Община Добричка, град Добрич

Ул."Независимост" № 20, централа: 058/600 889; факс: 058/600 806;
e-mail: obshtina@dobrichka.bg; web site: www.dobrichka.bg

СЛИЦЕ КЪМ ХОРАТА

УТВЪРДИЛ,
ПЕТКО ПЕТКОВ
КМЕТ НА ОБЩИНА ДОБРИЧКА

ИНСТРУКЦИЯ ЗА МИНИМАЛНОТО НИВО НА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ В ПОДДЪРЖАНИТЕ РЕГИСТРИ В ОБЩИНА ДОБРИЧКА

Глава първа
Общи положения

Чл.1 Настоящата инструкция е разработена в изпълнение на чл.23 и чл.24, ал.4 от ЗЗЛД и чл. 3 и чл. 5 от Наредба № 1/07.02.07г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Чл.2 Настоящата инструкция има за цел да регламентира:

(1)Механизмите на водене, поддържане и защита на регистрите съхраняващи лични данни на български граждани в Общинска администрация на община Добричка;

(2)Задълженията на длъжностните лица, обработващи лични данни, и тяхната отговорност при неизпълнение на тези задължения;

(3)Необходимите технически и организационни мерки за защита личните данни на посочените по-горе лица от неправомерно обработване.

Глава втора
Администратор на лични данни

Чл.3 Администратор на лични данни е Община Добричка, със седалище и адрес на управление: гр.Добрич, ул. «Независимост» № 20, представлявана от Кмета на общината.

Глава трета
Регистри на лични данни

Чл.4 (1) В регистрите се обработват и съхраняват лични данни на граждани /служители/ с цел:

1.Изпълнение на нормативно установено задължение на администратора;

2.Изпълнение на задача, която се осъществява в обществен интерес;

3.Упражняване на правомощия, предоставени със закон на администратора.

(2) В регистрите се обработват следните групи лични данни:

1.Относно физическата идентичност на лицата: имена, ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.;

2.Относно семейна идентичност на лицата: семейно положение (наличие на брак, развод, брой членове на семейството, в това число деца и др.);

3.Относно образованието: вид на образованието, допълнителна квалификация и др.;

4.Относно трудовата дейност: професионална биография, данни от трудовата книжка и др.;

5.Относно здравния статус на лицата;

6.Относно гражданско- правния статус на лицата (напр. свидетелство за съдимост), необходими за длъжностите, свързани с материална отговорност;

7.Относно обществена идентичност! : (расов или етнически произход, др.);

8.Относно икономическа идентичност: (имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа в дружества, др.);

9.Относно културна идентичност (интереси, др.);

10.Други.

(3)Обработваните лични данни в регистрите са съобразени с изискванията на чл.2, ал.2 от ЗЗЛД и са съотносими, свързани със и ненадхвърлящи целта, за която се обработват.

(4)Видове регистри съдържащи лични данни, форми на водене и място на съхранение, посочени в Приложение №1 към настоящата инструкция, което се актуализира при необходимост.

Глава четвърта

Определяне на нива на чувствителност за обработваните данни и препоръчителен вид на носителя на данните за трайно съхранение

Чл.5 (1) На хартиен и технически носител, както следва :

1.Данните се набират в писмена (документална) форма и се съхраняват в папки, дела, специални регистри и върху външни технически носители (CD или дискетно устройство);

2.Обработените лични данни в регистрите се съхраняват в работните помещения на служителите и в архива на община Добричка;

3.Служителите, обработващи лични данни, предприемат всички организационно- технически мерки за съхраняването(архивирането) и опазването на личните данни, в това число ограничаване на достъпа до тях на външни лица и служители;

4.Хартиените и технически носители не се изнасят извън сградата на общината

(2)В компютърна система:

1.Личните данни се въвеждат в бази от данни (програмни продукти, уеб-базирани приложения), които бази са инсталирани върху сървърни системи на администратора (работа в мрежа), локално върху работни станции, като част от локално инсталираните приложения за обработка на лични данни са свързани с

обществената мрежа (т.н уеб-базирани приложения за обработка на лични данни), като непосредствен достъп имат само служители, обработващи лични данни.

2.Компютрите на служителите, обработващи лични данни, както и сървърните системи са изолирани в помещения за самостоятелна работа.

3.Прави се ежедневен и месечен архив на базите данни, обработващи лични данни от съответните длъжностни лица и от мл.експерт ИОТ.

4.Архивите се съхраняват и на технически носители, които не се изнасят извън сградата на администратора на лични данни.

Глава пета
Определяне на лицата които отговарят за обработка на личните данни, техните права и задължения.

Чл.6 Длъжностните лица, обработващи лични данни в съответния регистър, са щатно определени, като задълженията им за обработване на лични данни е вменено с длъжностните им характеристики за длъжността, на която са назначени .

Чл.7 Длъжностните лица са задължени да събират; обработват и предоставят лични данни съгласно ЗЗЛД, които са необходими за изпълнение на тяхната длъжност и са им възложени от Администратора.

Чл.8 Данните се заличават /коригират/, когато се установи, че са неточни или непропорционални по отношение целите на настоящия регистър.

Чл.9 Служителят, обработващ лични данни, е длъжен да ги актуализира при необходимост.

Чл.10 Данните се поддържат във вид, който позволява идентифициране на съответните физически лица за срок, определен в съответния регистър.

Чл.11 Личните данни, съхранявани за по - дълъг период /за исторически, статистически или научни цели/ се поддържат във вид, непозволяващ идентифицирането на физическите лица.

Глава шеста
Списък от задължителни и препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразно вида и чувствителността на данните

Чл.12 Управлението на информационната инфраструктура на общината е централизирано - работи се в домейнова среда. Домейните са съвкупности от компютри, които може да се управляват колективно с помощта на домейн контролери, представляващи Windows Server 2003 или Windows Server 2008 системи, които "управляват достъпа до мрежата, до директорийната база данни и до споделените ресурси. В рамките на един домейн, потребителите се аутентикират (процес за проверка дали кандидат е този, за когото се представя, чрез въвеждане на потребителско име и парола (пред всеки компютър в домейна) пред един централен(главен) сървър наречен домейн контролер, който управлява всички взаимодействия потребител-домейн, свързани със сигурността и централизира администрирането. Домейн контролерът осигурява валидирането на всеки потребител.

Чл.13 (1) Мерките за защита и ограничаване на достъпа до мрежовите ресурси и бази данни, обработващи лични данни са :

1.Аутентикиране на потребителите(служителите)- потребителите се аутентикират (процес за проверка дали кандидат е този, за когото се представя, чрез въвеждане на потребителско име и парола пред всеки компютър в домейна) пред един централен(главен) сървър наречен домейн контролер, който управлява всички взаимодействия потребител-домейн, свързани със сигурността и централизира администрирането. Домейн контролерът осигурява валидирането на всеки потребител.

2.Организация и групиране на потребителите в т.н. групи за сигурност в активната директория на домейн-контролера-Необходимостта от възможност за напълно централизиран административен контрол, програмните продукта и информационните ресурси(в т.ч и бази данни за обработка на лични данни), с които разполага община Добричка, респективно делегиране на управлението(отдават се специални права и задължения на индивидуалните потребители и потребителски групи по отношение на наличните информационни ресурси) и контрол върху достъпа до тези ресурси, обуславят дефинирането на групите за сигурност в домейна.

3.Въвеждане на потребителско име и парола за работа с база данни, обработваща лични данни-всеки програмен продукт, уеб-базирано приложение и информационна система, обработваща лични данни, изисква въвеждането на потребителско име и парола от длъжностното лице за достъп до т

(3)На служителите, обработващи лични данни, се забранява да ги предоставят на трети лица и за целта подписват декларация, с която поемат задължението да не разпространяват личните данни на посетителите.

(4)Достъп до личните данни имат:

1.Кметът на община Добричка;

2.Заместник кметове и секретар съгласно правомощията им по ЗМСМА и Устройствения правилник на общината;

3.Служителите, обработващи лични данни, директори на дирекции в съответните ресори;

4.Достъп за справки в ЛДБ Население имат : секретаря на общината, директора на дирекция АПИОТУС, мл. експерт ИОТ, мл.експерт ЦУИ ;

5.Достъп за обработка и справки в ЛБД „Население" и НБД „Население" имат определени служители, като това им право и задължение е вменено в длъжностните им характеристики;

6.Достъп до личните данни на гражданите имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия;

(5)Достъпът до лични данни се осъществява по реда, предвиден в ЗЗЛД.

(6) Забранява се използването външните устройства на системата за въвеждане на друг вид информация.

Глава седма
Спецификация на техническите ресурси, прилагани за обработка на личните данни

Чл.14 (1) За хартиени и технически носители:

1.Данните се обработват в папки, дела и регистри или върху външни технически носители(CD или дискетно устройство).

(2)За компютърната система:

1.Сървъри под управлението на Windows 2003 Server Standard Edition R2 и Windows 2008 Server Standard Edition R2.

2.Работни станции под управлението на Windows XP Professional.

Глава осма
Организационна процедура за обработване на личните данни, включваща време, място и ред при обработване

Чл.15 Обработването на лични данни се извършва от съответния служител по щат на обособеното работно място в определеното за администрацията работно време.

Чл.16 Документите, съдържащи лични данни се обработват по ред съобразен със ЗЗЛД и настоящата инструкция.

Глава девета
Мероприятия за защита на техническите и информационните ресурси при аварии, произшествия и бедствия (пожар, наводнение и др.)

Чл.17 За безопасна работа и защита при възникване на авария Администратора е предвидил използване на непрекъсваеми токозахранващи устройства ДОЗ.

Чл.18 При пожар или наводнение материалите съдържащи лични данни се изнасят на безопасно място в сградата където се охраняват от служителите, обработващи личните данни.

Чл.19 Служителите обработващи лични данни периодично архивират всички материали, съдържащи лични данни на технически носители.

Глава десета
Средства за предотвратяване на умишлено повреждане или нерегламентиран достъп до личните данни

Чл.20 Чрез въвеждане на уникални ПОТРЕБИТЕЛСКО ИМЕ и ПАРОЛА за достъп до домейна - всеки служител обработващ лични данни и член на домейна, притежава уникално потребителско име и парола, които се генерират от системния администратор за достъп до домейна;

Чл.21Чрез въвеждане на уникални ПОТРЕБИТЕЛСКО ИМЕ и ПАРОЛА за достъп до бази данни, обработващи лични данни- всеки служител обработващ лични данни притежава уникално потребителско име и парола, които се генерират от системния администратор за достъп до базите данни, обработващи лични данни, известни само на тях и на системния администратор (с изключение на потребителските имена и пароли на служителите, обработващи лични данни в НБД чийто достъп се предоставя от ГД «ГРАО» София след подписване на споразумение за достъп и служителя отговарящ за поддържането на ЕИСУЧРДА, чиито потребителско име и парола се предоставят от МДААР), а в отсъствие на служителя, обработващ данните, паролата се съобщава на лицето, което ще го замества;

Чл.22 Чрез използване на антивирусна програма, поддържана в актуално състояние и защита в реално време, срещу вирусни атаки;

Чл.23 Чрез ежедневен архив на базите данни, обработващи лични данни, върху компютърни системи, на хартиен и външни технически носители, които се съхраняват в обособено сървърно помещение;

Чл.24 Заключване на работните кабинети при излизане на служителите от тях;
Чл.25 Работните места се охраняват от оперативни дежурни по ОбСС и управление при кризи при спазването на Инструкция за охранително-пропускателния режим в сградата на община Добричка и кметствата, осъществява се й видео наблюдение на сградата на общинската администрация;
Чл.26 Данъчната информация ежедневно се архивира и ежемесечно се предава в информационния масив на Дирекция "НАЛ" - Добрич;
Чл.27 Информацията по ГРАО се дублира, като се обновява ежедневно в Национална база данни София;
Чл.28 Информацията от трудовите и служебните досиета на служителите се дублира в ЕИСУЧРДА;
Чл.29 Сървърното помещение в община Добричка е климатизирано.

Глава единадесета
Ред за съхраняване и унищожаване на информационни носители

Чл.30 Обработените лични данни се съхраняват на хартиен и електронен носител.
Чл.31 При повреда на компютър системният администратор извършва подмяна на същия и презаписва информацията.
Чл.32 При приключване на съответен регистър данните се унищожават /архивират/ от назначена комисия, която представя протокол на администратора на лични данни.
Чл.33 Срок на съхранение на информационните носители е по ЗЗЛД.

Глава дванадесета
Ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ

Чл.34 Системният администратор единствен има право да генерира уникални ПОТРЕБИТЕЛСКОТО ИМЕ и ПАРОЛА за достъп до домейна и базите данни, с изключение на служителите, обработващи лични данни в НБД, чиито потребителско име и парола за достъп се предоставят от ГД „ГРАО"-София, след подписване на споразумение и служителя оттоварящ за поддържането на ЕИСУЧРДА, чиито потребителско име и парола се предоставят от МДААР.
Чл.35 Паролата се сменя периодично от системния администратор или в случай на узнаването й от нерегламентирано лице.
Чл.36 На служителите обработващи лични данни в НБД паролите за достъп периодично се подменят от ГД «ГРАО».

Глава тринадесета
Правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.

Чл.37 Системният администратор е длъжен:
1.Да извършва ежемесечна профилактика на компютърната система и актуализиране на системната информация;
2.Да поддържа надежден софтуер за борба с вируси;
3.Ежемесечно да проверява за неправомерно инсталиран софтуер;

4.Посредством налична техника и софтуер да се грижи за целостта на базата данни;

5.Да поддържа софтуерът за всекидневен и месечен архив на наличните бази данни.

Глава четиринадесета
Контрол

Чл.38 Кмета на Община Добричка възлага на Секретаря на Община Добричка да извършва периодичен контрол за спазване изискванията на настоящата инструкция.

Чл.39 За резултатите от контрола се докладва лично на Кмета на общината.

Чл.40 При констатирани нарушения кмета взема мерки за тяхното отстраняване.

Чл.41 (1)За неизпълнение на задълженията от страна на съответните длъжностни лица по тази инструкция и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда и ЗДС.

(2)Когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган се налага предвиденото в Закона за защита на личните данни административно наказание глоба или имуществена санкция.

Чл.42 В резултат от действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако извършеното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Глава петнадесета
Допълнителна разпоредба

§1. Настоящата Инструкция е задължителна за всички длъжностни лица от Общинска администрация при община Добричка, работещи с регистри с лични данни и влизат в сила след утвърждаването й от Кмета на общината със заповед.

Съгласували :

Секретар :
Соня Георгиева

Юрист :
Веселина Георгиева

Изготвил :
Росица Великова