Република Северна Македонија
Дирекција за безбедност
на класифицирани информации
Бр. 02 – 1039/13
Скопје, 30/11 2021 година

Врз основа на член 75 став 1 од Законот за класифицирани информации(*) („Службен весник на Република Северна Македонија“ бр. 275/19), член 55 став 2 од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија“ бр. 58/00, 44/02, 82/08, 167/10, 51/11 и „Службен весник на Република Северна Македонија“ бр. 96/19, 110/19), а во врска со член 119 и 120 од Законот за заштита на личните податоци(*) („Службен весник на Република Северна Македонија“ бр. 42/20) и член 47 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), директорот на Дирекцијата за безбедност на класифицирани информации донесе

ПЛАН И НАСОКИ ЗА СОЗДАВАЊЕ СИСТЕМ НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. Цел

Целта на овој документ е етапно да го опише процесот на овозможување пристап и успешна заштита на личните податоци што се обработуваат во Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата) од аспект на пропишаните технички и организациски мерки за заштита на личните податоци.

II. Запознавање со прописите

(1) Пред отпочнување со работа секој вработен, односно ангажирано лице кое ќе има право на пристап до личните податоци се запознава со прописите за заштита на личните податоци.

(2) Непосредниот раководител на организационата единица генерално ги запознава вработените и ангажираните лица со Законот за заштита на личните податоци(*), со прописите од областа на заштитата на личните податоци донесени

од страна на Дирекцијата, како и со непосредните обврски и одговорности за заштита на личните податоци коипто произлегуваат од нив.

(3) Деталното запознавање со прописите е обврска на вработениот, односно ангажираното лице.

(4) Непосредниот раководител задолжително го известува вработениот, односно ангажираното лице за достапноста на законските и подзаконските акти од областа на заштитата на личните податоци.

III. Овластување и Изјава за тајност и заштита на обработката на личните податоци

(1) На вработениот, односно ангажираното лице кое има право на пристап до личните податоци, во зависност од видот и обемот на пристапот, му се издава овластување за пристап до личните податоци.

(2) По запознавањето со прописите, а пред отпочнување на реализацијата на работните задачи, вработениот, односно ангажираното лице кое има право на пристап до личните податоци потпишува Изјава за тајност и заштита на обработката на личните податоци.

(3) Изјавата од ставот (2) на овој член своерачно ја потпишува вработениот, односно ангажираното лице.

(4) Вработениот, односно ангажираното лице има право на пристап до личните податоци само во рамките на неговите овластувања.

III. Корисничко име и лозинка

(1) Пристапот до личните податоци е ограничен во рамките на овластувањата и за пристап до информацискиот систем, вработениот, односно ангажираното лице треба да поседува корисничко име и лозинка, со што станува корисник на системот.

(2) Непосредниот раководител го известува администраторот на информацискиот систем за вработување или ангажирање на корисник со право на пристап до информацискиот систем за да му биде доделено корисничко име и лозинка, како и во случај на престанок на вработувањето или ангажманот на корисник, за да му бидат избришани корисничкото име и лозинката со што ќе му биде спречен пристапот до системот.

(3) Известувањето до администраторот на информацискиот систем се врши и при промени на работниот статус на вработениот кои имаат влијание на нивото на дозволен пристап до информацискиот систем.

(4) Вработениот, односно ангажираното лице во соработка со администраторот на информацискиот систем лице креира свое корисничко име и лозинка.

(5) Лозинката од ставот (4) на овој член ја креира лично вработеното лице и таа претставува комбинација од осум алфанумерички карактери – букви (мали и големи) и специјални знаци.

(6) Групни лозинки и кориснички имиња не се дозволени поради неможноста да се лоцира евентуална злоупотреба на личните податоци од страна на корисникот.

IV. Заштита на лозинки

(1) Лозинките се заштитуваат од неовластен пристап и откривање на друго лице и по истекот на три месеци автоматски се менуваат.

(2) Доколку корисникот не го користи системот подолго од 15 минути, се врши автоматско одјавување на корисникот.

(3) Доколку постојат три неуспешни обиди за влегување во системот, корисникот автоматски се отфрла од системот и треба да побара понатамошни инструкции од администраторот на информацискиот систем.

V. Водење евиденција и воспоставување на постапки за идентификација и проверка на авторизираниот пристап

(1) Дирекцијата во својство на контролор води евиденција и воспоставува постапки за идентификација и проверка на пристапот на корисниците кои имаат авторизиран пристап до системот.

(2) Информацискиот систем, односно софтвер треба да овозможи начин на следење на пристапот (logs) за да се знае кој, кога и до кои податоци пристапил.

(3) Постапката на следење на пристапот од ставот (2) на овој член овозможува да се утврди дали личните податоци се користеле со несоодветна причина и кој е одговорен за тоа.

VI. Напуштање на работното место

При напуштање на работното место, корисникот задолжително се одјавува од информацискиот систем.

VII. Заштита на информацискиот систем

(1) Со инсталирање на хардверска/софтверска заштитна мрежна бариера или рутер помеѓу информацискиот систем и интернет, информацискиот систем се заштитува од неовластени и злонамерни обиди за пристап преку надворешни мрежи.

(2) Информацискиот систем се заштитува од непознати закани и од нови вируси и шпионски софтвер (spyware) со ефективна и сигурна антивирусна и антиспајвер заштита.

(3) Дирекцијата во својство на контролор обезбедува ефективна и сигурна антиспам заштита која постојано се ажурира заради превенција од спам-пораки.

VIII. Физичка сигурност на информацискиот систем и работните простории

(1) Софтверските програми за обработка на личните податоци се инсталирани на софтвер кој е хостиран и администриран од страна на администророт на информацискиот систем.

(2) Физички пристап до просторијата во којашто се сместени серверите има само лице со посебно овластување за тоа од страна на директорот на Дирекцијата.

(3) Доколку е потребен пристап на друго лице до просторијата во која се сместени серверите, тогаш тоа лице е придружувано и под надзор на лицето овластено од директорот на Дирекцијата.

(4) Во просторијата во којашто се сместени серверите се применуваат мерки и контроли за заштита од кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

(5) За обезбедување непрекинато напојување на информацискиот систем со електрична енергија, како секундарен систем се инсталира уред за непрекинато напојување (UPS уред).

VIII. Примена и ревизија на процедурата

Член 3

(1) Овој план почнува да се применува од денот на неговото донесување и истиот се објавува на веб-страната на Дирекцијата.

(2) Овој план ќе се ревидира во случај на промена на основот на којшто е донесен и по потреба за изменување и дополнување на системот за заштита на личните податоци што се обработуваат во Дирекцијата.

Директор,

Стојан Славески