ОБЩИНА ХАЙРЕДИН

ЗАПОВЕД

№ РД-56 / 03.02.2020 г.

На основание чл.44, ал.2 от ЗМСМА и основание чл. 23, ал. 4 и чл. 24, ал. 4 от Закона за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679

УТВЪРЖДАВАМ

Вътрешни правила за мерките за защита на личните данни в Община Хайредин, които влизат в сила от 03.02.2020 г.

Контрол по изпълнението на заповедта възлагам на Секретаря на Община Хайредин.

Препис от настоящата заповед да се връчи на длъжностните лица за сведение и изпълнение.

ОБЩИНА ХАЙРЕДИН КМЕТ ОБЛАСТ ВРАЦА

Тодор Алексиев

Кмет на Община Хайредин

Вътрешни правила за мерките за защита на личните данни

ОБЩИНА ХАЙРЕДИН

1. Предмет

1.1. Общи положения

Настоящите вътрешни правила се издават на основание чл. 23, ал. 4 и чл. 24, ал. 4 от Закона за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679 и уреждат условията и реда за водене на регистри на лични дани и, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в ОБЩИНА ХАЙРЕДИН.

1.2. Дефиниции

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

1.2.2. „обработване" - 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;

1.2.3. „ограничаване на обработването" - маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

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

1.2.13. „основно място на установяване":

- по отношение на администратор, установен в повече от една държава членка - мястото, където се намира централното му управление в Съюза, освен в случаите, когато решенията по отношение на целите и средствата за обработването на лични данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване;

- по отношение на обработващ лични данни, установен в повече от една държава членка - мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно Регламент (ЕС) 2016/679;

1.2.14. „трансгранично обработване" означава или:

- обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или

-обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка;

1.2.15. „относимо и обосновано възражение" - възражение срещу проект на решение относно това дали е налице нарушение на Регламент (ЕС) 2016/679 или не, или дали предвижданото действие по отношение на администратора или обработващия лични данни отговаря на изискванията на Регламент (ЕС) 2016/679, което ясно доказва, че проектът за решение води до значителни рискове за основните права и свободи на субектите на данни и, където е приложимо, за свободното движение на лични данни в рамките на Съюза;

1.2.16. „услуга на информационното общество" - услуга по смисъла на член 1, параграф 1, точка б) от Директива (ЕС) 2015/1535 установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество.

1.3. Принципи при обработване на лични данни

При обработването на лични данни в ОБЩИНА ХАЙРЕДИН се спазват следните принципи:

поведение, местоположение или движение;

1.2.5. „псевдонимизация" - обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

1.2.6. „регистър с лични данни" - всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

1.2.7. „администратор" - физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

1.2.8. „обработващ лични данни" - физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

1.2.9. „получател" - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

1.2.10. „трета страна" - физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

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

1.2.12. „нарушение на сигурността на лични данни" - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

1.3.1. законосъобразност, добросъвестност и прозрачност;

1.3.2. ограничение на целите;

1.3.3. свеждане на данните до минимум;

1.3.4. точност;

1.3.5. ограничение на съхранението;

1.3.6. цялостност и поверителност;

1.3.7. отчетност.

1.4. Цели

Настоящите вътрешни правила имат за цел да регламентират:

1.4.1. Механизмите на водене, поддържане и защита на лични данни за администратра на лични данни ОБЩИНА ХАЙРЕДИН;

1.4.2. Задълженията на оправомощените лица, обработващи лични данни и тяхната отговорност при неизпълнение на тези задължения;

1.4.3. Необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

1.5. Обхват

Инструкцията е задължителна за работниците и служителите на ОБЩИНА ХАЙРЕДИН.

1.5.1 Всички работници и служители на Общинска администрация на Община Хайредин при встъпване в длъжност приемат да спазват конфиденциалност по отношение на базите данни с потребители на обществените административни услуги на Областна администрация на Софийска област, в т. ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения.

1.5.2 Обработване на личните данни се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

2. Администратор на лични данни

2.1. Индивидуализиране

Администратор на лични данни е ОБЩИНА ХАЙРЕДИН, ЕИК202798588, със седалище и

адрес на управление: обл. Враца, общ. Хайредин, с. Хайредин 3357, ул. "Георги Димитров" 135.

2.2. Водещи начала

2.1.1. Администраторът обработва лични данни във връзка с дейността си, като определя сам целите и средствата за обработването им, при спазване на относимите нормативни актове.

2.1.2. Община Хайредин обработва лични данни на основание спазване на законово задължение за администратора.

2.1.3. Личните данни се обработват самостоятелно от администратора на лични данни.

2.1.4. Администраторът може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита на личните данни.

3. Условия за достъп до лични данни

Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае" и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

4. Права на физическите лица

4.1. Право на уведомяване

Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

4.1.1. Данните, които идентифицират администратора;

4.1.2. Целите на обработването на личните данни и правното основание за обработването;

4.1.3. Категориите лични данни, отнасящи се до съответното физическо лице;

4.1.4. Получателите или категориите получатели, на които могат да бъдат разкрити данните;

4.1.5. Срока за съхранение на личните данни;

4.1.6. Информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост

при условията на Регламент (ЕС) 2016/679 - Общия регламент относно защитата на данните;

4.1.7. Право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

4.1.8. Правото на жалба до надзорен орган - за Република България Комисията за защита на личните данни;

4.1.9. Източника на данните;

4.1.10. Съществуване на автоматизирано вземане на решения, включително профилиране.

4.2. Изключения

Предходния параграф § 4.1. не се прилага, когато:

4.2.1. Обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

4.2.2. Вписването или разкриването на данни са изрично предвидени в закон;

4.2.3. Физическото лице, за което се отнасят данните, вече разполага с информацията по смисъла на 4.1.;

4.2.4. Е налице изрична забрана за това в закон.

5. Регистри на лични данни

В ОБЩИНА ХАЙРЕДИН се обработват лични данни в следните регистри:

5.1. Видове регистри

5.1.1. Регистър „Служители по трудово и служебно правоотношение“;

5.1.2. Регистър „Набиране на служители в Община Хайредин“; и

5.1.3. Регистри „Физически лица в Република България “.

5.2. Регистри „Физически лица в Република България “.

Видовете регистри „Физически лица в Република България“, поддържани в общинска администрация на Община Хайредин, категориите лични данни в тях, технологичното описание - носители на данни, технология на обработване, срок на съхранение, нива на защита и мерки са описани в Приложение № 1, представляващо неразделна част от настоящите Вътрашни правила.

6. Регистър "Служители по трудово и служебно правоотношение"

6.1. Общи правила

В регистъра се обработват лични данни на служителите, работниците по трудови договори и изпълнителите по граждански договори с оглед:

6.1.1. Индивидуализиране на трудови, служебни и граждански правоотношения;

6.1.2. Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

6.1.3. Използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;
- за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;
- за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови и служебни правоотношения и граждански договори;
- за извършване на превод на суми за трудови възнаграждения и свързаните с тях допълнителни плащания по банков път.

6.2. Категории лични данни

В регистъра се обработват следните категории лични данни:

6.2.1. Физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

6.2.2. Социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

6.2.3. Семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

6.2.4. Икономическа идентичност: данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др.;

6.2.5. Лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

6.2.6. Данни за здравословното състояние (медицинско свидетелство при постъпване на работа, периодични прегледи, преминавани с оглед характера на работата, изпълнявана по трудовото правоотношение и изискванията за безопасни условия на труд).

6.3. Технологични правила

6.3.1. Данните в регистъра се обработват на хартиен и технически носител. Форма на организация и съхраняване на личните данни – писмена (документална).

6.3.2. Местонахождение на картотечния шкаф – .....;

6.3.3. Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в ОБЩИНА ХАЙРЕДИН на администратора на лични данни и оправомощеното лице, назначено за обработването им, обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо;

6.3.4. Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

6.3.5. Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установените срокове.

6.3.6. Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

6.4. Длъжности

Длъжностите, свързани с обработването и защитата на лични данни от регистъра са следните:

6.4.1. Данните от регистъра се обработват от Главен счетоводител, в чиято длъжностна характеристика е определено задължение за обработване на данните на служителите и при спазване на принципа „Необходимост да се знае";

6.4.2. Достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове.

6.4.3. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

6.5. Оценка на въздействието

Оценка на въздействието на Регистър "Служители по трудово и служебно правоотношение" се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личнит е данни, при съобразяване със следните обстоятелства:

6.5.1. В регистъра се обработват лични данни за лица, чийто брой не надхвърля 100;

6.5.2. В регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите с оглед прилагане на изискванията на трудовото законодателство.

6.5.3. При отчитане на критериите по 6.3, нивото на въздействие на Регистър "Служители по трудово и служебно правоотношение" е средно.

6.5.4. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на Регистър "Служители по трудово и служебно правоотношение"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Персонал	средно	средно	средно	средно

6.6. Мерки за физическа защита

6.6.1. Личните данни от регистъра се обработват в кабинетите на длъжностните лица.

6.6.2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с ограничен достъп само за упълномощени лица.

6.6.3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в заключен шкаф, в помещение с ограничен достъп.

6.6.4. Помещенията, в които се обработват лични данни от регистъра са оборудвани със заключване на вратите и пожарогасителни средства.

6.6.5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в к оито са разположени елементи на комуникационно-информационните системи, е възможен с амо през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни з адължения включват обработване на лични данни от регистъра.

6.6.6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители и в предвидените в закона случаи.

6.7. Мерки за персонална защита

6.7.1. Лицата, обработващи лични данни, се запознават със Регламент (ЕС) 2016/679, ЗЗЛД,

подзаконовита нормативни актове, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност п ри постъпване на работа.

6.7.2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

6.7.3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

6.7.4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

6.8. Мерки за документална защита

6.8.1. Регистър "Служители по трудово и служебно правоотношение" се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид;

6.8.2. Обработването на личните данни се извършва в рамките на работното време на ОБЩИНА ХАЙРЕДИН;

6.8.3. Достъп до регистъра имат длъжностните лица в съответствие с принципа „Необходимост да се знае".

6.8.4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп;

6.8.5. Администраторът е отговорен за контрол на достъпа до регистъра;

6.8.6. Документите се съхраняват в отредените за целта служебни помещения в специално отредени за това шкафове;

6.8.7. Архивирането на документи се възлага на главният счетоводител при спазване на съответните защитни мерки за определеното ниво на защита;

6.8.8. Личните данни могат да бъдат размножавани и разпространявани от упълномощените

служители, само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица;

6.8.9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер);

6.8.10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя нарочен протокол от назначена със заповед на Управителя комисия. Унищожаването се извършва след изрично писмено разрешение на Управителя.

6.9. Мерки за защита на автоматизирани системи и мрежи

6.9.1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всяко длъжностно лице има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър;

6.9.2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства.

6.9.3. За защита на данните е инсталирана антивирусна програма и се извършва периодична про филактика на софтуера и системните файлове;

6.9.4. Администраторът е отговорен за управлението на регистъра. Само длъжностните лица имат достъп до регистъра;

6.9.5. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (ЦРБ);

6.9.10. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено надеждно заключване;

6.9.11. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм;

6.9.12. Контролът по използването на носителите по 6.9.11 се осъществява от администратора;

6.10. Организационни мерки

6.10.1. Осигурява се:

• Охрана на сградата с денонощна охрана, осъществявана от ....., назначен по трудово правоотношение.

• Забранено е използването на преносими лични носители на данни.

• Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

• При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

6.10.2. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

6.10.3. Криптографската защита при предаване на данни по електронен път или на пренос ими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

7. Регистър „Набиране на служители в Община Хайредин“

7.1. Общи правила

7.1.1. Индивидуализиране на трудови, служебни и граждански правоотношения;

7.1.2. Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

7.1.3. Използване на събраните данни за съответните лица за служебни цели:

• за всички дейности, свързани с набиране на персонала (Европейски формат на автобиография CV, удостоверения за компетентност и др.);

• за изготвяне на всякакви документи на лицата в тази връзка (договори и др.);

• за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до кандидатстване за работа.

7.2. Категории лични данни

7.2.1. В регистъра се обработват следните категории лични данни:

7.2.2. Физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

7.2.3. Социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

7.2.4. Лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

7.2.5. Данни за здравословното състояние (медицинско свидетелство при постъпване на работа);

7.3. Технологични правила

7.3.1. Данните в регистъра се обработват на хартиен и технически носител. Форма на организация и съхраняване на личните данни – писмена (документална).

7.3.2. Местонахождение на картотечния шкаф – .....;

7.3.3. Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в ОБЩИНА ХАЙРЕДИН на администратора на лични данни и оправомощеното лице, назначено за обработването им – обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо.

7.3.4. Данните се въвеждат директно в договори, документи, удостоверяващи трудов стаж, кореспонденция и др.

7.3.5. Данните в регистъра се съхраняват докато трае подбора и за срок от 1 година след приключването му.

7.3.6. Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

7.4. Длъжности

Длъжности, свързани с обработването и защитата на лични данни от регистъра са следните:

7.4.1. Данните от регистъра се обработват от Главен счетоводител или оправомощеното лице, назначено за обработването им, в чиято длъжностна характеристика е определено задължение за обработване на данните на служителите и при спазване на принципа „Необходимост да се знае".

7.4.2. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове.

7.4.3. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

7.5. Оценка на въздействието

7.5.1. Оценка на въздействието на Регистър „Набиране на служители в Община Хайредин"

се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни при съобразяване със следните обстоятелства:

- В регистъра се обработват лични данни за лица, чийто брой не надхвърля 100;
- В регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите с оглед прилагане на изискванията на трудовото законодателство.

7.5.2. Нивото на въздействие на Регистър „Набиране на Персонал " е средно.

7.5.3. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на Регистър „Набиране на служители в Община Хайредин"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Персонал	средно	средно	средно	средно

7.6. Мерки за физическа защита

7.6.1. Личните данни от регистъра се обработват в кабинетите на длъжностните лица.

7.6.2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с ограничен достъп само за упълномощени лица, отделно от другите регистри.

7.6.3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в заключен шкаф, в помещение с ограничен достъп.

7.6.4. Помещенията, в които се обработват лични данни от регистъра са оборудвани със заключване на вратите и пожарогасителни средства.

7.6.5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

7.6.6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители и в предвидените в закона случаи.

7.7. Мерки за персонална защита

7.7.1. Лицата, обработващи лични данни, се запознават със Регламент (ЕС) 2016/679, ЗЗЛД, подзаконовита нормативни актове, Наредба № 1 от 30 януари 2013 г. за минималното ниво

на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност п ри постъпване на работа.

7.7.2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

7.7.3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

7.7.4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

7.8. Мерки за документална защита

7.8.1. Регистър "Служители по трудово и служебно правоотношение" се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид;

7.8.2. Обработването на личните данни се извършва в рамките на работното време на ОБЩИНА ХАЙРЕДИН;

7.8.3. Достъп до регистъра имат длъжностните лица в съответствие с принципа „Необходимост да се знае".

7.8.4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп;

7.8.5. Администраторът е отговорен за контрол на достъпа до регистъра;

7.8.6. Документите се съхраняват в отредените за целта служебни помещения в специално отредени за това шкафове;

7.8.7. Архивирането на документи се възлага на главния счетоводител при спазване на съответните защитни мерки за определеното ниво на защита;

7.8.8. Личните данни могат да бъдат размножавани и разпространявани от упълномощени те служители само ако е необходимо за изпълнение на служебни задължения или ако са

изискани по надлежния ред от държавни органи или упълномощени лица;

7.8.9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер);

7.8.10. След изтичане на срока за съхранение документите от регистъра се унищожават чр ез нарязване или изгаряне, за което се съставя нарочен протокол от назначена със заповед на Управителя комисия. Унищожаването се извършва след изрично писмено разрешение на Управителя.

7.9. Мерки за защита на автоматизирани информационни системи и мрежи

7.9.1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всяко длъжностно лице има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър;

7.9.2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства.

7.9.3. За защита на данните е инсталирана антивирусна програма и се извършва периодична про филактика на софтуера и системните файлове;

7.9.4. Администраторът е отговорен за управлението на регистъра. Само длъжностните лица имат достъп до регистъра;

7.9.5. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (ЦРБ);

7.9.10. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено надеждно заключване;

7.9.11. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм;

7.9.12. Контролът по използването на носителите по 6.9.11 се осъществява от администратора;

7.10. Организационни мерки

7.10.1. Осигурява се:

- Охрана на сградата с денонощна охрана, осъществявана от .....;

- Забранено е използването на преносими лични носители на данни.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

7.10.2. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

7.10.3. Криптографската защита при предаване на данни по електронен път или на пренос ими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

8. Регистри „Физически лица в Република България "

8.1. Общи положения

В регистрите се обработват лични данни на лица, които влизат в сградата и при лежащите имоти на администратора на адрес: обл. Враца, общ. Хайредин, с. Хайредин 3357, ул."Георги Димитров" 135 и са необходими за извършване на която и да е от административните услуги предоставяни от ОБЩИНА ХАЙРЕДИН, като обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели:

8.1.1. Предоставяне и персонализиране на услугите, които заявявате и очаквате ОБЩИНА ХАЙРЕДИН;

8.1.2. Осигуряване на високо качество на извършваните услуги;

8.1.3. Осигуряване на законосъобразно упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;

8.1.4. Индивидуализиране на влизащите лица;

8.1.5. Установяване на периода на достъпа до сградите и охранявания периметър, включващ.....

8.2. Категории лични данни

В регистъра се обработват следните категории лични данни:

8.2.1. Физическа идентичност - име, ЕГН/ЛНЧ, данни за лична карта/паспорт, адрес, месторождение, телефони за връзка, един или повече специфични признаци и други; Семейната идентичност - семейно положение (наличие на брак, развод, брой членове на семейството, в т.ч. деца до 18 години), родствени връзки и др.;

8.2.2. Образование - вид на образованието, място, номер и дата на издаване на дипломата, допълнителна квалификация. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

8.2.3. Допълнителна квалификация – данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

8.2.4. Трудова дейност - професионална биография - данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

8.2.5. Медицински данни – физиологично, психическо и психологично състояние на лицата. Данните са изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи;

8.2.6. Икономическа идентичност - имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа в дружества и др.;

8.2.7. Други - лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, свързани с материална отговорност. Предоставят се на основание нормативно задължение.

8.3. Технологични правила

8.3.1. Данните в регистрите, съгласно Приложение 1 се структурират, с оглед спецификата на изпълняваните служебни функции от служителите на администратора, и с цел разграничаване на конкретните им задължения по закон.

8.3.2. Данните в регистрите се обработват на хартиен и технически носител;

8.3.2. Данните в регистрите се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи;

8.3.4. Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт;

8.3.5. Данните в Регистри „Физически лица в Република България“ са функционално структурирани в административните отдели на Община Хайредин, съответно:

- АПОИФСД;
- Секретната регистратура има и видеонаблюдение;
- Служба ГРАО;
- МДТ;
- ПВЗ;
- Дирекция Евроинтеграция икономически дейност и устройство на територията;
- Адм. секретар на Кмета на Общината;

- Адм. секретар на Кмета на Общината;
- Дом за стари хора;
- Читалища и библиотеки;
- Старши специалист ОМП;
- Домашен социален патронаж;
- СУ „Васил Воденичарски" с. Хайредин;
- ОУ „Г.Червеняшки" с. Михайлово;
- ЦДГ „Славейче" с. Хайредин

8.3.6. Данни в Регистри „Физически лица в Република България" се съхраняват по аналогичен ред и в попадащите в Община Хайредин кметства, съответно:

- Кметство с. Михайлово;
- Кметство с.Манастирище;
- Кметство с. Бързина;
- Кметство с.Ботево;
- Кметство с.Рогозен.

8.4. Длъжности

Със заповед на Кмета на Община Хайредин се определят лицата и длъжностите, свързани с обработването и защитата на лични данни от регистрите, са следните:

8.4.1. Със заповед на Кмета на Община Хайредин се определят лицата, имащи достъп до данните от регистрите, които се обработват чрез обработващ данни, а именно служители, чиито задължения са свързани с предоставяне и персонализиране на административните услугите, предлагани от ОБЩИНА ХАЙРЕДИН, при спазване на всички изисквания за защита на личните данни и прилагане на следните принципи:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
6. да не допускат неоторизирани лица в помещенията, в които се съхраняват данните.

8.4.2. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

8.4.3. За обработване на регистри, съдържащи лични данни служителят подписва декларация, че е запознат със Закона за защита на личните данни и с настоящите Вътрешни правла за защитата на личните данни, които се обработват от него.

8.4.4. Администраторът предоставя лични данни в изпълнение на нормативно установени задължения и в случаи, свързани с опазване на обществения ред.

8.4.5. Лични данни се предоставят служебно между дирекциите/отделите в областната администрация след обосновано искане, от ръководителя на съответната дирекция.

8.4.6. Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на Кмета на Община Хайредин обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.

8.4.7. Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите на лицата – Заместник кмет, Секретар на общината, директори на дирекции, началници на отдели, отговарящи за съответния ресор, в който се водят регистрите. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

8.5. Оценка за въздействие

Оценка на въздействието на регистър „Клиенти, субекти на лични данни“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на ли чните данни, при съобразяване със следните обстоятелства:

8.5.1. В регистрите „Физически лица в Република България “ се обработват лични данни за лица, чийто брой надхвърля 10 000;

8.5.2. В регистрите „Физически лица в Република България “се обработват лични данни с автоматизирани средства;

8.5.3. В регистрите „Физически лица в Република България “ се съдържат специални категории лични данни;

8.5.4. Нивото на въздействие на регистрите „Физически лица в Република България“ е от ниско до средно.

8.5.5. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

8.5.6. Оценка на нивото на въздействие на регистрите „Физически лица в Република България“, съответства на характера и спецификата на обработваните лични данни, във всеки отдел и/или дирекция, съгласно Приложение 1.

8.6. Мерки за физическа защита

8.6.1. Личните данни от регистрите се обработват от служители обработващи лични данни.

8.6.2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинети с ограничен достъп само за упълномощени лица;

8.6.3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп;

8.6.4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани с заключване на вратите и пожарогасителни средства.

8.6.5. Физическият достъп до зоните в помещенията на общината са с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от съответния регистър.

8.6.6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители.

8.7. Мерки за персонална защита

8.7.1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба №1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид за щита на личните данни, настоящите Вътрешни правила, Инструкция и правилата за информационна сигурност при постъпване на работа.

8.7.2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

8.7.3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

8.7.4. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

8.8. Мерки за документална защита

8.8.1. регистрите „Физически лица в Република България "се поддържат на електронен

носител (софтуер за .....).

8.8.2. Обработването на личните данни се извършва в рамките на работното време на Община Хайредин

8.8.3. Достъп до регистъра имат длъжностните лица в съответствие с принципа „Законосъобразност".

8.8.4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващи се шкафове в зоните с ограничен достъп, като и на сървъра на администратора.

8.8.5. Администраторът е отговорен за контрол на достъпа до регистрите „Физически лица в Република България ".

8.8.6. Документите се съхраняват в отредените за целта служебни помещения в.....

8.8.7. Архивирането на документи се възлага на определено от администратора длъжностно лице при спазване на съответните защитни мерки за определеното ниво на защита.

8.8.8. Личните данни могат да бъдат размножавани и разпространявани от упълномощени те служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

8.8.9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

8.8.10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на нарочна комисия. Унищожаването се извършва след изрично писмено разрешение на Управителя.

8.9. Мерки за защита на автоматизирани системи и мрежи

8.9.1. При работа с данните от регистрите се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

8.9.2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови кон фигурации за защита на операционната система, защитни стени, рутери и мрежови устройств а. За защита на данните е инсталирана антивирусна програма и се извършва периодична про филактика на софтуера и системните файлове.

8.9.3. Администраторът е отговорен за управлението на регистрите. Само длъжностните лица и имат достъп до регистъра.

8.9.10. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (ЦРБ).

8.9.11. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

8.9.12. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм.

8.9.13. Контролът по използването на тези носители се осъществява от....., под контрола на определеното със Заповед на Кмета длъжностно лице по защита на лични данни.

8.10. Организационни мерки

8.10.1. Осигурява се:

- Охрана на сградата с денонощна охрана, осъществявана от .....;
- Забранено е използването на преносими лични носители на данни.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

8.10.2. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

8.10.3. Криптографската защита при предаване на данни по електронен път или на пренос ими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

9. Защита при аварии, произшествия и бедствия

9.1. Докладване

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

9.2. Дневник

За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

9.3. Възстановяване

В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на администратора, като това се отразява в дневника по архиви ране и възстановяване на данни.

10. Предоставяне на лични данни на трети лица

10.1. Предоставяне на държавни институции

Данни от регистрите могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, ДАНС, МВР и т.н.).

10.2. Предоставяне на кредитни институции

10.2.1. В качеството си на работодател, администраторът предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори.

10.2.2. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

10.3. Предоставяне във връзка с куриерски услуги

Във връзка с използването на куриерски услуги - приемане, пренасяне и доставка и адресиране на пратките до физически лица администраторът посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

11. Задължения по чл. 25 ЗЗЛД

11.1. Унищожаване

11.1.1. След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

11.1.2. Унищожението се извършва посредством няколко начина, определени в зависимос т от наличните към момента на унищожението технически възможности за администратора, а именно: чрез разрязване с помощта на машина - шредер и/или чрез изгаряне или разрушава не (отваряне) на корпуса на носителя на данни.

11.2. Прехвърляне

В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

12. Заключителни клаузи

12.1. Периодични прегледи

Администраторът трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението - за заличаването им.

12.2. Основание за приемане

Настоящите вътрешни правила се приемат на основание чл. 23, ал. 4 от Закона за з ащита на личните данни, чл. 19, т. 2 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и при с пазване на сроковете по § 2 от Преходните и заключителни разпоредби на Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

12.3. Изменение

Настоящите вътрешни правила могат да бъдат изменяни само за прилагането на подходящи мерки и за доказване на съответствие от страна на администратора с действащата правна рамка - Закона за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679 и уреждане условията и реда за водене на регистри на лични дани и, минималното ниво на технически и

организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни.

12.4. Приложимо право

За всички неуредени въпроси с Настоящите вътрешни правила се прилага Българското законодателство.

Утвърдени със Заповед на Кмета .....

Дата: .....