ОБЩИНА БАНИТЕ, ОБЛАСТ СМОЛЯН
ОБЩИНСКА АДМИНИСТРАЦИЯ

Баните–п.к.4940, област Смолян, улица " Стефан Стамболов "-№ 3, БУЛСТАТ:000614952
централа: тел.: (03025) 22 20,
e-mail: obbanite@abv.bg; Информационен сайт: www.banite.egov.bg

У Т В Ъ Р Д И Л: Заповед № РД-175 / 25.04.2018 г.
КМЕТ НА ОБЩИНА БАНИТЕ: (П) (Печат)
(Милен Белчев)

П Р А В И Л А

ОТНОСНО МЕХАНИЗМА НА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ В ОБЩИНСКА АДМИНИСТРАЦИЯ-БАНИТЕ, ОБЛАСТ СМОЛЯН

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите правила се прилагат за лични данни по смисъла на Закона за защита на лични данни и се издават на основание чл.23, ал.4 от Закона за защита на личните данни и чл.19, т.2 от Наредбата № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и изискванията на новият европейски регламент за защита на личните данни-(ЕС2016/679 от 27 април 2016 г.) и регламентират:

1. Механизмите за водене, поддържане и защита на регистрите и всички други носители на информация, съхраняващи лични данни в Общинска администрация-Баните, област Смолян с цел гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на данните за 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. Всички други носители на информация, съдържаща лични данни.
4. 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.
5. Необходимите технически и организационни мерки за защита на личните данни, съдържащи се в регистрите и във всички други носители на информация, 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).

6. 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.

7. Процедури за докладване, управляване и реагиране при инциденти.

8. Организацията и реда за упражняване на контрол при обработването на лични данни от служителите на Община Баните, област Смолян.

(2) Правилата се утвърждават, допълват, изменят или отменят със заповед на Кмета на община Баните.

Чл. 2. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

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

(3) 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. Личните данни, които ще се съхраняват за по-дълъг период за исторически, статистически или научни цели, се поддържат във вид непозволяващ идентифицирането на физическите лица.

Чл. 3. Община Баните е администратор на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни и е вписана в Регистъра на администраторите на лични данни и на водените от тях регистри с Идентификационен № 157373.

РАЗДЕЛ ВТОРИ
ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

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

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

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

1. обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни;

2. физическото лице, за което се отнасят данните, е дало изрично своето съгласие;

3. обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане;

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

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

6. обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;

7. обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, осмен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните.

Чл. 5. (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. 6. (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 набиране на лични данни и целите, за които ще бъдат използвани, обработващият лични данни информира лицето.

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

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

(5) Хартиеният носител се подрежда в кадрови досиета или специални папки и се представя за проверка законосъобразността на изготвения документ и валидирането му чрез подписи на съответните длъжностни лица-кмет, заместник-кмет, секретар, директор на дирекция или друго длъжностно лице.

(6) При необходимост от поправка на личните данни, лицата предоставят такива на обработващия лични данни по негово искане на основание нормативно задължение.

(7) За достоверността на предоставените копия от регистри или други носители на информация, съдържащи лични данни, отговорност носи обработващият лични данни.

РАЗДЕЛ ТРЕТИ
ВИДОВЕ ДАННИ, ВКЛЮЧЕНИ В РЕГИСТРИТЕ ИЛИ В ДРУГИ НОСИТЕЛИ НА ИНФОРМАЦИЯ, СЪДЪРЖАЩА ЛИЧНИ ДАННИ

Чл. 7. (1) Регистрите или в други носители на информация, в които се набират или съхраняват лични данни са за:

1. физически лица в Република България;

2. служителите по служебно или по трудово правоотношение в Общинска администрация-Баните, област Смолян.

(2) Групите данни в регистрите или в другите носители на информация, които се отнасят до физическите лица могат да бъдат:

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

Семейна идентичност-семейно положение (семеен статус, наличие на брак, развод, брой членове на семейството, в т.ч. деца до 18 години), родствени връзки и други.

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-физиологично, психическо и психологично състояние на лицата. Данните са от значение 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 други.

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

РАЗДЕЛ ЧЕТВЪРТИ
ФОРМИ ЗА ВОДЕНЕ НА РЕГИСТРИТЕ ИЛИ В ДРУГИ НОСИТЕЛИ НА ИНФОРМАЦИЯ, СЪДЪРЖАЩА ЛИЧНИ ДАННИ

Чл. 8. Личните данни от лицата се подават до администратора на личните данни Община Баните, представлявана от Кмета на общината и длъжностното лице, определено за обработване на личните данни, регламентирано в Устройствения правилник или с нарочна заповед на Кмета на общината.

Чл. 9. (1) Информацията съдържаща лични данни на хартиен носител се съхранява в папки, които се подреждат в специални картотечни шкафове. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики.Предоставянето, промяната или прекратяването на оторизиран достъп до регистри или до други носители на информация се контролира от Кмета на община, Заместник-кмета на община, Секретаря на община и от директори на дирекции.

(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) Личните данни за всяко лице се набират в изпълнение на нормативно задължение-разпоредбите на закони, подзаконови нормативни актове, кодекси и други чрез: устно интервю с лицето; хартиен носител-писмени документи-молби, заявления, лични документи по текущи въпроси в процеса на работа, подадени от лицето, както и от външни източници (от съдебни, финансови, осигурителни, данъчни и други институции в изпълнение на нормативни изисквания).

(4) Личните данни от лицата се подават на администратора на лични данни-Община Баните и длъжностното лице, назначено за обработването им, на основание нормативно задължение във всички случаи, когато е необходимо.

(5) Достъп до личните данни има само обработващият лични данни и / или действащото под негово пряко или на администратора ръководство лице, което обработва данни или има достъп до тях.

(6) Обработващият данните се задължава да не предоставя достъп до предоставените му за обработка данни на трети лица, освен в предвидените от закона случаи. Обработващият данните изготвя и представя на администратора на лични данни списък на оторизираните да оперират с данните служители.

(7) Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана в раздел шести от настоящите правила.

Чл. 10. (1) Формата на организация и съхраняване на личните данни на технически носител се осъществява чрез тяхното въвеждане на твърд диск на сървъри от компютърната мрежа (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 с 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 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защите 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 главен експерт "Информационно обслужване и технологии" в ОбА-Баните. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни) или от главен експерт "Информационно обслужване и технологии" в ОбА-Баните.

РАЗДЕЛ ПЕТИ
МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

Чл. 11. (1) Администраторът на лични данни предприема необходимите технически и организационни мерки, за да защити данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

(2) Администраторът взема специални мерки за защита, когато обработването включва предаване на данните по електронен път.

(3) Мерките по ал. ал. 1 и 2 са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването и на естеството на данните, които трябва да бъдат защитени.

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

(5) В случаите, когато обработването на данните не се извършва от

администратора, той е длъжен да определи обработващ данните и да осигури достатъчни гаранции за тяхната защита.

(6) Отношенията между администратора и обработващия лични данни се уреждат със заповед на администратора, в който се определя обемът на задълженията, възложени от администратора на обработващия данните.

(7) Обработващият лични данни, както и всяко лице, действащо под ръководството на администратора или на обработващия, което има достъп до лични данни, може да ги обработва само по указание на администратора, освен ако в закон е предвидено друго.

(8) След постигане целта на обработване на личните данни администраторът е длъжен да ги:

1. унищожи, или

2. прехвърли на друг администратор, като предварително уведоми за това Комисията за защита на личните данни, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването;

3. съхранява само в предвидените в закон случаи.

Чл. 12. (1) Мерките за гарантиране нивото на сигурност:

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

2. компютърните работни конфигурации да използват Desktop операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, да са компетентно балансирани и функционално оптимизирани.

3. за всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахранващи устройства (UPS).

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

- Операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани последни пакети за сигурност;

- Антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;

- Активирана защитна стена и деинсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на Община Баните и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите.

(2) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица със специални кодове, които им се предоставят от служителя по информационно обслужване главен експерт „Информационно обслужване и технологии".

Чл. 13. Физически мерки за гарантиране нивото на сигурност:

(1) В помещенията, в които са разположени компютърни и комуникационни средства, е осигурена:

-система за ограничаване на достъпа;

- поетапно въвеждане на СОТ.

(2) Всички работни помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран. Всички магнито-оптични 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 огнеупорен и водоустойчив шкаф, който се заключва, а ключът се съхранява от служителя по информационно обслужване главен експерт „Информационно обслужване и технологии" в ОбА-Баните. Контролът по използването на тези носители се извършва от Секретаря на община Баните.

Чл. 14. Организационни мерки за гарантиране нивото на сигурност:

1. Със Заповед на кмета на общината се определят обработващите лични данни за различните видове регистри, които се водят в Общината и всички други носители на информация.

2. Организира се денонощна охрана на работните помещения в рамките на охраната на цялата административна сграда на Общината (оперативни дежурни) и поетапно въвеждане на СОТ.

3. Работата с информационните системи се организира съобразно Вътрешни правила за информационните системи в Община Баните.

4. Забранено е използването на преносими лични носители на данни в звената от общинската администрация, в които се обработват лични данни.

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

6. Проверка на всички работни компютърни конфигурации по чл.8 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни се извършва на всеки шест месеца от ръководителя на съответното звено и от служителя по информационно обслужване главен експерт „Информационно обслужване и технологии" в ОбА.

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

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

9. При внедряване на нов програмен продукт за обработване на лични данни, следва със заповед на кмета на общината да се състави комисия по тестване и проверка възможностите на продукта, с оглед спазване изискванията на Закона за защита на личните данни и осигуряване на максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

РАЗДЕЛ ШЕСТИ
ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 15. (1) Служителите от община Баните са длъжни да спазват и изпълняват тези правила, в съответствие с длъжностните им характеристики.

(2) Обработващият лични данни се задължава да осигури ограничаване на достъпа до помещенията, в които се съхраняват данните само за оторизираните служители (монтиране на специализирани/еднопосочни брави), заключване на помещенията или други пособия.

(3) Обработващият лични данни се задължава да осигури достъп до електронните бази данни само по отношение на оторизираните служители (дефиниране на права на достъп до нивата, пароли за достъп до програмната среда, пароли за отваряне на файловете).

(4) Обработващият лични данни се задължава да осигури подходяща защита на

електронните данни чрез: поддържане на резервно копие, активиране на антивирусна защита.

Чл. 16. (1) За обработване на регистри или други носители на информация, съдържащи лични данни служителят подписва декларация, че е запознат със Закона за защита на лични данни, с настоящите Правила и защитата на личните данни, които се обработват от него.

(2) За неизпълнение на задълженията, вменени на съответните длъжностни лица по тези Правила и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда, Закона за държавния служител и други специализирани закони, а когато неизпълнението на съответното задължение е констатирано и установено от компетентен орган, предвиденото в Закона за защита на личните данни административно наказание-глоба. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди на трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Чл. 17. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между дирекциите (звената) в Общината след обосновано искане, чрез докладна записка от ръководителя на съответната дирекция и разрешение от секретаря на общината.

Чл. 18. (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в Община Баните.

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

- потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

- съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник;

- информация за логиката на всяко автоматизирано обработване на лични данни, отнасящи се до него, поне в случаите на автоматизирани решения по чл. 34б от Закона за защита на личните данни.

Чл. 19. (1) Физическото лице може да упражни своето право на достъп до лични данни, посочен по-горе, безплатно веднъж на 12 месеца, а при смърт правата му се упражняват от неговите наследници.

(2) Физическото лице има право по всяко време да поиска от администратора на лични данни да:

- заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на Закона за защита на личните данни.

- уведоми третите лица, на които са били разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с горното, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

(3) Ако при осъществяване достъпа до лични данни по искане на едно лице е възможно да се разкрият лични данни за друго лице, администраторът на лични данни е длъжен да предостави достъп само до частта от тях, отнасяща се до заитересованото лице.

Чл. 20. (1) Правото на достъп се осъществява с писмено заявление или

заявление 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.

(2) Заявлението 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.

(3) Заявлението се завежда в Центъра за услуги и информация на гражданите (ЦУИГ).

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

Чл. 21. (1) Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен, считане от деня на подаване на искането, съответно 30-дневен, когато обективно се изисква по-дълъг срок за събиране на всички искани данни на лицето и това сериозно затруднява дейността на администратора.

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

Чл. 22. (1) При искане за заличаване, блокиране на лични данни, поради неправомерно обработване, несъответстващо на Закона за защита на личните данни, администраторът взема решение и извършва съответното действие в 14-дневен срок от подаване на заявлението или мотивирано отказва извършването им.

(2) При искане за уведомяване на трети лица, на които са разкрити личните данни за извършеното заличаване, коригиране, блокиране, администраторът на лични данни взема решение в 14-дневен срок и незабавно уведомява третите лица или мотивирано отказва да извърши уведомяването.

Чл. 23. (1) Достъп до данните на лицето се предоставя под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него лице. Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забрането от закон. Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

(2) Администраторът на лични данни уведомява писмено заявителя за решението или отказа си в съответния срок, лично срещу подпис, или по пощата с обратна разписка. Липсата на уведомление се смята за отказ.

(3) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение.

(4) Администраторът отказва пълно или частично предоставяне на данни на лицето, за което те се отнасят, когато от това би възникнала опасност за отбраната или националната сигурност или за защита на класифицираната информация и това е предвидено в специален закон.

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

(6) Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със Заповед на Кмета на общината обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.

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

РАЗДЕЛ СЕДМИ
ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 24. (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 се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания.

(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.

Чл. 25. (1) Регистрите или другите носители на информация, съдържащи лични данни не се изнасят извън сградата на администратора. Никое длъжностно лице или трето лице няма право на достъп до регистрите или другите носители на информация с лични данни, освен ако данни от същите не са поискани по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). В такива случаи достъпът е правомерен.

(2) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи-писмени разпореждания на съответния орган, в който се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до лични данни.

(3) Съдебен орган може да изиска лични данни, съдържащи се в регистри или други носители на информация, писмено с изрично искане, отправено до Кмета на общината. В подобни случаи, на органите на съдебната власт, се предоставя копие от съдържащите се в регистрите лични данни, заверени с подписа на обработващия лични данни и печат на Общината. За идентичността на предоставените копия от документи с оригиналите им, отговорност носи обработващият лични данни. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, обработващият лични данни е длъжен да информира лицето, но не и да възпренятства работата на съответните органи.

РАЗДЕЛ ОСМИ
ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 26. (1) При възникване и установяване на инцидент веднага се докладва на лицето, отговорно за защита на личните данни.

(2) За инцидентите се води дневник „За юридическа консултация", в който задължително се списват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(3) След предоставеното мнение от юрисконсулта на Общината и след анализ от Секретаря на общината в дневника се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

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

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

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. По смисъла на тези Правила:

„Администратор на лични данни" е Община Баните, област Смолян, представлявана от Кмета на общината.

„Обработване на лични данни" е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

„Регистър на лични данни и всички други носители на информация, съдържаща лични данни" е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.

„Обработващ лични данни" са длъжностни лица от Общинска администрация-Баните, област Смолян, определени със заповед от Кмета на общината.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите Правила се издават на основание чл. 23, ал.4 от Закона за защита на личните данни и чл.19, т.2 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и във връзка с изискванията на новият европейски регламент за защита на личните данни-(ЕС2016/679 от 27 април 2016 г.).

§2. За допуснати нарушения по настоящите правила, виновните длъжностни лица носят дисциплинарна отговорност, освен ако деянието не представлява престъпление.

§3. За неуредените в тези правила въпроси се прилагат разпоредбите на действащата нормативна уредба.

§4. Контролът по прилагането и спазването на тези правила се осъществява от Секретаря на община Баните, област Смолян.

§5. Настоящите правила влизат в сила от деня на тяхното утвърждаване със заповед на Кмета на общината.

Изготвил: (п)
Росен Кичуков
Секретар на община Баните
Баните, 24.04.2018 г.