РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА
РЕГИОНАЛНО УПРАВЛЕНИЕ НА ОБРАЗОВАНИЕТО – МОНТАНА

УТВЪРДЕНИ

СЪС ЗАПОВЕД № РД-05-392/19.07.2018 г.

ВЪТРЕШНИ ПРАВИЛА
НА
РЕГИОНАЛНО УПРАВЛЕНИЕ НА ОБРАЗОВАНИЕТО – МОНТАНА
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2018 Г.

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Регионално управление на образованието – Монтана, наричано по-долу само „РУО – Монтана“, е юридическо лице с БУЛСТАТ 821112035 и публична администрация, териториален орган към министъра на образованието и науката за управление и контрол на системата на предучилищното и училищното образование.

(2) РУО - Монтана е със седалище в гр. Монтана и адрес на управление: гр. Монтана, пл. „Жеравица“ № 1, ет. 7.

(3) Като юридическо лице, възникнало по силата на закона, РУО – Монтана осъществява своите правомощия по Силата на Закона за предучилищното и училищното образование и подзаконовите му нормативни актове, както и по силата на общите законови актове в Република България, регламентиращи дейността му като администрация.

(4) РУО – Монтана обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им. В този случай РУО – Монтана действа като администратор на лични данни.

(5) В случаите, в които РУО – Монтана обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от РУО – Монтана и трето лице, РУО – Монтана има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

Чл. 2. Настоящите Правила уреждат:

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

(2) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;

(3) Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;

(4) Лицата, които обработват лични данни, и техните задължения;

(5) Правилата за предаване на лични данни на трети лица в България и чужбина;

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

(7) Техническите ресурси, прилагани при обработката на лични данни.

Чл. 3. РУО – Монтана събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от Дружеството, са групирани в регистри на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

- работници и служители и изпълнители по граждански договори;
- кандидати за работа;
- клиенти;
- доставчици на услуги.

Чл. 4. (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

Чл. 5. (1) РУО – Монтана е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни, при обработването на лични данни РУО – Монтана спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

Чл. 6. (1) Принципите за защита на личните данни са:

1. ***Законосъобразност, добросъвестност и прозрачност*** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;
2. ***Ограничение на целите*** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;
3. ***Свеждане на данните до минимум*** – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;
4. ***Точност*** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;
5. ***Ограничение на съхранението*** – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;
6. ***Цялостност и поверителност*** – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. ***Отчетност*** – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(2) Ако конкретната цел или цели, за които се обработват лични данни от РУО – Монтана, не изискват или вече не изискват идентифициране на субекта на данните, РУО – Монтана не е задължено да поддържа, да се сдобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

Чл. 7. РУО – Монтана организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 8. РУО – Монтана прилага адекватна защита на личните данни, която включва:

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

Чл. 9. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

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

(3) Събирането, обработването и съхраняването на лични данни в регистрите на РУО – Монтана се извършва на хартиен, технически и/или електронен носител по

централизиран и/или разпределен способ в офис-помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 10. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б" – „ е" от Регламент 2016/679, физическите лица, чиито лични данни се обработват от РУО – Монтана, подписват декларация за съгласие по образец (***Приложение № 1***).

Чл. 11. (1) Право на достъп до регистрите с лични данни имат само служителите на РУО – Монтана, съобразно възложените им от закона правомощия и оторизираните служители на РУО – Монтана, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

(2) Оторизирането на служители се извършва на база длъжностна характеристика или чрез изричен акт на началника на РУО – Монтана.

(3) Служителите на РУО – Монтана носят отговорност за осигуряване и гарантиране опазването на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните служители.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл. 12. (1) Документите и преписките, по които работата е приключила, се архивират.

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

(3) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на

различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(4) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица на РУО – Монтана съобразно възложените им от закона правомощия и от началника на РУО – Монтана задължения.

Чл. 13. (1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец, съгласно ***Приложение № 2***. Встъпителен инструктаж във връзка с изпълнението на правилата за защита на личните данни се провежда на новопостъпващите служители.

Чл. 14. (1) Най-малко веднъж годишно (през м. януари) се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от РУО – Монтана регистри. Проверките се извършват от комисия, включваща служители на РУО – Монтана, които изготвят доклад за резултата от проверката.

(2) Докладът по ал. 1 трябва да включват преценка на необходимостта за обработка на личните данни или унищожаване. Докладите се адресират до длъжностното лице по защита на данните и до началника на РУО – Монтана.

Чл. 15. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го

докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 16. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, началника на РУО – Монтана може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

Чл. 17. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от РУО – Монтана регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, РУО – Монтана прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

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

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване в специални устройства (шредери) с висока степен на защита на информацията или по механичен начин.

(3) Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на началника на РУО – Монтана след уведомяване на Длъжностното лице по защита на данните

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3, съгласно образец, представляващ ***Приложение № 3***.

Чл. 18. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице се взима в законоустановените срокове в Административно-процесуалния кодекс.

(3) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(4) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец съгласно ***Приложение № 4***, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(5) Третите страни получават достъп до лични данни, обработвани в РУО – Монтана, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ и др.п.).

II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. ***Физическата защита*** в РУО - Монтана се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 20. (1). Основните ***организационни мерки за физическа защита*** в РУО – Монтана включват:

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

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

3. определяне на организацията на физическия достъп;

(2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения. В част от помещенията имат достъп и външни лица, за което се обособява „непублична" част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служителите, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част" – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни се използват* само от служителите, които за изпълнение на служебните си задължения имат достъп до данните, както и от лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи.

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

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

(6) *Използваните технически средства за физическа защита* на личните данни в РУО – Монтана са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае" с оглед изпълнението на работните им задължения.

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

(8) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Чл. 21. (1). Основните ***технически мерки за физическа защита*** в РУО – Монтана включват:

1. използване на ключалки и заключващи механизми;
2. шкафове, метални каси,
3. оборудване на помещенията с пожарогасителни средства.

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

(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва *ключалки* (механични) за ограничаване на достъпа единствено на оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(4) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 22. (1). Основните ***мерки за персонална защита*** на личните данни, приложими в РУО – Монтана, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за

извършен инструктаж за защита на личните данни по образец (***Приложение № 5***);

2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от РУО – Монтана;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между персонала и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

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

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Чл. 23. (1). Основните ***мерки за документална защита*** на личните данни, са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител* - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на РУО – Монтана, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на РУО – Монтана, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

3. *Регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";

4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.

5. *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на РУО – Монтана или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

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

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае", за да изпълняват техните задължения;

2. *Правила за размножаване и разпространение*, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл. 24. (1) ***Защитата на автоматизираните информационни системи (АИС) и/или мрежи*** в РУО – Монтана включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

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

1. *Идентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на АИС.
2. Ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;
3. Управление на *външни връзки и/или свързване*, включващо от своя страна:
    - Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите на РУО – Монтана. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения
4. *Защитата от зловреден софтуер* включва:
    - използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от началника на РУО – Монтана лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста.
    - използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от началника на РУО – Монтана лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.
    - активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.
    - забрана за пренос на данни от заразени компютри При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от началника на РУО – Монтана лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители,

електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

   - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на РУО – Монтана.
   - Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на загуба на техния основен носител.
   - Отговорност за архивиране има лицето, обработващо личните данни.
   - Срокът на архивиране следва да е съобразен с действащото законодателство.
   - Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа

6. Основни *електронни носители на информация са*: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове и други носители на информация, еднократно записваеми носители и др.)

7. *Персоналната защита на данните* е част от цялостната охрана на РУО – Монтана

8. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на РУО – Монтана.

9. Данните, които вече не са необходими за целите на РУО – Монтана и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. *Организация на телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на РУО – Монтана:

   - Отдалечен достъп до вътрешни мрежи на РУО – Монтана не е предвиден. По изключение, и след изричната оторизация от началника на РУО – Монтана, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

   - На персонала на РУО – Монтана може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до елекронните ригистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано с оторизираните от началника на РУО – Монтана лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от началника на РУО – Монтана и след становище на Длъжностното лице по регистрация. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на РУО – Монтана, както и в случаите на заплаха за сигурността на данните.

   - Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от началника на РУО – Монтана и на сайта на РУО – Монтана.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на РУО – Монтана, включват:

   - Оценка на сигурността, включваща оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване.

Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на РУО – Монтана, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

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

III. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 25. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) РУО – Монтана прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локализация, уникално потребителско

име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секунди), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

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

(4) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от РУО – Монтана период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 26. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 27. (1) В РУО – Монтана се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

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

Чл. 28. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

IV.ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 29. (1) Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

(2) Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса по седалището на РУО – Монтана или официалната електронна поща.

(3) Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.

(4) Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

(5) РУО - Монтана е длъжно в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако РУО – Монтана установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.

(6) Субектите на данни имат също правото да:

- оттеглят съгласието си за обработване по всяко време,

- възразят срещу употреба на личните им данни за целите на директния маркетинг;

- изискат информация за основанието, въз основа на което личните им данни са предоставени за обработване на обработващ извън целите на обработването

- възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;

- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;

- подават жалби до регулаторния орган;

- в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

ПРОМЕНИ НА ВЪТРЕШНИТЕ ПРАВИЛА

Чл. 30. РУО – Монтана може да променя тези Правила по всяко време. Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат.

Настоящите Правила влизат в сила в деня на утвърждаването им.

Изготвил:

Биляна Хараламписва