



Република Северна Македонија
Republika e Maqedonisë së Veriut

Министерство за јавна
администрација
Ministria e administratës



РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT
06.07.2026 год.-viti
МИНИСТЕРСТВО ЗА ЈАВНА АДМИНИСТРАЦИЈА
MINISTRIA E ADMINISTRATËS PUBLIKE

Бр.-Nr. 16-2392/13

06.07 2026 год.-viti
Скопје - Shkup

Република Северна Македонија

Министерство за јавна администрација

Врз основа на член 28 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20, 294/21 и 101/25) и Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“, бр. 122/2020), а во врска со Планот за создавање на систем за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци, Министерот за јавна администрација, ја донесе следната

ПРОЦЕДУРА

ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ НА ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО МИНИСТЕРСТВОТО ЗА ЈАВНА АДМИНИСТРАЦИЈА

I. ОПШТИ ОДРЕДБИ

Член 1

Со оваа Процедура се пропишуваат техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци што се применуваат во Министерството за јавна администрација (во натамошниот текст: министерството).

Член 2

Одредбите од овој правилник се применуваат на:

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

II. ПОСЕБНИ ОДРЕДБИ

Член 3

Министерот за јавна администрација ќе применува технички и организациски мерки кои се класифицираат во три нивоа: основно ниво, средно ниво и високо ниво.

Член 4

За сите документи задолжително ќе се применуваат техничките и организациските мерки кои се класифицирани на основно ниво.

За документи кои содржат матичен број на граѓанинот задолжително се применуваат техничките и организациските мерки кои се класифицирани на основно и средно ниво.

За документите кои се пренесуваат преку телекомуникациска мрежа, а содржат матичен број на граѓанинот, задолжително се применуваат техничките и организациските мерки кои се класифицирани на основно, средно и високо ниво.

III. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 5

Министерот за јавна администрација врши евидентирање и ја чува целокупната документација за софтверските програми за обработка на личните податоци и сите негови промени.

Член 6

Административните службеници од Секторот за апликативно одржување на системите за организациска поддршка и развој на ресурсите на јавната администрација во Министерството за јавна администрација, се должни да вршат одржување на информацискиот систем во министерството, согласно документацијата за техничките и организациските мерки.

Член 7

Во министерството се обезбедуваат следните технички мерки за тајност и заштита при обработката на личните податоци:

1. Единствено корисничко име за секој вработен;
2. Лозинка креирана од секој вработен, составена од комбинација на најмалку 8 (осум) алфанумерички карактери (од кои минимум една голема буква) и специјални знаци, што се менува автоматски во период не подолг од 3 месеци;
3. Автоматизирано одјавување од информацискиот систем по изминати 15 минути на неактивност, а за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
4. Автоматизирано отфрлање од информативниот систем по 3 (три) неуспешни обиди (внесување на погрешно корисничко име или лозинка) и автоматизирано

известување на овластеното лице дека треба да побара инструкции од администраторот на информацискиот систем;

5. Инсталирана е хардверска/софтверска заштитна мрежна бариера (firewall), како и рутер помеѓу информацискиот систем и интерната конекција;
6. Инсталирана е ефективна и сигурна антивирусна и антиспајвер заштита на информацискиот систем - заштита која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
7. Инсталирана е ефективна и сигурна антиспам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови; и
8. Серверите во министерството се приклучени на енергетска мрежа преку уред за непрекинато напојување.

Член 8

Обработка на личните податоци на странките заради водење на управните постапки во Министерството за јавна администрација се врши на компјутерите во министерството, на кои пристап имаат само административните службеници кои се овластени за водење на постапки согласно Правилниците за систематизација и организација на работни места во министерството.

Документите кои содржат лични податоци по истекот на рокот за чување согласно прописите за архивски материјал, се уништуваат. Документите во хартиена форма кои содржат лични податоци по истекот на рокот на нивното чување се уништуваат на шредер, и тоа во доволна мерка за да не бидат употребливи и читливи.

Личните податоци на вработените во министерството, како и личните податоци на странките и третите лица во постапките кои се водат пред министерството во било кое време, се чуваат во заклучени шкафови и пристап до нив имаат административните службеници кои се овластени за водење на тековните работи согласно Правилниците за систематизација и организација на работните места во министерството.

Вработените лица во Одделението за управување со човечки ресурси во министерството, го известуваат администраторот на информацискиот систем за вработувањето или ангажирањето на овластеното 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.

Член 9

Серверите кои содржат лични податоци се физички поставени и се хостираат во министерството во посебна просторија, до која пристап имаат само административните службеници кои се задолжени за одржување на информацискиот систем.

Доколку е потребен пристап на друго лице до просторијата во која се наоѓаат серверите, тогаш тоа лице треба да биде придружувано и надгледувано од административните службеници од ставот 1 на овој член.

За просторијата во која се наоѓаат серверите се преземаат мерки за заштита од потенцијални закани како што се кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Член 10

Административните службеници кои се вработуваат или се ангажираат во министерството пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со документацијата за техничките и организациските мерки.

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

Административните службеници кои се вработуваат или се ангажираат во министерството, пред нивното отпочнување со работа своерачно потпишуваат Изјава за тајност и заштита на обработката на личните податоци.

Изјавата за тајност и заштита на обработката на личните податоци 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 документацијата за техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци на министерството, освен ако со закон не е уредено поинаку, како и дека истите ќе ги чуваат како доверливи лични податоци.

Изјавата за тајност и заштита на обработката на личните податоци задолжително се чува во персоналните досиеја на лицата кои се вработуваат или се ангажираат.

Изјавата за тајност и заштита на обработката на личните податоци е составен дел на овој правилник (Прилог бр.1).

Член 11

Обврските и одговорностите на секое овластеното лице кое има пристап до личните податоци и до информацискиот систем се дефинирани и се утврдени со Процедура за

определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

Член 12

Начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавило, на кого е пријавен и преземените мерки се уредени со Процедура за пријавување, реакција и санирање на инциденти.

Член 13

Постапките и процедурите за правење сигурносни копии, како и начинот на чување се регулирани со Процедура за начинот на правење на сигурносна копија, за архивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Член 14

Постапките и процедурите за остварување на правото на пристап и исправка до личните податоци од страна на субјектите на личните податоци се регулирани со Процедура за правото на пристап и исправка до личните податоци од страна на субјектите на личните податоци.

Член 15

Постапките и процедурите за управувањето, уништувањето, како и за бришењето или чистењето на медиумот се определени со Процедура за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.

Член 16

Административните службеници во Секторот за апликативно одржување на системите за организациска поддршка и развој на ресурсите на јавната администрација во министерството се овластени лица кои ќе бидат одговорни за координација и контрола на постапките и упатствата утврдени во документацијата за техничките и организациските мерки на министерството.

Член 17

Министерството врши надворешна контрола на секои три години и внатрешна контрола секоја година на информатичкиот систем и информатичката структура во министерството, согласно прописите за заштита на личните податоци.

Надворешната контрола може да се врши од страна на независно трето лице.

Член 18

Личните податоци кои ќе се пренесуваат преку телекомуникациска мрежа од министерството до Управата за јавни приходи, а кои содржат и единствен матичен број на

вработените во министерството, се криптирани, односно заштитени со соодветни мерки кои гарантираат дека податоците нема да бидат читливи при преносот.

Основно ниво на технички и организациски мерки

Член 19

Министерството води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем и врши идентификација и проверка на авторизираниот пристап.

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

Креираните лозинки се менуваат автоматски во период не подолг од 3 месеци и се заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

Член 20

Авторизиран пристап до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи, имаат овластените лица, кои пак немаат пристап до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

Министерството води евиденција на овластените лица како и на нивоата на авторизиран пристап за секое овластено лице.

Доделувањето, менувањето или одземањето на авторизираниот пристап до личните податоци и информатичко комуникациската опрема го врши овластениот администратор на информацискиот систем.

Член 21

Со медиумите е овозможена идентификација и евидентирање на категориите на лични податоци и истите се чуваат на локација до која пристап имаат само овластените лица.

Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од претседателот на министерството.

Средно ниво на технички и организациски мерки

Член 22

Министерството обезбедува механизми за јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице и води евиденција на авторизираниот пристап со следните податоци: име и презиме на овластеното лице, работна станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Во евиденцијата од претходниот став од овој член се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците ги контролира офицерот за заштита на личните податоци и истите не може да се деактивираат.

Евиденцијата на авторизираниот пристап се чува најмалку пет години.

Офицерот за заштита на личните податоци врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Член 23

Министерството воспоставува систем за евидентирање на медиумите кои се примаат/испраќаат заради 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.

При пренесување на медиуми надвор од работните простории на контролорот, министерството превзема неопходни и дополнителни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Член 24

Министерството, преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето правно лице, врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци согласно со

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

Високо ниво на технички и организациски мерки

Член 25

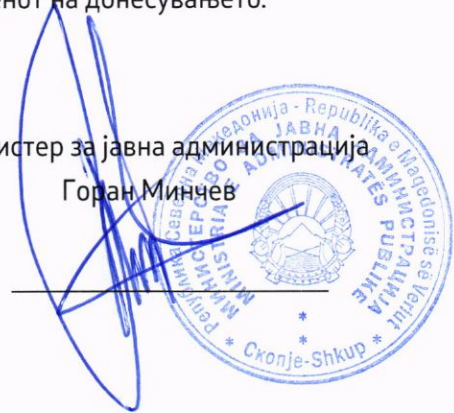
Медиумите можат да се пренесуваат надвор од работните простории на министерството само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице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

III. ЗАВРШНА ОДРЕДБА

Член 26

Оваа Процедура влегува во сила и ќе се применува со денот на донесувањето.

Министер за јавна администрација
Горан Минчев



Прилог 1

Врз основа на одредбите од податоци („Службен весник на Република Северна Македонија“ бр. 42/20, 294/21 и 101/25) и Правилникот за безбедност на обработката на личните податоци податоци („Службен весник на Република Северна Македонија“ бр. 122/2020), на ден _____ година, ја давам следната

ИЗЈАВА

за обезбедување тајност и заштита на обработката на личните податоци

Јас, долупотпишаниот/ата _____, распореден/а на работното место _____ во Министерството за јавна администрација, согласно со Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“, бр. 122/2020), а во врска со Политиката за воспоставување на систем за заштита на личните податоци во Министерството за јавна администрација, се обврзувам дека:

- ќе ги почитувам начелата поврзани со обработката на личните податоци;
- ќе ги применувам техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот и ќе ги чувам како доверливи личните податоци, како и мерките за нивна заштита; и
- ќе вршам обработка на личните податоци согласно упатствата добиени од Министерството за јавна администрација.

Потпис
