Република Северна Македонија

Правила за технички и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци

Скопје, август 2021 година

МАПАС
Агенција за супервизија на капитално финансирано пензиско осигурување

СОДРЖИНА

Врз основа на член 36 од Законот за заштита на личните податоци („Службен весник на Република Македонија" број 42/20), а во врска со член 6 ставови (1) и (2) од Правилникот за безбедност на обработка на личните податоци ("Службен весник на Република Македонија" бр.122/2020), и член 8 став (1) точка о) од Статутот на Агенцијата за супервизија на капитално финансирано пензиско осигурување (бр.01-385/3 од 18.03.2013, бр. 02-13/5 од 22.01.2014, 02-1316/4 од 11.11.2014, 02-83/3 од 30.01.2015, 02/1259/6 од 27.11.2018 и 02-464/6 од 29.03.2019 година) претседателот на Советот на експерти на Агенцијата за супервизија на капитално финансирано пензиско осигурување, на ??.??.2021 година, донесе:

Правила за технички и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци

I. Општи одредби

Предмет на уредување

Член 1

Со овие Правила се пропишуваат техничките и организациските мерки што Агенцијата за супервизија на капитално финансирано пензиско осигурување (во понатамошниот текст: Агенцијата) во својство на контролор ги применува за да обезбеди тајност и заштита на обработката на личните податоци.

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

"Доверливост" е пристап до личните податоци единствено од лица кои имаат овластување за нивна обработка од страна на контролорот;

"Интегритет" е заштита на точноста на личните податоци, при што се гарантира дека личните податоци се точни, целосни и ажурирани;

"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;

"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;

"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;

"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);

"Управување со ризик" е идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на контролорот 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;

"Систем за заштита на личните податоци" е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на Агенцијата, а кои се во функција на спроведување на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци.

"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 Агенцијата.

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

"Лозинка" е доверлива информација составена од множество на карактери кои се користат за проверка на овластеното лице и операторот.

"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.

"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.

"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, кои се чуваат во информацискиот систем на Агенцијата.

"Овластено лице" е лице, вработено или ангажирано во Агенцијата, кое има авторизиран пристап до личните податоци кои се чуваат во информацискиот систем на Агенцијата, документите и до информатичко комуникациската опрема.

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

документите и до информатичко комуникациската опрема.

"Офицер за заштита на лични податоци" е овластено лице вработено во Агенцијата кое врши работи поврзани со заштита на личните податоци со кои располага Агенцијата, согласно Законот за заштита на личните податоци.

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

"Информатичка инфраструктура" е целата информатичко комуникациска опрема на Агенцијата, во рамките на која се собираат, обработуваат и чуваат личните податоци.

"Интернет портал" е дел од инфор лацискиот систем на Агенцијата кој овозможува ограничен пристап на овластеното лице и оператор преку web форма до податоците за кои е овластен да ги обработува.

"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.

"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.

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

Примена

Член 3

Агенцијата применува 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.

Одржување на информацискиот систем

Член 4

Агенцијата ја евидентира и ја чува целокупната документација за софтверските програми за обработка на личните податоци, како и за сите нејзини промени.

Физичките или правните лица кои вршат одржување на информацискиот систем на Агенцијата се должни да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

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

Пренос на лични податоци во трети земји

Член 5

Агенцијата 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 личните податоци.

Обработка на личните податоци

Член 6

Во Агенцијата овие правила 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

Ниво на мерки за безбедност на обработката на личните податоци

Член 7

Агенцијата применува 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.

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

а) стандардно и
б) високо ниво.

II. Стандардно ниво на мерки за безбедност на обработката на личните податоци

Член 8

За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно ниво.

За документите кои содржат лични податоци што се однесуваат на: кривични дела, изречени санкции и мерки од контрола, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

За документи кои содржат: посебни категории на лични податоци и лични податоци кои се однесуваат на членовите на пензиските фондови, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

За документите кои содржат матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно ниво.

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 стандардно и високо ниво.

Технички мерки

Член 9

Агенцијата применува соодветни технички мерки за обезбедување на тајност и заштита на обработката на личните податоци, кои се чуваат во информацискиот систем, при пристапот на интернет порталот од страна на овластеното лице, и тоа:

- Креирање на единствено корисничко име за секое овластено лице на интернет порталот на Агенцијата;
- Лозинка креирана од овластеното лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
- Автоматска промена на лозинките на секои три месеци;
- Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;
- Корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, пристап до поединечни апликации и/или поединечни

збирки на личните податоци потребни при извршување на работните задачи;

- Псевдонимизација и криптирање на личните податоци;
- Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;
- Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да побара инструкција од администраторот на информацискиот систем (во натамошниот текст: администратор;
- Инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол') или рутер помеѓу информацискиот систем и интернет мрежата или друга форма на надворешна мрежа, како заштитна мерк против недозволени или злонамерни обиди за влез или неовластено пријавување на системот;
- Инсталирање на ефективна анти-вирусна и анти-спајвер заштита на информацискиот систем која постојано ќе се ажурира и
- Приклучување на информацискиот систем на енергетска мрежа преку уред за непрекинато напојување.
- обезбедување на веб-страницата на Агенцијата со примена на технички мерки со кои го гарантира точниот идентитет на страницата, како и доверливоста на информациите на страницата.

Член 10

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

- Креирање на единствено корисничко име;
- Лозинка креирана од секој оператор на интернет порталот. Лозинката е составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
- Автоматска промена на лозинките на секои три месеци;
- Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;
- Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;

- Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на операторот дека треба да побара инструкција од администраторот;
- Воспоставување на ефективна и сигурна антивирусна заштита и анти–спајвер заштита на информацискиот систем, со постојано набљудување и ажурирање заради превентива од непознати и непланирани закани од нови вируси и спајвери;
- 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;
- Ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
- Приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.
- Мерките од став 1 на овој член ги спроведува администраторот и врши нивна периодична проверка во информацискиот систем на Агенцијата.
- Надворешниот субјект треба да ја известува Агенцијата за промена на операторот со цел да биде доделено ново корисничко име и лозинка. Претходното корисничко име и лозинка се бришат.
- Известувањето од став 3 на овој член се врши и при било кои други промени на операторот што имаат влијание врз нивото или обемот на дозволениот пристап до личните податоци добиени преку информацискиот систем на Агенцијата.

Организациски мерки

Член 11

Агенцијата применува соодветни организациски мерки за тајност и заштита на обработката на личните додатоци, и тоа:

- ограничен пристап или идентификација за пристап до личните податоци;
- уништување на документи по истекот на рокот за нивно чување согласно прописите за архивска граѓа;
- воспоставување на мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и
- почитување на техничките упатства при инсталирање и користење на информатичко-комуникациската опрема на која се обработуваат личните податоци

Вработеното лице кое ги врши работите за човечки ресурси во Агенцијата, со претходна согласност од страна на Претседателот на Агенцијата, 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. Вработеното лице кое ги врши работите за човечки ресурси во Агенцијата, извес ување до администраторот го врши писмено.

Член 12

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

- Почитување на целосна доверливост и сигурност на лозинките и на останатите форми на идентификација, официјално издадени од Агенцијата за пристап до информацискиот систем кој содржи лични податоци;
- Електронско уништување на документи кои содржат лични податоци по истекување на рокот за чување;
- Изнесувањето на медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;
- Обезбедување физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци; и
- Почитување на кориснички упатства за користење на софтверска апликација преку која се пристапува до информацискиот систем на Агенцијата кој што во себе содржи лични податоци и начинот на преземање на личните податоци од истиот.

Физичка сигурност на информацискиот систем

Член 13

Агенцијата треба да обезбеди физичка сигурност на информацискиот систем. Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани, хостирани и администрирани од страна на Агенцијата.

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

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 3 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 Агенцијата.

Во случајот од ставот 5 на овој член, меѓусебните права и обврски на Агенцијата 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.

Офицер за заштита на лични податоци

Член 8

Претседателот на Советот на експерти на Агенцијата определува офицер за заштита на личните податоци кој ги врши следниве работи:

- учествува во донесувањето на одлуки поврзани со обработката на личните податоци, како и со остварувањето на правата на субјектите на личните податоци;
- ја следи усогласеноста на работењето на Агенцијата со прописите кои се однесуваат на обработката на личните податоци, со овој правилник и со документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;
- ја координира контролата на постапките и упатствата утврдени во овој правилник и во документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци и
- предлага обука на вработените во врска со заштитата на личните податоци.

Информирање за заштитата на личните податоци

Член 9

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

За лицата кои се ангажираат за извршување на работа во Агенцијата во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

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

Лицата кои се вработуваат или се ангажираат во Агенцијата, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци која е дадена во прилог на оваа одлука.

Изјавата од ставот (4) на овој член особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од Агенцијата, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита

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

Агенција 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 10

Обврските и одговорностите на администраторот на информацискиот систем, Агенцијата ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

Офицерот за заштита на личните податоци во Агенцијата 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 доколку такви се констатирани, како и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Член11

Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, Агенцијата ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

Агенцијата 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.

Идентификација и проверка

Член 12

Агенцијата задолжително води евиденција за овластените лица кои имаат авторизиран

пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизирани пристап.

Кога проверката се врши врз основа на корисничко име и лозинка, Агенцијата 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.

Евиденција на овластените лица кои имаат авторизиран пристап до документите и информацискиот систем

Член 13

Агенцијата води евиденција на вработените лица кои имаат авторизиран пристап до документите и информатичкиот систем, која содржи:

- Име и презиме на вработениот;
- Работна станица и корисничко име за сите вработени кога пристапуваат до системот, заедно со нивото на авторизиран пристап, датумот и времето на пристапување и личните податоци кон кои е пристапено;
- Видот на пристапот со операциите кои се преземени при обработка на податоците;
- Запис од авторизација за секое пристапување;
- Запис за секој неавторизиран пристап;
- Запис од автоматизирано отфрлање од информацискиот систем и
- Идентификување на систем од кој се врши надворешен обид за пристап во оперативните функции или лични податоци без потребно ниво на авторизација.

Контрола на пристап

Член 14

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

Агенцијата 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.

Администраторот на информацискиот систем кој е овластен согласно Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица може да доделува, менува или да го одзема авторизирани пристап до личните податоци и информатичко - комуникациската опрема само врз основа на налог од страна на

Претседателот и во согласност со критериумите кои се утврдени од страна на Агенцијата.

Контрола на информацискиот систем и информатичката инфраструктура

Член 15

Информацискиот систем и информатичката инфраструктура на Агенцијата подлежи на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

Агенцијата 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 задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување.

Со извештајот од ставот (4) на овој член треба да се содржани и 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 контролорот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

Управување со медиуми

Член 16

Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на Претседателот на Агенцијата.

За пренесените медиуми надвор од работните простории на Агенцијата, се преземаат неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Уништување, бришење или чистење на медиумот

Член 17

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 со механичко разделување на неговите составни денови, при што истиот повторно да не може да биде употреблив.

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

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.

Идентификација и проверка

Член 18

Агенцијата треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице.

Контрола на физички пристап

Член 19

Во документацијата за технички и организациски мерки, Агенцијата определуваа критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Евидентирање на инциденти

Член 20

Во Правилата за пријавување, реакција и санирање на инциденти. Агенцијата 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.

За повторно враќање на личните податоци, Агенцијата издава писмено овластување на администраторот на информацискиот систем.

Сигурносни копии

Член 21

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

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.

Сигурносните копии кои се чуваат на друга оддалечена локација од местото каде е сместен информатичкиот систем треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

Офицерот за заштита на лични податоци и администраторот вршат проверка на спроведување на мерките од овој член.

Сигурносни копии задолжително се прават на крајот од работната седмица на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уни тени.

Пристап до документи

Член 22

Пристапот до документите *е* ограничен само за овластени лица на Агенцијата.

За пристапувањето до документите задолжително се воспоставуваат 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 се воспоставени соодветни процедури за таа цел со документацијата за техничките и организациските мерки.

Правило "чисто биро"

Член 23

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

Начин на чување на документи

Член 24

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

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 2 на овој член, Агенцијата треба да примени други мерки за да се спречи секој неовластен пристап до документите.

Уништување на документи

Член 25

Уништувањето на документите се врши со ситнење или на 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.

Копирање или умножување на документите

Член 26

Копирањето или умножувањето на документите може да се врши единствено со контрола на овластените лица на Агенцијата, а уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

III. Високо ниво на мерки за безбедност на обработката на личните податоци

Член 27

Високо ниво на техничките и организациските мерки за безбедност на обработка на личните податоци ги опфаќа следните видови на мерки: криптирано пренесување на документи, копирање или умножувањето на документи по претходно овластување и заштита при физички пренос на документите.

Член 28

Агенцијата треба да обезбеди заштита на личните податоци при нивната размена со надворешните субјекти преку медиуми и електронска комуникациска мрежа, овозможувајќи криптирана врска за размена, строги правила за идентификација при размената (лозинки тешки за пробивање) и електронско потпишување на документите за размена. Криптираните документи може да ги декриптира само администраторот или лице овластено од него.

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

Член 29

Копирањето или умножувањето на документи кои содржат лични податоци може да се врши единствено со претходно писмено овластување од страна на претседателот на Советот на експерти на Агенцијата.

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

Член 32

Во случај на физички пренос на документите Агенцијата 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

Со денот на донесување на овие Правила престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци бр.01-528/9 од 27.4.2015 година

Овие Правила влегуваат во сила со денот на нивното донесување и истите ќе се објават на огласната табла на Агенцијата.

Изработил: Емилија Рамова Е. Рамова

16.8.2021 година

Претседател на Советот на експерти
Максуд Али