20110952310

ФОНД ЗА ЗДРАВСТВЕНО ОСИГУРУВАЊЕ НА МАКЕДОНИЈА

Врз основа на член 56 став 1 точка 14 од Законот за здравствено осигурување („Службен весник на Република Македонија“ број 25/2000, 96/2000, 50/2001, 11/2002, 31/2003, 84/2005, 37/2006, 18/2007, 36/2007, 82/2008, 98/2008, 6/2009, 67/2009, 50/2010, 156/2010 и 53/2011), а во врска со член 23 од Законот за заштита на личните податоци („Службен весник на Република Македонија" број 7/05, 103/2008, 124/2008 и 124/2010), Управниот одбор на Фондот за здравствено осигурување на Македонија на седницата одржана на 4 јули 2011 година, донесе

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ФОНДОТ ЗА ЗДРАВСТВЕНО ОСИГУРУВАЊЕ НА МАКЕДОНИЈА

I. Општи одредби

Предмет на уредување

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што се применуваат во Фондот за здравствено осигурување на Македонија (во понатамошниот текст на правилникот „Фонд“).

Техничките и организациските мерки утврдени во овој правилник, соодветно се применуваат и во подрачните служби на Фондот.

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. **Авторизиран пристап** е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на Фондот;
2. **Администратор на информацискиот систем** е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;
3. **Документ** е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникациска мрежа;
4. **Идентификација** е постапка за идентификување на овластеното лице на информацискиот систем;
5. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на Фондот, во рамките на која се собираат, обработуваат и чуваат личните податоци;
6. **Информациски систем** е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;

7. **Инцидент** е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;

8. **Контрола на пристап** е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;

9. **Овластено лице** е лице вработено или ангажирано кај Фондот кое има авторизиран пристап до документите и до информатичко комуникациската опрема;

10. **Лозинка** е доверлива информација составена од множество на карактери кои се користат за проверка на овластеното лице;

11. **Медиум** е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени;

12. **Офицер за заштита на личните податоци** е лице овластено од директорот на Фондот за самостојно и независно вршење на работите во смисла на член 26-а од Законот за заштита на личните податоци;

13. **Проверка** е постапка за верификација на идентитетот на овластеното лице на информацискиот систем;

14. **Сигурносна копија** е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање;

15. **Посебни категории на лични податоци** се лични податоци кои го откриваат расното или етничко потекло, политичко, верско, филозофско или друго уверување, членството во синдикална организација и податоци што се однесуваат на здравјето на луѓето, вклучувајќи ги и генетските податоци, биометриски податоци или податоци кои се однесуваат на или сексуалниот живот.

Изразите кои се користат во овој правилник а не се опфатени во став 1 на овој член, го имаат значењето што им е дадено во Законот за заштита на личните податоци („Службен весник на Република Македонија" број 7/2005, 103/2008 и 124/2009).

Обработувач на збирка на лични податоци

Член 3

Одредбите од овој правилник се применуваат и кога Фондот во согласност со прописите за заштита на личните податоци обработката на личните податоци ја доверува (пренесува) на друг субјект - обработувач на збирка на лични податоци.

Фондот нема да ја довери (пренесе) обработката на личните податоци на друг субјект - обработувач на збирка на лични податоци, кој применува технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци од ниво пониско од нивото што го применува Фондот, односно не се согласи при обработката да применува мерки што се применуваат во Фондот.

Одредбите од членот 26 на овој правилник соодветно се применуваат и при проверката на постапувањето на обработувачот при обработката на личните податоци во смисла на член 26 став 3 од Законот за заштита на личните податоци.

Обработка на личните податоци

Член 4

Одредбите од овој правилник се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци и
- друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Нивоа на технички и организациски мерки

Член 5

(1) Во Фондот се применуваат технички и организациски мерки, кои обезбедуваат тајност и заштита на обработката на личните податоци, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка.

(2) Техничките и организациските мерки од ставот (1) на овој член се класифицираат во три нивоа:

- основно;
- средно и
- високо.

Примена на нивоа

Член 6

(1) За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на основно ниво.

(2) За документите кои содржат лични податоци што се однесуваат на остварување на правата и обврските од здравственото осигурување, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(3) За документи кои содржат посебни категории на лични податоци, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

(4) За документите кои содржат матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(5) За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

(6) Со документацијата за технички и организациски мерки, директорот на Фондот ќе пропише и обезбеди мерки на заштита на личните податоци, на ниво соодветно на видот на документот согласно одредбите на овој член.

Правила за обработка на личните податоци надвор од работните простории

Член 7

Обработката на личните податоци надвор од работните простории на Фондот и на подрачните служби, се врши врз основа на писмено овластување од секторскиот директор или раководителот на подрачната служба и во согласност со соодветното ниво на технички и организациски мерки кои се применувале за обработка на податоците содржани во документите.

Евидентирање и чување на документација за софтверски програми

Член 8

Фондот обезбедува евидентирање и чување на целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.

Одржување на информацискиот систем

Член 9

(1) Физичките или правните лица кои вршат одржување на информацискиот систем на Фондот треба да се обврзат да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки на Фондот.

(2) Одредбите од ставот (1) на овој член се применуваат и ако физичките или правните лица вршат обработка на личните податоци на Фондот.

Пренос на лични податоци во други држави

Член 10

Кога за потребите на хардверско и/или софтверско одржување или на други активности на информацискиот систем, е неопходно да се пренесат лични податоци во други држави, преносот може да се врши согласно условите утврдени во прописите за заштита на личните податоци, и според процедури утврдени во Политиката за заштита на информатичкиот систем на Фондот.

II. Основно ниво на технички и организациски мерки

Документација за технички и организациски мерки

Член 11

(1) Заради воспоставување на техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци предвидени во овој правилник директорот на Фондот донесува:

- Политика за заштита на информатичкиот систем на Фондот;
- Процедура за заштита на личните податоци во работењето со документи во електронска форма;
- Процедура за заштита на личните податоци во работењето со документи во пишана форма.

(2) Офицерот за заштита на личните податоци во Фондот врши редовна проценка на потребата од измена на актите од став (1) и донесување на нови акти заради усогласување со прописите за заштита на личните податоци.

Технички мерки

Член 12

Во Фондот задолжително се обезбедуваат следните технички мерки за тајност и заштита на обработката на личните податоци:

1. единствено корисничко име;
2. лозинка креирана од секое овластено лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, на поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;

4. автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;

5. автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да се побара инструкција од администраторот на иинформацискиот систем;

6. инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол“) или рутер помеѓу информацискиот 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;

7. ефективна и сигурна анти-вирусна и анти–спајвер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;

8. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови; и

9. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Организациски мерки

Член 13

(1) Фондот задолжително ги обезбедува следните организациски мерки за тајност и заштита на обработката на личните податоци:

1. ограничен пристап или идентификација за пристап до личните податоци;

2. организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;

3. уништување на документи по истекот на рокот за нивно чување;

4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и

5. почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.

(2) Раководителот на одделението кое ги врши работите за човечки ресурси, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем, а раководителот на одделението во кое работи вработениот доставува барање до администраторот за да му биде доделено корисничко име и лозинка. Раководителот на одделението кое ги врши работите за човечки ресурси го известува администраторот за престанокот на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.

(3) Известувањето од ставот (2) на овој член се врши и при кои било други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.

Физичка сигурност на информацискиот систем

Член 14

Фондот со посебни процедури, во Политиката за заштита на информатичкиот систем на Фондот ќе воспостави правила за обезбедување на физичката сигурност на информацискиот систем во согласност со прописите за заштита на личните податоци.

Информирање за заштитата на личните податоци

Член 15

(1) Лицата кои се вработуваат или се ангажираат во Фондот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(2) За лицата кои се ангажираат за извршување на работа во Фондот, во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Фондот пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Лицата кои се вработуваат или се ангажираат, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

(5) Изјавата од ставот (4) задолжително содржи податоци за лична идентификација на давателот на изјавата, работно место на кое е распореден, дата и место кога е дадена изјавата и следниот текст:

Изјавувам дека

- сум запознаен/а со прописите и конкретните обврски и одговорности за заштита на личните податоци;
- ќе ги почитувам начелата за заштита на личните податоци;
- ќе вршам обработка на личните податоци согласно упатствата добиени од Фондот за здравствено осигурување на Македонија во својство на контролор и обработувач, освен ако со закон поинаку не е уредено;
- ќе се придржувам до документацијата за технички и организациски мерки усвоена од Фондот за здравствено осигурување на Македонија;
- ќе ги чувам како доверливи личните податоци кои ќе ги обработувам; и
- ќе ги чувам како доверливи мерките за заштита на личните податоци.

(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат во Фондот.

(7) Фондот задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Обврски и одговорности на администраторот на информацискиот систем

Член 16

(1) Обврските и одговорностите на администраторот на информацискиот систем, се дефинираат и утврдуваат во правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема во Политиката за заштита на информатичкиот систем на Фондот.

(2) Фондот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

(3) Во извештајот од ставот (2) на овој член се внесуваат констатираните неправилности и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Член 17

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, се дефинира и утврдува во правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема во Политиката за заштита на информатичкиот систем на Фондот.

(2) Фондот задолжително ги запознава овластените лица од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Евидентирање на инциденти

Член 18

Во правилата за пријавување, реакција и санирање на инциденти, се определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавило, на кого е пријавен и мерките кои се преземени за негово санирање.

Идентификација и проверка

Член 19

(1) Фондот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

(2) Кога проверката се врши врз основа на корисничко име и лозинка, Фондот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

(3) Во Политиката за заштита на информатичкиот систем на Фондот ќе се утврдат правила со кои ќе се обезбеди лозинките автоматски да се менуваат по изминат временски период не подолг од три месеци, и да се чуваат заштитени со соодветни методи така што нема да бидат разбирливи додека се валидни.

Контрола на пристап

Член 20

(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.

(2) Фондот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

(3) Во евиденцијата на овластените лица утврдена во член 19 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

(4) Администраторот на информацискиот систем кој е овластен согласно Политиката за заштита на информатичкиот систем на Фондот може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите утврдени во Политиката за заштита на информатичкиот систем на Фондот.

Управување со медиуми

Член 21

(1) Со Политиката за заштита на информатичкиот систем на Фондот ќе се утврдат правила за постапување со медиумите со кои ќе се овозможи идентификација и евидентирање на категориите на лични податоци, и чување на медиумите на локација до која пристап имаат само овластени лица утврдени во Политиката.

(2) Пренесувањето на медиуми кои содржат лични податоци надвор од работните простории е строго забрането, освен во случаите на пренос на заштитни копии кои се утврдени со посебна процедура или во посебни случаи со претходно добиено одобрение од директорот на секторот за информатика.

Уништување, бришење или чистење на медиумот

Член 22

(1) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

(2) Уништувањето на медиумот се врши со механичко разделување на неговите составни делови, при што истиот повторно да не може да биде употреблив.

(3) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

(4) За случаите од ставовите (2) и (3) на овој член комисиски се составува записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 23

(1) Администраторот на системот е одговорен за проверка на примената на правилата за начинот на правење на сигурносна копија, архивирање и чување, како и за повторното враќање на зачуваните лични податоци.

(2) Правилата од ставот (1) на овој член, во согласност со прописите за заштита на личните податоци ќе се утврдат со Политиката за заштита на информатичкиот систем на Фондот.

Начин на чување на сигурносните копии

Член 24

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

Глава III. Средно ниво на технички и организациски мерки

Дополнителни правила за технички и организациски мерки

Член 25

(1) Директорот на Фондот, од редот на вработените назначува офицер за заштита на личните податоци кој ќе врши координација и контрола на постапките и упатствата утврдени во донесената документација за техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци.

(2) За офицер за заштита на личните податоци може да биде назначено едно или две лица кои заеднички ја вршат улогата на офицер за заштита на личните податоци.

(3) Офицерот за заштита на личните податоци во Фондот најмалку еднаш во три месеци ги врши следните контроли и за тоа изготвуваат извештај:

- Контрола на примената на техничките и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци,
- Контрола на евиденција за секој авторизиран/неавторизиран пристап до информацискиот систем,
- Контрола на доверливоста и сигурноста на лозинките и на останатите форми на идентификација,
- Контрола на начинот за пристап на вработените и ангажираните лица во Фондот до интернет заради преземање и снимање документи од веб локации, електронска пошта или други извори,
- Контрола на уништување на документи кои содржат лични податоци по истекување на рокот за чување, како и за начинот на уништување и бришење на медиумите,
- Контрола на начинот на управување со медиуми кои се носители на лични податоци,
- Контрола на примената на правилото „чисто биро",
- Контрола на писмените овластувања издадени од страна на Директорот на Фондот за вршење на обработка на личните податоци и за пренесување на медиуми надвор од работните простории на Фондот,
- Контрола на начинот на воспоставување физичка сигурност на работните простории и опремата каде што се обработуваат и чуваат личните податоци,
- Контрола на начинот на пристап до целиот информациски систем преку персоналните компјутери,
- Контрола на начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци,
- Контрола на евиденцијата за физички пристап до просторијата во која се сместени серверите, и
- Контрола на постапката за потпишување на изјави за тајност и заштита на обработката на личните податоци од страна на вработените и ангажираните лица во Фондот.

(4) Офицерот за заштита на личните податоци го известува директорот на Фондот за утврдените наоди за инциденти и повреди на правилата и процедурите поврзани со заштита на лични податоци.

(5) Во случај на поголеми инциденти и повреди на правилата и процедурите и со цел спречување на повторно случување на истите, офицерот за заштита на личните податоци ги известува и директорот на секторот за информатика односно одговорниот службеник за безбедноста на информациските системи во Фондот.

(6) Офицерот за заштита на личните податоци спроведува периодични проверки на усогласеноста на правилата за заштита на личните податоци во Фондот со прописите за заштита на лични податоци.

Контрола на информацискиот систем и информатичката инфраструктура

Член 26

(1) Фондот задолжително спроведува внатрешна и надворешна контрола на информацискиот систем и информатичката инфраструктура, 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.

(2) Фондот врши внатрешна контрола секоја година, а надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години.

(3) Правилата за внатрешна и надворешна контрола на информацискиот систем и информатичката инфраструктура, во согласност со прописите за заштита на личните податоци ќе се утврдат со Политиката за заштита на информатичкиот систем на Фондот.

Идентификација и проверка

Член 27

Фондот воспоставува механизми кои овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице.

Евидентирање на авторизираниот пристап (логови)

Член 28

(1) Фондот води евиденција за секој авторизиран пристап која содржи особено: име и презиме на овластеното лице, 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.

(2) Поблиските правила за евидентирање на авторизираниот пристап, во согласност со прописите за заштита на личните податоци ќе се утврдат со Политиката за заштита на информатичкиот систем на Фондот.

Контрола на физички пристап

Член 29

Во Политиката за заштита на информатичкиот систем на Фондот ќе се определат критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Член 30

(1) Фондот воспоставува систем за евидентирање на медиумите кои се примаат со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е

примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.

(2) Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на Фондот.

(3) За пренесените медиуми надвор од работните простории на Фондот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Евидентирање на инциденти

Член 31

(1) Во Правилата за пријавување, реакција и санирање на инциденти, Фондот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени и кои биле рачно внесени при враќањето.

(2) За повторно враќање на личните податоци, директорот на сектор информатика издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 32

Со Политиката за заштита на информатичкиот систем на Фондот, во согласност со прописите за заштита на личните податоци ќе се утврдат правила за правењето и чувањето на сигурносните копии.

Тестирање на информацискиот систем

Член 33

(1) Фондот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци согласно документацијата за технички и организациски мерки и прописите за заштита на личните податоци.

(2) Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето правно лице.

Глава IV. Високо ниво на технички и организациски мерки

Сертификациони постапки

Член 34

Фондот, кога за тоа има потреба со оглед на видот на податоците, местото каде се испраќаат или обработуваат, или од други причини, може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите за податоците во електронски облик и електронски потпис.

Пренесување на медиуми

Член 35

Медиумите можат да се пренесуваат надвор од работните простории само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице овластено од него.

Пренесување на личните податоци преку електро комуникациска мрежа

Член 36

Личните податоци можат да се пренесуваат преку електро комуникациска мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Глава V. Друга рачна обработка на личните податоци

1. Основно ниво на технички и организациски мерки

Примена

Член 37

Одредбите од членовите 3, 5, 6, 7, 11, 13, 15, 17 и 18 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Пристап до документите

Член 38

(1) Пристапот до документите е дозволен само за овластени лица на Фондот.

(2) За пристапувањето до документите задолжително се воспоставуваат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

(3) Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Член 39

Фондот задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Чување на документи

Член 40

(1) Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, се применуваат други мерки кои што ќе го спречат секој неовластен пристап до документите.

(3) Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш треба се применуваат сите мерки за нивна најдобра заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 41

(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.

(2) Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

2. Средно ниво на технички и организациски мерки

Контрола

Член 42

Одредбите од членовите 25 и 26 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Начин на чување на документите

Член 43

(1) Плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, се применуваат други мерки за да се спречи секој неовластен пристап до документите.

3. Високо ниво на технички и организациски мерки

Копирање или умножување на документите

Член 44

(1) Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на директорот на Фондот, односно раководителот на подрачната служба.

(2) Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 45

Во случај на физички пренос на документите, задолжително се преземаат мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат.

Глава VI. Преодни и завршни одредби

Член 46

Со денот на отпочнувањето на примената на овој правилник, престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на личните податоци и другите податоци со кои располага и ги обработува Фондот за здравствено осигурување на Македонија („Службен весник на Република Македонија“ број 64/2008).

Начинот и условите за обезбедување на технички и организациски мерки за тајност и заштита на обработката на личните податоци се уредуваат со документацијата од членот 11 на овој правилник.

Документацијата од членот 11 на овој правилник, директорот на Фондот ќе ја донесе во рок од шест месеци по влегувањето во сила на правилникот.

Член 47

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

Бр. 02-10378/18
4 јули 2011 година
Скопје

Управен одбор
Претседател,
Ирфан Хоџа, с.р.