20100741364

АГЕНЦИЈА ЗА СУПЕРВИЗИЈА НА КАПИТАЛНО ФИНАНСИРАНО ПЕНЗИСКО ОСИГУРУВАЊЕ

Врз основа на член 52 од Законот за заштита на личните податоци („Службен весник на Република Македонија" бр. 7/05 и 103/08), Управниот одбор на Агенцијата за супервизија на капитално финансирано пензиско осигурување на седницата, одржана на 27.05. 2010 година, го донесе следниот

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки кои ги применува Агенцијата за супервизија на капитално финансирано пензиско осигурување (во понатамошниот текст Агенцијата) заради обезбедување на тајност и заштита на обработката на личните податоци.

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

"Систем администратор" е овластено лице за координирање и контрола на техничките и организациски мерки кои се применуваат за обезбедување тајност и заштита на личните податоци кои се чувааат во информацискиот систем на Агенцијата.

"Корисник" е физичко лице, вработено или ангажирано во Агенцијата кое има пристап до личните податоци кои се чуваат во информацискиот систем на Агенцијата.

"Оператор" е физичко лице, вработено или ангажирано кај надворешните субјекти кое има пристап до личните податоци кои се добиваат преку информацискиот систем на Агенцијата.

„Информациски систем на Агенцијата" е целокупниот информациски систем на Агенцијата составен од персонални компјутери, сервер на база на податоци, апликациски сервер, сервер за чување на податоци, интернет портал и останати апликации и опрема кои се користат за обработка на податоци.

"Интернет портал" е дел од информацискиот систем на Агенцијата кој овозможува ограничен пристап на корисникот преку web форма до податоците за кои е овластен да ги обработува.

Член 3

Агенцијата треба да обезбеди мерки за заштита на личните податоци, кои се чуваат во информацискиот систем, при пристапот на интернет порталот од страна на корисникот и тоа:

1. Креирање на единствено корисничко име и лозинка за секој корисник на интернет порталот на Агенцијата. Лозинката е составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
2. Автоматска промена на лозинките на секои 3 месеци;
3. Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;

4. Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;

5. Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на корисникот дека треба да побара инструкција од систем администраторот и

6. Воспоставување на ефективна и сигурна антивирусна заштита на системот, со постојано набљудување и ажурирање заради превентива од непознати и непланирани закани од нови вируси.

Мерките од став 1 на овој член ги спроведува систем администраторот на Агенцијата и врши нивна периодична проверка.

Вработениот кој е задолжен за управување со човечките ресурси во Агенцијата треба да го известува систем администраторот за почеток на вработување или ангажирање на секој корисник со право на пристап до информацискиот систем, со цел да биде доделено ново корисничко име и лозинка. При престанок на вработувањето или ангажирањето корисничкото име и лозинката се бришат.

Известувањето од став 3 на овој член се врши и при било кои други промени во работниот или статусниот дел на ангажирањето на корисникот што има влијание врз нивото или обемот на дозволениот пристап до збирката на личните податоци.

Член 4

Агенцијата треба да обезбеди мерки за заштита на личните податоци, кои се чуваат во информацискиот систем на Агенцијата, при пристапот на интернет порталот од страна на надворешните субјекти (пензиски друштва, Фондот на пензиското и инвалидското осигурување на Македонија и чуварите на имот на пензиските фондови) и тоа:

1. Креирање на единствено корисничко име и лозинка за секој оператор на интернет порталот. Лозинката е составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци; ;

2. Автоматска промена на лозинките на секои 3 месеци;

3. Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;

4. Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот; и

5. Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на операторот дека треба да побара инструкција од систем администраторот и

6. Воспоставување на ефективна и сигурна антивирусна заштита на системот, со постојано набљудување и ажурирање заради превентива од непознати и непланирани закани од нови вируси.

Мерките од став 1 на овој член ги спроведува систем администраторот на Агенцијата врши нивна периодична проверка.

Надворешниот субјект треба да ја известува Агенцијата за промена на операторот со цел да биде доделено ново корисничко име и лозинка. Претходното корисничко име и лозинка се бришат.

Известувањето од став 3 на овој член се врши и при било кои други промени на операторот што имаат влијание врз нивото или обемот на дозволениот пристап до личните податоци добиени преку информацискиот систем на Агенцијата.

Член 5

Агенцијата води електронска евиденција на корисници и оператори кои имаат авторизиран пристап на интернет порталот на информацискиот систем на Агенцијата и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

Агенцијата води електронска евиденција за авторизираниот пристап со следните податоци: име и презиме на корисникот или операторот, работна станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребно ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците од ставовите (1) и (2) на овој член треба да бидат контролирани од страна на систем администраторот и истите не може да се деактивираат.

Евиденцијата од ставот (1) на овој член се чува најмалку десет години.

Систем администраторот врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Член 6

Агенцијата треба да обезбеди организациски мерки за заштита на личните податоци во поглед на информирањето на вработените, физичката заштита на работните простории и опремата и заштита на информацискиот систем во целина, вклучувајќи го и преносот на личните податоци.

Член 7

Агенцијата треба да обезбеди организациски мерки за заштита на личните податоци при автоматизираната обработка на податоците, која вклучува читање или обработка на лични податоци, и тоа:

1. Целосна доверливост и сигурност на лозинките и на останатите форми на идентификација за пристап до информацискиот систем кој содржи лични податоци;

2. Електронско уништување на документи кои содржат лични податоци по истекување на рокот за чување;

3. Изнесувањето на медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;

4. Воспоставување физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци;

5. Почитување на процедурите за пристап до целокупниот информациски систем преку персоналните компјутери;

6. Почитување на процедурите од корисничката документација за пристап до софтверската апликација; и

7. Почитување на процедурите од техничката документација за користење на софтверската апликација и информацискиот систем на Агенцијата кој содржи лични податоци.

Член 8

Агенцијата треба да обезбеди мерки за заштита на личните податоци при автоматизираната обработка, која вклучува читање или обработка на лични податоци, до кои пристапуваат надворешните субјекти (пензиските друштва, Фондот на пензиското и инвалидското осигурување на Македонија и чуварите на имот на пензиските фондови) и тоа:

1. Почитување на целосна доверливост и сигурност на лозинките и на останатите форми на идентификација, официјално издадени од Агенцијата за пристап до информацискиот систем кој содржи лични податоци;

2. Електронско уништување на документи кои содржат лични податоци по истекување на рокот за чување;

3. Изнесувањето на медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;

4. Обезбедување физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци; и

5. Почитување на техничкото упатство издадено од Агенцијата за користење на софтверската апликација преку која се пристапува до информацискиот систем на Агенцијата кој што во себе содржи лични податоци и начинот на преземање на личните податоци од истиот.

Член 9

Лицата кои се вработуваат во Агенцијата, пред нивното започнување со користење на информатичкиот систем на Агенцијата треба да се запознаат со процедурите за заштита на личните податоци.

Во договорите со лицата коишто се ангажираат за извршување на работа во Агенцијата треба да се наведат обврските и одговорностите за заштита на личните податоци.

Пред непосредното започнување со работа на контролорите поврзана со пристап или обработка на личните податоци, Агенцијата дополнително ги информира за непосредните обврски за заштита на личните податоци.

Секој вработен или ангажиран во Агенцијата потпишува изјава во која е наведено дека е запознат со процедурите за заштита на личните податоци.

Член 10

Агенцијата треба да ги запознае надворешните субјекти од член 4 став 1 на овој правилник со значењето и мерките за заштита на личните податоци и да потпише договори со субјектите во кои тие ќе се обврзат на заштита на личните податоци до коишто пристапуваат или ги обработуваат, користејќи го информацискиот систем на Агенцијата.

Член 11

Агенцијата треба да обезбеди соодветна заштита – мрежна бариера (“firewall”) помеѓу нејзиниот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот.

Член 12

Информацискиот систем и информатичката инфраструктура на Агенцијата подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата

содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

Надворешната контрола од став 1 на овој член се врши од страна на независно правно лице на секои три години.

Внатрешната контрола од став 1 на овој член се врши еднаш годишно.

Овластените лица за извршените контроли од ставовите (2) и (3) на овој член изготвуваат извештај во кој задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се констатираат недостатоците и да се предложат неопходни мерки за нивно отстранување.

Извештајот заедно со предлог мерките се доставува до директорот на Агенцијата.

Член 13

Информацискиот систем на Агенцијата е затворен според дефиницијата во Законот за податоците во електронски облик и електронски потпис. Дозволен е пристап само од локација на Агенцијата и од локациите (интернет адреси) на ограничен број надворешни субјекти.

Член 14

Агенцијата треба да врши редовно снимање на сигурносна копија и архивирање на податоците во системот, за да не дојде до нивно губење или уништување.

Член 15

Агенцијата треба да обезбеди заштита на личните податоци при нивната размена со надворешните субјекти, преку овозможување на криптирана врска за размена, строги правила за идентификација при размената (лозинки тешки за пробивање) и електронско потпишување на документите за размена.

Мерките за заштита од став 1 на овој член Агенцијата може да ги пренесе и на надворешните субјекти со потпишување на договор.

Член 16

Со овој правилник престанува до важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија бр. 80/2007“).

Член 17

Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Македонија“.

Бр. 01-1088/3
27 мај 2010 година
Скопје

Претседател
на Управниот одбор,
Анета Димовска, с.р.