Утвърдил *

/Мариела Живкова/

Дата: 12.10.2018 г.

И Н С Т Р У К Ц И Я

ЗА ПОЛУЧАВАНЕ, ОБРАБОТВАНЕ, СЪХРАНЯВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ В „РЕГИОНАЛНО ДЕПО ЗА ОТПАДЪЦИ – МОНТАНА“ ЕООД

I. ПРЕДМЕТ

Чл. 1. (1) С настоящата инструкция се урежда минималното ниво на техническите, физическите и организационни мерки в за защита на личните данни при тяхното получаване, обработване и съхраняване в поддържаните от „Регионално депо за отпадъци – Монтана“ ЕООД регистри.

(2) Инструкцията се утвърждава на основание чл.23, ал.4 и чл.24, ал.4 от Закона за защита на личните данни, в съответствие с Регламент (ЕС) 2016/679, обнародван в Официален вестник на Европейския съюз от 04.05.2016г., в сила от 25.05.2018г.

(3) Тази инсрукция се утвърждават, изменят, допълват и отменят със заповед на управителя на „Регионално депо за отпадъци – Монтана“ ЕООД.

Чл.2 Инструкцията регламентира :

1. механизмите за водене, поддържане и защита на личните данни, съдържащи се в поддържаните от дружеството регистри с цел осигуряване на неприкосновеност на личния живот на гражданите;
2. задълженията и отговорностите на длъжностните лица, обработващи лични данни или работещи под ръководството на такива, отношенията на тези лица с администратора;
3. необходимите организационни, физически и технически мерки за защита на личните данни, съдържащи се в регистрите от неправомерно обработване или достъп;
4. видовете регистри, които се водят в дружеството и тяхното описание;
5. процедурите за докладване, управление и реакция при инциденти.
6. Правила за защита на личните данни при видеонаблюдение

II. ЛИЧНИ ДАННИ

Чл. 3. (1) Лични данни са всяка информация , отнасяща се до физическо лице , което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Личните данни се събират за конкретни, точно определени и законни цели , обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

* *Заличена информация на основание чл.2 от ЗЗЛД*

(3) **Личните данни се подържат** във вид , който позволява идентифициране на съответните **физически** лица за период не по – дълъг от необходимия за целите, за които тези данни се обработват . Личните данни . които ще се съхраняват за по – дълъг период за исторически , статистически или научни цели , се поддържат във вид , непозволяващ идентифицирането на физическите лица .

III. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл.4 (1) Обработване на личните данни е всяко действие или съвкупност от действия , които могат да се извършат по отношение на личните данни с автоматични или други средства , като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране , заличаване или унищожаване на данните.

(2) Обработване на личните данни се състои и в осигуряване на достъпа до определена информация. То се извършва само от лица, чиито служебни задължения или конкретно възложена задача предвижда това.

(3) Обработването на лични данни е допустимо само в случаите , когато е налице някое от следните **основания :**

1. физическото лице, за което се отнасят данните, е дало изрично своето **съгласие** да бъдат обработени – съгласието се дава само лично **и** е недвусмислено;

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 договор и предприети по негово искане ;

3. обработването е необходимо за спазване на **законово задължение,** което се прилага спрямо администратора;

4. обработването е необходимо, за да се защитят **животът** и здравето на физическото лице, за което се отнасят данните;

5.обработването е необходимо за изпълнението на задача, която се осъществява в **обществен интерес** ;

6. обработването е необходимо за реализиране на **законните интереси на администратора** на лични данни или на трето лице, на което се разкриват данните, с изключение на случаите, при които над тези интереси преимущество имат интересите на физическото лице, субект на данните.

(4) Основанията по т.1-6 от предходната алинея се прилагат при условията на алтернативност. Съгласие по ал.3, т.1 не се изисква при наличие на поне едно от останалите пет основания.

Чл.5 Управителят на „Регионално депо за отпадъци – Монтана“ ЕООД със заповед възлага обработването на личните данни на служители на дружеството /обработващи/. Обработването може да се възложи на повече от един обработващ данните, съобразно спецификата на изпълняваните функции и с цел разграничаване на конкретните им задължения.

Чл. 6 (1) За необходимостта от набиране на лични данни и целите, за които ще бъдат използвани, обработващият лични данни информира лицето.

(2) След одобрение на документите, съдържащи лични данни от **ресорния ръководител,** същите заедно с приложенията към тях се обработват в регистрите от обработващия лични данни и се съхраняват на магнито – оптичен носител.

(3) Набраните данни на технически носител остават в отделни файлове на компютъра, като достъп до тях има само обработващият лични данни.

(4) Хартиеният носител се подрежда в кадрови досиета или специални папки и се представя за проверка законосъобразността на изготвения документ И валидирането му чрез подписи на управителя или други служители на дружеството.

IV. ВИДОВЕ РЕГИСТРИ

Чл.7 (1) Регистрите, в които се събират и съхраняват данни в „Регионално депо за отпадъци – Монтана“ЕООД са за :

1. физическите лица в Република България;
2. служителите на трудово и служебно правоотношение в дружеството.

(2) Категоиите лични данни в регистрите, които се отнасят до физическите лица могат да бъдат относно :

- Физическа идентичност - име, адрес, ЕГН , номер, дата и място на издаване на лична карта, адрес, месторождение, телефони за връзка, електронна поща, подпис, свидетелство за съдимост и др.
- Семейната идентичност - семейно положение (наличие на брак, развод, брой на членове на семейството, в т.ч. деца до 18 години), родствени връзки и др.
- Образование - вид на образованието, място, номер и дата на издаване на диплома;
- допълнителна квалификация;
- Трудова дейност;
- професионална биография;
- Медицински данни /чувствителни/ – физиологично, психическо и психологично състояние на лицата.
- Икономическа идентичност - имотно и финансово състояние,
- участие и/или притежаване на дялове или ценни книжа в дружества и др.
- лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, които заемат.

(3) Видовете регистри с лични данни, които се водят в „Регионално депо за отпадъци – Монтана“ЕООД са описани в Приложение №1, което е неразделна част от тези правила. Приложението се утвърждава, изменя, допълва и отменя със заповед на управителя на дружеството.

V. НАЧИН НА ВОДЕНЕ НА РЕГИСТРИТЕ

Чл. 8. Личните данни от лицата се подават до администратора на личните данни „Регионално депо за отпадъци – Монтана“ЕООД, представлявана от управителя, както и до лицата, определени за обработване на лични данни по реда на чл.5 от тези правила.

Чл. 9. (1) Информацията, съдържаща лични данни на хартиен носител се съхранява в папки, които се подреждат в специални картотечни шкафове. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри се контролира от служители на дружеството.

(2) Картотечните шкафове могат да бъдат поставени в помещения, предназначени за самостоятелна работа на обработващия лични данни или в общи помещения за работа с изпълняващи други дейности.

(3) Личните данни за всяко лице се набират в изпълнение на нормативно задължение – разпоредбите на закони, кодекси, подзаконови нормативни актове и други чрез:

- устно интервю с лицето ;

• хартиен носител - писмени документи – съобщения , преписи от актове , молби , заявления, лични документи по текущи въпроси в процеса на работа, подадени от лицето или предоставени по служебен път;

• външни източници (от финансови, административни, съдебни и други органи).

Чл.10 (1) Достъп до лични данни има само обработващият ги и действащо под пряко негово ръководство оторизиран служител на дружеството.

(2) Обработващият данните се задължава да не предоставя достъп до предоставените му за обработка данни на трети лица, освен в предвидените от закона случаи.

Чл.11(1) Формата на организация и съхраняване на личните данни на технически носител се осъществява чрез тяхното въвеждане на твърд диск на сървъри от компютърната мрежа или на изолиран компютър. Компютърът е свързан в локалната мрежа , със защитен достъп до личните данни , с който може да работи само обработващ лични данни.

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора.

(3) Достъп до файловете за обработка на лични данни имат само работещите с тях.

(4) Защита на електронните данни от неправомерен достъп , повреждане , изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва от служителите по информационно обслужване. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър.

VI. ТЕХНИЧЕСКИ, ФИЗИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ГАРАНТИРАНЕ НИВОТО НА СИГУРНОСТ.

Чл.12 (1) Администраторът на личните данни предприема необходимите технически, физически и организационни мерки, за да защити данните от случайно или незаконно използване, загуба или друга форма на незаконно обработка.

(2) Администраторът може да обработва данните сам или чрез възлагане на обработващ данните. Когато е необходимо по организационни причини, обработването може да се възложи на повече от един обработващ, включително с цел разграничаване на конкретните им задължения.

(3) След като постигне целта на обработване на данните администраторът е длъжен да ги :

1. унищожи;

2. прехвърли на друг администратор, като предварително уведоми за това КЗЛД в предвидените от закона случаи и при идентичност на целите на обработването;

3. съхранява в предвидените от закона и срокове случаи.

Чл.13 (1) Техническите мерки за гарантиране нивото на сигурност са :

1. Компютърните сървъри за база данни да са на съвременно техническо ниво. Сървърния хардуер да използва RAID технологии за дискова подсистема , hot-swap твърди дискове и оперативна памет с механизъм за откриване и корекции на грешки .

2. компютърните работни конфигурации да използват Desktop операционни системи съобразно изискванията на приложния софтуер за работа с лични данни. 3. За всички компютърни конфигурации , сървъри и комуникационни средства , от които

зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахранващи устройства (UPS).

4. Минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва :

- Операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани пакети за сигурност;
- Антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
- Активирана защитна стена и деинсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер;

(2) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица със **специални кодове**, които им се предоставят от служителите по информационно обслужване.

(3) Администраторът предприема мерки за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент.

Чл.14 Физически мерки за гарантиране нивото на сигурност са :

1. Лични данни могат да се обработват във всички работни помещения;
2. За работните помещения се установява регламентиран достъп. Когато не се използват от служители, работните помещения се заключват;
3. Достъпът на външни лица до работните помещения се разрешава само за изпълнение на служебни задачи. За времето на престой външното лице се придружава от служител;
4. Работните компютърни конфигурации на служителите се разполагат в работните помещения.

Чл.15 Организационните мерки за гарантиране на нивото на сигурност са :

1. със заповедта по чл.5 на обработващия лични данни се възлагат задължения и отговорности за всички регистри, поддържани в дружеството.
2. организира се охрана на работните помещения в рамките на охраната на цялата сграда (оперативни дежурни) и СОТ;
3. забранено е използването на преносими лични носители на данни в помещенията на дружеството;
4. работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;
5. пренасянето на лични данни през чрез интернет се осъществява само чрез служебна електронна поща;

VII. ОБРАБОТВАЩ ЛИЧНИ ДАННИ. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ:

Чл.16 Обработващият лични данни се задължава :

1. да ограничи достъпа до помещенията, в които се съхраняват данните само за оторизираните служители /монтиране на специални метални шкафове, заключване на помещенията/ и др.
2. да осигури достъп до електронните бази данни само по отношение на оторизираните служители /дефиниране на права на достъп до нивата, пароли за достъп до програмната среда, пароли за отваряне на файловете/;
3. да осигури подходящо защита на електронните данни чрез активиране на антивирусна защита и др.

Чл.17 Всеки обработващ лични данни подписва декларация, че е запознат и ще спазва изискванията на Закона за защита на личните данни и настоящата инструкция, която е нерадзелна част от настоящата като приложение №2.

Чл.18(1) Длъжностното лице по защита на лични данни участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни в „Регионално депо за отпадъци – Монтана“ ЕООД.

(2) Длъжностното лице по защита на личните данни :

1. информира и съветва, администратора, обработващите лични данни и лицата, които извършват обработване за техните задължения по силата на Регламент (ЕС) 2016/679 и Закона за защита на личните данни;

2. при поискване предоставя съвети във връзка с изготвени оценки на въздействието;

3. сътрудничи и действа като точка за контакт на надзорния орган;

4. изпълнява и други задачи възложени му с регламента, ЗЗЛД и тази инстракция.

VIII. ПРАВА НА ФИЗИЧЕСКОТО ЛИЦЕ - СУБЕКТ ИА ДАННИТЕ

Чл.19 (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в „Регионално депо за отпадъци – Монтана“ЕООД.

(2) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни :

- потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, категориите данни и за получателите или категориите получатели, на които данните се разкриват;
- съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват;
- информация за начина на автоматизирано обработване на лични данни, отнасящи се до него в случаите на автоматизирани решения по чл. 34б от ЗЗЛД.

(3) Физическото лице има право по всяко време да поиска от администратора да:

- заличи, коригира или блокира негови лични данни, обработването на които не се обработва по силата на нормативен акт и не отговаря на изискванията на ЗЗЛД;
- уведоми третите лица, на които са били разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с горното, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

Чл.20 (1) Правото на достъп се осъществява с писмено искане или искане по електронен път по Закона за електронните документи и електронния подпис до управителя на дружеството лично или от изрично упълномощено от субекта на данните лице, чрез нотариално заверено пълномощно.

(2) Искането съдържа :

- име , адрес и други данни за идентифициране на субекта на данните;
- описание на искането ;
- предпочитана форма за предоставяне на информацията;
- подпис, дата на подаване и адрес за кореспонденция;
- приложено пълномощно, когато искането се подава от упълномощено лице.

(3) Искането се завежда в деловодството на дружеството.

(4) При подаване на искане за осигуряване на достъп до лични данни управителят на дружеството разглежда исканитж и разпорежда на обработващия лични данни да осигури достъп.

Чл.21 (1) Срокът за разглеждане на искането и произнасяне по него е 30 - дневен,

(2) В посочените по ал.1 срокове, администраторът на лични данни взема решение за предоставяне на пълна или частична информация или мотивирано отказва предоставянето й.

Чл.22 (1) Достъпът до данните се предоставят в посочената в искането форма - устна или писмена справка, или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице, или по електронен път.

(2) Администраторът уведомява писмено или по електронен път искателя за предоставянето на данни. Уведомяването за отказ се извършва лично срещу подпис или по пощата с обратна разписка. Липсата на уведомление се смята за отказ.

(3) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на искателя се отказва достъп до тях с мотивирано решение. Администраторът отказва пълно или частично предоставяне на данни на лицето, за което те се отнасят, когато от това би възникнала опасност за отбраната или националната сигурност или за защита на класифицираната информация и ако това е предвидено в специален закон.

(4) Отказът може да се оспори по реда на АПК, за което заявителят се уведомява с писмото за отказ.

Чл.23 (1) При искане за заличаване, блокиране на лични данни, поради неправомерно обработване , несъответстващо на ЗЗЛД администраторът взема решение и извършва съответното действие в 30-дневен срок от подаване на искането или мотивирано отказва извършването им.

(2) При искане за уведомяване на трети лица, на които са разкрити личните данни за извършеното заличаване, коригиране, блокиране, администраторът на лични данни взема решение в 30- дневен срок от постъпване на искането и незабавно уведомява третите лица или мотивирано отказва да извърши уведомяването.

(3) Отказите по ал.1 и ал.2 може да се оспорят по реда на АПК, за което искателят се уведомява.

IX. РАЗДЕЛ ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 24. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от заинтересованото лице, за което се отнасят данните, освен ако не е налице друго основание за тяхната обработка

(2) При неполучаване на съгласието по ал.1 или при изричен отказ да се даде, в случайте в които не е необходимо, данните не се предоставят.

(3) Не се изисква съгласие на лицето, в случаи, в които предоставянето на лични данни на съответното лице :

- се основава и е в изпълнение на закон или на подзаконов нормативен акт;
- извършва се под контрола на компетентен държавен орган;
- свързано е с извършването на престъпления, административни нарушения или непозволени увреждания.

(4) Решението за предоставяне или отказ на достъп до лични данни за съответното лице администраторът съобщава на третото лице в 30 - дневен срок от подаване на искането.

X. ПРОЦЕДУРИ ЗА ДОКЛАД И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл.26 (1) При възникване или установяване на инцидент веднага се докладва на длъжностното лицето за защита на личните данни.

(2) За инцидентите от длъжностното лице по ал.1 се води дневник. В него се вписват - предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(3) В дневника се записват и последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни. Това се отразява в дневника по архивиране и възстановяване на данни.

(5) В случаите на компрометирането на парола тя се подменя с нова, като събитието се отразява в дневника.

XI. СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл. 27. Лични данни на физическите лица, получени за целите, за които се обработват, се съхраняват за сроковете, предвидени в съответните специални закони.

Чл.28 Личните данните на физическите лица на хартиен носител се унищожават чрез машинно нарязване, за което надеждно се изготвят протоколи за унищожаване.

XII. РЕД ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, СЪБРАНИ ЧРЕЗ ВИДЕОНАБЛЮДЕНИЕ

Чл.29(1) Администраторът поддържа система за видеонаблюдение с цел недопускане на престъпления и други правонарушения. Видеонаблюдение се осъществява и с цел осигуряване безопасността на гражданите и охрана на имущество на администратора.

(2) Записите, направени чрез системата съдържат лични данни в случай, че съдържат субекти на данните.

(3) Системата създава видео запис, направен от камерите в наблюдаваната зона, заедно с времето, датата и местоположението. Не се използват уебкамери.

(4) Записът е автоматичен - при детекция на движение, а за камерите на "Сметището" - постоянен.

Чл.30 (1) Наблюдението на камерите и преглед на запис е инсталирано на две работни места - при пазачите и на кантара.

(2)Не е предоставена възможност за изтриване и контрол на записите.

Чл.31 (1) Достъп до видеозаписите имат следните служители на администратора – Димитър Цеков – гл.технолог

(2) Посочените служители могат да предоставят видеозаписи от камерите след писмено разрешение на представителя на дружеството на представители на Районно управление на полицията в Монтана и органите на прокуратурата, за което се съставя приемо-предавателен протокол.

Чл.32(1) Записите се съхраняват за:

- 17 дена за камерите в "Сепариращата инсталация";
- 5 месеца за камерите на "Портала";
- 1 седмица за камерите на "Сметището".

(2) Изтриването на записите е автоматично - при запълване на дисковете за запис, като изтриването започва от най-стария запис.

(3) Записите се запазват извън посочения по - горе срок в случаите, когато е нужно за целите на разследване на престъпления или нарушения.

Чл.33 При осъществяване на видеонаблюдението субектите на данните се уведомят за извършването му чрез публикация на настоящата инструкция на интернет-страницата на администратора.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1 „Администратор на лични данни“ е „Регионално депо за отпадъци – Монтана“ЕООД, представлявано от управителя на дружеството.

§2 "Регистър на лични данни" е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизиран , децентрализирана или разпределена на функционален или географски принцип.

§3 „Обработващи лични данни” са служители на „Регионално депо за отпадъци – Монтана“ ЕООД, определени със заповед на управителя.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата инструкция се издава на основание чл. 23, ал. 4 и чл.24, ал.4 от ЗЗЛД

§ 2. За допуснати нарушения по настоящата инструкция, виновните носят дисциплинарна отговорност, освен ако деянието не представлява престъпление.

§ 3. За неуредените в тази инструкция въпроси се прилагат разпоредбите на действащата нормативна уредба.

§4. Контролът по прилагането и спазването на тази инструкция се осъществява от управителя на „Регионално депо за отпадъци – Монтана“ ЕООД.

§ 5. Настоящата инструкция влиза в сила от датата на утвърждаването от управителя на дружеството.