НАРЕДБА № 1 от 7.02.2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни

Издадена от председателя на Комисията за защита на личните данни, обн., ДВ, бр. 25 от 23.03.2007 г.

Глава първа

ОБЩИ УСЛОВИЯ

Чл. 1. (1) С тази наредба се определя минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита.

(2) Мерките по ал. 1 включват следните средства за защита на личните данни:

1. програмно-апаратни;

2. физически;

3. организационни;

4. нормативни.

Чл. 2. Наредбата има за цел да осигури адекватно ниво на защита на личните данни в поддържаните регистри с лични данни чрез осигуряване на минимално необходимите технически и организационни средства и мерки.

Глава втора

ЛИЦА, ОСЪЩЕСТВЯВАЩИ ПРИЛАГАНЕТО И КОНТРОЛА ЗА ИЗПЪЛНЕНИЕ НА НАРЕДБАТА

Чл. 3. (1) Прилагането на необходимите технически и организационни мерки за защита на личните данни се осъществява от администратора на лични данни или от лице по защита на личните данни.

(2) Администраторът може да назначи едно или повече лица по защитата на личните данни, които отговарят за координиране и прилагане на мерките по ал. 1.

(3) Лицата, мерките и средствата за защита на лични данни се определят с вътрешни правила (инструкция или заповед) на администратора на лични данни.

Чл. 4. Администраторът има следните права и задължения:

1. определя политиката за защита на личните данни в организацията;

2. осигурява организацията по водене на регистрите съгласно предвидените мерки

за гарантиране на адекватна защита;

3. определя конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;

4. утвърждава вътрешните правила за защита на регистрите;

5. периодично информира персонала по въпросите на защитата на личните данни;

6. осъществява контрол по спазване на изискванията за защита на регистрите;

7. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

8. оказва съдействие при осъществяване на контролните функции на комисията;

9. подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;

10. определя правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка.

Чл. 5. (1) Вътрешните правила по чл. 3, ал. 2 включват:

1. определяне на нива на чувствителност за обработваните лични данни и препоръчителен вид на носителя на данните за трайно съхраняване (хартиен, електронен, технически);

2. определяне на лицата, които отговарят за обработката на лични данни, техните права и задължения;

3. списък от задължителни и препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразено вида и чувствителността на данните;

4. спецификация на техническите ресурси, прилагани за обработка на личните данни;

5. организационна процедура за обработване на личните данни, включваща време, място и ред при обработване, като чрез регистрация на всички извършени действия с регистрите в компютърната среда е препоръчително да се създава системен файл-дневник, достъпен само за системния администратор и лицето по защита на личните данни;

6. мероприятия за защита на техническите и информационните ресурси при аварии, произшествия и бедствия (пожар, наводнение и др.);

7. средства за предотвратяване на умишлено повреждане или нерегламентиран достъп до личните данни;

8. ред за съхраняване и унищожаване на информационни носители;

9. ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;

10. 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.

(2) Администраторът провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 6. Администраторът осигурява контролиран достъп на служителите при обработване на лични данни във връзка със:

1. техническите и програмно-информационните ресурси, използвани при обработката и защитата на личните данни;

2. информационните носители и извършваните действия по тяхното регистриране, преместване, подреждане, копиране, преобразуване и друг вид обработка;

3. личните данни в регистрите, както и контрол на лицата, извършващи действия по обработване на личните данни съгласно предоставените им права;

4. разполагането, поддържането и преместването на техническите ресурси, използвани за обработка на личните данни.

Чл. 7. Администраторът осигурява при въвеждане, промяна или предаване на лични данни в регистрите съхраняване на информация за:

1. времето (дата и час) на въвеждане, промяна или предаване на личните данни;

2. лицата, извършващи въвеждането, промяната или предаването на личните данни;

3. лицата, предоставили личните данни;

4. личните данни, които са били въведени, променени или предадени в регистрите.

Чл. 8. Лицето по защита на личните данни е задължено да подпомага администратора при изпълнение на действията му по чл. 4, ал. 2, 3, 8 и 9 , чл. 5, ал. 3, 4, 5, 6, 7, 8, 9 и 10 , чл. 6 и 7 .

Глава трета

НИВА НА ЗАЩИТА

Чл. 9. В зависимост от рисковете при обработване на личните данни и вида им се определят следните нива на защита: начално, средно и високо.

Чл. 10. Мерките за защита, класифицирани при начално ниво, се предприемат за всички регистри с лични данни, обработвани само на хартиен носител.

Чл. 11. Мерките за защита, класифицирани при начално и средно ниво, се предприемат за всички регистри с лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър или в мрежа, несвързани с обществената мрежа.

Чл. 12. Мерките за защита, класифицирани при начално, средно и високо ниво, се предприемат за всички регистри с лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър или в мрежа, свързани с обществената мрежа.

Глава четвърта

МЕРКИ ПРИ НАЧАЛНО НИВО НА ЗАЩИТА

Чл. 13. (1) Администраторът приема правила за сигурност, които са задължителни за служителите, оторизирани с достъп до регистри с лични данни.

(2) Минималното съдържание на правилата по ал. 1 включва:

1. подробно описание на регистрите;

2. мерки за гарантиране на нивото на сигурност: оторизиран достъп на служители само до данни и ресурси, необходими за изпълнение на техните задължения; заключване на помещенията; заключване на шкаф/каса за съхранение на регистъра;

3. права и задължения на служителите;

4. процедури за докладване, управляване и реагиране при инциденти.

Чл. 14. Администраторът актуализира правилата по чл. 13, ал. 1 при промяна в регистрите или в техния начин на организация.

Чл. 15. Процедурата за докладване и управление на инциденти по чл. 13, ал. 1, т. 4 задължително включва регистриране на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 16. (1) Служителите на администратора имат оторизиран достъп само до тези регистри, които са необходими за изпълняване на техните задължения.

(2) Администраторът създава механизми за предотвратяване на достъп до регистрите на служители, различни от оторизираните.

(3) Предоставянето, промяната или прекратяването на оторизиран достъп до регистри в съответствие с критериите, приети от администратора, се извършва единствено от оторизираните съгласно правилата по чл. 13, ал. 1 служители.

Чл. 17. (1) Информацията, която се съдържа в регистрите, трябва да бъде идентифицирана, инвентаризирана и съхранявана на място с ограничен достъп само за определени от администратора служители.

(2) Унищожаването на регистрите от тези помещения се извършва само от администратора или изрично упълномощено от него лице.

(3) Временните регистри трябва да отговарят на съответното ниво за сигурност и се унищожават веднага след отпадане на целите, за които са били създадени.

Чл. 18. (1) Администраторът носи отговорност за законосъобразното прилагане на процедурите за създаване на архивни копия и за възстановяване на данни.

(2) Приетите процедури за създаване на архивни копия и за възстановяване на данни трябва да гарантират, че данните могат да бъдат реконструирани в състоянието, в което са били по време на изгубването или унищожаването им.

Чл. 19. (1) При обработване в регистър с лични данни по смисъла на чл. 5, ал. 2 във връзка с ал. 1 от закона се предприемат допълнителни мерки за регистриране на всеки достъп до лични данни/регистри (журнален запис), който да се съхранява най-малко две години.

(2) При обработване в регистър с лични данни по ал. 1 се прилагат и мерките по чл. 13 , 14 , 15, 16, 17 и 18 .

Глава пета

МЕРКИ ПРИ СРЕДНО НИВО НА ЗАЩИТА

Чл. 20. Средното ниво на защита на личните данни включва осигуряване на мерките, предвидени в чл. 13 , 14 , 15, 16, 17 и 18 . При изготвяне на правилата за това ниво следва да се предвидят следните допълнителни мерки за защита:

1. възможност за установяване самоличността на лицето, отговорно за сигурността;

2. включване на процедури за създаване на архивни копия и възстановяване на данни;

3. периодични проверки, които следва да се извършват, за да се наблюдава спазването на правилата и мерките, които трябва да се предприемат за отстраняване на нарушенията.

Чл. 21. Във връзка с периодичния контрол по чл. 20, т. 3 администраторът е длъжен да представи резултатите при поискване от Комисията за защита на личните данни.

Чл. 22. (1) Администраторът създава механизми, позволяващи недвусмислено, персонализирано идентифициране на всеки служител, който се опитва да стартира и да получи достъп до информационната система и да установи дали всеки един

служител е оторизиран.

(2) Администраторът задължително поставя ограничения на обхвата за повторни опити за получаване на неоторизиран достъп до информационната система.

Чл. 23. Само надлежно оторизираните служители съгласно правилата по чл. 13 могат да имат достъп до помещенията, където се намират информационни системи с лични данни.

Чл. 24. Администраторът създава система за регистриране на достъпа до регистрите, получавани и/или предавани на технически носител или по електронен път в локалната мрежа, която позволява прякото или косвеното идентифициране на вида данни, датата и времето, изпращащия, как са обработени получените/изпратените данни, както и получателя, който трябва да е надлежно оторизирано лице.

Чл. 25. Временните файлове трябва да отговарят на съответното ниво за сигурност и се унищожават веднага, след като се изпълнят целите, за които са били създадени.

Чл. 26. (1) В регистъра по чл. 24 се отразяват извършените процедури за възстановяване на данни, като се посочват лицето, заето с процеса, възстановените данни и кои от тях са възстановени ръчно.

(2) При всякакви процедури за възстановяване на данни е необходимо писмено възлагане от страна на администратора.

Чл. 27. Архивното копие и процедурите за възстановяване на данни се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните, и във всички случаи се предприемат мерките за сигурност, изисквани в наредбата.

Чл. 28. (1) При обработване на регистър с лични данни по смисъла на чл. 5, ал. 2 във връзка с ал. 1 от закона се предприемат допълнителни мерки за носителите, съдържащи лични данни, като тези носители могат да се разпространяват само ако данните са криптирани или е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(2) При обработване на регистър с лични данни по ал. 1 се прилагат и мерките по чл. 19 , 20 , 21, 22, 23, 24, 25, 26 и 27 .

Глава шеста

МЕРКИ ПРИ ВИСОКО НИВО НА ЗАЩИТА

Чл. 29. Високо ниво на защита на личните данни включва осигуряване на мерките, предвидени в чл. 20 , 21 , 22, 23, 24, 25, 26 и 27 .

Чл. 30. (1) Задължителната информация, която следва да бъде регистрирана при

високо ниво на защита, е: идентичност на служителя; дата на достъп; регистърът, за който е получен достъп; вид на достъпа и кога достъпът е бил отказан.

(2) Извън информацията по ал. 1 администраторът регистрира и информация, която позволява да се идентифицира записът, до който е имал достъп служителят.

(3) Информацията по ал. 1 и 2 се съхранява за период най-малко две години.

(4) Правилата за регистриране на данните по предходните алинеи се определят от администратора, който лично или чрез лично назначено от него лице осъществява контрол за спазването им и за недопускане на деактивирането им.

(5) Администраторът отговаря за извършване на редовни проверки на записаната информация по контрола и изготвя отчет за тях, установени най-малко веднъж месечно.

Чл. 31. (1) При обработване на лични данни по смисъла на чл. 5, ал. 2 във връзка с ал. 1 от закона се предприемат допълнителни мерки, свързани с разпространението им по телекомуникационни мрежи, под формата на криптиране или използване на друг механизъм, гарантиращ, че данните са нечетливи или не са променени.

(2) При обработване на лични данни по ал. 1 се прилагат и мерките по чл. 28 , 29 и 30 .

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на тази наредба:

1. "Лице по защита на личните данни" е физическо или юридическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на минимално необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.

2. "Ниво на защита" е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.

3. "Потребител" е всяко едно лице, оторизирано от администратора, с достъп до регистър.

4. "Достъп до лични данни" е предоставената възможност на потребителя да използва регистрите.

5. "Инцидент" е непредвидимо обстоятелство, което би могло да засегне сигурността на данните.

6. "Носител на лични данни" е физически обект, който е възможно да бъде обработен в информационна система и на който могат да се запишат данни или могат да се възстановят от същия.

7. "Временни файлове" са сбор от данни или информация на електронен носител, създадени за период от време до започване изпълнението на целите, за които са определени.

8. "Архивни копия" са копия на данните, които се съдържат в компютърен файл, съхранявани на подходящ носител, чрез които може да се осъществи възстановяването.

9. "Възстановяване на данни" са процедури по реконструиране на личните данни в състоянието, в което са били по време на изгубването или унищожаването им.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. Администраторът на лични данни е длъжен да приведе своите вътрешни правила в съответствие с тази наредба:

1. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за сигурност на начално ниво, предвидени в нея, трябва да бъдат изпълнени до два месеца от нейното влизане в сила;

2. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за сигурност на средно ниво, предвидени в нея, трябва да бъдат изпълнени до шест месеца от нейното влизане в сила;

3. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за сигурност на високо ниво, предвидени в нея, трябва да бъдат изпълнени до една година от нейното влизане в сила.

§ 3. Наредбата се приема на основание чл. 23, ал. 5 от Закона за защита на личните данни.