Врз основа на член 66 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), Училишниот одбор на **ООУ „Пере Тошев“ Росоман**, на ден 16.12.2021 година донесе

ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ООУ „ПЕРЕ ТОШЕВ“ РОСОМАН

ОПШТИОДРЕДБИ

Предмет на уредување
Член 1

(1) Со Правилникот за безбедност на обработка на личните податоци во **ООУ „Пере Тошев“ Росоман** се пропишуваат упатства за постапување на контролорот при применувањето на техничките и организациските мерки за обезбедување на безбедност на обработката на личните податоци согласно со законските прописи.

(2) Одредбите од овој Правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Содржина на Правилникот за безбедност на обработка на личните податоци во ООУ„Пере Тошев“ Росоман
Член 2

Правилникот за безбедност на обработка на личните податоци на **ООУ „Пере Тошев“ Росоман** содржи: поимник, примена и одржување на информациски систем, пренос на лични податоци во трети земји, безбедност на обработка на личните податоци (четири фази на управување со ризици), нивоа на мерки за безбедност на обработката на личните податоци и примена на нивоата на мерки за безбедност на обработката на личните податоци (стендардно и високо ниво - со сите објаснувања) и преодни и завршни одредби.

Поимник
Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. Доверливост е пристап до личните податоци единствено од лица кои имаат овластување за нивна обработка од страна наконтролорот;
2. Интегритет е заштита на точноста на личните податоци, при што се гарантира дека личните податоци се точни, целосни иажурирани;
3. Достапност е непречен пристап и континуирана расположливост (business continuity) на информацискиот систем на кој се врши обработка на личните податоци од страна на овластените лица;
4. Неотповикливост е обезбедување на потврда на автентичноста на идентитетот на овластеното лице кое се најавува на информацискиот систем при што овластеното лице не може да ја негира преземената активност илидејствие;
5. Автентификација е постапка која што овозможува потврдување на идентитетот на

овластеното лице кое се најавува и пристапува на информацискиот систем на кој се врши обработка на личнитеподатоци;

6. Систем за заштита на личните податоци е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци во согласност со прописите за заштита на личнитеподатоци;

7. Авторизиран пристап е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории наконтролорот;

8. Документе секој запис кој содржи лични податоци и истиот тој запис може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникацискамрежа.

9. Информатичка инфраструктура е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личнитеподатоци;

10. Информациски систем е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да гикористи;

11.Управување со ризик е идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на контролорот за минимизирање, набљудување и контрола на веројатноста и сериозноста која што може да произлезе при обработката на личните податоци, а која може да предизвика материјална или нематеријална штета врз процесите со кои се врши обработка на личнитеподатоци;

12. Администратор на информацискиот систем е лице овластено за планирање и за применување на технички и организациски мерки и лице задолжено за контрола на обезбедувањето тајност и заштита на обработката на личнитеподатоци;

13. Инцидент е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личнитеподатоци;

14.Контрола на пристап е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластенотолице;

15. Лозинка е доверлива информација составена од множество на карактери кои се користат за проверка и автентикација на овластенотолице;

16. Колаче (cookie) е информација која што се креира и испраќа од веб-серверот до веб-пребарувачот, а која потоа се испраќа назад, како непроменета информација од веб- пребарувачот секогаш кога повторно ќе се пристапи до веб-серверот кој ја креирал информацијата.

17. Овластено лице е лице кое е вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема на кои се обработуваат личниподатоци;

18. Работна станица е секој уред (десктоп, лаптоп) кој поврзан во мрежа претставува дел од опремата на контролорот, а на кој, односно со кој се врши обработка на личните податоци во информацискиотсистем;

19. Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени;и

20. Сигурносна копија е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторновраќање.

Применаи одржување на информацискиот систем
Член 3

Одредбите од Правилникот за безбедност на обработка на личните податоци во ООУ „Пере Тошев“ Росоман се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Член 4

Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот- Директорот на ООУ „Пере Тошев“ Росоман, треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички мерки и за организациски мерки. Овие одредби се применуваат и ако физичките или правните лица вршат обработка на личните податоци наконтролорот.

Пренос на лични податоци во трети земји
Член 5

Во случајна хардверско одржување и/или софтверско одржување, како и поради други активности на информацискиот систем може да се врши пренос на лични податоци во трети земји само во согласност со условите утврдени во Законот за заштита на личните податоци.

БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕПОДАТОЦИ

Систем за заштита на личните податоци
Член 6

(1) Контролорот на училиштето е должен да воспостави систем за заштита на личните податоци во училиштето преку примена на соодветни технички и организациски мерки се со цел да обезбеди ниво на безбедност соодветно на безбедносниот ризик.

(2) Безбедносен ризик преставува веројатност на случување на настан кој може да резултира со компромитирање, особено случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци, или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци (во натамошниот текст:ризик).

(3) Техничките и организациските мерки опфаќаат:

- криптирање на личните податоци и псевдонимизација на личните податоци;
- способност за обезбедување на континуирана доверливост, интегритет, достапност иотпорност на информацискиот систем заобработка;
- способност за на времено воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент;
- повторно воспоставување на достапноста до личните податоци и пристапот до нив вослучај на физички или технички инциденти
- процес на редовното тестирање, оценување и евалуација на ефективноста на техничкитеи организациските мерки со цел да се гарантира безбедноста наобработката.

(4) Процесот за управување со системот за заштита на личните податоци е дефиниран во Политиката за системот за заштита на личните податоци на контролорот кој треба да им одговара на природата, обемот и сложеноста на активностите коишто контролорот на

ООУ „Пере Тошев“ Росоман ги врши при обработката на личните податоци и ризиците на коишто еизложен.Контролорот е должен Политиката за системот за заштита на личните податоци да ја ревидира и усогласува согласно промените во неговоработење и да врши оценка и ажурирање на техничките и организациските мерки кои се соодветни на времето во кое се дизајнираат и имплементираат во согласност со најновите технолошки достигнувања (a state of the art technology).

Управување со ризик
Член 7

При утврдувањето и проценатана ризикот, управувањето со ризик контролорот во училиштето ги зема во предвид ризиците кои се поврзани со обработката, особено ризиците од случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

Член 8

Управувањето со ризикот ги опфаќа следните четири фази:

- **Фаза I)** Список на сите процеси со кои се врши обработка на лични податоци,
- **Фаза II)** Процена на ризиците за секој процес на обработка на лични податоци,
- **Фаза III)** Спроведување и проверка на планирани мерки,
- **Фаза IV)** Спроведување на безбедносни проверки.

Прва фаза (I) - Списокот на процеси со кои се врши обработка на личните податоци преку целосно или делумно автоматизиранаобработка на личните податоци или другаобработка на лични податоци, треба да гиопфати:

- хардверот (на пример: сервери, лаптопи, хард дискови и другимедиуми);
- софтверот (на пример: оперативни системи и софтверски програми развиени за потребите наконтролорот);
- комуникациски канали (на пример: оптички кабли, интернет,безжична мрежна технологија –Wi-Fi);
- документи во хартиена форма (на пример: печатени документи,фотокопии).

Втора фаза (II)Проценатана ризиците за секој процес на обработка на личниподатоци треба најмалку да ги опфати:

(а). утврдување на потенцијалните влијанија и ефекти врз правата и слободите на физичките лица на кои се однесува и тоа за следните потенцијални закани, односно настани:

- неовластен пристап до личнитеподатоци;
- непосакувани промени на личните податоции
- привремена или целосна недостапност до личнитеподатоци.

(б). идентификување на изворите на ризик кој што може да биде причина за секој непосакуван настан, а имајќи ги во предвид внатрешните и надворешните човечки ресурси, како и другите внатрешни и надворешни извори како што се: водата, опасните материјали, пожарот,поплавите, земјотресите, вирусите и слично.

(в). идентификување на можните закани кои би можеле да се случат преку медиуми од

кои зависат личните податоци, а се однесуваат на софтверот, хардверот, комуникациските канали, документите во хартиена форма, информациите и слично, а кои можат да бидат:

- употребени на несоодветен начин (злоупотреба на овластувањата, грешка приракување);
- изменети (заразен софтвер или заразен хардвер - keylogger, инсталирање на злонамерен софтвер,инсталирање на вирус, итн);
- изгубени(кражба на лаптоп или губење на мемориски уред –УСБ);
- набљудувани (гео-локација наопремата);
- оштетени (вандализам, кршење, деградација);
- преоптоварени (медиумот за складирање е целосно пополнет, блокирање на софтверот, denial of service attack, пропуштање да се направи back up исл.).

(г).утврдување на постојни или планирани мерки што овозможуваат решавање на секој ризик; како што се: контрола на пристап, сигурносни копии, безбедност на просториите, информациска ревизорска трага, криптирање или анонимизација.

Трета фаза (III) - Контролорот задолжително врши спроведување и проверка на планираните меркисо цел да се обезбеди доказ дека тие се применуваат и тековно сетестираат.

Четврта фаза (IV) – Контролорот за должително спроведува периодични безбедносни проверки а што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.

Нивоа на мерки за безбедност на обработката на личните податоци и примена на нивоата на мерки за безбедност на обработката на личните податоци

Член 9

(1) Според природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, контролорот на училиштето е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личнитеподатоци.Техничките и организациските мерки се класифицирани во двенивоа:

- **стандардно ниво** и

- **високо ниво**.

(2) Контролорот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци согласно со овој Правилник, при што треба да обезбеди соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и заштита од нивно случајно губење, уништување илиоштетување. Исто така контролорот ја демонстрира примената на мерките според барањата, вклучувајќи ги причините и основите за изборот на примената на стандардното, односно високото ниво.

СТАНДАРДНОНИВО

Документација за технички и организациски мерки
Член 10

(1) Контролорот во ООУ „Пере Тошев“ Росоман е должен во Политиката за системот за заштита на личните податоци да ги утврди и начелата за безбедност и заштита на личните податоци кој се содржани во документацијата за технички и организациски мерки. Врз основа на Политиката за системот на лични податоци контролорот донесува подетални политики и процедури во кои се опишани техничките мерки и организациските мерки.

(2) Начела за безбедност и заштита на личнитеподатоци кои ги користи контролорот на училиштето при обработката на личните податоци се: начело на законитост, правичност и транспарентност; начело на ограничување нацелите; начело на минимален обем наподатоци; начело на точност; начело на ограничување на рокот начување и начело на интегритет идоверливост.

(3) Документацијата за техничките и организациските мерки се однесувана:

- идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци, односно анализа на ризик;
- општ описна техничките и организациските мерки заобезбедување тајност и заштита на обработката на личните податоци соодветно наризикот;
- активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици воконтролорот;
- начинотна обезбедување на автентикација на овластенителица и обезбедување на контрола на пристап во информацискиот систем;
- дизајнирање, одржување и развивање на софтверските програми кои служат за

обработка на личните податоци (data protection by design and by default);

- начинот на обезбедување евиденција за секој пристап до информацискиот систем (оперативните системи, заштитниот sид- firewall , серверот дизајниран специјално за употреба како сервер за датотеки– fire server, базите на податоци, системот за управување со документи- DMS System и слично);
- начинот на управување со инциденти и начинот на обезбедување на опремата на контролорот на која се врши обработка на личнитеподатоци;
- начинот на обезбедување на преносливитемедиуми и заштита на внатрешната мрежанаконтролорот;
- начинот на обезбедување на веб-страната наконтролорот;
- начинот на обработка на личните податоци кои се псевдонимизирани и начинот на обработка на лични податоци кои секриптирани;
- начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личнитеподатоци;
- начинот на ангажирање и контрола на надворешни субјекти, односно обработувачи;
- обврските и одговорностите на администраторот на информацискиот систем при користење на документитеи информатичко комуникациската опрема;
- обврските и одговорностиена овластените лица при користење на документите и информатичко комуникациската опрема;
- начинот и процесите за пријавување, реакција и санирање наинциденти;
- начинот на архивирање и чување, како и начинот за повторно враќање на зачуваните

лични податоци, начинот на правење на сигурносна копија;

- начинотна уништување на документите,уништување, бришење и чистење на медиумите идруги мерки.

(4) Погоренаведената документација контролорот ја менува и дополнува кога ќе се направат промени во информацискиот систем и информатичката инфраструктура, а најмалку еднаш годишно врши нејзино оценување, нејзина евалуација и нејзино ажурирање.

1. **Технички мерки**

Обезбедување на опремата на која се врши обработка на личните податоци

Член 11

Контролорот во училиштето е должен да обезбеди примена на технички мерки со кои ќе се обезбедува опремата на која се врши обработка на личните податоци итоа:

- автоматскоодјавување од информацискиот систем и тоа после изминување на определен период на неактивност, период кој не може да биде подолг од 15 минути. За повторно активирање на системот, контролорот треба да биде сигурен дека е обезбедено само овластените лица да пристапуваат со примена на автентикацијата восогласност со овојправилник;
- во случај на одреден број на неуспешни обиди за најавување воинформацискиот систем, кои се во спротивност со политиките за автентикација на контролорот, треба да се обезбеди автоматизирано отфрлање од информацискиот систем. Бројот на не успешни обиди контролорот го определува соодветно на ризикот и природата на работата и работните процеси во однос на обработката на личните податоци. Бројот на не успешни обиди не може да биде повеќе од 5 (пет) последователни не успешни обиди;
- редовно ажурирањена антивирусен софтвер и на софтверскитепрограми;
- инсталиран заштитен sид -firewall и ограничување на овластените порти за комуникација на оние што се строго неопходни за правилна работа на софтверските програми инсталирани на работните станици наконтролорот;
- зачувување на податоците на корисниците на серверите на контролорот за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително со мерки за синхронизација или со резервни дополнителни мерки за заштита врз основа на анализа на ризикот;
- конфигурирани софтверски програми со кои безбедносните ажурирање ќе се вршат автоматски;
- ограничување на опцијата зада може да се приклучуваат преносливите медиуми во системите со примарнаважност. Такви преносливи медиуми се:УСБ, надворешни хард дискови и слично;
- (Data autorun for removable media) односно Исклучен автоматски режим на работа за

преносливите медиуми;

- алатките за далечинската администрација мора да бидат нагодени на начин што претходно задолжително треба да обезбедат согласност од корисникот (овластеното лице) на работната станица пред каква било интервенција на самата работнастаница;
- приклучување на информацискиот систем на енергетска мрежа и тоа преку уред за непрекинатонапојување;
- физичка безбедност;
- нагодување на информацискиот систем кое ќе обезбеди дека корисникот (овластено

лице) на работната станица може да забележи дали се врши далечинска

администрација, како и за тоа кога истата завршила (на пример со прикажување на порака на екранот дека далечинската администрација завршила);

- забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;
- бришење на податоците што се наоѓаат на работна станица која треба да сепредаде;
- во случај работната станица да биде компромитирана, задолжително испитување и

по можност пронаоѓање на изворот, како и каква било трага од упадот во информацискиот систем на контролорот, со цел откривање дали се загрозени и другиелементи;

- ограничување на употребата на софтверски програми што бараат администраторски

права, како и безбедносен надзор на софтверот и хардверот што се користат во системот на контролорот, вклучувајќи и редовно следење на тимот за брза реакција (MKD-CIRT) во однос на неговите предупредувања и совети за ранливостите откриени во софтверот и хардверот;

- ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичнитенедостатоци;
- инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатана ризик, а најмалку еднаш неделнои
- подигнување на нивото на свесност во однос на тоа што овластените лица треба да

се посветат и податоците за контакт на лицата што треба да ги контактираат во случај на инцидент или појава на не обичен настан што влијае на информациите и комуникацијата на системите на контролорот.

Автентикација на овластените лица

Член 12

(1) Контролорот во училиштето ќе ја обезбедува најавата во информацискиот систем при тоа најавата да може да се врши преку единствен идентификатор кој се поврзува само со едно овластенолице.

(2) Единствениот идентификатор контролорот може да го обезбедипреку:

- информација којаединственоовластенотолицеќе ја знае и користи, а тоа е

корисничко име и лозинка за секое овластено лице, при што лозинката треба да биде составена од комбинација на најмалку осум алфанумерички карактери,комбинација од мали и големи букви, симболи, броеви и интерпукцискизнаци;

- нешто што само овластеното лице го поседува (паметна картичка – smart card);
- нешто што овластеното лице го прави (на пример: дигитален потпис)и
- други начини на автентикација кои според најновите технолошки достигнувања.

(3) Автентикацијата на овластените лица, контролорот ја врши најмалку преку еден од наведените начини.

(4) Контролорот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, воспоставува постапки за идентификација и проверка на авторизираниотпристап. Во случај кога проверката се врши врз основа на корисничко име и лозинка, контролорот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите, при што лозинките задолжително автоматски се менуваат во рок кој не може да биде подолг од 3 (три)месеци.

Контрола на пристап до информацискиот систем
Член 13

(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работнизадачи.

(2) Администраторот на информацискиот систем кој е овластен од страна на контролорот на училиштето, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна наконтролорот. Додека пак контролорот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои сеавторизирани.

Обезбедување евиденција за секој пристап
Член 14

(1) Со цел да обезбеди идентификување на секој неовластен, односно измамнички пристап или злоупотреба на лични податоци, како и да се утврди потеклото на овие инциденти, контролорот воспоставува и води евиденција за секој пристап до информацискиотсистемlogs, серверот дизајниран специјално за употреба како сервер за датотеки (file server), базите на податоци, софтверот за управување со документи, софтверот за управување со врски со клиенти ислично.

(2) Евиденцијата треба да ги содржи следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво наавторизација, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиотсистем, податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции.

(3) Операциите кои овозможуваат евидентирање на податоците треба да бидат контролирани од страна на офицеротза заштита на личните податоци и од страна на овластеното лице за заштита на личните податоци.

(4) Во однос на евиденцијата на податоците за пристап, контролорот може да користи и алатки кои податоците ги генерираат во едноставна и лесно разбирлива форма зачитање.

(5) Евиденцијата на податоците за пристап се чува најмалку 5(пет)години.

(6) Офицеротза заштита на личните податоци и овластеното лице за заштита на личните податоцивршат контрола на податоците, најмалку еднаш во месецот и за тоа се изготвува извештај.

(7) Контролорот ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиотсистем и обезбедува заштита на системот за евиденција за пристап до информацискиот систем, од било каков неовластен пристап.

(8) Овластените лица го известуваат раководството лице за било која аномалија или безбедносен инцидент веднаш, а најдоцна во рок од 12 часа од моментот на инцидентот.

(9) Контролорот во ООУ „Пере Тошев“ Росоман ја известува Агенцијата за

заштита на личните податоци за секое нарушување на безбедноста на личните податоци.
(10) Контролорот не смее да ги користи информациите од евиденцијата за пристап до информацискиот систем за било каква цел различна од таа што е предвидена дека информацискиот систем се користи соодветно.

Заштита на внатрешната мрежа
Член 15

(1) Во училиштето, контролорот обезбедува заштита на својата внатрешна мрежа

преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци и тоа најчестопреку:

- управување со Wi-Fi мрежата кое опфаќа користење на најсовремените методи на криптирање (на пример: WPA2, WPA2-PSK и употреба на комплексна лозинка која на определен временски период семенува);
- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (како што се на пример: VoIP, peer to peer,итн.);
- Wi-Fi мрежата која е отворена за употреба на лица кои не се овластени, односно лица кои се надворешни посетители задолжително да биде одвоена од внатрешнатамрежа. Внатрешната мрежа се користи исклучиво од страна на наставниците и директорот;
- во случај на пристап од далечина, задолжително воспоставување на VPN конекција, со задолжителна автентикација на овластеното лице: паметна картичка или уред за генерирање лозинка за еднократна употреба;
- обезбедување на системот со тоа што ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет;
- далечинското одржување задолжително да се изврши преку VPN
- обезбедување на внатрешната мрежа и
- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен sид, прокси сервери, обезведување влезниот сообраќај да биде преку портата 443, блокирање на сите другипристапи.

(2) Контролорот врз основа на анализата на ризикот, покрај наведенитемерки

може да примени и други мерки се со цел да се зајакне заштитата на внатрешнамрежа.

Обезбедување на преносливи медиуми
Член 16

Согласно анализата на ризикот од нарушување на безбедноста на личните податоци во случај на кражба или загуба на преносливите медиуми како што се компјутерот или лап топот, на кои се врши обработка на личните податоци, контролорот во ООУ „Пере Тошев “ Росоман е должен да применува соодветни технички мерки.

Техничките мерките опфаќаат:

- подигање насвеста на овластените лицаза специфичните ризици поврзанисо користење на преносливи медиуми и утврдените процедури за намалување на овиеризици;
- спроведувањена меркитеза правење насигурносна резервна копија или синхронизација на мобилните работни станици, со цел да заштитат од губење на зачуванитеподатоци;
- мерки за криптирање за заштита на мобилни работни станици и медиуми за

мобилно
складирање: лаптоп, УСБ, кабели, надворешни хард-дискови, ЦД-РОМ, ДВД;

- употреба на услуги во облак кој се користи за правење на сигурносни копии само по претходна анализа на нивните услови и безбедноснигаранции;
- поставување на филтер за приватност на екраните на мобилните работни станици штосе користат на јавни места, или употреба на мобилни работни станици со интегриран филтер заприватност;
- ограничување на обемот на податоците кои може да се зачуваат на мобилните работни станици на она што е строго неопходно со дополнителна заштита;
- кога мобилните уреди се користат за собирањеподатоци во движење и шифрирање

на податоците на самиот уред;

- заклучувањенауредот и тоа по неколку минути неактивност и прочистување на податоците собрани веднаш штом се пренесат во информацискиот систем на контролорот и слично.

Обезбедување на серверите
Член 17

(1) Контролорот на училиштето е должен на врвот на својата листа од аспект на примената на технички и организациски мерки да ги има своите сервери на кои се централизира обработката на голема количина на лични податоци.

(2) При тоа контролорот ги применува следните мерки:

- единствено овластените лица кои ги имаат потребните знаења може да имаат пристап до алатките и административни панели на серверите;
- инсталирање на сите важни ажурирања (сите updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (autoupdate);
- правење на сигурносни копии;
- редовна проверка на сигурносните копии;
- правење на back up;
- примена напосебнаполитика за креирање и употреба на лозинките за администраторите на информацискиот систем (на пример: промена на лозинките по секое заминување на администраторот, употреба на повеќе факторскалозинка);
- примена на TLS-протокол со замена на SSL13 или друг протокол што обезбедува шифрирање и автентикација, како минимум за каква било размена на податоци преку интернет и потврда на нејзината соодветна примена преку соодветниалатки;
- употребанаперсонализиранитепрофили и тоа за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација (specific account for each application) во случај кога се врши администрирање на базите на податоци;
- примена на мерки против напади преку инјектирање на SQL код и друго.

Обезбедување на веб-страната
Член 18

(1) Контролорот на својата веб-страна треба да примени технички мерки кои ќе го гарантираат точниот идентитет на страната и доверливоста на информациите што ги

испраќа или ги собира преку веб-страната.

(2) Контролорот работа ја врши преку следните мерки:

- Имплементација на криптографски протокол на веб – страната на училиштето користејќи ја единствено најновата верзија и со проверка на неговата правилна имплементација;
- Задолжителна употреба на криптографски протокол наменет за веб-страната, вклучително и формулари за собирање лични податоци или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавнодостапни;
- Ако се користат колачиња што не се потребни од услугата, контролорот

обезбедува предходна согласност од интернет корисникот откако ќе го извести кориснискот, а пред тоа се депонира колачење;

- Ограничување на портите наменети за комуникација за правилно функционирање На инсталираните апликации. Ако веб серверот прифаќа само врски со HTTPS протокол, само IP мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти треба да бидатблокирани и
- Обезбедување за пристап до алатките и административните интерфејси, при што особено да се ограничи употребата да биде достапна само до овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни.

Член 19

Контролорот на својата веб-страна не треба да ја применува постојаната практика со која го зголемува ризикот од можна злоупотреба, несакана, случајна или намерна неовластена обработка на личните податоци (да не пренесува лични податоци преку URL без примена на протокол за криптирање, или користење на небезбедни услуги, или употреба на сервери кои хостираат бази на податоци или сервери како работни станици, или пак поставување на базите на податоците на серверите директно достапни преку интернет, или споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластенилица).

Превенирање, реакција и санирање на инциденти

Член 20

(1) Контролорот го определува начинот на управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци.

(2) Контролорот врз основа на анализата на ризик утврдува план за управување со континуитет на својот информациски систем, вклучувајќи и список на овластените лица кои се одговорни за превенирање, како и навремено повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на настанат физички или техничкиинцидент.

(3) Исто така контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кој го пријавило, на кого е пријавен и мерките кои се преземени за неговосанирање доколку дојде до управувањето со инциденти. Ги определува постапките кои се применуваат за повторно враќање на

личните податоци и начинот на евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на личните податоци.
(4) Овластените лица, обработувачите и подобработувачите треба да го известат и предупредат контролорот во случај на настанат инцидент.

Обврски и одговорности на администраторот на информацискиот систем и на овластените лица

Член 21

(1) Администратор на информацискиот систем ракува, користи документите и опремата во согласност со закон. Врз основа на спроведената анализа на ризик, контролорот ги определува обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.
(2) Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола. Исто така контролорот задолжително ги информира администраторот и овластените лица за техничките и организациските мерки кои се превземени.

(3) Во извештајот се наведуваат констатираните и предложените мерки за отстранување на тие неправилности.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 22

(1) Контролорот врз основа на анализата на ризикот прави сигурносни копии на личните податоци на редовни временски интервали, со цел да го намали ефектот во случај на нивно непосакувано губење илиоштетување.

(2) Сигурносните копии треба да се прават и тестираат редовно, за што контролорот усвојува План за обезбедување континуитет кој ги предвидува сите можни инциденти.Контролорот прави целосна сигурносна копија, односно full back-up во редовни временски интервали по негова оценка, а најмалку еднаш месечно, применувајќи ги техничките и организациските мерки на безбедно ниво.

(3) Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личнитеподатоциврз основа на анализата на ризикот, обемот и временската динамика на промена на податоците, прави сигурносни копии во интервали кои го минимизираат ризикот врз ефектот на податоците за кои при инцидент би настапило нивно непосакувано губење или оштетување.

(4) Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, за да биде оневозможено било каква модификација. За сигурносните копии контролорот го применува безбедносното ниво на технички и организациски мерки.

Начин на архивирање и чување на податоците

Член 23

(1) Контролорот, во однос на личните податоци за кои се уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, врши архивирање на безбеден начин, особено ако архивираните податоци се чувствителни податоци (посебни категории на лични податоци), или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци, доколку бидаткомпромитирани.

(2) Контролорот определува постапка за управување со архивскиот материјал во

однос на тоа кои податоци треба да се архивираат, како и каде се чуваат и кој, како и под кои услови има пристап донив. Исто така контролорот задолжително донесува соодветен документ „Список со рокови на чување на личните податоци“.

(3) Во документот „Списокот со рокови на чување на личните податоци“ се наведени роковите кои ги има училиштето наведено во Планот за архивски знаци.

Управување со преносливи медиуми
Член 24

(1) Преносливите медиуми на кои се врши обработка на личните податоци контролорот во училиштето обезбедува доказ дека се чуваат на локација до која пристап имаат само овластени лица утврдени од неговастрана.Пренесувањето на медиумите надвор од работните простории на училиштето се врши само со претходно добиено овластување од страна наконтролорот.

(2) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени нанего.

(3) Уништувањето на медиумот се врши на начин кој ќе гарантира дека податоците кои биле снимени на него не можат повторно да бидат реконструирани.Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените личниподатоци.

(4) за уништувањето на медиумот и бришењето на податоците кои биле снимени на медиумот конторлорот изготвува Записник (информациска трага) во кој се содржани сите податоци со кој ќе може да се изврши целосна индентификација на медиумот (на личните податоци кои биле снимени, а сега се уништени).

Физичка безбедност
Член 25

(1) Контролорот на училишето задолжително применува зајакнато ниво на безбедност во однос на просториите во кои се сместени и се чуваат серверите и мрежната опрема преку кои се врши обработка на личните податоци со примена на соодветни мерки кои обезбедуваат дека само лица кои се посебно овластени од контролорот имаат пристап, како и мерки со кои се намалува ризикот од потенцијални закани итоа:

- инсталирање на алармни системи против упад и нивна периодичнапроверка;
- примена на мерки и контроли за превенција од кражба, пожар, експлозии, чад, вода,

прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетнозрачење;

- обезбедување на одделни областиво објектот каде се чуваат серверите според анализата на ризик како што може да биде употреба на посебна контрола за пристап за сервер салата;
- обезбедување безбедност на клучевите и шифрите за аларми кои овозможуваат пристап допросториите;
- список на лица или категории на лица кои се овластени да влезат во просториите каде се чува опрема на која се врши обработка на личнитеподатоци;
- посебна физичка заштита на ИТ-опремата преку специфични методи и тоа:

систем за спречување на пожар, систем за штитење од пожари, ситем за спречување на

поплави, систем за штитење од земјотреси, систем за штитење од електрична енергија, од висок напон на електрична енергија, систем за штитење од климатизација,итн.;

- одржување на просториите за серверите, климатизација, UPS, драјверите и водење наевиденција за пристап до просториите каде што се чуваат серверите кои содржат личниподатоци;
- преиспитување и редовно ажурирајте на дозволите за пристап до заштитените области, како и
- обезбедување надоказ дека само овластените лица можатда пристапат до просториите соограничен пристап.

(2) Заради физичка безбедност меѓусебните права и обврски на контролорот и правното или физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите треба да бидат уредени со договор кој е склучен во писмена форма кој ќе содржи мерки за безбедност на личните податоци согласно со Законот за заштита на личнитеподатоци.

Контрола на информацискиот систем и информатичката инфраструктура
Член 26

Во документацијата за технички и организациски мерки согласно со овој Правилник, задолжително треба да се содржани постапките за овластување на офицерот за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштитана личните податоци и со донесената документација за технички и организацискимерки. Инфромацискиот систем и информатичката инфраструктура на контролорот задолжително подлежат на годишна внатрешна контрола, со цел да се утврши дали заштитата на личните податоци е во согласност со Законот за заштита на лични податоци.

Криптирање на лични податоци
Член 27

(1) Конорлорот врз основа на анализата на ризикот врз основа на природата,
обемот, контекстот и целите на обработка на личните податоци врши криптирање на личните податоци. Секогаш применуванајсовремени технички решенија за криптирање со кои се обезбедува интегритетот, доверливоста и автентичноста на личните податоци.

(2) Во согласност со најсовремените технички решенија, контролорот применува
признати и безбедни алгоритми на криптирање и тоа: SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC користејќи SHA-256, berypt, serypt или PBKDF2 за чување лозинки, AES или AES-CBC за симетрично криптирање, RSA-OAEP v 2.1 за асиметрично криптирање; а воедно обезбедува заштита ма тајните клучеви за криптирањесо ограничувачки права за пристап и посебно креирана безбедна лозинка за пристап.

Управување со обработувачи
Член 28

(1) Контролорот на училиштето е должен да воспостави процес на управување при користење на услуги за обработка на личните податоци од страна на обработувачи, а со цел да се воспостават соодветни процедури за одлучување при изборот на обработувачот, управување со обработката на личните податоци, како и исполнување на договорените обврски и одговорности од страна на обработувачот.

(2) Контролорот е должен да применува процедура за одлучување за избор на обработувач со која задолжително ќе предвиди:
- Анализа на потенцијалните обработувачи во однос на нивните технички и организациски мерки за обезбедување на гаранција дека обработката на личните податоци ќе се одвива во согласност со барањата предвидени во прописите за заштита на личните податоци и
- Анализа на ризиците врз работењето на контролорот што можат да произлезат при обработката на личните податоци од страна наобработувачите.

Ангажирање на обработувачи
Член 29

(1) Во случај кога контролорот ќе одлучи да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувачот, должен е да обезбеди потврда дека личните податоци се обработуваат под негов надзор и дека личните податоци мора да бидат обработувани со безбедносни гаранции.

(2) Контролорот може да пренесе работи само на обработувач кој може да обезбеди доволно гаранции, особено во однос на потребното знаење од областа на заштитата на личните податоци, сигурноста и ресурсите.

(3) Меѓусебните права и обврски на контролорот и обработувачот во училиштето мора да бидат уредени со договор при што контролорот пред да го склучи договорот е должен да побара од обработувачот (давател на услугата), да му ја презентира својата безбедносна политика во однос информацискиот систем и информатичкта инфраструктура. Безбедносната политика треба да содржи податоци со кои ќе се гарантита безбедноста на личните податоци (пр.дали и како се врши криптирање на податоците според нивната чувствителност; дали и како се врши криптирање на пренос; постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;гаранции во однос на следливост; управување со правата напристап, автентификација и други мерки).

Член 30

Договорот за уредување на меѓусебните права и обврски на контролорот и обработувачот треба да содржи одредби особено за:

- предметот, должината и целта на обработката на личните податоци;
- обврските во однос на доверливоста на доверените лични податоци;
- минималните стандарди за автентикација на овластените лица;
- обврските за обработувачот да преземе технички и организациски мерки со цел да обезбеди безбедност на обработката на личните податоци;
- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

2. <u>Организациски мерки</u>

Организациски мерки за безбедност наличните податоци
Член 31

(1) Контролорот е должен да обезбеди соодветни организациски мерки за безбедност на личните податоци врз основа на резултатите од анализата на

спроведениот ризик, а особено даобезбеди:

- ограничен пристап со идентификација за пристап до личните податоци;
- организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и другиизвори;
- уништување на документи по истекот на рокот за нивно чување;
- почитување на технички упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци и
- мерки кои се однесуваат за физичкасигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци.

(2) Вработеното лице кое ги врши работите за човечки ресурси кај контролорот го известува администраторот на информацискиот систем за вработување или ангажирање на секое овластено лице со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да бидат избришани корисничкото име и лозинката за да не може да ги користат.

Информирање и едуцирање за заштитата на личните податоци

Член 32

(1) Лицата кои се вработуваат или се ангажираат кај контролорот пред нивното отпочнување со работа мода да се запознаат со прописите за заштита на личните податоци, како и со донесената документација за технички и организацискимерки, односно мора да бидат запознаени со Законот за заштита на лични податоци.

(2) За лицата кои се ангажираат кај контролорот за извршување на некоја работа во договорот за нивно ангажирање мора да бидат наведени обврските и одговорностите во врска со заштитата на личните податоци.

(3) Контролорот пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личнитеподатоци, како и за сите мерки кои се должни да ги оставруваат при вршењето на работата, а се однеуваат за заштитата на личните податоци согласно законските прописи.

(4) Лицата кои се вработуваат или пак се ангажираат кај контролорот пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци. Изјавата задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кајконтролорот.

(5) Исто така контролорот задолжително врши континуирано информирање и едуцирање на раководството и овластените лица за непосредните обврски и одговорности за заштита на личнитеподатоци.

Пристап до документите

Член 33

Пристапот до документите треба биде ограничен само за овластени лица на контролорот. За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои сепристапува.

Чување на документи

Член 34

(1) Чувањето на документите треба да се врши на начин што ќе се применат соодветни механизми за попречување на секое неовластеноотворање.

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап додокументите. Ако документите не се чуваат заштитени на определен начин тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Правилото „ЧИСТО БИРО“

Член 35

Контролорот задолжително го применува правилото „ЧИСТО БИРО“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица. Тоа значи дека при крајот на работното време потребно е сите документи да бидат тргнати од бирото и да бидат ставени во плакарите (ормарите) кои се чуваат под клуч. До клучот пристап имаат само овластените лица од страна на контролорот.

Уништување на документи

Член 36

(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно тие документи да не можат да бидатупотребливи.За ова се составува Записник кој ги содржи сите податоци за целосна индентификација на документот кој се поништува.

(2) Доколку станува збор за уништување на поголем дел од документите, или уништување на документите на кои им поминал рокот за уништување тоа се прави на начин што се известува Архивот на Република Северна Македонија и понатаму уништувањето се спроведува кај надлежен орган.

Начин на чување на документите

Член 37

(1) Плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап додокументите.

ВИСОКО НИВО

1.Технички мерки

Дополнителни мерки

Член 38

Контролорот на ООУ„Пере Тошев“ Росоман врз основа на анализата на ризикот воведува и применува дополнителни мерки за безбедност на личните податоци со кои ќе демонстрира дополнителна усогласеност со прописите и добрите практики за заштита

на личните податоци кои се во согласност со законските прописи.

Управување со лозинки
Член 39

(1) Контролорот на училиштето е должен да користи алатки за управување со лозинки со кои обезбедува различни лозинки за секоја услуга, или софтверска програма, соодветно се чуваат, при што за пристап до сите лозинки обезбедува главна лозинка (master password), која треба да биде зајакнато комплексна, односно да биде составена од комбинација на најмалку 12 алфанумерички карактери мали и големи букви, симболи, броеви и специјални интерпукциски знаци и да се менува во период не подолг од 30дена.

(2) Контролорот во согласност со анализата на ризикот, за одредени овластени лица администраторот на информацискиот систем или лицата кои ја креираат и користат главна лозинка (master password), може да изврши дисперзија на ризикот преку управување со лозинката со дополнителен фактор согласно правилото n-2.

(3) Информацијата за лозинката да биде поделена на две или повеќе лица кои заеднички ќе се најавуваат на начин што секој ќе знае само дел од информацијата која ја сочинува лозинката, или едно овластено лице ја знае лозинка, а друго ја поседува и употребува паметна картичка-smard card.

(4) На тој начин ќе се обезбеди соодветна заштита на личните податоци, која ќе биде и мора да биде во согласност со законските прописи.

Сертификација за заштита на лични податоци
Член 40

(1) Контролорот, покрај внатрешната контрола согласно со овој Правилник, а на доброволна основа, може да изврши и проверка на процесите и интерните документи за заштита на личните податоци заради сертификација на процесите преку кои се обработуваат личните податоци, со цел да демонстрира усогласеност со прописите за заштита на личните податоци при операциите на обработка.

(2) Сертификацијата се врши од Агенцијата за заштита на лични податоци или од сертификациони тела согласно со Зконот за заштита на личните податоци.

Управување со преносливи медиуми
Член 41

(1) Контролорот е должен да воспостави систем за евидентирање на медиумите кои се примаат со цел да се овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием намедиумот.

(2) Одредбитеод овој членќе сепримену ваат иза евидентирање на медиумите кои се испраќаат од страна наконтролорот.

(3) За пренесените медиуми надвор од работните простории на контролорот треба да бидат преземени сите потребни неопходни мерки за да се спречи неовластено обработување на личните податоци снимени нанив.

Тестирање на информацискиот систем
Член 42

Контролорот задолжително врши тестирање на информацискиот систем пред

неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува безбедност на личните податоци согласно со прописите за заштита на личните податоци.Тестирањето на информацискиот систем се врши преку обработка на документи кои содржат имагинарни лични податоци.

Пренесување на медиуми
Член 43

Медиумите можат да се пренесуваат надвор од работните простории само ако личните податоци се криптирани или ако личните податоци се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, односно претпознатливи, при што само администраторот на информацискиот систем или лице овластено од администраторот може да ги декриптира, односно да ги прочита.

Сертификациони постапки
Член 44

Контролорот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги.

Пренесување на личните податоци преку мрежа за електронски комуникации
Член 45

Личните податоци можат да се пренесуваат преку мрежата за електронски комуникации само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи припреносот. Само на овој начин-крипирање, ќе бидат заштитени личните податоци.

2.Организациски мерки

Копирање и умножување надокументите
Член 46

(1) Копирањето или умножувањето на документите може да се врши единствено од страна на овластени лица определени од страна на контролорот во кои задолжително при копирањето и умножувањето на документите треба да се придржува до мерките и начинот на копирањето и умножувањето на документите без да се поврди правото на заштита на личните податоци.

(2) Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на личниподатоци.

Пренесување на документи
Член 47

Во случај на физички пренос на документите контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат.

ПРЕОДНИ И ЗАВРШНИОДРЕДБИ

Период на прилагодување
Член 48

Овој правилник влегува во сила со денот на донесувањето, ќе се применува по истекот на осум дена од денот на објавување на огласна табла на ООУ „Пере Тошев“ Росоман.

16.12.2021 година

Претседател на Училишен Одбор
на ООУ„Пере Тошев“ Росоман

_____

Милован Андонов