СРЕДНО УЧИЛИЩЕ „МАКСИМ РАЙКОВИЧ“

гр. Лясковец 5140, ул. „Манастирска“ №1, тел. 0619/ 2 20 95, факс 0619/2 20 95
e-mail: sou_mr@mail.bg, www.sou-mrlc.com

ИНСТРУКЦИЯ

(ВЪТРЕШНИ ПРАВИЛА)

за мерките и средствата за защита на личните данни, събирани, обработвани, съхранявани и предоставяни от

СУ „МАКСИМ РАЙКОВИЧ“ – гр. ЛЯСКОВЕЦ

Тази Инструкция (вътрешни правила) се отнася до всички служители, работници и лица, наети по договори в СУ „МАКСИМ РАЙКОВИЧ“, като с подписване на съответен трудов/граждански договор служебно правоотношение за наемане на работа/за извършване на определени дейности служителят/работникът/лицето се съгласява да се съобразява с текста на Инструкцията и да изпълнява разпоредбите на този документ.

ПРЕАМБЮЛ

§1. СУ „МАКСИМ РАЙКОВИЧ“, с ЕИК: 000122417 с адрес, гр. Лясковец, ул. „Манастирска“ №1, тел.: 0619/22095, Е-мейл адрес: sou_mr@mail.bg, представлявано от Даниела Арабаджиева – ДИРЕКТОР, **е администратор на лични данни** съобразно изискванията на Закона за защита на личните данни.

§2. СУ „МАКСИМ РАЙКОВИЧ не притежава сертификати съгласно изисквания на ISO стандарти или други, свързани със сигурност на информацията.

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Тази Инструкция урежда организацията и вътрешния ред на СУ „МАКСИМ РАЙКОВИЧ“ наричано по-нататък за краткост, „СУ“, в качеството му на администратор на лични данни, както и нивото на технически и организационни мерки, предвидени и предприети при обработването на лични данни, и допустимия вид защита.

Чл. 2. Инструкцията е изготвена в съответствие с разпоредбите на *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните)*, *Закона за защита на личните данни (ЗЗЛД)* и цели защита на интересите на контрагентите, потребителите – физически лица и физическите лица, представляващи юридическите, както и на служителите на СУ „МАКСИМ РАЙКОВИЧ“, и на всякакви лица, наети от СУ „МАКСИМ РАЙКОВИЧ“ на граждански договор за извършване на определени услуги и дейности, от незаконосъобразно и недобросъвестно обработване на личните им данни.

Чл. 3. За целите на тази Инструкция използваните по-долу понятия имат следното значение:

1. „Администратор на лични данни“: СУ „МАКСИМ РАЙКОВИЧ“, което самостоятелно или чрез възлагане на друго лице обработва лични данни, като определя надлежно целите и средствата за обработването.

2. „Лице по защита на личните данни“: длъжностно лице, притежаващо необходимата компетентност, което е упълномощено от СУ „МАКСИМ РАЙКОВИЧ“ със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на минимално

необходимите технически и организационни мерки за защита на личните данни при тяхното обработване за съответния регистър.

3. „Лични данни“: всяка информация, отнасяща се до контрагентите, доставчиците, потребителите и всякакви бизнес партньори (физически лица и физическите лица, представляващи юридическите лица) на СУ „МАКСИМ РАЙКОВИЧ“, както и тази, свързана със служителите и работниците на СУ „МАКСИМ РАЙКОВИЧ“, които са идентифицирани или информация, чрез която същите могат да бъдат идентифицирани пряко или непряко посредством идентификационен номер или един, или повече специфични признаци.

4. „Обработване на лични данни“: всяко действие или съвкупност от действия, които СУ извършва по отношение на личните данни с автоматични или неавтоматични средства (така напр. събиране, записване, организиране, групиране, съхраняване, адаптиране, актуализиране или коригиране, изменение, възстановяване, консултиране употреба, разкриване чрез предаване или предоставяне, разпространяване, комбиниране, блокиране, заличаване, унищожаване и др.).

5. „Оператор на лични данни“: физическо или юридическо лице, на което е възложено с длъжностна характеристика, заповед или договор да събира, изменя, актуализира, складира, поддържа, употребява и/или използва във връзка с обработването на документация от името на Администратора, съхранява, архивира, заличава и т.н., лични данни в съответния регистър.

6. „Ограничен достъп до лични данни“: достъп на физическите лица, действащи под ръководството на лицето по защита, отговарящо за всеки отделен регистър, във връзка с обработката на личните данни от съответния регистър.

7. „Потребител на лични данни“: служител, работник или трето лице, което по длъжност, заповед, договор или по силата на тези вътрешни правила има право на достъп или му е възложен достъп до определени лични данни (включително интервюиращите при интервюта за наемане на работа, планове за развитие и обучения, и др.).

8. „Регистър на лични данни“ („Регистър“): всяка структурирана съвкупност от лични данни, достъпна по определени критерии, съобразно вътрешните документи на СУ „МАКСИМ РАЙКОВИЧ“, която може да бъде централизирана или децентрализирана и е разпределена на функционален принцип.

9. „Специални категории лични данни“: лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

10. „Специфични признаци“: признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето, титуляр на лични данни.

11. „Съгласие на физическо лице“: всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява тези данни да бъдат обработвани.

Чл. 4. (1) СУ „МАКСИМ РАЙКОВИЧ“ обработва само законно събрани лични данни, необходими за и относими към конкретни, точно определени и законни цели. Личните данни, които СУ „МАКСИМ РАЙКОВИЧ“ събира и обработва следва да бъдат точни, коректни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни, неверни или несъответстващи на, респективно надхвърлящи, целите, за които се обработват, както и в случаите, когато са изпратени погрешка или друга причина, несъответстваща на волята на субекта на лични данни същите да бъдат обработвани от СУ „МАКСИМ РАЙКОВИЧ“.

(2) Като администратор на лични данни СУ „МАКСИМ РАЙКОВИЧ“ поддържа личните данни във вида и формата, които позволяват идентифициране на самоличността на физическите лица, за срок не по-дълъг от предвидения в тези Вътрешни правила и който е необходим за изпълнение на целите, за които личните данни се обработват. След изтичането на съответния необходим за изпълнение на целите срок данните биват надлежно унищожавани, съгласно реда, уточнен в Процедура за унищожаване на лични данни или биват анонимизирани, т.е. субектите, за които се отнасят не подлежащите на съхранение лични данни, биват де-идентифицирани и преместени в архив.

(3) СУ „МАКСИМ РАЙКОВИЧ“ спазва принципа за забрана на обработване на специални категории лични данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход; разкриване на политически, религиозни или философски убеждения; членство в политически партии или организации; сдружения с религиозни, философски, политически или синдикални цели; лични данни, които се отнасят до здравето, сексуалния живот или до човешкия геном), като изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от ЗЗЛД.

(4) Когато СУ „МАКСИМ РАЙКОВИЧ“ обработва специални категории лични данни във връзка с наличие на законодателно изискване за извършване на тази обработка, заложено в нормативен акт на друга държава, извършването на обработката следва да бъде предшествано от предварително одобрение на Длъжностното лице по защита на личните данни.

Чл. 5. Обработването на личните данни от СУ „МАКСИМ РАЙКОВИЧ“ се извършва на базата на едно или няколко от следните основания:

(1) Обработването е необходимо за изпълнение на нормативно задължение, чийто адресат е Администраторът;

(2) Обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на такъв договор и предприети по искане на това физическо лице;

(3) Физическото лице, за което се отнасят данните, е дало своето изрично съгласие за една или повече конкретно зададени от Администратора цели;

(4) Контрагентите и изобщо посетителите (физически лица и физическите лица, представители на юридическите) и служителите/работниците/лицата, назначени на договор в СУ „МАКСИМ РАЙКОВИЧ“ се идентифицират с оглед осигуряване на достъп до определени помещения, посредством официален документ за самоличност или друг документ, който ги идентифицира;

В тази връзка, документът за самоличност не се копира, а оригиналът се връща на субекта на лични данни, освен в случаите на изпълнение на задължение по реда на Закона за мерките срещу изпирането на пари или ако е приложимо съобразно изискванията на друга императивна разпоредба;

(5) Обработването е необходимо за защита живота и здравето на физическите лица, чиито данни се събират или на друго физическо лице;

(6) Обработването е необходимо за изпълнение на задача за защита на обществения интерес;

(7) Обработването е необходимо за защита легитимните интереси на Администратора, в случай че тези се ползват с преимущество пред основните права и свободи и свързани с тях интереси на пълнолетното физическо лице – субект на обработваните лични данни. Легитимните интереси на Администратора включват по-конкретно, но не ограничено, следните случаи:

- Извършване на (предварителна) оценка на клиенти, доставчици и партньори, включващо обработка на лични данни, които са необходими във връзка с (предварителна) оценка на изброените, включително потвърждаване на тяхната идентичност (тази дейност може да включва използване ресурсите и на трети лица); провеждане на анализи и проучвания на базата на публично достъпна информация в поддържани регистри – кредитни, търговски и всякакви други;
- Сключване и изпълнение на договори с клиенти, доставчици и партньори, включително извършване на дейности по сканиране и/или видео наблюдение (например с цел получаване на достъп до помещения или системи на СУ „МАКСИМ РАЙКОВИЧ“), запис и финансово уреждане на предоставени услуги на и от СУ „МАКСИМ РАЙКОВИЧ“;
- Разработване и усъвършенстване на административни услуги, в това число извършване на анализи, проучвания и др.;

- Поддържане на връзка с потребителите на административни услуги и информационни активности: Това основание включва дейности като поддържане и подобряване на контактите с клиенти, доставчици на услуги и партньори, включително извършване на анализи на пазара, изготвяне на стратегии, в това число такива за онлайн активности (напр. информации, анализ на използваните услуги, предоставяни от СУ „МАКСИМ РАЙКОВИЧ“ офлайн и/или онлайн, на уебсайта на СУ „МАКСИМ РАЙКОВИЧ“);
- Изпълнение на проекти, вътрешно управление и докладване, включващо вътрешно управление на активите на СУ, провеждане на одити и ревизии, мониторинг и преразглеждане на взаимоотношенията на СУ с доставчици на услуги и партньори и други физически лица;
- Здраве и сигурност - Това основание включва защита на интересите на СУ, неговите служители, клиенти, доставчици и бизнес партньори и извършване на дейности, включващи защита здравето и сигурността на горепосочените лица, защита на активите на СУ, верификация статуса на учениците, доставчиците и бизнес партньорите и съответно техните права за достъп в СУ;
- Осигуряване на съответствие със законодателството - това основание е адресирано до обработката на лични данни чрез извършване на определени действия, необходими за постигане на съответствие с нормативно наложено задължение, включително разкриване на лични данни по искане на публични органи, в това число данъчни, трудови и други органи.

Когато е налице възможност за извършване на обработка на лични данни на база едно от горепосочените в чл. 7 основания (Легитимен интерес), СУ следва да се консултира с Длъжностното Лице по Защита на Личните Данни в предварителен порядък с цел уточняване на процеса по обработка на лични данни на това основание.

Чл. 6. (1) Когато и доколкото обработването на лични данни на физическото лице – субект на личните данни, се извършва въз основа на съгласие, физическото лице изразява своето съгласие относно обработването свободно и информирано.

(2) Физическото лице има право по всяко едно време, докато личните му данни биват обработвани от СУ „МАКСИМ РАЙКОВИЧ“ (на основание валидно дадено съгласие), да поиска блокирането или унищожаването (изтриването) им/на част от тях, в случаите, в които оспорва тяхната точност или обработването им е незаконосъобразно и може да оттегли даденото съгласие, доколкото обработването на съответните, отнасящи се до него, лични данни, е изпълнило целите, за които същите са били събирани.

(3) В случаите, когато данните не са получени непосредствено от физическото лице – субект на данните или с неговото изрично съгласие, СУ „МАКСИМ РАЙКОВИЧ“ го информира за следното,

доколкото субектът не разполага вече с тази информация и доколкото това няма да представлява неоправдано и непропорционално усилие за училището:

- бизнес целите и правното основание, за които данните за лицето се обработват;
- срока на обработването на тези данни;
- категориите и вида предоставени данни и техния източник, в това число и публичните източници;
- когато е приложимо, категориите получатели, на които ще бъдат предоставяни данните;
- данни за контакт с Длъжностното лице по защита на личните данни в СУ „МАКСИМ РАЙКОВИЧ“.

Чл. 7. (1) Всяко лице, чиито лични данни се обработват от СУ „МАКСИМ РАЙКОВИЧ“, има право на достъп до личните си данни, за което подава писмено заявление до Длъжностното лице по защита на лични данни или до официалния представител на училището, а когато не е предварително известен към кое лице да насочи искането си – до общо известния и-мейл адрес на СУ, а Администраторът има задължение своевременно да осигури предаването на тази молба на отговорен служител, който да се погрижи за навременното, по възможност незабавно, обработване на запитването и надлежното предоставяне на информация в съответствие с изискванията на закона.

Писмено заявление следва да бъде подадено на хартиен носител или по електронен път, лично или чрез упълномощено лице.

(2) Подаването на заявление и упражняването от страна на физическото лице на правата по чл.7 се извършва безплатно. Администраторът има право да наложи такса в приемлив и разумен размер, когато искането е явно неоснователно или прекомерно като напр. поредно заявление за достъп без основателна причина, и/или се отнася до предоставянето на допълнително копие от вече разкрита информация.

Таксата се изчислява въз основа на административните разходи, свързани с предоставянето на исканата информация.

Заявлението, независимо дали е подадено по обикновена или електронна поща, се завежда в входящия дневник на СУ „МАКСИМ РАЙКОВИЧ“.

(3) Достъп до данните на лицето се осигурява под формата на:

* писмена справка;

* преглед на данните от самото лице или от изрично упълномощеното от него такова;

* предоставяне на копие от исканата информация, включително в машинно-четаем формат, ако същата се обработва чрез автоматизирани средства;

* предоставяне на исканата информация по електронен път, освен в случаите, когато това е забранено от закон;

* предоставяне на копие от исканата информация на предпочитан носител, освен в случаите, когато това е забранено от закон.

(4) При подаване на искане за осигуряване на достъп представляващият Администратора за всеки отделен регистър разглежда заявлението за достъп и/или разпорежда на оператора на лични данни за съответния регистър да осигури искания от лицето достъп в предпочитаната от заявителя форма. Длъжностното лице по защита на лични данни може да даде препоръки във връзка със спазването на подходяща форма за отговора или други насоки, ако намери за необходимо. Срокът за разглеждане на заявлението и произнасяне по него е 30-дневен от деня, следващ подаване на искането, без ненужно забавяне. Решението се съобщава писмено на заявителя лично срещу подпис или по пощата с обратна разписка.

Когато данните не съществуват или не могат да бъдат разкрити с оглед определено правно основание или законово задължение на Администратора, на заявителя се отказва достъп до тях с мотивирано решение.

(5) Отказът за предоставяне на достъп може се обжалва от лицето пред посочен в писмото-отговор орган и срок.

(6) Достъп до личните данни на лицата, съдържащи се на технически носител, има само лицето по защита на лични данни за съответния регистър и/или лицето, действащо под негово ръководство при обработване на лични данни, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има служителят, определен от директора на СУ.

(7) Предоставянето на информация се осъществява съобразно „Процедура по предоставяне на информация на физически лица при подаване на заявления и в съответствие с правото на пренос на данни, във връзка с разпоредбите на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година, 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 (GDPR)“.

Чл. 8. (1) Администраторът не изключва употребата на приложения, които подпомагат/осигуряват вземането на автоматизирани решения на база лични данни (профилиране), дотолкова, доколкото решенията, които биват вземани, не са изцяло и само негативни за съответните физически лица. В такъв случай дадено решение за съответното физическо лице не може да бъде основано само на автоматизираните приложения.

(2) Ограничението по горната ал. 1 не се прилага, когато:

1. Използването на автоматизирани приложения е необходимо за изпълнение на задача, чието изпълнение е свързано с нормативно задължение на Администратора;

2. Автоматизираното решение е взето от Администратора за целите на подписване/изпълнение/управление на договор, когато физическото лице е поискало да влезне в такива договорни отношения с Администратора;
3. Физическото лице е дало своето изрично съгласие,

Като администраторът все пак съблюдава и защитава легитимните интереси на субекта на извършваното профилиране.

Чл. 9. Всички служители и работници в СУ „МАКСИМ РАЙКОВИЧ“ при постъпване на работа с подписване на трудов, респективно на граждански договор/служебно правоотношение, се задължават да спазват конфиденциалност по отношение на цялата база данни, съдържаща включително информация за самите служители и работници, както и контрагенти и потребители на СУ „МАКСИМ РАЙКОВИЧ“, а също и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения и ангажименти.

Глава втора

ПОДДЪРЖАНИ РЕГИСТРИ

Чл. 10. СУ „МАКСИМ РАЙКОВИЧ“ поддържа следните регистри:

1. „Персонал“;
2. „УЧЕНИЦИ“
3. „Доставчици“
4. „Видеонаблюдение“

Чл. 11. За защита на личните данни в изрично посочените регистри в чл. 10 от тази Инструкция от тяхното случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване, СУ „МАКСИМ РАЙКОВИЧ“ организира и предприема конкретни технически и организационни мерки, съобразени със съвременните технологични постижения и с рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Глава трета

ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ

Чл. 12. СУ събира и обработва лични данни автоматизирано и не автоматизирано /на хартиен носител/.

Чл. 13. (1) Данните в СУ „МАКСИМ РАЙКОВИЧ“, обработвани електронно, се съхраняват в електронни системи, собственост на СУ. Сървърите, на които се съхраняват данни от системите са позиционирани на територията на ЕС.

Достъпът до системите се осъществява през електронни компютърни устройства, разположени в офисните помещения на СУ „МАКСИМ РАЙКОВИЧ“. Отдалечен достъп до сървърите е наличен. Личните данни на електронни носители могат да бъдат достъпни чрез учредяване на отдалечен достъп на съответния служител.

(2) Достъпът до базата данни, поддържана от СУ „МАКСИМ РАЙКОВИЧ“, е ограничен. Системния администратор извършва действия по поддръжка на системите чрез своя отделен индивидуален администраторски акаунт.

Чл. 14. (1) СУ „МАКСИМ РАЙКОВИЧ“ обработва лични данни и във вътрешната Е-мейл система. Достъпът до системата е ограничен пароли.

(2) В случай че в системата попадне информация, съдържаща специални категории лични данни, същата незабавно се премества на сигурно място в базата данни.

(3) Използваната Е-мейл система е в mail.bg/abv.bg

Чл. 15. (1) СУ „МАКСИМ РАЙКОВИЧ“ обработва данни за ученици, родители, служители и външни лица и чрез поддържаната телефонна система. Част от обработваната през телефонните линии информация може да включва и лични данни.

(2) Провежданите телефонни разговори не се записват. При необходимост разговорите се отразяват в ежедневна справка на хартиен носител, посочвайки две имена, телефонен номер и адрес на физическото лице, което е направило обаждането, както и въпроса/темата на разговора.

(3) Канцеларията е основната структурна единица в СУ „МАКСИМ РАЙКОВИЧ“, която ръководи и управлява дейностите, свързани по-конкретно, но не само с поддръжка и обновяване на софтуерни продукти, обновяване на техниката и оборудването, създаване и поддръжка на базата данни, поддръжка и актуализация на интернет сайта, осигуряване на лицензирани софтуерни продукти и др. в съгласуване със Системния администратор.

(4) Системния администратор се грижи за правилното функциониране на персоналните компютри, навременното отстраняване на софтуерни и хардуерни проблеми, съхранението на всички получени лицензии за софтуерни продукти и т.н. При работа с данните се използват софтуерни продукти, които са адаптирани към специфичните нужди на Администратора на лични данни – СУ „МАКСИМ РАЙКОВИЧ“.

(5) В СУ „МАКСИМ РАЙКОВИЧ“ е одобрен списък на използваните софтуерни продукти. В случай на необходимост от нов софтуерен продукт системният администратор предлага закупуването му и извършва всички дейности по инсталиране и имплементиране в системите на СУ „МАКСИМ РАЙКОВИЧ“ след получаване на необходимия лиценз.

(6) В изпълнение на разпоредбите на Закона за националния архивен фонд, СУ „МАКСИМ РАЙКОВИЧ“ е разработила и прилага ефективно вътрешни правила, които регламентират реда за организирането, съхраняването и използването на документите, експертизата, обработването и предаването на документите в Държавен архивен фонд в държавните архиви, след изтичане на сроковете им за съхранение.

Глава четвърта

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА, СРОКОВЕ ЗА СЪХРАНЕНИЕ, НИВА НА ДОСТЪП

Раздел първи – ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл. 16. (1) Администраторът е предприел съответни технически и организационни мерки за защита на личните данни, както следва:

1. Програмно-технически – защита с индивидуални потребителски профили с пароли за достъп за всеки служител и работник, както и други средства за защита при пренасяне на информацията, в това число надеждна и защитена идентификация на изпращача и на получателя на информацията, осигуряване на конфиденциалност, интегритет на пренасяната информация, защита от вируси, копия за възстановяване за срока, определен за съхранението на данните за всеки отделен регистър, стандартна криптографска защита на операционните системи, съобразена с най-новите технологични възможности, на системите за управление на бази данни, както и на комуникационното оборудване, забранен достъп до информацията, намираща се се на сървъра, чрез отдалечен достъп посредством интернет;
2. Физически – система от мерки по защита на сградите, помещенията и съоръженията, в които се обработват и съхраняват лични данни и контрол върху достъпа до тях, в това число чрез чип-карти за достъп до помещения, ключалки, обособени шкафове, включително шкафове със заключване, метални каси, пожаро-известителна система, оборудване в помещенията, отговарящо на нуждите, целите и нивото на въздействие на обработване на лични данни;
3. Организационни и административни (документални) –определение от директора на СУ „МАКСИМ РАЙКОВИЧ“; псевдонимизация на определени категории лични данни; определяне на регистрите, които ще се поддържат и на електронен носител, регламентиране на достъпа до регистрите, определяне на срокове за съхранение и процедури за унищожаване на лични данни; определяне на правила за управление и съхранение на досиета, отнасящи се до (бъдещ) персонал; определяне на правила за архивиране на документи както на хартиени, така и на електронни носители; регулярни обучения на отговорните лица – служители на СУ „МАКСИМ РАЙКОВИЧ“, по въпросите за защита на личните данни, въз основа на законодателството и практика в областта;

4. Нормативни – предвидени в законови и подзаконови нормативни актове, в това число и наличие на съгласие за поемане на задължение за неразпространение на лични данни от лицата, които ги обработват;
5. Следване на принципа *Privacy by design* – СУ „МАКСИМ РАЙКОВИЧ“ въвежда както към момента на определянето на средствата за обработване, включително и най-вече при разработването на нови бизнес модели/бизнес процеси/продукти/системи за работа, така и към момента на самото обработване, подходящите, предвидени в настоящата Инструкция, технически и организационни мерки за защита на личните данни, в това число псевдонимизация;
6. Следване на *de minimis* принципа - СУ „МАКСИМ РАЙКОВИЧ“ ограничава обработването на лични данни до такива, които са разумно адекватни на и относими към конкретното приложимо основание, на база на което се извършва обработката и което кореспондира на бизнес целите на тази обработка. Доколкото лични данни не се явяват необходими за приложимото към конкретната обработка основание и бизнес цели, т.е. надхвърлят ги, СУ прави всичко възможно да унищожи тези лични данни.

(2) По отношение на личните данни от поддържаните регистри се прилагат и допълнителни мерки, детайлно посочени съответните раздели, отнасящи се до тях в тази Инструкция.

Раздел втори – СРОКОВЕ ЗА СЪХРАНЕНИЕ

Чл. 17. (1) Сроковете за съхранение на лични данни са, както следва:

1. Персонал - 50 години по отношение на ведомостите за работни заплати и възнаграждения и 5 години по отношение на всички останали документи, различни от ведомости за заплати и възнаграждения, част от трудовото досие/от досието на служителя по гражданско правоотношение. Този срок започва да тече след отпадане на договорното основание, за което се съхраняват личните данни на лицата;
2. УЧЕНИЦИ
   - Дневници – 5 (пет) години;
   - Лични картони – неопределен срок /постоянен/ - собствен архив;
3. За Регистър „Видеонаблюдение“ – 30 дни.

(2) СУ „МАКСИМ РАЙКОВИЧ“ следва, за целия срок на съхранение на личните данни по отделните регистри, да спазва технологията за безопасно поддържане и съхранение, обновяване, заличаване, унищожаване и т.н., на лични данни.

(**3)** Когато в процедура по подбор СУ „МАКСИМ РАЙКОВИЧ“ е изискала да се представят оригинали или нотариално заверени копия на документи, удостоверяващи физическа и психическа годност на кандидата за работа, 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. В такъв случай СУ „МАКСИМ РАЙКОВИЧ“ връща документите по начина, по който са подадени.

Раздел трети – НИВА НА ДОСТЪП

Чл. 18. (1) Право на достъп до данните имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично писмено искане;
2. Директор на училището, заместник-директори, ЗАТС, Счетоводство, Системен администратор и други лица, определени със заповед на директор – при изпълнение на правомощията им по Кодекса на труда, Кодекса за социално осигуряване, Данъчно-осигурителния процесуален кодекс, Закона за движение по пътищата, Закона за защита на личните данни, тези Вътрешни правила и др.;
3. Държавни органи, надлежно легитимирали се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието и имената на лицата, на които е необходимо да се осигури достъп до личните данни;
4. Лицето по защита на личните данни.
5. Служба по трудова медицина;
6. Външни лица в случай на необходимост от поддръжка на IT системите в СУ „МАКСИМ РАЙКОВИЧ“.
7. Представители, в това число и служители на дружество, което предоставя услуги по живото застраховане на всички физически лица, чиито лични данни се обработват;
8. Представители, в това число и служители на дружество, което по силата на договор извършва съхранение на архив на документацията;
9. Представители, в това число и служители на дружество, с което Администраторът организира бизнес пътувания – командировки.
10. Представители, в това число и служители на дружество, което предоставя куриерски услуги на Администратора.

(2) Данните от регистъра могат да се предават на трети лица само с изричното съгласие на субектите на лични данни и при спазване на останалите условия, предвидени в действащото българско законодателство. Данните от регистрите могат да бъдат предавани по електронен път, само ако са надлежно защитени в съответствие с инструкциите на Длъжностното лице по защита на личните данни.

Изрично е забранено:

1. Да използват личните данни при спазване разпоредбите на Кодекса на труда;
2. Да използват личните данни в изпълнение на задълженията си по Закона за здравното осигуряване, Кодекса за социално осигуряване;
3. Да не изнасят и съхраняват личните данни извън специално определените за целта места, регламентирани с режим на специален достъп;

Коментар [EPCL1]: Изброяването тук отново е примерно и подлежи на евентуална корекция

4. Да не използват личните данни по нерегламентиран начин /фалшифициране и друг вид злоупотреба/.

Чл. 19. (1) Право на достъп до данните в регистър „Видеонаблюдение“ имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
2. Лицето по защита на лични данни за регистър „Видеонаблюдение“ и други лица определени със заповед на Директора;
3. Лицата, ангажирани с техническа поддръжка на системата за видеонаблюдение;
4. Държавни органи, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

(2) Данните от регистъра не могат да бъдат предавани по електронен път извън територията на офиса освен при предаването им на държавни органи във връзка със задължителни инструкции (заповеди) на тези органи.

Глава пета

ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ

Чл. 20. Лица по защита на личните данни за всеки от регистрите в СУ „МАКСИМ РАЙКОВИЧ“ са:

- ЗАТС;
- Заместник-директори;
- Счетоводител;
- Администратор база данни;
- Системен администратор;
- ДЛЗЛД;

Чл. 21. (1) В СУ „МАКСИМ РАЙКОВИЧ“ е определено Длъжностно лице по защита на личните данни, което е лице за контакт с Комисията за защита на личните данни.

(2) Длъжностното лице по защита на лични данни има следните правомощия:

1. Осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. Следи за спазването на конкретните мерки за защита и контрол на достъпа, съобразно спецификата на водените регистри;
3. Осъществява контрол по спазване на изискванията за защита на регистрите;
4. Поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

5. Контролира, съвместно със системния администратор спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. Конкретизира, съвместно системния администратор, техническите ресурси, прилагани за обработка на личните данни;
7. Следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, като напр. чрез регистрация на всички извършени действия с регистрите в компютърната среда;
8. Определя ред за съхраняване и унищожаване на информационни носители, включително следи за периодично архивиране на информацията;
9. Съвместно с лицето, поддържащо системите определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на пароли;
10. Съвместно с лицето, поддържащо системите 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.;
11. Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;
12. Организира предоставянето на правомерен достъп на трети лица до информацията в отделните регистри;
13. Организира предоставянето на правомерен достъп на служителите с ограничен достъп до информацията в регистрите;
14. Осигурява достъп на лицата до личните им данни.

Чл. 22. Директорът на СУ определя лицата, които обработват лични данни в СУ „МАКСИМ РАЙКОВИЧ“.

Чл. 23. Служителите на СУ „МАКСИМ РАЙКОВИЧ“ са длъжни да:

1. Обработват лични данни законосъобразно и добросъвестно;
2. Използват личните данни, до които имат достъп, съобразно целите, за които тези се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. Актуализират регистрите на личните данни, до които имат достъп (при необходимост);
4. Заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. 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.

Чл. 24. (1) Забранява се събирането, обработването, съхранението и разпространението на лични данни от неупълномощени служители на СУ „МАКСИМ РАЙКОВИЧ“.

(2) Неспазване на разпоредбите на тези Вътрешни правила представлява нарушение на трудовата дисциплина и договорните правоотношения с СУ „МАКСИМ РАЙКОВИЧ“, за което съответните лица носят отговорност съгласно Закона за защита на личните данни и Кодекса на труда.

Чл. 25. (1) Програмно-техническите средства за защита на личните данни се определят от Длъжностното лице по защита на личните данни след съгласуване Директор на СУ „МАКСИМ РАЙКОВИЧ“.

(2) При внедряване на нов програмен продукт за обработване на лични данни следва да се съставя нарочна комисия по тестване и проверка на възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване на максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване. За всеки отделен случай се назначава нарочна приемна комисия, в състава на която задължително участва служител, отговарящ за процеса, свързан с новия програмен продукт и с ролите на потребителите. В състава на комисията участва и служител, който е упълномощен да издаде или инициира издаването на заповед, с която да бъдат определени правата и задълженията на служителите (потребителите) в СУ „МАКСИМ РАЙКОВИЧ“, които ще използват ново разработения продукт.

Глава шеста

ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ОПРЕДЕЛЯНЕ НА СЪОТВЕТНО НИВО НА ЗАЩИТА

Чл. 26. (1) Оценка на въздействие е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица в случай на нарушаване на поверителността, цялостността или наличността на личните данни.

(2) Оценка на въздействието се извършва с цел определяне на адекватното ниво на техническите и организационни мерки и допустимия вид на обработваните лични данни за всеки обособен регистър поотделно. Същата се извършва периодично, поне на всеки две години или при настъпване на съществена промяна в характера на обработваните лични данни и броя на засегнатите лица, като се прилага процедурата за оценка на въздействието.

(3) В случай че извършена оценка на въздействието покаже, че обработването би могло да породи висок риск за субектите, ако Администраторът не предприеме мерки за ограничаване на риска, то следва да се проведе предварителна консултация с КЗЛД преди обработването на личните данни за съответния регистър.

Чл. 27. Нива на защита:

(1) „Персонал“ – „средно ниво“;

(2) „Ученици“ - „високо ниво“;
(3) „Видеонаблюдение“ се определя степен на защита - „ниско ниво“;

Глава седма

ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ НАРУШАВАНЕ СИГУРНОСТТА НА ЛИЧНИ ДАННИ, АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

Чл. 28. (1) Администраторът предприема превантивни действия за защита на личните данни, като съставя план за действие при различни форми на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от СУ „МАКСИМ РАЙКОВИЧ“ – предприемат се конкретни действия в зависимост от конкретната бедствена/аварийна ситуация;
2. защита от пожари – пожаро-известителна система, незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи на реда;
3. защита от наводнения – предприемат се действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(2) В случай на нарушение на сигурността на обработваните лични данни СУ „МАКСИМ РАЙКОВИЧ“ следва изрично приетата процедура за действие при установяване на пробив в системите на Администратора, съгласно Процедура при нарушение на сигурността с лични данни.

Глава осма

СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл. 29. (1) Лични данни на физическите и юридическите лица, събирани от СУ „МАКСИМ РАЙКОВИЧ“, се съхраняват до осъществяване на целите, за които са били събрани и се обработват, в рамките на периода, предвиден съгласно тази Инструкция.

(2) След постигане целите по смисъла на този чл. 32, (1) личните данни на физическите лица се унищожават в съответствие с процедурата за унищожаване на лични данни и документира в съответен протокол.