Врз основа на член 157 став 1 точка 1 и член 215 став 2 од Законот за пензиското и инвалидското осигурување („Службен весник на Република Македонија“ бр. 98/12, 166/12, 15/13, 170/13, 43/14, 44/14, 97/14, 113/14, 160/14, 188/14, 20/15, 61/15, 97/15, 129/15, 147/15, 154/15, 173/15, 217/15, 27/16, 120/16, 132/16, 35/18, 220/18, 245/18 и „Службен весник на Република Северна Македонија“ бр.180/19, 275/19, 31/20 и 267/20), а во врска со член 119 и 120 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20, Управниот одбор на Фондот на пензиското и инвалидското осигурување на Северна Македонија, на седницата одржана на 28.10.2021 година, донесе:

П Р А В И Л Н И К
за техничките и организациските мерки за безбедност и заштита на обработката на личните податоци

I. Општи одредби

Член 1

Со овој правилник се уредуваат правилата и стандардите кои ги применува Фондот на пензиското и инвалидското осигурување на Северна Македонија (во натамошниот текст: Фондот) и истиот се применува на сите збирки на лични податоци кои Фондот ги собира, чува и обработува, со цел да обезбеди заштита на личните податоци за обврзниците, осигурениците и корисниците на права од пензиското и инвалидското осигурување, за кои Фондот води евиденција.

Заштитата на обработката на личните податоци од ставот (1) на овој член, Фондот ја обезбедува со примена на технички и организациски мерки, кои обезбедуваат тајност и заштита на податоците, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка.

Техничките и организациските мерки утврдени во овој Правилник, соодветно се применуваат и во филијалите и деловниците на Фондот.

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. **Доверливост** е пристап до личните податоци единствено од лица кои имаат овластување за нивна обработка;
2. **Интегритет** е заштита на точноста на личните податоци, при што се гарантира дека личните податоци се точни, целосни и ажурирани;
3. **Овластено лице** е лице вработено или ангажирано во Фондот, кое има авторизиран пристап до документите и до информатичко комуникациската опрема на кои се обработуваат лични податоци;
4. **Проверка** е постапка за верификација на идентитетот на овластеното лице на информацискиот систем;
5. **Офицер за заштита на личните податоци** е лице овластено од Директорот на Фондот за самостојно и независно вршење на работите, согласно членовите 41,42 и 43 од Законот за заштита на личните податоци;
6. **Достапност** е непречен пристап и континуирана расположливост (business continuity) на информацискиот систем на кој се врши обработка на личните податоци од страна на овластените лица;
7. **Автентикација** е постапка која што овозможува потврдување на идентитетот на овластеното лице кое се најавува и пристапува на информацискиот систем на кој се врши обработка на личните податоци;
8. **Неотповикливост** е обезбедување на потврда на автентичноста на идентитетот на овластеното лице кое се најавува на информацискиот систем при што овластеното лице не може да ја негира преземената активност или дејствие;
9. **Безбедносен ризик** е веројатност на случување на настан кој може да резултира со компромитирање, особено случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци, или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци (во натамошниот текст: ризик);
10. **Управување со ризик** е идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на Фондот, за минимизирање, набљудување и контрола на веројатноста и сериозноста која што може да произлезе при обработката на личните податоци, а која може да предизвика материјална или нематеријална штета врз процесите со кои се врши обработка на личните податоци;

11. **Систем за заштита на личните податоци** е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на Фондот, а кои се во функција на спроведување на техничките и организациските мерки за безбедност на обработката на личните податоци;

12. **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;

13. **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;

14. **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;

15. **Идентификација** е постапка за идентификување на овластеното лице на информацискиот систем;

16. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на Фондот, во рамките на која се собираат, обработуваат и чуваат личните податоци;

17. **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;

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

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

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

21. **Колаче (cookie)** е информација која што се креира и испраќа од веб-серверот до веб-пребарувачот а која потоа се испраќа назад, како непроменета информација од веб-пребарувачот секогаш кога повторно ќе се пристапи до веб-серверот кој ја креирал информацијата;

22. **Работна станица** е секој уред (десктоп, лаптоп) кој поврзан во мрежа претставува дел од опремата на Фондот, а на кој, односно со кој се врши обработка на личните податоци во информацискиот систем;

23. 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 и

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

Член 3

Фондот ги утврдува целите, безбедноста и начинот на обработката на личните податоци согласно овој Правилник.

Безбедност на обработка на личните податоци

Член 4

Одредбите од овој Правилник се применуваат на:

-Целосно и делумно автоматизирана обработка на личните податоци со псевдоминизација и криптирање на личните податоци;

-Обезбедување на континуирана доверливост, интегритет, достапност и отпорност на информацискиот систем за обработка;

-Навремено, повторно воспоставување на достапност до личните податоци и пристап до нив во случај на физички или технички инцидент и

-Процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел гарантирање на безбедноста на обработката.

Управување со ризик

Член 5

Фондот при утврдувањето и процена на ризикот (управување со ризик) ги зема во предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

Управувањето со ризикот од ставот (1) на овој член ги опфаќа следните фази:

а) список (преглед) на сите процеси со кои се врши обработка на лични податоци;
б) процена на ризиците за секој процес на обработка на лични податоци;
в) спроведување и проверка на планираните мерки; и
г) спроведување на периодични безбедносни проверки.

Фондот задолжително врши спроведување и проверка на планираните мерки од став (2) точка в) на овој член, а со цел да се обезбеди дека тие се применуваат и тековно се тестираат.

Фондот задолжително спроведува периодични безбедносни проверки од став (2) точка г) на овој член, за што се подготвува акционен план, чија имплементација се следи од страна на раководството на Фондот.

Нивоа на технички и организациски мерки

Член 6

Техничките и организациските мерки, Фондот ги класифицира во две нивоа: стандардно и високо ниво.

Примена на нивоа

Член 7

За сите документи задолжително се применуваат технички и организациски мерки од стандардно ниво.

За документите кои содржат лични податоци задолжително се применуваат технички и организациски мерки од стандардно ниво.

За документите кои содржат, матичен број на граѓанинот задолжително се применуваат технички и организациски мерки од високо ниво.

За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци/или матичен број на граѓанинот задолжително се применуваат технички и организациски мерки од стандардно и високо ниво.

За документите кои содржат, посебни категории на лични податоци, задолжително се применуваат технички и организациски мерки од стандардно и високо ниво.

II. Стандардно ниво на технички и организациски мерки

Документација за технички и организациски мерки

Член 8

Технички и организациски мерки во Фондот се обезбедуваат преку документација за технички и организациски мерки и тоа:

-План за создавање систем на технички и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци,

-Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица,

-Правила за пријавување, реакција и санирање на инциденти,

-Правила за начинот на правење на сигурносна копија, архивирање и чување, како и повторно враќање на зачуваните лични податоци,

-Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.

Технички мерки

Член 9

Фондот при автоматизираната обработка на личните податоци задолжително применува технички мерки за обезбедување тајност и заштита на податоците преку:

-Единствено корисничко име;
-Лозинка креирана за секое овластено лице, составена од комбинација на најмалку осум алфа нумерички карактери (од кои минимум една голема буква) и специјални знаци;
-Автоматизирано задолжително менување на лозинката после првото најавување;
-Времетраење на лозинката е 30 дена;
-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 работењето;
-Автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути) а за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
-Автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име и/или лозинка) и автоматизирано известување на овластеното лице дека треба да се побара инструкција од администраторот на информацискиот систем;

-Автентикација на овластеното лице со дигитален потпис;
-Инсталирана хардверска и софтверска заштита, огнен ѕид (firewall) и 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;
-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;
-Ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови; и
-Приклучување на информацискиот систем на енергетска мрежа преку уреди за непрекинато напојување.

Сегрегација на должности и одговорности

Член 10

Обврските и одговорностите на секое овластено лице, кое има пристап до личните податоци и до информацискиот систем, Фондот, ги дефинира и утврдува во правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко-комуникациската опрема.

Фондот, задолжително ги информира 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.

Контрола и пристап

Член 11

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

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.

Во евиденцијата на овластените лица, се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

Администраторот на информацискиот систем кој е овластен со Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци може да се доделува, менува или одзема

авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на контролорот.

Евиденција на пристап (logs)

Член 12

Фондот води евиденција за секој авторизиран пристап кој треба да ги содржи следните податоци: 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.

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 потребното ниво на авторизација.

Евиденцијата од ставот 1 на овој член, се чува најмалку пет години.

Операциите кои овозможуваат евидентирање на податоците од ставовите 1 и 2 на овој член треба да бидат контролирани од страна на офицерот за заштита на личните податоци.

Офицерот за заштита на личните податоци врши периодична проверка на податоците од ставовите 1 и 2 на овој член и изготвува извештај за извршената проверка доколку констатира неправилности.

Евиденција на инциденти

Член 13

Во процедурата за управување со сигурносните инциденти во информациониот систем, се определува начинот на евиденција на секој инцидент, времето кога се појавил, овластеното лице кое го пријавил, нивото на значењето, на кого е пријавен и мерките кои се преземени за негово санирање/разрешување.

Обезбедување на преносливите медиуми

Член 14

Фондот согласно анализата на ризикот од нарушување на безбедноста на личните податоци во случај на кражба или друг начин на загуба на преносливите

медиуми (мобилна опрема) на кои се врши обработка на личните податоци применува соодветни технички мерки.

Техничките мерките од ставот 1 на овој член го опфаќаат најмалку следното:

- подигање на свеста на овластените лица за специфичните ризици поврзани со користење на преносливи медиуми (на пример: кражба на опремата) и утврдените процедури за намалување на овие ризици;

-спроведување на мерки за правење на сигурносна резервна копија или синхронизација на мобилните работни станици, со цел да заштитат од губење на зачуваните податоци;

-мерки за криптирање за заштита на мобилни работни станици и медиуми за мобилно складирање (лаптоп, УСБ, надворешни хард-дискови, ЦД-РОМ, ДВД, итн.).

- употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на нивните услови и безбедносни гаранции.

Покрај мерките од ставот 2 на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, Фондот ги применува и следните мерки:

- поставување на филтер за приватност на екраните на мобилните работни станици што се користат на јавни места, или употреба на мобилни работни станици со интегриран филтер за приватност;

- ограничување на обемот на податоци кои може да се зачуваат на мобилните работни станици на она што е строго неопходно со дополнителна заштита и ограничување за време на патувања, особено во странство;

- спроведување на дополнителни мерки за заштита од кражба (на пример кабел за безбедност, видливо обележување на опремата итн.) и мерки што ги намалуваат негативните ефекти (на пример автоматско заклучување, криптирање); и

- кога мобилните уреди се користат за собирање податоци во движење (на пример: лични асистенти, паметни телефони, лаптопи, итн.), шифрирање на податоците на самиот уред.

Исто така, заклучување на уредот по неколку минути неактивност и прочистување на податоците собрани веднаш штом се пренесат во информацискиот систем на Фондот.

Заштита на внатрешната мрежа

Член 15

Фондот обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци, а особено преку:

- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (VoIP, peer to peer, итн.);

- управување со Wi-Fi мрежата кое опфаќа користење на најсовремените методи на криптирање (на пример: WPA2 или WPA2-PSK и со употреба на комплексна лозинка која на определен временски период се менува);
- Wi-Fi мрежата која е отворена за употреба на лица кои не се овластени (на пример надворешни посетители) задолжително да биде одвоена од внатрешната мрежа;
- во случај на далечински пристап, задолжително воспоставување на VPN конекција, со задолжителна автентикација на овластеното лице (на пример: паметна картичка, уред за генерирање лозинка за еднократна употреба – OTP и слично);
- обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително да се изврши преку VPN); и
- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен ѕид, прокси сервери, итн. (на пример: ако веб серверот користи HTTPS, да се обезбеди влезниот сообраќај да биде преку портата 443 и со блокирање на сите други пристапи).

Фондот врз основа на анализата на ризикот, покрај мерките наведени во ставот (1) од овој член, може да примени и други мерки со кои ќе ја зајакне заштитата на својата внатрешна мрежа.

Овезбедување на серверите

Член 16

Фондот согласно анализата на ризик од аспект на примената на технички и организациски мерки, за приоритет ги има своите сервери на кои се централизира обработката на голема количина на лични податоци. При тоа, Фондот ги применува следните мерки:
- единствено овластени лица кои ги имаат потребните знаења може да имаат пристап до алатките и административни панели на серверите;
- примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);
- примена на посебна политика за креирање и употреба на лозинките за администраторите на информацискиот систем (на пример: промена на лозинките по секое заминување на администраторот, употреба на повеќе факторска лозинка...);
- инсталирање на сите важни ажурирања (updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (auto update);
- правење на сигурносни копии и нивна редовна проверка; и

- примена на TLS протокол (со замена на SSL13) или друг протокол што обезбедува шифрирање и автентикација, како минимум за каква било размена на податоци преку интернет и потврда на нејзината соодветна примена преку соодветни алатки.

Во случај кога се врши администрирање на базите на податоци, контролорот ги применува најмалку следните мерки:

- употреба на персонализирани профили за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација (specific account for each application); и
- примена на мерки против напади преку инјектирање на SQL код, скрипти и слично.

Обезбедување на веб-страницата

Член 17

Фондот кој има своја веб-страница треба да примени технички мерки со кои ќе го гарантира точниот идентитет на страницата (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа особено преку следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на контролорот (ако има повеќе од една), користејќи ја единствено најновата верзија и со проверка на неговата правилна имплементација;
- задолжителна употреба на криптографски протокол (TLS) за сите страници од веб страницата, вклучително и формулари за собирање лични податоци, или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавно достапни;
- ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации.

Ако веб серверот прифаќа само врски со HTTPS протокол, само IP мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти мора да бидат блокирани;

- обезбедување дека само овластени лица ќе можат да имаат пристап до алатките и административните интерфејси, при што особено да се ограничи употребата да биде достапна само до овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни; и
- ако се користат колачиња што не се потребни од услугата, контролорот обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;

(2) Контролорот кој има своја веб-страница не треба да применува практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена обработка на личните податоци, а особено:

- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);
- користење на небезбедни услуги; - употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораки и слично;
- поставување на базите на податоци на сервери кои се директно достапни преку интернет; и
- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

Обврски и одговорности на администраторот на информацискиот систем

Член 18

Обврските и одговорноста на администраторот на информацискиот систем, Фондот ги дефинира и утврдува во правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко-комуникациската опрема.

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

Во извештајот од ставот 2 на овој член, треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Идентификација и проверка

Член 19

Фондот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проврка на авторизираниот пристап.

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.

Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци утврден во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и да се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 20

Фондот е одговорен за проверка на примената на правилата за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Во Правилата од ставот 1 на овој член, задолжително треба да се содржани постапките за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени и уништени.

Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Фондот, задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци согласно ставот 4 на овој член.

Начин на архивирање и чување на податоците

Член 21

Фондот, во однос на личните податоци за кои сè уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, врши архивирање на безбеден начин, особено ако архивираните податоци се чувствителни податоци (посебни категории на лични податоци), или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци, доколку бидат компромитирани.

Согласно ставот 1 од овој член, Фондот определува постапка за управување со архивскиот материјал во однос на тоа кои податоци треба да се архивираат, како и каде се чуваат и кој, како и под кои услови има пристап до нив.

Фондот задолжително донесува соодветен документ „Список (преглед) со рокови на чување на личните податоци“ во кој ќе бидат содржани информации за моментот на активирање на периодот (рокот) за чување на личните податоци, идентификуваните периоди (рокови) за чување на личните податоци, причините за чување на личните податоци, законскиот основ за чување на личните податоци и сопственикот на податоците.

Фондот е должен документот од ставот 3 на овој член да го ревидира и усогласува годишно согласно промените во работењето и законските услови за чување на личните податоци.

Управување со преносливи медиуми

Член 22

Преносливите медиуми на кои се врши обработка на личните податоци Фондот обезбедува дека се чуваат на локација, до која пристап имаат само овластени лица утврдени од негова страна.

Пренесувањето на медиумите од ставот 1 на овој член надвор од работните простории се врши само со претходно овластување од страна на директорот на Фондот или врз основа на склучен договор за соработка.

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.

Уништувањето на медиумот се врши на начин кој ќе гарантира дека податоците кои биле снимени на него не можат повторно да бидат реконструирани (на пример: со механичко разделување на неговите составни делови).

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

За случаите од ставовите 4 и 5 на овој член Фондот обезбедува информациска трага (на пример: записник), која ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци кои биле снимени на истиот.

Криптирање на личните податоци

Член 23

Кога Фондот врз основа на анализата на ризикот, а земајќи ги предвид природата, обемот, контекстот и целите на обработката на личните податоци, врши криптирање на личните податоци, секогаш применува најсовремени технички решенија за криптирање со кои го обезбедува интегритетот, доверливоста и автентичноста на личните податоци.

Во согласност со ставот 1 на овој член Фондот применува единствено признати и безбедни алгоритми за криптирање (како на пример: SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC користејќи SHA-256, bcrypt, scrypt или PBKDF2 за чување лозинки, AES или AES-CBC за симетрично криптирање, RSA-OAEP v2.1 за асиметрично криптирање...), а воедно обезбедува заштита на тајните клучеви за криптирање со ограничувачки права за пристап и посебно креирана безбедна лозинка за пристап.

Фондот донесува внатрешна процедура во која задолжително се пропишува начинот на управување со тајните клучеви и сертификати, земајќи го предвид и управувањето со ризикот на заборавени лозинки.

Физичка безбедност

Член 24

Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани во просториите на Фондот, хостирани административни од страна на овластени лица на Фондот.

Физички пристап до просторијата во која се сместени серверите може да имаат само лица посебно овластени од директорот на Фондот.

Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице треба да биде придружувано и надгледувано од лицето од ставот 2 на овој член.

Просторијата во која се сместени серверите се заштитува од ризиците во опкружувањето преку примени на мерки и контроли со кои се намалува ризикот од потенцијални закани вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

По исклучок од ставот 1 на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на Фондот.

Во случајот од ставот 5 на овој член, меѓусебните права и обврски на Фондот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Контрола на информацискиот систем и информатичката инфраструктура

Член 25

Информацискиот систем и информатичката инфраструктура на Фондот задолжително подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за техничките и организациски мерки се применуваат.

На Фондот се врши надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

Надворешната контрола од став 1 на овој член се врши преку обработка на документи од страна на независно трето правно лице.

Во извештајот од извршената контрола од ставот 1 на овој член задожително треба да има мислење за тоа во колкава мера постапките и уптствата содржани во документацијата за техничките и организациски мерки се применуваат и се во

согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни колективни мерки за нивно отстранување.

Во извештајот од ставот 4 на овој член треба да се содржани податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

Извештајот од ставот 4 на овој член се анализира од страна на офицерот за заштита на личните податоци, кој доставува предлози на Фондот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

Извештајот од ставот 4 на овој член, треба да биде доставен за увид на Агенцијата за заштита на личните податоци.

Обработувач на збирка на лични податоци

Член 26

Одредбите од овој Правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Управување со обработувачи

Член 27

Фондот, применува процедура за одлучување за избор на обработувач, за кој предвидува:

-анализа на потенцијални обработувачи во однос на нивните технички и организациски мерки за обезбедување на гаранција дека обработката на личните податоци е во согласност со прописите за заштита на личните податоци, како и за обезбедување на заштита на правата на субјектите на лични податоци; и

-анализа на ризиците врз работењето на Фондот што можат да произлезат при обработката на личните податоци од страна на обработувачите.

Ангажирање на обработувачи

Член 28

Во случај кога Фондот ќе одлучи да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувачот, должен е да обезбеди дека личните податоци се обработуваат под негов надзор над безбедноста на личните податоци, при што личните податоци мора да бидат обработувани со безбедносни гаранции.

Во случаите од ставот 1 на овој член, Фондот може да пренесе работи само на обработувач кој може да обезбеди доволно гаранции, особено во однос на потребното знаење од областа на заштитата на личните податоци, сигурноста и ресурсите.

Меѓусебните права и обврски на Фондот и обработувачот се уредени со договор при што Фондот пред да го склучи договорот е должен да побара од обработувачот (давател на услугата), да му ја презентира својата безбедносна политика во однос информацискиот систем и информатичкта инфраструктура на која ќе се врши обработката на личните податоци во име на контролорот.

Безбедносната политика од ставот 3 на овој член треба да содржи податоци со кои ќе се гарантира безбедноста на личните податоци, и тоа:

- дали и како се врши криптирање на податоците според нивната чувствителност;
- постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;
- дали и како се врши криптирање на преносот на податоци;
-гаранции во однос на следливост (логови, информациска ревизорска трага...);
- управување со правата на пристап;
- автентикација; и
- други мерки за безбедност на обработката на личните податоци.

Договорот од ставот 3 на овој член треба да содржи одредби особено за:

- предметот, должината и целта на обработката на личните податоци;
- обврските за обработувачот да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци;
- обврските во однос на доверливоста на доверените лични податоци;
- минималните стандарди за автентикација на овластените лица;
- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;
-правилата за управување и известување на контролорот во случај на инциденти, односно во случај на нарушување на безбедноста на личните податоци;
- обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на контролорот; и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

Организациски мерки

Организациски мерки за безбедност на личните податоци

Член 29

Организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, во Фондот, се обезбедуваат со:

-целосна доверливост и сигурност на лозинките и другите форми на идентификација;
-организациски правила за пристап до деловите од системот потребни за извршување на работната задача;
-мерки на физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат податоците;
-почитување на техничките упатства при инсталирање и користење на опремата на која се обработуваат податоците;
-информирање и обука на вработените;
-уништување на документи по истекот на рокот за нивно чување.

Вработеното лице кое ги врши работите за човечки ресурси во Фондот, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице, со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката односно заклучени за натамошен пристап.

Известувањето, се врши и при било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.

Информирање и едуцирање за заштита на лични податоци

Член 30

Вработените во Фондот и лицата кои се ангажираат за извршување на работи во Фондот, должни се да обезбедат тајност, заштита на личните податоци на осигурениците и корисниците на права и другите лични податоци и истите да ги обработуваат и користат според техничките и организациските мерки на Фондот.

Вработените во Фондот и лицата од став 1 од овој член задолжително го применува правилото "чисто биро" при обработка на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

За документите кои се пренесуваат надвор од работните простории на Фондот, задолжително се применуваат соодветни мерки така што личните податоци содржани во истите нема да бидат видливи и достапни за трети лица или други неовластени лица.

Информирање за заштитата на личните податоци

Член 31

Лицата кои се вработуваат во Фондот, пред нивното отпочнување со работа се запознаваат со заштитата на личните податоци на осигурениците и корисниците на права од пензиското и инвалидското осигурување и на другите податоци кои ги води Фондот.

Лицата кои се ангажираат за извршување на работи во Фондот, во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци и другите податоци кои ги води Фондот.

Лицата од ставот 1 и 2 на овој член, пред отпочнување со работа, своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

Изјавата од ставот 3 на овој член треба да содржи:

-име и презиме на работникот

-назив на работното место

-дека ќе ги почитува начелата за заштита на личните податоци

-дека ќе ги применува техничко- организациските мерки за тајност и заштита на обработка на личните податоци и ќе ги чува како доверливи личните податоци како и мерките за нивна заштита.

-ќе врши обработка на личните податоци во Фондот и на други лица нема да издава било каков податок од збирките на лични податоци или било каков друг личен податок, кој му е достапен и кој го дознал или ќе го дознае при работата во Фондот.

Изјавата од став 3 на овој член своерачно е потпишана, и задолжително се чува во досието на вработениот.

Пристап до документите

Член 32

Пристапот до документите треба да биде ограничен само за овластени лица во Фондот.

За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

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

Правило чисто биро

Член 33

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

Чување на документи

Член 34

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отварање.

Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот 1 на овој член, Фондот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Ако документите не се чуваат заштитени на начин определен во ставовите 1 и 2 на овој член, тогаш Фондот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 35

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

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.

Начин на чување на документите

Член 36

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.

Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот 1 на овој член, Фондот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

III. Високо ниво за технички и организациски мерки

Член 37

Високото ниво на технички и организациски мерки, подразбира:
-примена на електронски сертификати за идентификација и автентификација,
-криптирање на податоците кога се пренесуваат на медиуми,
-криптирање или посебна заштита со соодветни методи кога се пренесуваат преку телекомуникациска мрежа.

Дополнителни правила за технички мерки

Член 38

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.

Високото ниво на технички и организациски мерки, Фондот го пропишува преку:

-управување со лозинки,

-сертификација за заштита на личните податоци,

-управување со преносливи медиуми,

-тестирање на информацискиот систем,

-сертификациони постапки,

-пренесување на медиуми,

-пренесување на личните податоци преку мрежа за електронски комуникации.

Управување со лозинки

Член 39

Фондот користи алатки за управување со лозинки со кои обезбедува дека различните лозинки за секоја услуга, или софтверска програма соодветно се чуваат, при што за пристап до сите лозинки обезбедува главна лозинка (master password), која е зајакнато комплексна, односно составена е од комбинација на најмалку 12 алфанумерички карактери (букви/мали и големи), симболи, броеви и специјални интерпукциски знаци) и да се менува во период не подолг од 30 дена.

Фондот во согласност со анализата на ризикот, за одредени овластени лица (на пример за администраторот на информацискиот систем или лицата кои креираат и користат главна лозинка (master password), може да изврши дисперзија на ризикот преку управување со лозинката со дополнителен фактор согласно правилото n-2 (на

пример: информацијата за лозинката да биде поделена на две или повеќе лица кои заеднички ќе се најавуваат на начин што секој ќе знае само дел од информацијата која ја сочинува лозинката, или едно овластено лице ја знае лозинка, а друго ја поседува и употребува паметна картичка – smart card).

Сертификација за заштита на личните податоци

Член 40

Фондот, покрај внатрешната контрола, а на доброволна основа, може да изврши и проверка на процесите и интерните документи за заштита на личните податоци заради сертификација на процесите преку кои се обработуваат личните податоци, со цел да демонстрира усогласеност со прописите за заштита на личните податоци при операциите на обработка.

Сертификацијата се врши од Агенцијата или од сертификациони тела согласно прописите за заштита на личните податоци.

Управување со преносливи медиуми

Член 41

Фондот е должен да воспостави 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.

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

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.

Пренесување на медиуми кои содржат лични податоци надвор од просториите на Фондот се врши само со претходно овластување од Директорот на Фондот или врз основа на склучен договор за соработка.

Тестирање на информацискиот систем

Член 42

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 со документацијата за технички и организациски мерки и прописите за заштита на личните податоци.

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.

Сертификациони постапки

Член 43

Фондот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги.

Пренесување на медиуми

Член 44

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 мрежа за електронски комуникации

Член 45

Личните податоци можат да се пренесуваат преку мрежата за електронски комуникации само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Организациски мерки

Копирање или умножување на документите

Член 46

Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на Фондот.

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 47

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

IV. Преодни и завршни одредби

Член 48

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 8 од овој Правилник.

Документацијата од членот 8 од овој Правилник, директорот на Фондот ја донесува во рок од шест месеци од денот на влегување во сила на овој Правилник.

Член 49

Со влегувањето во сила на овој Правилник, престанува да се применува Правилникот за заштита на податоците на Фондот на пензиското и инвалидското осигурување на Македонија („Службен весник на Република Македонија" бр. 73/2015).

Член 50

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

Број 02-6200/1
Скопје, 28.10.2021 год.

УПРАВЕН ОДБОР
Претседател,

Боро Варошлија