НАРЕДБА № 1

от 30 януари 2013 г.

за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни

(<u>отменена, считано от 25.05.2018 г.</u>)

Глава първа.
ОБЩИ ПОЛОЖЕНИЯ

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

Чл. 2. Наредбата има за цел да осигури адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

Чл. 3. (1) Администраторът на лични данни определя вида на личните данни, целите и средствата за обработването им, освен ако те не са определени със закон.

(2) При осъществяване на дейността по ал. 1, администраторът структурира съвкупност от лични данни за целите на съответен регистър.

(3) Администраторът обработва лични данни в поддържаните регистри, при спазване на принципите по чл. 2, ал. 2 и 3 от Закона за защита на личните данни.

Чл. 4. (1) Администраторът предприема необходимите технически и организационни мерки за защита на личните данни, за да гарантира адекватно ниво на защита, което отговаря на обработваните лични данни и въздействието при нарушаване на защитата им.

(2) Мерките по ал. 1 имат за цел да гарантират поверителност, цялостност и наличност на личните данни.

Глава втора.
ВИДОВЕ ЗАЩИТА

Чл. 5. Видовете защита на личните данни са физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи и криптографска защита.

Чл. 6. (1) Физическата защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

(2) Основните организационни мерки на физическата защита са:

1. определяне на зоните с контролиран достъп;

2. определяне на помещенията, в които ще се обработват лични данни;

3. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;

4. определяне на организацията на физическия достъп;

5. определяне на режима на посещения;

6. определяне на използваните технически средства за физическа защита;

7. определяне на екип за реагиране при нарушения.

(3) Основните технически мерки на физическата защита са:

1. ключалки;

2. шкафове;

3. метални каси;

4. оборудване на зоните с контролиран достъп;

5. оборудване на помещенията;

6. устройства за контрол на физическия достъп;

7. охрана и/или система за сигурност;

8. средства за защита на периметъра;

9. пожарогасителни средства;

10. пожароизвестителни и пожарогасителни системи;

11. детектори за субстанции (метали, взривни вещества и др).

Чл. 7. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;

2. познаване на политиката и ръководствата за защита на личните данни;

3. знания за опасностите за личните данни, обработвани от администратора;

4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

5. съгласие за поемане на задължение за неразпространение на личните данни;

6. обучение;

7. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае”.

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;

2. политиката и ръководствата за защита на личните данни;

3. опасностите за личните данни, обработвани от администратора.

(5) Лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

(6) Администраторът поддържа информация за изпълнение на задълженията си по ал. 2, т. 5, 6 и 7.

Чл. 8. (1) Документалната защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

(2) Основните мерки на документалната защита са:

1. определяне на регистрите, които ще се поддържат на хартиен носител;

2. определяне на условията за обработване на лични данни;

3. регламентиране на достъпа до регистрите;

4. контрол на достъпа до регистрите;

5. определяне на срокове за съхранение;

6. правила за размножаване и разпространение;

7. процедури за унищожаване;

8. процедури за проверка и контрол на обработването.

Чл. 9. (1) Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи са:

1. политика за защита на личните данни, ръководства по защита и стандартни операционни процедури;

2. определяне на роли и отговорности;

3. идентификация и автентификация;

4. управление на регистрите;

5. контроли на сесията;

6. външни връзки/свързване;

7. телекомуникации и отдалечен достъп;

8. наблюдение;

9. защита от вируси;

10. планиране на случайността/непредвидените случаи;

11. поддържане/експлоатация;

12. управление на конфигурацията;

13. копия/резервни копия за възстановяване;

14. носители на информация;

15. физическа среда/обкръжение;

16. персонална защита;

17. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;

18. определяне на срокове за съхранение на личните данни;

19. процедури за унищожаване/заличаване/изтриване на носители.

Чл. 10. (1) Криптографската защита представлява система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.

(2) Основните мерки на криптографската защита са:

1. стандартните криптографски възможности на операционните системи;

2. стандартните криптографски възможности на системите за управление на бази данни;

3. стандартните криптографски възможности на комуникационното оборудване;

4. системи за разпределение и управление на криптографските ключове;

5. нормативно определените системи за електронен подпис.

Глава трета.
ОЦЕНКА И НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 11. (1) За определяне на адекватното ниво на техническите и организационни мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни.

(2) Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

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

Чл. 12. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение, която се основава на автоматизирано обработване и на чието основание се вземат мерки, които пораждат правни последици за лицето или го засягат в значителна степен;

2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном.

3. лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;

4. лични данни в широкомащабни регистри на лични данни;

5. данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

Чл. 13. Определят се следните нива на въздействие:

1. „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. „Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 14. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри, съгласно Приложение № 1.

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2, определя нивото на въздействие на съответния регистър.

(4) За група съвместно съхранявани или обработвани регистри нивото на въздействие е най-високото от определеното за всеки от регистрите от групата съгласно Приложение № 2.

Глава четвърта.
НИВА НА ЗАЩИТА

Чл. 15. (1) В зависимост от нивото на въздействие се определя и съответно ниво на защита.

(2) Нивото на защита представлява съвкупност от технически и

организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, както и криптографска защита на личните данни.

Чл. 16. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) Нивата на защита са, както следва:

1. при ниско ниво на въздействие – ниско ниво на защита;

2. при средно ниво на въздействие – средно ниво на защита;

3. при високо ниво на въздействие – високо ниво на защита;

4. при изключително високо ниво на въздействие – изключително високо ниво на защита.

Чл. 17. Минималното ниво на технически и организационни мерки, които следва да осигури администраторът (Приложение № 3) е, както следва:

1. при ниско ниво на защита – мерките по чл. 6, ал. 2, т. 2 – 4, ал. 3, т. 1, 2, 5 и 9, чл. 7, ал. 2, т. 1, 3 и 5, чл. 8, ал. 2, т. 1 – 3, 5 и 7, чл. 9, ал. 2, т. 3, 4, 6, 9, 13, 14, 16,18 и 19;

2. при средно ниво на защита – мерките по т. 1, както и мерките по чл. 6, ал. 2, т. 1 и 6, чл. 7, ал. 2, т. 2, 4, 6 и 7, чл. 8, ал. 2, т. 4 и 6, чл. 9, ал. 2, т. 7, 11 и 15, чл. 10, ал. 2, т. 1, 2 и 3;

3. при високо ниво на защита – мерките по т. 2, както и мерките по чл. 6, ал. 2, т. 5 и 7, ал. 3, т. 4, 6 – 8, 10 и 11, чл. 8, ал. 2, т. 8, чл. 9, ал. 2, т. 1, 2, 5, 8, 10, 12 и 17, чл. 10, ал. 2, т. 4 и 5;

4. при изключително високо ниво на защита администраторът предприема мерките по т. 3, както и мерки, произтичащи от международни политики за сигурност или актове с международен характер.

Глава пета.
ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 18. (1) Прилагането на необходимите технически и организационни мерки за защита на личните данни се осъществява от администратора на лични данни или от определено от него лице по защита на личните данни.

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

Чл. 19. Администраторът има следните задължения:

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

2. приема инструкция по чл. 23, ал.4 от Закона за защита на личните данни;

3. осигурява организацията по водене на регистрите;

4. прилага конкретни мерки за защита съобразно спецификата на водените регистри;

5. осъществява контрол по спазване на изискванията за защита на регистрите, установява обстоятелства, свързани с нарушаване на тяхната защита, и предприема мерки за тяхното отстраняване;

6. актуализира поддържаните регистри с лични данни;

7. извършва периодична оценка на въздействието по чл.11;

8. оказва съдействие при осъществяване на контролните функции на Комисията за защита на личните данни.

Чл. 20. (1) Инструкцията по чл. 19, т. 2 включва:

1. индивидуализиране на администратора на лични данни;

2. общо описание на поддържаните регистри – категории лични данни и основание за обработване;

3. технологично описание на поддържаните регистри – носители на данни, технология на обработване, срок за съхранение и предоставени услуги;

4. определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им;

5. оценка на въздействие и определяне на съответно ниво на защита съгласно глава трета;

6. описание на предприетите технически и организационни мерки;

7. действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.);

8. предоставяне на лични данни на трети лица – основание, цел, категории лични данни;

9. срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им;

10. определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни;

(2) Информацията по т. 2-10 от предходната алинея се описва за всеки един от поддържаните регистри.

Допълнителна разпоредба

§ 1. По смисъла на тази наредба:

1. „Лице по защита на личните данни” е физическо 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 необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.

2. „Носител на лични данни” е физически обект, на който могат да се

запишат данни или могат да се възстановят от същия.

3. „Резервни копия за възстановяване” са копия на данните, съхранявани на носител, чрез които може да се осъществи възстановяването.

4. „Поверителност” е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

5. „Цялостност” е изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

6. „Наличност” е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

7. „Особено голяма група физически лица” е съвкупност от физически лица, чиито брой надхвърля 1000000;

8. „Голяма група физически лица” е съвкупност от физически лица, чиито брой надхвърля 10000;

9. „Група физически лица” е съвкупност от физически лица, чиито брой надхвърля 2;

10. „Лица, заемащи висши държавни длъжности” са лицата по чл. 2, ал. 1 от Закона за публичност на имуществото на лица, заемащи висши държавни длъжности.

11. „Широкомащабни регистри на лични данни” са разпределени масиви с лични данни, чието управление не може да бъде осъществено със стандартните средства за управление на база данни.

Преходни и заключителни разпоредби

§ 2. Администраторът на лични данни е длъжен да осигури минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита в съответствие с тази наредба:

1. в срок до 6 месеца от влизане на наредбата в сила администраторът е длъжен да определи нивото на въздействие на обработваните от него регистри;

2. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за защита на ниско ниво, предвидени в нея, трябва да бъдат изпълнени до 6 месеца след определяне на нивото на въздействие;

3. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за защита на средно ниво, предвидени в нея, трябва да бъдат изпълнени до 9 месеца след определяне на нивото на въздействие;

4. за регистри с лични данни, водени към момента на влизане в сила на тази наредба, мерките за защита на високо и изключително високо ниво, предвидени в нея, трябва да бъдат изпълнени до една година след определяне на нивото на въздействие.

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

§ 4. Тази наредба отменя Наредба № 1 от 7 февруари 2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (ДВ, бр. 25 от 2007 г.).

ПРЕДСЕДАТЕЛ: /п/

ВЕНЕТА ШОПОВА

Приложение № 1 към чл. 14, ал. 1

Оценка на нивото на въздействие на регистър

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Име на регистъра				

Приложение № 2 към чл. 14, ал. 4

Оценка на нивото на въздействие на група от „n“ регистри

	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Регистър 1				
Регистър 2				
……				
Регистър n				
Ниво на въздействие за групата от „n“ регистри:				

Приложение № 3 към чл. 17

видове защити / нива на защита	физическа		персонална	документална	автоматизирани информационни системи и/или мрежи		криптографска
	организационни мерки	технически мерки	организационни мерки	организационни мерки	организационни мерки	технически мерки	технически мерки
ниско	* определяне на помещенията, в които ще се обработват лични данни; * определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; * определяне на организацията на физическия достъп;	*ключалки; * шкафове; * пожарогасителни средства; * оборудване на помещенията;	* познаване на нормативната уредба в областта на защитата на личните данни; * знания за опасностите за личните данни, обработвани от администратора; * съгласие за поемане на задължение за неразпространение на личните данни;	* определяне на регистрите, които ще се поддържат на хартиен носител; * определяне на условията за обработване на лични данни; * регламентиране на достъпа до регистрите; * определяне на срокове за съхранение; * процедури за унищожаване;	* персонална защита; * определяне на срокове за съхранение на личните данни; * процедури за унищожаване/заличаване/изтриване на носители;	* идентификация и автентификация; * управление на регистрите; * външни връзки/свързване; * защита от вируси; * копия/резервни копия за възстановяване; * носители на информация;	
средно	* **ниско ниво +** * определяне на използваните технически средства за физическа защита; * определяне на зоните с контролиран достъп;	* **ниско ниво**	* **ниско ниво +** * обучение; * споделяне на критична информация между персонала; * познаване на политиката и ръководствата за защита на личните данни; * тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;	* **ниско ниво +** * контрол на достъпа до регистрите; * правила за размножаване и разпространение;	* **ниско ниво +** * физическа среда/ обкръжение;	* **ниско ниво +** * телекомуникации и отдалечен достъп; * поддържане/ експлоатация;	* стандартните криптографски възможности на операционните системи; * стандартните криптографски възможности на системите за управление на бази данни; *стандартните криптографски възможности на комуникационното оборудване;
високо	* **средно ниво +** * определяне на екип за реагиране при нарушения; * определяне на режима на посещения;	* **средно ниво +** * пожароизвестителни и пожароизвестителни системи; * оборудване на зоните с контролиран достъп; * охрана и/или система за сигурност; * устройства за контрол на физическия достъп; * детектори за субстанции; * средства за защита на периметъра;	* **средно ниво**	* **средно ниво +** * процедури за проверка и контрол на обработването;	* **средно ниво +** * политики за защита на личните данни, ръководства по защита и стандартни операционни процедури; * планиране на случайността/непредвидените случаи; * тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;	* **средно ниво +** * определяне на роли и отговорности; * контроли на сесията; * наблюдение; * управление на конфигурацията;	* **средно ниво +** * нормативно определените системи за електронен подпис; *системи за разпределение и управление на криптографските ключове;
изключително високо	* **високо ниво +** * мерки, произтичащи от международни политики за сигурност или актове с международен характер.						