

# **НАРЕДБА № 47 от 11.07.2012 г. за изискванията към информационните системи на пенсионноосигурителните дружества**

Издадена от председателя на Комисията за финансов надзор, обн., ДВ, бр. 57 от 27.07.2012 г., в сила от 28.07.2013 г.

## **Раздел I Общи положения**

**Чл. 1.** С наредбата се уреждат:

1. изискванията към системата за управление на информационната сигурност на пенсионноосигурителното дружество;
2. изискванията при обмен на информация и предоставяне на електронни услуги;
3. водените от пенсионноосигурителното дружество регистри.

**Чл. 2.** Пенсионноосигурителното дружество изгражда и поддържа информационна система в съответствие с изискванията на тази наредба, другите приложими нормативни актове и стандарти и приетите вътрешни документи на дружеството, като отчита спецификата и обема на дейността по допълнително пенсионно осигуряване и организационната си структура.

## **Раздел II Система за управление на информационната сигурност**

**Чл. 3.** (1) Пенсионноосигурителното дружество е длъжно да изгради система за управление на информационната сигурност въз основа на изискванията на международен стандарт ISO/IEC 27001:2005.

(2) Системата за управление на информационната сигурност трябва да обхваща следните основни аспекти на сигурността: оценка и управление на риска, управление на персонала, физическа сигурност, контрол на достъпа, сигурност при избора, закупуването и ползването на софтуер и хардуер, планове и действия в извънредни ситуации и кризи.

(3) Пенсионноосигурителното дружество се съобразява в дейността си с добрите практики, заложиени в международен стандарт ISO/IEC 27002:2005 (ISO/IEC 17799:2005).

**Чл. 4.** (1) Съответствието с изискванията на стандарта по чл. 3, ал. 1 се доказва по избор на пенсионноосигурителното дружество чрез:

1. сертификация;
2. представянето на документи, доказващи това съответствие без сертификация.

(2) В случаите по ал. 1, т. 2 се представят следните документи:

1. политика за сигурност на дружеството по отношение на информационната му система (политика за сигурност на дружеството);
2. правила за защита на информационната система и архивната информация;
3. правила за мрежова защита;
4. правилата за контрол на физическата и работната среда;
5. план за осигуряване на непрекъсваемостта на информационно-технологичните процеси;
6. други относими документи.

**Чл. 5.** (1) Управителният орган на пенсионноосигурителното дружество приема неговата политика за сигурност и другите необходими вътрешни правила и документи по чл. 4, ал. 2 и осигурява реализацията им, а при необходимост - и актуализацията им.

(2) Прилагането на принципите и изискванията, заложи в политиката за сигурност на дружеството, трябва да:

1. гарантира общо ниво на сигурност при разработката, експлоатацията и поддръжката на информационната система;
2. обезпечи разработването и поддръжането на обща архитектура за сигурност на информационната система;
3. осигури идентифициране и анализ на рисковете, свързани с информационната система и определянето на необходимите механизми за противодействие;
4. обезпечи защитата на информацията чрез осигуряване на поверителност, цялостност и достъпност на информационните активи в дружеството, включително и при извънредни обстоятелства.

(3) Политиката за сигурност на дружеството трябва да отговаря на изискванията в приложимите нормативни актове и стандарти и да съдържа най-малко:

1. основните принципи, на които се базира;
2. задълженията и отговорностите на звената и служителите на дружеството за

нейното прилагане, за изграждането и експлоатацията на информационната система и за изпълнение на предвидените мерки за сигурност;

3. правилата за управление на рисковете, свързани с информационната система, в т.ч. идентифицирането на рисковите фактори, тяхната оценка и предприемането на необходимите мерки за противодействие срещу тях;

4. реда за приемането, актуализирането и оповестяването ѝ.

**Чл. 6.** (1) За удостоверяване на съответствието със стандарта по чл. 3, ал. 1 пенсионноосигурителното дружество представя на заместник-председателя на комисията, ръководещ управление "Осигурителен надзор" (заместник-председателя на комисията):

1. заверено копие от документа, удостоверяващ сертификацията - в случаите, когато пенсионноосигурителното дружество е сертифицирано;

2. документите по чл. 4, ал. 2 - когато сертификацията на дружеството преустанови действието си;

3. изменените или допълнени документи по чл. 4, ал. 2 - при извършени промени в тях, когато дружеството не е сертифицирано.

(2) Документите по ал. 1, т. 1 или 2 се представят в срок седем дни от сертификацията или преустановяването на действието на сертификацията, а по ал. 1, т. 3 - в срок седем дни от промяната.

(3) Заместник-председателят на комисията може да изисква допълване или коригиране на документите по ал. 1, т. 2 и 3, както и други данни и информация във връзка с тях, и да определя срок за представянето им. Когато представените документи не отговарят на изискванията на тази наредба, заместник-председателят на комисията може да приложи мярката по чл. 344, ал. 1, т. 1 от Кодекса за социално осигуряване (КСО).

## **Раздел III**

### **Изисквания при обмен на информация и предоставяне на електронни услуги**

**Чл. 7.** (1) Пенсионноосигурителното дружество използва официален e-mail адрес за получаване на служебна кореспонденция от комисията и други институции, с които дружеството осъществява обмен на информация. Дружеството уведомява заместник-председателя на комисията за промяна в официалния e-mail адрес поне три работни дни преди промяната.

(2) Служителите в дружеството използват единствено персоналната си служебна електронна поща за получаване и изпращане на служебна кореспонденция по електронен път. Електронните съобщения, изпратени от служителите на пенсионноосигурителното

дружество във връзка с изпълняваните от тях задължения, трябва да съдържат задължително идентифицираща информация за контакт със съответния служител. В края на всяко изходящо електронно съобщение автоматично се прикачват указания към адресата за действия при погрешно получаване.

**Чл. 8.** (1) Информационната система на пенсионноосигурителното дружество трябва да предоставя възможност за създаване и поддържане на единно електронно досие на всяко осигурено лице или пенсионер в управляван от дружеството пенсионен фонд. Досието трябва да съдържа всички налични данни за лицето и да му позволява да извършва справки и да проследява осигурителната си история.

(2) Заявленията и молбите на хартиен носител, подадени от осигурените лица, пенсионерите и техните наследници, както и актовете на дружеството във връзка с тях се включват в електронното досие на съответното лице чрез снемане на електронен образ от тях и от приложените към тях документи със сканиращо устройство във вид и по начин, позволяващи разчитането им. Пълното и точно съответствие на снетия електронен образ със снемания документ се удостоверява с електронен подпис от лицето, извършило снемането.

(3) Документите по ал. 2 се съхраняват от пенсионноосигурителното дружество. Пенсионноосигурителното дружество може да възложи с писмен договор дейностите по сканиране и/или съхраняване на документите на специализиран външен изпълнител. В този случай дружеството:

1. отговаря за действията на външния изпълнител като за свои действия;

2. предвижда в договора с външния изпълнител:

а) задължения за опазването на поверителността на предоставените документи и информация и за оказване на съдействие от негова страна на органите и служителите на Комисията за финансов надзор при осъществяването на техните правомощия;

б) забрана за възлагане на дейностите, предмет на договора, на подизпълнители;

3. наблюдава и оценява рисковете, свързани с изнасянето на дейностите, както и осъществяването им от страна на външния изпълнител.

(4) Пенсионноосигурителното дружество е длъжно да издаде на всяко осигурено лице или пенсионер при поискване от негова страна уникален идентификатор за използване на електронните услуги, които дружеството предлага.

(5) Осигурените лица, пенсионерите и техните наследници имат право да получат копие от електронните документи в електронното досие на хартиен или електронен носител след представяне на необходимите удостоверителни документи.

(6) Разрешението за достъп и отказът за достъп до електронното досие и за използването на електронни документи от него по реда на ал. 5 се издават в писмена

форма от управляващия и представляващ пенсионноосигурителното дружество или от упълномощен от него служител. Отказът за достъп задължително се мотивира.

(7) Отказът по ал. 6 може да се обжалва от заявителя по реда и в сроковете, предвидени в правилника за организацията и дейността на съответния пенсионен фонд.

**Чл. 9.** Информационната система трябва да предоставя възможност за:

1. отчитане и удостоверяване на времето за настъпването на факти с правно значение с точност до година, дата, час, минута и секунда;

2. изготвяне на извлечение от индивидуалната партида във всеки един момент, за създаване и отпечатване на необходимите първични документи и за предоставяне на копията по чл. 8, ал. 5 във всички офиси на дружеството;

3. връзка с всички офиси и осигурителни посредници на дружеството за регистриране на подадените при тях документи;

4. получаването и изпращането на документи, подписани с електронен подпис;

5. изготвяне и обмен в електронен формат, определен от надзорния орган, на изискваните ежедневни, периодични и изготвяни при поискване отчети и справки;

6. оперативна размяна на информация с институциите, с които пенсионноосигурителното дружество осъществява обмен на данни, съобразно предвидените за това стандарти, формати и образци.

**Чл. 10.** (1) Подадените документи до дружеството по електронен път се регистрират от определени от управителния орган лица. След регистриране на постъпил в дружеството входящ електронен документ се генерира и се изпраща потвърждение до заявителя за получаването му.

(2) Лицата по ал. 1 извършват проверка за редовността, пълнотата и верността на предоставените данни. При установяване на нередности на подателя се изпраща електронно съобщение с указания и срок за отстраняването им.

**Чл. 11.** При предоставяне на електронна услуга пенсионноосигурителното дружество предварително информира нейния ползвател по ясен и разбираем начин относно:

1. техническите стъпки по предоставянето на услугата, тяхното правно значение и срока за предоставянето ѝ;

2. възможността издаденият акт да бъде съхраняван в електронна форма от дружеството и начина за достъп до него;

3. техническите средства за установяване и отстраняване на грешки при въвеждането на информация, преди да бъдат направени изявленията във връзка с услугата.

**Чл. 12.** Електронната страница на пенсионноосигурително дружество трябва да осигурява удобен за ползване достъп:

1. до публикуваната на нея информация;
2. на всяко осигурено лице или пенсионер до данните за индивидуалната му партия и до електронното му досие след въвеждането на идентификатор.

## **Раздел IV**

### **Регистри**

**Чл. 13.** Информационната система на пенсионноосигурителното дружество трябва да поддържа в актуално състояние следните основни компоненти, съответно приложими за управляваните от дружеството пенсионни фондове:

1. регистри на:
  - а) осигурителните договори - в т. ч. по видове за доброволния фонд (договор с лични вноски, договор с работодател или с лице по чл. 230, ал. 3, т. 3 КСО и договор с друг осигурител);
  - б) служебно разпределените лица с номер и дата на протокола за служебно разпределение;
  - в) пенсионните договори;
  - г) договорите за разсрочено изплащане на натрупаните средства по индивидуалните партии;
2. регистър на индивидуалните партии на осигурените лица и пенсионерите, който трябва да съдържа данните съгласно чл. 24 и 25 от Наредба № 9 от 2003 г. за начина и реда за оценка на активите и пасивите на фондовете за допълнително пенсионно осигуряване и на пенсионноосигурителното дружество, на стойността на нетните активи на фонда, за изчисляване и обявяване на стойността на един дял и за изискванията към воденето на индивидуалните партии (ДВ, бр. 109 от 2003 г.), както и партидата на резерва за гарантиране на минималната доходност по чл. 193, ал. 7 КСО;
3. регистър на постъпилите молби за изтегляне или изплащане на средства поотделно за всеки управляван фонд;
4. регистри на заявленията за участие по чл. 6 от Наредба № 33 от 2006 г. за индивидуалните заявления за участие във фонд за допълнително задължително пенсионно осигуряване (ДВ, бр. 83 от 2006 г.) - за фондовете за допълнително задължително пенсионно осигуряване;

5. регистри на заявленията за промяна на участието или прехвърляне на средства по чл. 20 от Наредба № 3 от 2003 г. за реда и начина за промяна на участие и за прехвърляне на натрупаните средства на осигурено лице от един фонд за допълнително пенсионно осигуряване в друг съответен фонд, управляван от друго пенсионноосигурително дружество (ДВ, бр. 90 от 2003 г.);

6. регистър на постъпилите молби за прехвърляне на средства от една осигурителна партида в друга на един и същи пенсионен фонд на съпруг(а) или на роднини по права линия до втора степен - за фонд за допълнително доброволно пенсионно осигуряване;

7. регистър на притежаваните активи поотделно за всеки управляван фонд за допълнително пенсионно осигуряване, аналогичен на регистъра по чл. 123а, ал. 4, т. 4 КСО, със записи за ежедневната оценка на всеки актив;

8. регистър на професионалните схеми - за фонд за допълнително доброволно пенсионно осигуряване по професионални схеми;

9. регистър на деловодната кореспонденция на пенсионноосигурителното дружество, в т. ч. регистър на жалбите;

10. други регистри, които пенсионноосигурителното дружество води в съответствие с нормативната уредба или вътрешните си правила.

## **Раздел V**

### **Административнонаказателна отговорност**

**Чл. 14.** (1) Пенсионноосигурително дружество или негови служители, които извършат или допуснат извършване на нарушение на тази наредба, се наказват съгласно чл. 351 КСО.

(2) Нарушенията на разпоредбите на наредбата се установяват с актове, съставени от длъжностни лица, упълномощени от заместник-председателя на комисията.

(3) Наказателните постановления се издават от заместник-председателя на комисията или от упълномощено от него длъжностно лице.

(4) Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на Закона за административните нарушения и наказания.

## **ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**§ 1.** (1) В 7-дневен срок от влизане в сила на наредбата пенсионноосигурителното дружество представя пред заместник-председателя на комисията заверено копие от документа, удостоверяващ сертификация за съответствие със стандарта по чл. 3, ал. 1,

съответно - документите по чл. 4, ал. 2.

(2) Заместник-председателят на комисията може да изисква допълване или коригиране на внесените документи по чл. 4, ал. 2, както и други данни и информация във връзка с тях, и да определя срок за представянето им. Когато представените документи не отговарят на изискванията на тази наредба, заместник-председателят на комисията може да приложи мярката по чл. 344, ал. 1, т. 1 КСО.

**§ 2.** В чл. 6, ал. 4 от Наредба № 33 от 2006 г. за индивидуалните заявления за участие във фонд за допълнително задължително пенсионно осигуряване (ДВ, бр. 83 от 2006 г.) думите "изискванията за създаване и поддръжка на информационна система на пенсионноосигурително дружество, утвърдени от заместник-председателя на Комисията за финансов надзор, ръководещ управление "Осигурителен надзор" се заменят с "наредбата по чл. 123ж, ал. 1 КСО".

**§ 3.** Наредбата се издава на основание чл. 123ж, ал. 1 КСО и е приета с Решение № 135-Н от 11.07.2012 г. на Комисията за финансов надзор.

**§ 4.** Наредбата влиза в сила една година след обнародването ѝ в "Държавен вестник".