите и данните е регламентиран в настоящите Правила или с изрични разпореждания на директора, съгласувани с ДЛЗД.

Чл.78. (1) При водене на регистрите на технически носител, личните данни се въвеждат на

твърд диск, на изолиран компютър, ако не е разпоредено друго от системния администратор или директора, след съгласуване с ДЛЗД.

(2) Компютърът по ал.1, може да бъде свързан в локална мрежа, но със защитен достъп до личните данни. Мрежата, изградена и използвана в помещенията на институцията се базира изключително на комуникационни устройства, които предоставят богат набор от възможности, свързани със сигурността на достъпа до информация.

Чл.79. (1) При работа с данните могат да се използват софтуерни продукти по обработка на данните, относно счетоводното отчитане, възнагражденията на персонала и други. Софтуерните продукти трябва да са адаптирани към специфичните нужди на администратора на лични дани и към изискванията за защита на данните.

(2) Достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите на лични данни чрез парола за отваряне на тези файлове.

Чл.80. Контрол върху воденето и съхраняването на регистрите осъществяват Длъжностното лице по защита на данните и Директора.

Чл.81. ДЛЗД съвместно със съответните отговорни за регистрите служители, извършват периодични прегледи на личните дани съдържащи се в регистрите, а ДЛЗД изготвя и представя пред ръководството на институцията доклад от проверките.

Глава ОСМА
СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИТЕ ДАННИ

Раздел I
Съхраняване на лични данни

Чл.82. (1) Документите и регистрите, по които работата е приключила, се архивират.

(2) Трайното съхраняване за нуждите на архивирането на документи на хартиен носител, съдържащи лични данни, се извършва в помещения, определени за архив, за срокове, съобразени с действащото законодателство и тези Правила. Помещенията, определени за архив, са оборудвани с пожароизвестителни системи и пожарогасители, със системи за контрол на достъпа и задължително се заключват.

(3) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация.

(4) Архивиране на личните данни на технически носител се извършва периодично (*всеки ден, всяка седмица или всеки месец – в зависимост от указанията на системния администратор и ДЛЗД за всеки носител и категория данни*) от опериращия с личните данни служител с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на местоположение, различно от мястото на компютърното оборудване, с което се обработват данните.

(5) Архивирането по предходната алинея се извършва на надеждни оптични

носители (*сървъри, външни твърди дискове, USB-флашки и др.*), достъп до които има само обработващият съответните лични данни и изрично оторизирани за това длъжностни лица.

Чл.83. (1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец. (*Списък на приложенията*)

Чл.84. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от институцията регистри.

(2) Резултатите от всяка проверка се обобщават в доклад на ДЛЗД до директора на институцията, в който се включва и преценка на необходимостта за обработка на личните данни или тяхното унищожаване.

Раздел II
Срокове на съхраняване на лични данни

Чл.85. (1) ***СУ „Св. Климент Охридски“*** не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните или за срок, установен като изискуем съгласно нормативната уредба.

(2) Образователната институция може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

Раздел III
Унищожаване на лични данни

Чл.86.(1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от ***СУ „Св. Климент Охридски“*** регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, ***СУ „Св. Климент Охридски“*** прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер машина.

(3) Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар.1, б.”е” от ОРЗД).

(4) При унищожаване на личните данни не трябва да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването.

Чл.87. (1) Унищожаването се осъществява от служители, упълномощени с изричен писмен акт на директора и след задължително уведомяване на Длъжностното лице по защита на данните.

(2) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по предходната алинея.

Глава ДЕВЕТА
ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Раздел I
Достъп, предоставян на компетентните държавни / общински органи

Чл.88. Достъпът на трети лица до лични данни обработвани от ***СУ „Св. Климент Охридски“*** е категорично забранен, освен предвидените в закона и/или в настоящите Вътрешни правила случаи.

Чл.89. (1) ***СУ „Св. Климент Охридски“*** осигурява достъп до обработваните лични данни на физически лица, когато същите са изискани по надлежен ред от компетентни държавни и/или общински органи (*МОН, РУО на МОН, НАП, НОИ и др.*) и когато задължението за предоставяне на данните е предвидено в нормативен акт.

(2) На компетентните органи се осигурява достъп до личните данни или данните се предоставят съгласно законовите изисквания в зависимост от всеки конкретен случай.

(3) Решението си за предоставяне или отказ на достъп до лични данни за съответното лице институцията съобщава на третите лица в подходящ срок от подаване искането, без ненужно забавяне.

Раздел II
Предоставяне на данни на обработващ

Чл.90. (1) ***СУ „Св. Климент Охридски“*** може, при необходимост и във връзка с дейността си, да предоставя лични данни на трети лица, действащи в качеството на обработващ.

(2) Институцията избира за обработващ(и) само доставчици, които могат да осигурят и гарантират техническа, физическа и организационна сигурност и които отговарят на поставените изисквания по отношение на всички лични данни, които ще обработват

(3) Взаимоотношенията с обработващ(и) задължително се регламентират с изричен писмен акт.

(4) При сключването на договор/споразумение с обработващ, ***СУ „Св. Климент Охридски“*** задължително:

1. предвижда и изисква от обработващия достатъчно гаранции за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

2. информира за предоставянето физическите лица, чиито данни ще бъдат предадени на обработващ.

Раздел III

Трансфер на данни извън ЕС

Чл.91. (1) ***СУ „Св. Климент Охридски“*** **не извършва** трансфер и не предоставя лични данни в страни извън ЕС.

(2) При възникнала необходимост, такъв трансфер, може да се реализира само при някоя от следните хипотези:

1. субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;

2. предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

3. предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;

4. предаването е необходимо поради важни причини от обществен интерес;

5. предаването е необходимо за установяването, упражняването или защитата на правни претенции;

6. предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

7. предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

(3) За предоставянето на данните се сключва писмено споразумение (*договор*).

Глава ДЕСЕТА

ДЕЙСТВИЯ ПРИ НАРУШЕНИЯ НА СИГУРНОСТТА

Раздел I

Общи положения

Чл.92. (1) Нарушение на сигурността на личните данни е всяко събитие, при което се реализира случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или неоторизиран достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

(2) Нарушение на сигурността на личните данни е и всяко действие или бездействие, което компрометира сигурността, конфиденциалността или целостта на данните, или на физическите, технически, административни или организационни защити.

(3) Не е нарушение на сигурността констатираният потенциален риск от възникване на събитие по ал.1, без същото да се е реализирало.

Раздел II

Процедурни действия при установяване на нарушение

Чл.93.(1) При всяко идентифициране на признаци за нарушение на сигурността, лицето което го е констатирало е длъжно да докладва на ДЛЗД, а когато това е невъзможно, на директора на институцията.

(2) Докладването се извършва в писмена форма, по имейл или друг подходящ начин, който позволява да се установи извършването и документирането на нарушението, да се определи и спази срока за уведомяване. При докладването служителят предоставя цялата налична информация по случая и предприема необходимите действия и мерки за съхраняване на всички доказателства свързани с нарушението.

(3) ДЛЗД извършва незабавна проверка на подадения по ал.1 сигнал, като при проверката установява реализирано ли е нарушение на сигурността, в какво се изразява нарушението, кои данни са засегнати и до кои субекти на данни се отнасят.

(4) При спешност и когато това е възможно и допустимо, ДЛЗД предприема мерки за преустановяване на нарушението, неутрализиране или редуциране на щетите от него.

(5) ДЛЗД докладва незабавно на директора на институцията за нарушението на сигурността на данните, като предоставя информация за вида на нарушението, времето на установяване, вида на щетите, предприетите до момента мерки за преустановяване на нарушението, неутрализиране или ограничаване на щетите.

(6) След съгласуване с ръководството на институцията, ДЛЗД предприема всички необходими мерки за предотвратяване или редуциране на последиците от нарушението, като следва и изпълнява стриктно всички получени инструкции.

Чл.94.(1) Във всеки конкретен случай на нарушение на сигурността, ***СУ „Св. Климент Охридски“*** провежда вътрешно разследване с цел да се установи риска за субектите в резултат на конкретното нарушение.

(2) При извършване на вътрешното разследване се прави разпит на служителите и лицата, отговорни за боравене с личните данни (*IT специалист, ръководител „Човешки ресурси”, счетоводител и т.н.*).

(3) При извършване на вътрешното разследване всяко от лицата, отговорни за боравене с лични данни представя на ДЛЗД становище, придружено със съответните доказателства.

Чл.95.(1) При всеки констатиран случай на нарушение на сигурността, се прави оценка на риска.

(2) Остатъчният риск бива пресметнат, като се има предвид степента на риска и нужните мерки за премахването му.

(3) Резултатът от извършения анализ се обективира от ДЛЗД в доклад, който съдържа всички насоки за предприемане на мерки.

Раздел III

Докладване за нарушението на надзорния орган

Чл.96.(1) Когато нарушението на сигурността поради естеството и мащаба си създава риск за правата и свободите на субектите на данни, директора на институцията уведомява КЗЛД.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо, не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД за нарушение на сигурността следва да съдържа следната информация:

1. контактна информация за връзка с администратора;

2. описание на естеството на нарушението на сигурността;

3. когато това е възможно, посочване на категориите и приблизителният брой на засегнатите субекти на данни и приблизителното количество на засегнатите записи на лични данни;

4. описание на евентуалните последици от нарушението на сигурността;

5. описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици;

6. информация за причините за забавяне на уведомяването, в случаите, когато същото не е осъществено в срока по ал.2.

(4) В случай, че не може да се подаде в пълнота едновременно, информацията за нарушението може да се подаде поетапно без по-нататъшно ненужно забавяне.

(5) Уведомяване на надзорния орган може да не се предприема, когато се установи че не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица – субекти на данните.

Раздел IV

Докладване за нарушението от обработващия на администратора

Чл.97.(1) Когато е установено нарушение на сигурността по отношение на лични данни, които ***СУ „Св. Климент Охридски“*** обработва в качеството си на обработващ, ДЛЗД или директора отправя уведомление за нарушението до администратора на данните.

(2) Уведомлението по ал.1 следва да съдържа всички необходими подробности за допуснатото нарушение. Отправилият уведомлението следва да изисква предоставянето на потвърждение за получаване от страна на администратора (*мейл, факс или други*).

(3) В случаите по ал.1, ***СУ „Св. Климент Охридски“*** като обработващ данните не следва да прави директно уведомяване на надзорния орган по правилата на предходния член.

Раздел V

Съобщаване за нарушението на засегнатите субекти на данни

Чл.98.(1) Когато нарушението на сигурността на личните данни поражда висок риск за правата и свободите на физическите лица, директора, без ненужно забавяне и при спазване на приложимото законодателство съобщава за нарушението на засегнатите физически лица – субекти на данни.

(2) Съобщението по ал.1 следва да бъде дадено на ясен и прост език, да дава информация за естеството на нарушението на сигурността на личните данни и да съдържа най-малко следното:

1. описание на естеството на нарушението;

2. евентуалните последици от нарушението;

3. предприетите или предложени от администратора мерки за справяне с нарушението на сигурността, включително по целесъобразност мерки за намаляване на евентуалните негативни последици;

4. името и координатите на ДЛЗД или на друга точка за контакт, от която може да получи повече информация.

Чл.99.(1) Задължението за съобщаване не се прилага, когато е налице някое от следните условия:

1. администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2. администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. съобщаването би довело до непропорционални усилия на администратора. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

(2) В случаите, когато нарушението на сигурността засяга лични данни, които ***СУ „Св. Климент Охридски“*** обработва в качеството си на обработващ от името на друг администратор, задължението за съобщаване на засегнатите субекти на данни възниква за администратора.

Раздел VI

Документиране на нарушението на сигурността на данните

Чл.100.(1) Процедурата по действия при нарушение на сигурността на данните и по докладване и управление на инциденти задължително включва действия по документиране на нарушението, което се реализира чрез регистриране на събитието/инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е докладвано, последствията от него и мерките за отстраняването му, извършените уведомявания и съобщения.

(2) ***СУ „Св. Климент Охридски“*** води регистър на нарушенията на сигурността, който съдържа следната информация:

1. дата на установяване на нарушението;

2. описание на нарушението, в т.ч. източник, вид и мащаб на засегнатите данни, причина за нарушението (*когато е приложимо*);

3. описание на извършените уведомявания на надзорния орган (*когато е приложимо*);

4. описание на извършените уведомявания на администратора (*уведомяване от обработващия, когато е приложимо*);

5. описание на извършените съобщения на засегнатите субекти на данни (*когато е приложимо*);

6. посочване на предприетите мерки за предотвратяване и/или ограничаване на негативните последици за субектите на данни и за инситуцията;

7. предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(3) Регистърът се води в електронен формат от оправомощено за това лице.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила са в сила и се прилагат от 15.09.2022 г.

§ 2. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни,.

(2) Разработените към настоящите Вътрешни правила приложения са примерни образци на документи, които се съставят при и по повод обработката на лични данни:

§ 3. (1) Изменения и допълнения на Вътрешните правила се правят по реда на издаването и утвърждаването им.

(2) ***СУ „Св. Климент Охридски“*** може да променя тези Правила по всяко време.

(3) Всички промени незабавно се свеждат до знанието на лицата, които засягат.

§ 4. Всички лица с ръководни функции в ***СУ „Св. Климент Охридски“***носят отговорност за спазването на тези правила от страна на персонала и следва да въведат подходящи практики, процеси и обучение.

§ 5. (1) Настоящите Вътрешни правила се свеждат до знанието на всички служители на образователната институция, както и до ангажираните с изпълнение на граждански договор лица.

(2) Лицата по ал.1 са длъжни да спазват Правилата ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

(3) За неизпълнение на задълженията по Правилата и действащото към съответния момент национално и европейско законодателство за защита на личните данни, съответните лица носят дисциплинарна и имуществена отговорност.

§ 6. Контрол по изпълнението на настоящите Вътрешни правила за обработване и защита на лични данни се осъществява от Директора и Длъжностното лице по защита на данните.

ОПИС НА ПРИЛОЖЕНИЯТА

№	Наименование	Файл
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		

Приложение № 1

ДЕКЛАРАЦИЯ

Долуподписаният/ата .....,

ЕГН……., л.к. № ……., издадена на ..... г.

от МВР гр .....,

в качеството си на ..... ,
(длъжност/позиция)

в ***СУ „Св. Климент Охридски“*** на основание чл. 47, ал. 1, т. 6 от Вътрешните правила за обработване и защита на лични данни, обработвани в образователната институция,

ДЕКЛАРИРАМ:

1. Че съм запознат/а с:
- нормативната уредба в областта на защитата на личните данни;
- политиката и ръководствата за защита на личните данни в образователната институция;
- опасностите за личните данни, обработвани от администратора.

2. Че поемам задължения за:
- несподеляне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
- неразгласяване на лични данни, до които съм получил/а достъп при и по повод изпълнение на задълженията си, ако това не е предвидено изрично в закон или не застрашава живота и здравето на физическото лице.

Дата:…… **ДЕКЛАРАТОР**:
гр./с/ (подпис и фамилия)