АГЕНЦИЈА ЗА ПОШТИ
Бр. 02-206/10
22.09. 2022 год.
СКОПЈЕ

АГЕНЦИЈА ЗА ПОШТИ

ПРАВИЛА ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ

ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Септември, 2022 година

Врз основа на член 19 став (1) алинеја 3 од Законот за поштенските услуги („Службен весник на Република Македонија“ бр.158/10, 27/14, 42/14, 187/14, 146/15, 31/16, 190/16, 64/18, 248/2018, бр.27/2019 и “Службен весник на Република Северна Македонија” бр. 275/2019 и бр.150/2021), член 36 од Законот за заштита на лични податоци („Службен весник на Република Северна Македонија“ бр. 42/20), а вв со член 6 став (1) и (2) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Директорката на Агенцијата за пошти ги донесе следниве:

ПРАВИЛА ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. Општи одредби

Член 1

Предмет на уредување

Со овие Правила се пропишуваат техничките и организациски мерки што Агенцијата за пошти (во понатамошниот текст: Агенцијата) во својство на контролор ги применува за да обезбеди тајност и заштита на личните податоци.

Член 2

Поимник

Одделни изрази употребени во овие Правила го имаат следново значење:

„Доверливост“ е пристап до личните податоци единствено од лица кои имаат овластувања 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 (bussines continuity) на информацискиот систем на кој се врши обработката на личните податоци од страна на овластени лица;

„Автентикација“ е постапка која што овозможува потврдување на идентитетот на овластеното лице кое се најавува и пристапува кон информациското систем на кој се врши обработка на личните податоци;

„Неотповикливост“ е обезбедување на потврда на автентичноста на идентитетот на лице кое се најавува на информациското систем при што овластеното лице не може да ја негира превземената 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 лични податоци“ е збир од документирани политики, кодекси на пракса, насоки, процедури и работни инструкции донесени од страна на Агенцијата, а кои се во функција на спроведување на технички и организациски 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 за 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 или операторот;

„Медиум“ е физички уред кој се користи при обработка на лични 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, содржана 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 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 комуникациска опрема;

„Оператор“ е овластено физичко лице, вработено или ангажирано кај надворешни субјекти кое има пристап до личните податоци кои се добиваат преку информацискиот ситем на Агенцијата;

„Офицер за заштита на лични податоци“ е овластено лице вработено во Агенцијата кое врши работи поврзани со заштита на лични податоци со кои располага Агенцијата, согласно ЗЗЛП;

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

„Информатичка инфрастрктура“ е целата информатичко комуникациска опрема на Агенцијата, во рамките на која се собираат, обработуваат и чуваат личните податоци;

„Интернет портал“ е дел од информацискиот 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-центарот 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.

Член 3

Примена

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.

Член 4

Одржување на информацискиот систем

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.

Член 5

Обработка на личните податоци

Во Агенцијата овие правила се применуваат за:

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

Член 6

Ниво на мерки за безбедност на обработката на личните податоци

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 организациски мерки од ставот 1 на овој член се класифицираат во две нивоа:

- Стандардно ниво,
- Високо ниво.

Член 7

Стандардно ниво на мерки на безбедност на обработката на личните податоци

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

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

За документите кои содржат матичен број на лицето 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 лицето задолжително се применуваат технички и организациски мерки кои се класифицираат на стандардно и на високо ниво.

Член 8

Технички мерки

Агенцијата применува соодветни технички мерки за обезбедување тајност и заштита на обработката на личните податоци, кои се чуваат во информациското систем, при пристапот на интернет порталот од страна на овластено 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 информациското систем;
- корисничко име и лозинка која овозможува пристап на овластеното лице до информациското систем во целина, пристап до поединечните апликации и/или поединечни збирки на лични податоци потребни за извршување на работните задачи;
- псевдономизација и криптирање на личните податоци;
- воспоставување на автоматизирано одјавување од системот по изминување на одреден период неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;
- автоматизирано отфрлање од информациското систем по три неуспешни обиди за најавување (внесување на погрешно име или лозинка) и автоматизирано известување на овластеното лице дека треба да побара инструкција од администраторот на информациското систем (во натамошниот текст администратор);
- инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол“) или рутер помеѓу информациското систем и интернет мрежата или друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или неовластено пријавување на системот;
- инсталирање на ефективна анти-вирусна, анти-спајвер заштита на информациското систем која постојано ќе се ажурира и

- приклучување на информациското систем на енергетска мрежа преку уред за непрекинато напојување,
- обезбедување на веб-страницата на Агенцијата со примена на технички и организациски мерки со кои го гарантира точниот идентитет на страницата , како и доверливоста на информациите на страницата.

Член 9

Агенцијата треба да обезбеди технички мерки за тајност и заштита на личните податоци, кои се чуваат во информациското систем на Агенцијата, при пристапот на интернет порталот од страна на надворешни субјекти и тоа:

- креирање единствено корисничко име;
- лозинка креирана од секој оператор на интернет порталот, 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 информациското систем;
- воспоставување на автоматизирано одјавување од системот по изминување на одреден период неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;
- автоматизирано отфрлање од информациското систем по три неуспешни обиди за најавување (внесување на погрешно име или лозинка) и автоматизирано известување на овластеното лице дека треба да побара инструкција од администраторот на информациското систем (во натамошниот текст администратор);
- инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол“) или рутер помеѓу информациското систем и интернет мрежата или друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или неовластено пријавување на системот;
- инсталирање на ефективна анти-вирусна, анти-спајвер заштита на информациското систем која постојано ќе се ажурира, и
- Приклучување на информациското систем на енергетска мрежа преку уред за непрекинато напојување.

Мерките од став 1 од 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 се додаде ново корисничко име и лозинка. Претходното корисничко име и лозинка се бришат.

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

Член 10

Организациски мерки

Агенцијата применува соодветни организациски мерки за тајност и заштита на обработката на личните податоци, 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 заштита на работните простории и на информатичко комуникациска опрема каде што се собираат, обработуваат и чуваат личните податоци, и
- почитување на техничките упатства при инсталирање и користење на информатичко-комунмикациската опрема на која се обработуваат личните податоци.

Вработеното лице кое ги врши работите за човечки ресурси во Агенцијата, со претходна согласност од страна на директорот на Агенцијата, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до документите и информацискиот систем, како и воспоставување постапка за идентификација и проверка на авторизиран 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.

Член 11

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

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

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

Член 12

Контрола на пристап

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

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 авторизираниот пристап до личните

податоци и информатичко комунациската опрема само врз основа на налог на директорот и во согласност со критериумите кои се утврдени од страна на Агенцијата.

Член 13

Контрола на информацискиот систем и информатичката инфраструкстура

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.

Надворешаната 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 личните податоци 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 мислење и се предложени мерките за отстранување на недостатоците.

Извештајот од став (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.

Член 14

Управување со медиуми

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

Член 15

Уништување, бришење или чистење на медиумот

По пренесување 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 делови, 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 3 и 4 од овој член се составува комисиски записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Член 16

Идентификација и проверка

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 на секое овластено лице.

Член 17

Контрола на физички пристап

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

Член 18

Евидентирање 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 лични податоци кои се вратени и кои биле рачно внесени при враќањето во Правилата за пријавување, реакција и санирање на инциденти.

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

Член 19

Сигурносни копии

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

Сигурносните копии задолжително се прават секој ден и на крајот на работната седмица, а по потреба и секој последователен работен ден во месецот.

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

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

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

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

Член 20

Пристап до документите

Пристапот до документите е ограничен само до овластените лица на Агенцијата.

За пристапувањето до документите, задолжително да се воспостават механизми за идентифкиација на овластените лица и за категории на лични податоци до кои се пристапува. Доколку е потребен пристап на друго лице до документите, тогаш се воспоставени соодветни процедури за таа цел со документација за технички и организациски мерки.

Член 21

Правило „чисто биро“

Агенцијата 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.

Член 22

Начин на чување на документи

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.

Член 23

Уништување на документи

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

Во случајот од став (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.

Член 24

Копирање или умножување на документите

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.

Член 25

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

Член 26

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 27

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

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

Член 28

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.

Член 29

Преодни и завршни одредби

Со денот на донесување на овие Правила престанува да важи Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на лични податоци бр. 02-278/8 од 17.10.2019 година.

Овие Правила влегуваат во сила со денот на нивното донесување и истите ќе се објават на веб страницата на Агенцијата за пошти.

АГЕНЦИЈА ЗА ПОШТИ

Директорка

Билјана Аврамоска Ѓореска