



REPUBLIC OF BULGARIA  
NOVI PAZAR MUNICIPALITY  
Mayor's phone: +359 + 0537 / 2 3466  
Fax: +359 + 0537 / 2 40 10  
Fax: +359+0537/95530  
<http://novipazar.acstre.com>  
E-mail: [npazar@icon.bg](mailto:npazar@icon.bg)  
[novipazar@novipazar.bg](mailto:novipazar@novipazar.bg)

РЕПУБЛИКА БЪЛГАРИЯ  
ОБЩИНА НОВИ ПАЗАР  
КМЕТ телефон: +359 + 0537 / 2 3466  
Факс: + 359 + 0537 / 2 40 10  
Факс: +359+0537/95530  
Зам кмет :  
телефон +359 + 0537 / 95523  
+359 + 0537 / 95525



Община Нови пазар е сертифицирана по ISO 9001:2015

УТВРЪЖДАВАМ:  
ИВАЙЛО КАМАДЖИЕВ  
КМЕТ НА ОБЩИНА НОВИ ПАЗАР



## ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ-ОБЩИНА НОВИ ПАЗАР

### І. ОБЩИ ПОЛОЖЕНИЯ

**Чл. 1. (1)** Настоящите вътрешни правила („Правилата“) уреждат условията и реда за водене на регистри по Закона за защита на личните данни (ЗЗЛД), както и организацията и реда за упражняване на контрол при обработването на лични данни от служителите на Община Нови пазар.

**(2)** 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.

**(3)** В зависимост от конкретната ситуация, Общинска администрация-Нови пазар, може да обработва данни в качеството на администратор или обработващ.

**(4)** 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.

**(5)** Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 год., относно защитата на физическите лица и във връзка с обработването на лични данни и относно свободното движение на такива данни.

**Чл. 2. (1)** Вътрешните правила се приемат с цел да регламентират:

1. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при

неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

2. Видовете регистри, които се водят в Общината и тяхното описание.

3. Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

4. 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.

5. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

6. Процедури за докладване, управляване и реагиране при инциденти. Уведомяване на надзорния орган в случай на нарушения в сигурността.

7. Правила за предаване на лични данни на трети лица в България и чужбина.

(2) Вътрешните правила се утвърждават, допълват, изменят и отменят от Кмета на Община Нови пазар.

**Чл. 3.** Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни.

**Чл. 4.** Община Нови пазар е администратор на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни и е регистрирана в Комисията за защита на личните данни.

**Чл. 5.** Дефиниции и принципи:

(1) За целите на настоящите Правила, използваните понятия имат следното значение:

- **ЗЗЛД** – Закон за защита на личните данни;
- **КЗЛД** – Комисия за защита на личните данни;
- **ОРЗД /GDPR/** - Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 год., относно защитата на физическите лица, във връзка с обработването на лични данни и относно свободното движение на такива данни;

- **Длъжностно лице по защита на данните /DPO/** - физическо лице или организация, определени съгласно изискванията на ЗЗЛД;

- **Администратор на лични данни** – физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработване на лични данни. В настоящите Правила „администратор” обозначава Общинска администрация – Нови пазар;

- **Обработващ лични данни** – лице или организация, което въз основа на договор/заповед обработва лични данни, предоставени от Общинска администрация-Нови пазар за уговорените цели;

- **Известия по защита на данните** – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който Общинска администрация – Нови



пазар събира информация за тях. Тези известия могат да бъдат, както общи (например адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел;

- **Обработване на данни** – е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други 13 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;

- **Псевдомизиране** – обработване 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.

- **Съгласие** – всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързано с него.

- **„Анонимизиране** е процес, в резултат на който, се създава информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран.

- **Лични данни** са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано /„субект на данни“/;

- **Нарушение на сигурността на лични данни** е 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.

- **Носител на лични данни** е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

- **Оторизирано лице** е лице, което по силата на естеството на преките си служебни задължения и/или изричното оторизиране, има право за достъп до определена категория лични данни;

- **Получател** е физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с 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.

- **Предоставяне на лични данни** са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

- **Регистър на лични данни** е 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;

- **Регламент** – Регламент /ЕС/ 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО /Общ регламент относно защитата на данните/.

- **Субект на данните** е идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;

- **Съгласие на физическото лице /субекта на данните/** представлява ясен утвърдителен акт, с който се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни. Например чрез писмена декларация, включително по електронен път, или устна декларация.

- **Трето лице /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.

- **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.

- **Чувствителни лични данни** – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

(2) Принципите за защита на личните данни са:

1. **Законосъобразност, добросъвестност и прозрачност** – обработвани 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 са подходящи, свързани със ограничени до необходимото във връзка с целите на обработването;

4. **Точност** – поддържане в актуален вид и предприемане на всички разумни мерки на 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.

## **II. ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ**

**Чл. 6.** Целите на обработването на лични данни са:

(1) управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на Общината в качеството му на работодател;

(2) администриране на отношенията с клиенти на общината и предоставяне на услуги;

(3) сключване и изпълнение на договори с доставчици за предоставяне на услуги на Общината.

**Чл. 7.** Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

(1) Субектът на данните се информира предварително за обработването на неговите лични данни;

(2) Личните данни се събират за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели;

(3) Личните данни съответстват на целите, за които се събират;

(4) Личните данни трябва да са точни и при необходимост да се актуализират;

(5) Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват;

(6) Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период, не по-дълъг от необходимия, за целите, за които тези данни се обработват.

**Чл. 8.** За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

(1) Субектът на данните е дал своето съгласие;

(2) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

(3) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;



(4) Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;

(5) Обработването е необходимо за изпълнение на задача от обществен интерес;

(6) Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, трябва да са описани в приложимите известия по защита на данните.

### III. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

**Чл. 9. (1)** Общината събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, публичен орган предоставящ услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от Общината, 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.

**(2)** **Относно лицата, заети по трудови или граждански правоотношения в общината, и на кандидатите за работа,** се събират следните лични данни:

а) Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни;

б) Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на Дружеството като работодател.

д) Лицата, заети по трудови или граждански правоотношения в общината и кандидатите за работа попълват Декларация-съгласие, предоставените лични данни да бъдат съхранявани, обработвани и предоставяни с цел изпълнение на нормативните задължения на Кмета на Община Нови пазар, в качеството му на работодател – Приложение № 7.

**(3)** **Относно физически лица, клиенти на общината,** се събират лични данни, които са необходими за изпълнението на законовите задължения на общината като публичен орган предоставящ услуги, както следва:

- име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни.

(4) Относно физически лица, доставчици на услуги на общината, се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на общината от външни доставчици, както следва:

- име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.

(5) Общината обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните му права и задължения в областта на трудовото и осигурително законодателство.

#### IV. СЪГЛАСИЕ

**Чл. 10. (1)** Субектът на данни е съгласен с обработването, ако изрази това ясно и недвусмислено – чрез изявление или друг потвърждаващ акт. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси.

1. Субектът на данни попълва Декларация за съгласие по образец - Приложение № 2 към настоящите Правила;

2. В случаи на необходимост при обработка на лични данни на непълнолетни лица Родителя или Настойника попълва Форма за съгласие да се обработят личните данни – Приложение № 3;

(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

1. Субектът на данни попълва Декларация за оттегляне на съгласие по образец - Приложение № 4 към настоящите Правила;

2. Родителя или Настойника за непълнолетни лица попълва Форма за оттегляне на съгласие по образец – Приложение № 5.

(3) Декларациите за съгласие се съхраняват от общината, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

#### V. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

**Чл. 11. (1)** Администраторът възлага обработването на личните данни на негови служители (обработващи). Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

(2) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

**Чл. 12. (1)** Личните данни в регистрите се набират от администратора на лични данни респективно - обработващият лични данни чрез устно интервю и/или на хартиен носител.



(2) За необходимостта от набирането на данните и целите, за които ще бъдат използвани, обработващият данните информира лицето, след което се предоставят на ресорния ръководител на хартиен носител. Ако намери за необходимо ресорният ръководител, съгласува решението си с длъжностните лица, упражняващи оперативен и цялостен контрол.

(3) Субекта на данни има право на достъп до събирана и съхранявана информация в Общинска администрация-Нови пазар – Приложение № 6.

(4) За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

(5) Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки в определени шкафови и не се изнасят от сградата на администрацията, освен от обработващия лични данни, при служебна необходимост и на технически носител като на всеки 7 дни обработващия лични данни ги архивира.

## **VI. ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ВОДЯТ В ОБЩИНА НОВИ ПАЗАР**

**Чл. 13. (1)** Регистрите, в които се събират и съхраняват данни в Община Нови пазар са за:

1. физическите лица в Република България
2. служителите на трудово и служебно правоотношение в Общинска администрация Нови пазар

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

Физическа идентичност - име, ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка 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.

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.

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

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

Медицински данни/чувствителни/ - физиологично, психическо и психологично състояние на лицата. Данните са от значение при сключване на граждански брак и при заемане на длъжности и изпълнение на функции, изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи.

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

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

(3) Видовете регистри с лични данни, които се водят в Община Нови пазар са



описани в Приложение № 1, което е неразделна част от настоящите „Правила“.

(4) Приложение № 1 се утвърждава, допълва, изменя или отменя със заповед на Кмета на Община Нови пазар.

## **VII. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ**

**Чл. 14.** Форма на организация и съхраняване на личните данни на хартиен носител:

(1) Папките са разположени в офис шкафове в кабинетите на служителите, които се заключват. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри се контролира от директори на дирекции и началници на отдели.

(2) Местонахождение на картотечния шкаф - може да бъде поставен в помещение, предназначено за самостоятелна работа на обработващия лични данни или в общо помещение за работа с изпълняващи други дейности.

(3) Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконовни нормативни актове, кодекси и други) чрез:

- устно интервю с лицето;
- хартиен носител - писмени документи (заявления) по текущи въпроси в процеса на работа, подадени от лицето;
- външни източници (съдебни, финансови, осигурителни, данъчни и др. институции в изпълнение на нормативни изисквания).

(4) Личните данни от лицата се подават до администратора на личните данни Община Нови пазар, представлявана от Кмета на общината и длъжностното лице, определено за обработване на лични данни със Заповед на кмета на общината.

(5) Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана в настоящите Вътрешни правила.

**Чл. 15.** Форма на организация и съхраняване на личните данни на технически носител:

(1) Личните данни се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на Наредба № 1 от 7.02.2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

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

лични данни. Данните се въвеждат в компютъра от хартиен носител.

(3) Достъп до файловете за обработка на лични данни имат само работещите с нея. Носители с лични данни могат да се разпространяват само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(4) Достъп до файловете за обработка на лични данни има само определено със Заповед на кмета лице обработващо лични данни чрез парола за отваряне на тези файлове, известна на него.

(5) 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 отговорен служител. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

## **VIII. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ**

### *Раздел I*

#### *Технически мерки*

**Чл. 16. (1)** Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са:

- охрана на сградата /помещенията/;
- устройства за заключване чрез ключ;
- политика на допускане на външни лица до помещенията на общината само с придружител от персонала на общината.

(2) Помещенията на общината са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

### *Раздел II*

#### *Мерки за документална защита*

**Чл. 17. (1)** Общината установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани във Вътрешни правила за документооборота.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.

(3) На хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изискванията на действащото законодателство или пряко свързани с осъществяване на нормалната дейност на Общинска администрация, сключване на



договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения.

(4) Личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения е/или нормалната бизнес дейност на администрацията, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

(5) Достъпът до документите с лични данни е ограничен и се предоставя само на упълномощени служители, в съответствие с принципа „Необходимо да се знае”.

(6) Личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събирани или до изтичане на определения в действащото законодателство срок.

(7) Документите, съдържащи лични данни, сроковете на които са изтекли и не са необходими за нормалното функциониране на администрацията или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване –шредер машина, електронно изтриване и други подходящи за целта методи, съобразени с физически носител на данни).

(8) Личните данни, оценени с по-висока степен на риск, освен мерките по-горе се прилагат и следните допълнителни мерки:

1. Контрол на достъп до документите, сграничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица в съответствие с принципа „Необходимо да се знае”, за да изпълнят техните задължения.

2. Правила за размножаване и разпространение , които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква 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.Неразрешено копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

### *Раздел III*

#### *Персонални мерки на защита*

**Чл. 18. (1)** Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:

- поемат задължение за неразпространение на личните данни, до които имат достъп;
- се запознават с нормативната база, вътрешните правила и политики на общината относно защитата на личните данни;
- преминават обучение за реакция при събития, застрашаващи сигурността на данните;
- са инструктирани за опасностите за личните данни, които се обработват от общината;
- се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с тези Правила ред.

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на общината, свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

#### *Раздел IV*

#### *Мерки за защита на автоматизирани информационни системи и криптографска защита*

**Чл. 19. (1)** Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени (firewalls) и др.

(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.

**Чл. 20. (1)** Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия, др., се осигурява посредством:

- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).

(2) Служителя, отговорен за защита на личните данни, докладва периодично на ръководството на общината за предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

(3) Пренасянето на лични данни през (чрез) интернет се осъществява чрез електронна поща, като задължително се осигурява криптиране на данните.

(4) 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.

(5) Със Заповед Кмета на Общината се определят обработващите лични данни за различните видове регистри, които се водят в Общината;

### **IX. ПРАВА НА СУБЕКТА НА ДАННИ**

**Чл. 21.** 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.

**Чл. 22.** Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса на Общинска администрация.

**Чл. 23.** Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

**Чл. 24. (1)** Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в Община Нови пазар.

**(2)** Правото на достъп се осъществява с писмена форма на искане от субекта на данни по образец – Приложение № 6 или по електронен път по реда на Закона за електронните документи и електронния подпис/ до Кмета на общината лично или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно. Подаването на заявлението е безплатно.

**(3)** Формата за искане от субекта на данни съдържа:

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

**(4)** Заявлението се завежда в Центъра за административно обслужване на общината.

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

- устна справка;
- писмена справка;
- преглед на данните от самото лице или от упълномощеното такова;
- копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

**(6)** При подаване на заявление за осигуряване на достъп до лични данни, представляващият администратора - Кмета на общината и упълномощените от него зам.-кмет и секретар по ресори разглеждат заявленията и разпореждат на обработващия лични данни да осигури искания достъп от лицето в предпочитаната от него форма.

**(7)** Срокът за разглеждане на заявлението и произнасянето по него е 14- дневен от деня на подаването му. Срокът може да бъде мотивирано удължен до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

**(8)** Администраторът уведомява писмено заявителя за решението си - то може да бъде за предоставяне на достъп или отказ за достъп. Уведомяването става лично срещу подпис или по пощата с обратна разписка.

**(9)** Отказът на достъп до лични данни трябва да бъде мотивиран. Основанията за отказ са:

- когато данните не съществуват;
- когато данните не могат да бъдат предоставяни на определено правно основание.

**(10)** За отказ се счита и липсата на уведомление.

(11) Отказът за предоставяне на достъп до лични данни може да се обжалва от лицето в съда.

(12) Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на Кмета <sup>1</sup> обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.

(13) Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите на лицата - зам.-кмет, секретар, директори на дирекции, началници на отдели, отговарящи за съответния ресор, в който се водят регистри. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

**Чл. 25. (1)** Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

(3) Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.

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

## **Х. НАРУШЕНИЯ НА СИГУРНОСТТА**

**Чл. 26. (1)** Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Служителя, отговорен за защита на личните данни, като му предоставят цялата налична информация.

(2) Служителя, отговорен за защита на личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Служителя, отговорен за защита на личните данни, докладва незабавно на Кмета на общината за наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(4) След съгласуване с Кмета на общината, служителят отговорен за защита на личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с Кмета на общината би забавило реакцията и би нанесло големи щети, служителят отговорен за защита на личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай той, уведомява незабавно кмета за предприетите мерки и съобразява последващи действия с получените инструкции.

**Чл. 27. (1)** В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от



кмета на общината, служителя отговорен за защита на личните данни, организира уведомяването на КЗЛД.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД съдържа следната информация:

(а) описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

(б) името и координатите за връзка на служителя, отговорен за защита на личните данни;

(в) описание на евентуалните последици от нарушението на сигурността;

(г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, служителя отговорен за защита на личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

**Чл. 28. (1)** Общината води регистър на нарушенията на сигурността, който съдържа следната информация:

(а) дата на установяване на нарушението;

(б) описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);

(в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

(г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Общината;

(д) предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(2) Регистърът се води в електронен формат от служителя, отговорен за защита на личните данни.

## **XI. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА**

**Чл. 29. (1)** Общината може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор.

(2) В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на обработващ, Общината:

(а) изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

(б) сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;

(в) информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:

(а) Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;

(б) Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;

(в) Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове.

(г) Трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществен интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

## **XII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ**

**Чл. 30. (1)** Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Общината. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при всяко въвеждане Автоматизирана информационна система/АИС/, която е свързана с обработване на лични данни, включително:

- първоначалното въвеждане на нови технологии или прехода към нови технологии;
- автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;
- обработване на чувствителни лични данни в голям мащаб;
- мащабно, систематично наблюдение на публично обществена зона.

(3) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

## **XIII. УНИЩОЖАВАНЕ НА ДАННИТЕ**

**Чл. 31. (1)** Унищожаване на личните данни се извършва от Общината или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове, за което се изготвят актови протоколи от отговорните длъжностни лица на отделните административни подразделения.

(2) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.



(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

#### **XIV. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ**

§.1. Настоящите Вътрешни правила се приемат на основание член 24, параграф 2 от Регламент /ЕС/ 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО.

§.2. Всички служители на общинска администрация, чиито служебни задължения включват обработване на лични данни, са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват. Запознаването се удостоверява с подпис.

§.3. Настоящите Вътрешни правила се публикуват на официалната страница на общинската администрация на община Нови пазар

§.4. За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Регламент /ЕС/ 2016/679, Закона за защита на личните данни, както и действащото приложимо законодателство, което регламентира обработката на лични данни.

§.5. Настоящите Вътрешни правила влизат в сила от деня на утвърждаването им със заповед на кмета на община Нови пазар.

§.6. Настоящите Вътрешни правила се преглеждат и актуализират при всяка промяна в нормативната уредба и се допълват, изменят или отменят със заповед на Кмета на Община Нови пазар. Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат.

Настоящите правила са приети със Заповед № 1378 от 4 Декември 2018 год. на Кмета на Община Нови пазар и влизат в сила от деня на утвърждаването им.

Съгласуват: .....

Маруся Денчева

Секретар на Община Нови пазар

Проверил: .....

Татяна Николова

Главен юрист

Изготвил: .....

Анка Маринова

Мл. експерт „СИ, ОМП, ГЗ и ЗЛД“