20252404653

ФОНД ЗА ЗДРАВСТВЕНО ОСИГУРУВАЊЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на член 27-в, член 54 став 2 и 56 став 1 точка 14 на Закон за здравствено осигурување („Службен весник на Република Македонија“ број 25/2000, 34/2000, 96/2000, 50/2001, 11/2002, 31/2003, 84/2005, 37/2006, 18/2007, 36/2007, 82/2008, 98/2008, 6/2009, 672009, 50/2010, 156/2010, 53/2011, 26/2012, 91/2013, 187/2013, 43/2014, 44/2014, 97/2014, 112/2014, 113/2014, 188/2014, 20/2015, 61/2015, 98/2015, 129/2015, 150/2015, 154/2015, 192/2015, 217/2015, 27/2016, 37/22016, 120/2016, 142/2016 и 171/2017 и „Службен весник на Република Северна Македонија“ број 275/2019, 77/2021, 285/2021, 60/2023, 154/2023, 209/2023, 144/2025 и 154/2025), а во врска со член 119 и 120 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20, 294/21), Управниот одбор на Фондот за здравствено осигурување на Република Северна Македонија, на седницата одржана на 19 ноември 2025 година, донесе

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА БЕЗБЕДНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ФОНДОТ ЗА ЗДРАВСТВЕНО ОСИГУРУВАЊЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Предмет

Член 1

Со овој правилник се утврдува документацијата што се применува во Фондот за здравствено осигурување на Република Северна Македонија (во понатамошниот текст: „Фондот“) за постапување при спроведување на техничките и организациските мерки за овластените лица кои имаат пристап до лични податоци на информацискиот систем на Фондот, со цел обезбедување на безбедност и заштита при обработката на личните податоци.

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

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

- Цел на заштита е обезбедување на правно усогласена обработка на личните податоци преку соодветни технички и организациски мерки, со цел да се ублажат ризиците и да се избегнат негативните влијанија врз правата и слободите на физичките лица;
- Минимизирање на личните податоци е цел на заштита преку ограничување на обработката на личните податоци на она што е соодветно, релевантно и неопходно за конкретната цел. Минимизирањето се однесува на дизајнот на системите за обработка на личните податоци, количината на обработени лични податоци, обемот на обработка, достапноста и периодот на чување;
- Доверливост е цел на заштита преку која треба да се обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци;

- Интегритет е цел на заштита преку која се гарантира дека личните податоци што се обработуваат се целосни, точни и ажурирани. Интегритетот се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции;

- Достапност е цел на заштита преку која треба да се обезбеди непречен пристап и контитуирана расположливост на личните податоци, односно пристапот до личните податоци и нивната обработка се можни без одложување, како и дека личните податоци може да се користат правилно во предвидениот процес;

- Неповрзливост е цел на заштита преку која треба да се обезбеди дека личните податоци се обработуваат строго ограничувајќи се на целта за која првично биле собрани, како и дека нема да се спојуваат или да се поврзуваат со други лични податоци што се собрани за други цели;

- Транспарентност е цел на заштита преку која треба да се обезбедат информации за обработката на личните податоци, односно можност да се идентификува на различно ниво кои податоци се собираат и се обработуваат, кога и за кои цели на обработка, кои системи и процеси се користат за да се утврди дали личните податоци се обработуваат според определената цел, како и кој има одговорност во различните процеси на нивната обработка;

- Интервенирање е цел на заштита преку која треба да се обезбеди ефективно остварување на правата на субјектите на лични податоци, како и применување на мерки за идентификување и автентикација на субјектите на лични податоци кои сакаат да ги остварат своите права;

- Ризик е постоење можност за појава на настан што сам по себе претставува штета (вклучително и неоправдано вмешување во правата и слободите на физичките лица) или може да доведе до дополнителна штета за едно или за повеќе физички лица. Сериозноста на ризикот е комбинација од влијанието на штетата и веројатноста дека настанот и последователната штета ќе се случат. Ризикот во контекст на заштита на личните податоци секогаш се оценува во однос на негативните влијанија врз правата и слободите на физичките лица;

- Процес на управување со ризик е систематска примена на политики, процедури и практики за управување со активностите кои се однесуваат на: комуницирање, консултирање, утврдување на контекстот, идентификување, анализирање, евалуирање, третирање, следење и проверување на ризикот;

- Систем за заштита на лични податоци е збир од документирани политики, кодекси на однесување, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на технички и организациски мерки за постигнување на целта на заштита согласно прописите за заштита на личните податоци;

- Информациски систем е целина од компоненти преку кои се обработуваат личните податоци при активностите за нивна обработка. Ова ги опфаќа вклучените системи (на пример: работни станици, сервери, мрежни или безбедносни уреди), услуги (на пример: процедура, единствена функција или збир од функции што служат за одредена цел) и податоци (на пример: специфични полиња од лични податоци што се користат за обработка), односно целата информациско-комуникациска опрема на Фондот, во рамките на која се собираат, обработуваат и чуваат личните податоци;

- Инцидент или настан е појава или промена на одредени околности кои што влијаат врз правата и слободите на физичките лица;

- Авторизиран пристап е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информациско-комуникациска опрема или за пристап до одредени работни простории на Фондот;

- Администратор на информацискиот систем е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето безбедност на обработката на личните податоци;

- 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 информацисko-комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско-комуникациска мрежа;

- Идентификација е постапка за идентификување на овластеното лице на информацискиот систем;

- Автентикација – е постапка која што овозможува потврдување на идентитетот на овластеното лице кое се најавува на информацискиот систем, при што овластеното лице не може да ја негира преземената активност или дејствие;

- 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 дејствије;

- Контрола на пристап е операција за доделување на пристап до личните податоци или до информацисko-комуникациската опрема со цел проверка на овластеното лице;

- Овластено лице е лице вработено или ангажирано во Фондот, согласно закон или меѓусебен договор, кое има авторизиран пристап до документите и до информацисko-комуникациската опрема;

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

- 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;

- Офицер за заштита на личните податоци (ОЗЛП) е лице овластено од директорот на Фондот за самостојно и независно вршење на работите во смисла на член 41-а од Законот за заштита на личните податоци;

- Проверка е постапка за верификација на идентитетот на овластеното лице на информацискиот систем;

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

- Посебни категории на лични податоци се лични податоци кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето или податоци за сексуалниот живот или сексуалната ориентација на физичкото лице;

- Контролор е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или посебните критериуми за негово определување;

- 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.

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 42/20 и 294/21).

Воспоставување на информациски систем

Член 3

(1) Имајќи ги предвид современите технолошки решенија, трошоците за нивна имплементација, како и природата, обемот, контекстот и целите на обработката на податоците, заедно со ризиците од различна веројатност и тежина по правата и слободите на физичките лица, Фондот воспоставува ефикасен и одржлив информациски систем во согласност со прописите за заштита на личните податоци, преку примена на соодветни технички и организациски мерки, со цел да обезбеди ниво на безбедност кое одговара на утврдениот ризик.

(2) За воспоставување на информацискиот систем, Фондот изработува соодветна документација за системот, која во основа опфаќа:

- прикажување на определената цел за обработка на личните податоци;
- прикажување на редоследот на активности за обработка на личните податоци;
- прикажување на сите употребени и генерирани лични податоци;
- опишување на техничките компоненти што се користат (хардвер, софтвер и инфраструктура);
- евиденција на активностите за обработка;
- разграничување со други активности кои што не се однесуваат на обработка на лични податоци;
- прикажување на релации со други системи за контрола и верификација на движењето на личните податоци.

(3) Пред воспоставување на информациски систем, Фондот ја проценува подготвената документација од ставот (2) на овој член според:

- начелата поврзани со обработката на личните податоци;
- законитост на обработката на личните податоци;
- правата на субјектите на личните податоци;
- неопходноста од вршење на проценка на влијанието на заштитата на личните податоци;
- примената на соодветни технички и организациски мерки од страна на обработувачите;
- условите за пренос на лични податоци.

(4) Со исполнување на условите од ставот (3) на овој член, Фондот изработува анализа и процена на ризикот според Методологијата за управување со ризик на Фондот, со цел да се избегнат негативните влијанија врз правата и слободите на физичките лица.

(5) Според проценатa на ризикот од ставот (4) на овој член, Фондот, идентификуваните ризици ги ублажува до соодветно ниво на прифатливост на ризикот, преку избор и примена на соодветни технички и организациски мерки за да се обезбеди ниво на безбедност соодветно на ризикот.

(6) За воспоставување на информациски систем, Фондот презема активности за усогласување на околностите од ставот (3) на овој член со соодветното ниво на прифатливост на ризикот од проценатa на ризикот од ставот (4) на овој член.

(7) Документираниот процес од овој член, во однос на воспоставување на информациски систем, се смета за систем за заштита на личните податоци според прописите за заштита на личните податоци.

Одржување на информацискиот систем

Член 4

(1) Фондот го преиспитува и ажурира информацискиот систем, особено во однос на техничките и организациските мерки кои ги применува во планирани временски интервали за да обезбеди безбедност на обработката на личните податоци, согласно прописите за заштита на личните податоци.

(2) 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 лични податоци, согласно договор со надворешно правно лице. Фондот нема да ја довери (пренесе) обработката на личните податоци на друг субјект-обработувач, кој применува технички и организациски мерки за безбедност 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.

Пренос на лични податоци во трети земји

Член 5

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем, може да се врши пренос на лични податоци во трети земји, само согласно условите утврдени во прописите за заштита на лични податоци. Трансферот на личните податоци на корисник кои се дадени во други држави, Фондот го врши само во случаите кога:

- постои согласност од страна на носителот на личните податоци;
- трансферот е потребен заради склучување или исполнување на договор од интерес на носителот на лични податоци, како и меѓу Фондот и трето лице;
- и во други случаи утврдени со закон, а во согласност со важечките законски и подзаконски акти од областа на заштитата на лични податоци и интерните акти на Фондот релевантни за заштитата на личните податоци на субјектите.

Преносот на податоци во други држави, кои не обезбедуваат исто ниво на заштита на податоци како во Република Северна Македонија, може да се врши по претходно одобрение од страна на Агенцијата за заштита на лични податоци, под услов да бидат обезбедени соодветни гаранции за заштита на приватноста, правата и слободите на субјектот на личните податоци.

Систем за заштита на лични податоци

Член 6

(1) Во согласност со член 3 став (1) а со цел обезбедување на заштита на личните податоци на осигурениците на Фондот на ниво на безбедност соодветно на ризикот, се воспоставува систем за заштита на личните податоци преку примена на технички и организациски мерки.

(2) Техничките и организациските мерки од ставот (1) на овој член ги вклучуваат сите неопходни мерки за гарантирање на целите на заштитата и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање.

(3) Фондот задолжително ги преиспитува и ги ажурира техничките и организациските мерки, при што секогаш ги применува оние мерки кои се соодветни за гарантирање на целите на заштита пропишани со одредбите на овој правилник.

(4) Процесот за управување со системот за заштита на личните податоци од ставот (1) на овој член се дефинира преку интерните акти на Фондот согласно на природата, обемот и сложеноста на активностите коишто Фонот ги врши при обработката на личните податоци и ризиците на коишто е изложен системот.

(5) Фондот задолжително ја ревидира и ажурира документацијата во врска со системот за заштита на личните податоци според направените промени во неговите операции на обработка на личните податоци.

Управување со ризик

Член 7

(1) При идентификување, анализа и процена на ризиците (процес на управување со ризик), Фондот задолжително ги зема предвид ризиците кои се поврзани со обработката на личните податоци за да ги обезбеди целите на заштитата, и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање.

(2) Управувањето со ризикот од ставот (1) на овој член опфаќа неколку фази, и тоа:

а) список (преглед) на информацискиот систем во целина со сите системи, услуги и податоци што се користат за обработка на личните податоци;

б) процена на ризиците за секој процес на обработка на личните податоци;

в) спроведување и проверка на планираните мерки и

г) спроведување на периодични безбедносни проверки.

(3) Списокот на системи, услуги и податоци што се користат за обработка на личните податоци од ставот (2) точка а) на овој член треба да биде опфатен со описот на техничките и организациските мерки кои се применуваат за обезбедување безбедност на обработката на личните податоци.

(4) Управувањето со ризиците од ставот (2) точка б) на овој член, за секој ризик, го вклучува најмалку следното:

(а) идентификување на потенцијалните влијанија и ефекти врз правата и слободите на засегнатите физички лица во однос на можните закани за целите на заштитата како што следува:

- минимизирање на личните податоците (на пример: имплементација на периоди за чување, криптирање или анонимизација),
- достапност (на пример: привремена или целосна недостапност на личните податоци),
- интегритет (на пример: несакани промени на личните податоци),
- доверливост (на пример: неовластен пристап до личните податоци),
- неповрзливост (на пример: ограничување на овластувањата за обработка, користење и пренос),
- транспарентност (на пример: записи за пристап до личните податоци) и
- интервенирање (на пример: имплементација на стандардизирани процедури за обезбедување на правото на пристап на субјектите на личните податоци);

(б) идентификување на изворите на ризик кои што би можеле да бидат причина за секој непосакуван настан, со соодветно разгледување на внатрешните и на надворешните човечки ресурси (на пример, администратор на информациски систем, овластено лице, надворешен напаѓач, конкурент), како и други внатрешни и надворешни извори (на пример: вода, опасни материјали, пожар, вирус);

(в) идентификување на лице или субјект со одговорност и овластување да управува со конкретниот ризик (сопственик на ризик);

(г) идентификување на можните закани кои би можеле да се случат преку медиуми на кои се обработуваат личните податоци (на пример: хардвер, софтвер, комуникациски канали, документи во хартиена форма, итн.), кои би можеле да се:

- користат на несоодветен начин (на пример: злоупотреба на овластувањата, грешка при ракување);
- изменат (на пример: „заразен“ софтвер или хардвер со снимач на записите на тастатурата, инсталирање на злонамерен, односно малициозен софтвер итн.);
- изгубат (на пример: кражба на лаптоп или губење мемориски уреди);
- надгледуваат (на пример: геолокација на опремата);
- оштетат (на пример: вандализам, деградација поради природно абење);
- преоптоварат (на пример: медиумот за чување на лични податоци е целосно пополнет, напад на одбивање услуга итн.);

(д) процена на веројатноста за појава (веројатност) во однос на претходните елементи предвидени во овој став на скала за процена: ретко, повремено и често;

(ѓ) процена на нивото на влијание во однос на претходните елементи предвидени во овој став на скала за процена: ниско, средно и високо;

(е) процена на сериозноста на ризикот во однос на претходните елементи предвидени во овој став на скала за процена: незначителен ризик, ризик и висок ризик.

(5) Фондот задолжително врши спроведување и проверка на планираните мерки од ставот (2) точка в) на овој член за да обезбеди дека тие се применуваат и тековно се тестираат.

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

Безбедност на обработка на личните податоци

Член 8

Одредбите од овој правилник се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци евидентирана по процесите и
- друга рачна обработка на личните податоци што се дел од активностите на постоен процес каде има евидентирано обработка на лични податоци.

Нивоа на технички и организациски мерки

Член 9

(1) Во Фондот се применуваат технички и организациски мерки, кои обезбедуваат безбедност на обработката на личните податоци, соодветни на природата, обемот и целите на заштита при обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица.

(2) Фондот применува основно или високо ниво на технички и организациски мерки, пропорционално на евидентираните активности за обработка на личните податоци.

Примена на нивоа

Член 10

(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 високо ниво.

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

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

(6) Со документацијата за технички и организациски мерки, врз основа на резултатите од спроведената методологија за управување со ризици, 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 11

Обработката на личните податоци надвор од работните простории на Фондот и на подрачните служби, се врши врз основа на писмено овластување од генералните директори или секторски директори, 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 12

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

Основно ниво на технички и организациски мерки Документација за технички и организациски мерки

Член 13

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

- Изјава за приватност;
- Изјава за приватност при вршење на видео надзор;
- Политика за приватност;
- Политика за колачиња;

- Политика за системот за заштита на лични податоци;
- Политика за информациска сигурност на Фондот;
- Упатство за примена на Методологија за управување со ризици;
- Останати интерни акти (процедури, упатства и постапки) за заштита во доменот на примена на информациско-технолошки комуникации.

(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 14

Во Фондот задолжително се обезбедуваат следните технички мерки за безбедност 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 информацискиот систем;
6. инсталирана хардверска/софтверска заштитна мрежна бариера („firewall“) или мрежен пренасочувач (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 15

(1) Фондот задолжително ги обезбедува следните организациски мерки за безбедност 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 информацисko-комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и

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

(2) Раководителот на одделението или овластено лице од секторот за човечки ресурси 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 16

Фондот со посебни интерни акти ја обезбедува физичката сигурност на информацискиот систем во согласност со прописите за заштита на личните податоци.

Информирање за заштитата на личните податоци

Член 17

(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.

(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 18

(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 информациско-комуникациската опрема, како што е опишано во интерните акти на Фондот, согласно прописите за заштита на личните податоци.

(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 19

(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 информациско-комуникациската опрема, како што е опишано во интерните акти на Фондот, согласно прописите за заштита на личните податоци.

(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 20

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 21

(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 интерните акти на Фондот согласно прописите за заштита на личните податоци, се утврдуваат 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 22

(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информациско-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 информациско-комуникациската опрема со права различни од тие за кои се авторизирани.

(3) Во евиденцијата на овластените лица утврдена во член 22 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

(4) Администраторот на информацискиот систем кој е овластен да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информациско-комуникациската опрема, истото го прави само во согласност со критериумите утврдени во интерните акти на Фондот кои се во согласност со прописите за заштита на личните податоци на Фондот.

Управување со медиуми

Член 23

(1) Со интерни акти изработени од Фондот, согласно прописите за заштита на личните податоци, се утврдуваат правила за постапување со медиумите со кои овозможуваат идентификација и евидентирање на категориите на лични податоци, и чување на медиумите на локација до која пристап имаат само овластени лица утврдени во интерните акти.

(2) Пренесувањето на медиуми кои содржат лични податоци надвор од работните простории е строго контролирано, со соодветни технички и организациски мерки, кои се утврдени со интерни акти на Фондот, со засебни договори во случаи со пренос на трета страна или во посебни случаи со претходно добиено одобрение од Агенцијата за заштита на лични податоци за договори со трети страни кои вклучуваат пренос надвор од границите на државата.

Уништување, бришење или чистење на медиумот

Член 24

(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 25

(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 интерни акти на Фондот.

Начин на чување на сигурносните копии

Член 26

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.

Дополнителни правила за технички и организациски мерки

Член 27

(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 безбедност 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 годишно врши контроли и за тоа изготвува извештај. Контролите се пропишани во интерните акти на Фондот, согласно правилата за заштита на лични податоци и правилникот за безбедност на обработка на лични податоци на Агенцијата за заштита на лични податоци.

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

(5) Во случај на поголеми инциденти и повреди на правилата и интерните акти со цел спречување на повторно случување на истите, офицерот за заштита на личните податоци ги известува и надлежните директори на сектори и генералните директори, 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 информациски систем

Член 28

(1) Фондот задолжително спроведува внатрешна и надворешна контрола на информацискиот систем во чии рамки е 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 на секои три години.

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

Идентификација и проверка

Член 29

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 авторизиран пристап (логови)

Член 30

(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 интерните акти на Фондот.

Контрола на физички пристап

Член 31

Во интерните акти на Фондот согласно прописите за заштита на лични податоци ќе се определат критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Член 32

(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 33

(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, генералните директори или овластени лица од нив, издаваат писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 34

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 35

(1) Фондот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот овозможува безбедност 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.

Високо ниво на технички и организациски мерки
Сертификациони постапки

Член 36

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 безбедност на обработката на личните податоци, преку примена на сертификациони постапки, согласно прописите за податоците во електронски облик и електронски потпис.

Пренесување на медиуми

Член 37

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 или лице овластено од него може да ги декриптира.

Пренесување на личните податоци преку електро-комуникациска мрежа

Член 38

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.

Друга рачна обработка на личните податоци
Основно ниво на технички и организациски мерки

Примена

Член 39

Одредбите од членовите 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 16 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 40

(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 41

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 42

(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 43

(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.

Контрола

Член 44

Одредбите од членовите 28 и 29 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 45

(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.

Високо ниво на технички и организациски мерки
Копирање или умножување на документите

Член 46

(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 47

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.

Преодни и завршни одредби

Член 48

Начинот и условите за обезбедување на технички и организациски мерки за безбедност на обработката на личните податоци се уредуваат со документацијата од членот 16 на овој правилник.

Документацијата од членот 16 на овој правилник, директорот на Фондот ќе ја донесе во рок од 12 месеци од денот на влегување во сила на овој Правилник.

Член 49

Со влегување во сила на овој Правилник, престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци во Фондот за здравствено осигурување на Македонија („Службен весник на Република Македонија“ број 95/2011).

Член 50

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

Бр. 02-26218/6
20 ноември 2025 година
Скопје

Управен одбор
Претседател,
Дритан Даути, с.р.