

20191923044

ВЛАДА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на член 210 став (2) од Законот за странци („Службен весник на Република Македонија“ бр. 97/18 и „Службен весник на Република Северна Македонија“ бр. 108/19), Владата на Република Северна Македонија, на седницата, одржана на 10 септември 2019 година, донесе

УРЕДБА ЗА ОБЕЗБЕДУВАЊЕ НА ТАЈНОСТ, ЗАШТИТА И БЕЗБЕДНОСТ НА ПОДАТОЦИТЕ СОДРЖАНИ ВО ИНТЕГРИРАНАТА БАЗА НА ПОДАТОЦИ ЗА СТРАНЦИ ВКЛУЧУВАЈЌИ ПОДАТОЦИ ЗА АЗИЛ, МИГРАЦИИ И ВИЗИ

Член 1

Со оваа уредба се уредуваат обезбедувањето на тајноста, заштитата и безбедноста на податоците содржани во Интегрираната база на податоци за странци вклучувајќи податоци за азил, миграции и визи (во натамошниот текст: Базата).

Член 2

Обезбедувањето тајност и заштита на податоците содржани во Базата (во натамошниот текст: податоците) се врши со примена на технички и организациски мерки од страна на надлежните органи согласно закон и прописите донесени врз основа на закон.

Член 3

Примената на техничките и организациските мерки од членот 2 од оваа уредба, од страна на надлежните органи се врши согласно прописите за заштита на личните податоци.

Член 4

(1) Лицата вработени во Министерството за внатрешни работи и Министерството за труд и социјална политика на кои им е доделен пристап, ги користат и обработуваат податоците со извршување на своите работни задачи на соодветни работни станици на кои се инсталирани апликации како дел од информацискиот системот на Министерството за внатрешни работи со кој се пристапува до податоците.

(2) Лицата вработени во Министерството за надворешни работи и Агенцијата за вработување на Република Северна Македонија кои пристапуваат до податоците преку сопствени информациски системи, ги користат и обработуваат податоците со извршување на своите работни задачи на соодветни работни станици на кои се инсталирани апликации како дел од овие информациски системи.

(3) Инсталирањето на апликациите како и сервисирањето на техничката опрема во врска со работните станици од ставот 1 на овој член се врши од страна на овластени лица од надлежните органи или надворешни субјекти определени од страна на корисниците на Базата.

(4) Надлежните органи спроведуваат процес на континуирано информирање (обука) на лицата кои пристапуваат до Базата, за нивните непосредни обврски и одговорности за заштита на личните податоци.

(5) Надлежните органи вршат периодични контролори над примената на мерките за обезбедување тајност, заштита и безбедност на податоците содржани во Базата според однапред определена динамика, согласно прописите за заштита на личните податоци и други прописи.

Член 5

(1) На лицата од членот 4 став 1 од оваа уредба им се креира единствено корисничко име и соодветна лозинка, со помош на кои тие се идентификуваат во делот на информацискиот систем на Министерството за внатрешни работи со кој се пристапува до податоците.

(2) Со корисничкото име и лозинката од ставот 1 на овој член лицата не можат да им овозможат пристап до податоците на други лица.

Член 6

Делот од информацискиот систем на Министерството за внатрешни работи со кој се пристапува до податоците поседува потсистем за управување со корисничките имиња и за управување со лозинки за корисничките имиња (во натамошниот текст: потсистемот).

Член 7

(1) Со управувањето на корисничките имиња од страна на потсистемот се овозможува пристап до соодветно ниво на пристап определено со групи и улоги согласно работните задачи утврдени за конкретни работни места во Министерството за внатрешни работи, односно во Министерството за труд и социјална политика.

(2) Покрај управувањето со корисничките имиња од ставот 1 на овој член, потсистемот овозможува и пристап до делот од системот на Министерството за внатрешни работи со кој се пристапува до податоците и со употреба на кориснички имиња креирани во други соодветни информациски системи на Министерството за надворешни работи и Агенцијата за вработување на Република Северна Македонија.

Член 8

Со управувањето со лозинките за корисничките имиња, потсистемот овозможува:

- лицата да ги изберат или променат своите лозинки;
- избор на квалитетни лозинки кои претставуваат комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
- промена на лозинките на одреден временски период не подолг од три месеци;
- лицата да извршат промена на привремената лозинка при првото пријавување на системот;
- меморирање и пренесување на лозинките во заштитена (криптирана или хеширана) форма;
- одржување на листа на претходно користени лозинки за соодветното лице и спречување на нивно повторно користење;
- неприкажување на лозинките на екран при нивното внесување;
- памтење на датотеките за лозинки одделно од останатите системски податоци на апликацијата;
- автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолг од 15 минути) и повторно активирање на системот со одново внесување на корисничкото име и лозинка;
- автоматизирано блокирање на корисничкото име на лицето после негови три неуспешни обиди за најавување, по што одредените лица назначени од страна на надлежниот орган започнуваат постапка за утврдување на причините;
- деактивирање на корисничките имиња и ресетирање на лозинките на корисничките имиња преку соодветен механизам.

Член 9

(1) Во делот од информацискиот систем на Министерството за внатрешни работи со кој се пристапува до податоците се забележува секој пристап до податоци за: корисничкото име, работната станица од каде се пристапува до делот од информацискиот систем на Министерството со кој се пристапува до податоците, датумот и времето на пристапување, нивото на пристапот, податоците до кои е пристапено, записот за секое пристапување и записот за автоматско отфрлање од информацискиот систем, како и пристапите до податоците кои доаѓаат од информациските системи на Министерството за надворешни работи и Агенцијата за вработување на Република Северна Македонија.

(2) Во забележувањето од ставот 1 на овој член се внесуваат и податоци за секој обид на неавторизиран пристап до податоците, како и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап до оперативните функции на делот од информацискиот систем на Министерството за внатрешни работи кој овозможува пристап до податоците без потребното ниво на авторизација, како и податоци за директниот пристап до Базата од страна на администраторите на Базата.

(3) Евиденцијата во која се забележува секој пристап до податоците содржани во информацискиот систем од овој член, се чуваат најмалку пет години.

(4) Офицерот за заштита на личните податоци од надлежните органи најмалку еднаш месечно врши периодични проверки на евиденцијата во која се забележани податоците за пристапувањето до информацискиот систем од овој член, за што изготвува извештај.

Член 10

(1) Техничката опрема која го овозможува функционирањето на делот од информацискиот систем на Министерството за внатрешни работи со кој се пристапува до податоците (базните сервери, апликативните сервери, серверот за извештаи, рутерите, свичевите и огнените ѕидови) е сместена во посебни простории во Министерството за внатрешни работи кои имаат контрола и набљудување на пристапот.

(2) Со контролата на пристап се врши идентификација и се овозможува пристап во просториите само на лицата кои вршат администраторско одржување на Базата, при што се забележуваат податоци за датумот, времето на влез и излез и името и презимето на лицето кое влегува, од страна на надлежната организациска единица во Министерството за внатрешни работи.

(3) Набљудувањето на пристапот до просториите се врши континуирано со видео надзор, согласно прописите од оваа област.

(4) Во случај кога е потребен пристап на друго лице до просториите, истото се спроведува со придружба и надгледување од страна на лицата определени во ставот 2 на овој член.

(5) Просториите од ставот 1 на овој член се заштитуваат од ризиците во опкружувањето преку примена 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.

Член 11

Безбедноста на податоците се врши со правење на сигурносни копии, архивирање и чување на податоците, повторно враќање на зачуваните податоци, како и со остварување на безбедна комуникација помеѓу надлежните органи во процесот на поврзување и синхронизирање на нивните информациски системи.

Член 12

(1) Сигурносни копии на податоците се прават секој работен ден, на крајот од работната седмица и секој последен работен ден во месецот.

(2) Сигурносните копии се прават на начин со кој се гарантира постојана можност за реконструирање на податоците во состојба во која биле пред да бидат изгубени или уништени.

(3) При администраторското одржување на Базата се проверува функционалноста на сигурносните копии за вршење на реконструкција на податоците, при што се составува записник за извршената проверка.

(4) Сигурносните копии се чуваат надвор од објектот во кој се наоѓаат просториите од членот 10 став 1 од оваа уредба и се физички и криптографски заштитени од било каква модификација.

Член 13

Остварување на безбедна комуникација помеѓу надлежните органи во процесот на поврзување и синхронизирање на нивните информациски системи се остварува со пренесување на криптирани или посебно заштитени со соодветни мерки податоци, кои гарантираат дека тие нема да бидат читливи при нивниот пренос.

Член 14

Пријавување, реакција и санирање на инциденти, надлежните органи го вршат согласно прописите за заштита на личните податоци.

Член 15

Со влегувањето во сила на оваа уредба престанува да важи Уредбата за обезбедување на тајност, заштита и безбедност на податоците содржани во интегрираната база на податоци за странци вклучувајќи податоци за азил, миграции и визи („Службен весник на Република Македонија“ бр. 119/12).

Член 16

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

Бр. 45-5613/1
10 септември 2019 година
Скопје

Претседател на Владата
на Република Северна Македонија,
Зоран Заев, с.р.