Врз основа на член 15 од Законот за катастар на недвижности („Службен весник на Република Македонија“ бр.55/13, 41/14, 115/14, 116/15, 153/15, 192/15, 61/16, 172/16, 64/18 и „Службен весник на Република Северна Македонија“ бр.124/19), член 18 од Статутот на Агенцијата за катастар на недвижности (бр.01-7492/10 од 30.04.2013, бр. 01-548/8 од 30.01.2015 година, „Службен весник на Република Македонија“ бр.173/2018 и „Службен весник на Република Северна Македонија“ бр.161/20), а согласно член 8 од Политиката за создавање на систем за заштита на лични податоци во Агенцијата за катастар на недвижности бр. 0204-12218/1 од 24.08.2021, директорот на Агенцијата за катастар на недвижности донесе

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

Планот за создавање на технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци има за цел да претставува еден вид на водилка која го опишува чекор по чекор процесот кој е неопходен за успешна заштита на личните податоци од технички и организационен аспект.

1. Запознавање со прописите

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.
Непосредниот раководител на организационата единица, генерално ги запознава вработените и ангажирание лица со Законот за заштита на личните податоци, со прописите од областа на заштита на личните податоци донесени од страна на АКН, како и непосредните обврски и одговорности за заштита на личните податоци кои произлегуваат од нив. Деталното запознавање со прописите е обврска на вработениот, односно ангажираното лице.

Непосредниот раководител е должен да го извести вработенот односно ангажираното лице за достапноста на законските и подзаконските акти од областа на заштита на личните податоци.

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

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.
По запознавањето со прописите, а пред отпочнување со реалната работа, вработениот односно ангажираното лице кое има право на пристап до личните податоци потпишува Изјава за тајност и заштита на обработката на личните податоци.
Изјавата ја пополнува и своерачно потпишува вработениот/ангажираното лице.
Вработеното/ангажираното лице има право на пристап до личните податоци само во рамките на неговите овластувања.

3. Корисничко име и лозинка

Пристапот до личните податоци е ограничен во рамките на овластувањата и за пристап до информациониот систем, вработениот односно ангажираното лице треба да поседува корисничко име и лозинка, со што станува корисник на системот. Непосредниот раководител го известува систем администраторот за вработување или ангажирање на корисник со право на пристап до информациониот систем, за да му биде доделено корисничко име и лозинка, како и во случај на престанок на вработувањето или ангажманот, за да му бидат избришани корисничкото име и лозинката со што ќе му биде спречен пристапот до системот. Известување до систем администраторот се врши и при промени на работниот статус на вработениот кои имаат влијание на нивото на дозволен пристап до информациониот систем. Вработеното/ангажираното лице во соработка со систем администраторот креира свое корисничко име и лозинка. Лозинката ја креира лично вработенотоо лице и таа претставува комбинација од осум алфанумерички карактери од кои минимум една голема буква и специјални знаци. Групни лозинки и кориснички имиња не се дозволени,

поради неможноста да се лоцира евентуална злоупотреба на личните податоци од страна на корисникот.

4. Заштита на лозинки

Лозинките треба да бидат заштитени со соодветни методи, а по истекот на три месеци тие треба автоматски да се менуваат. Доколку корисникот не го користи системот подолго од 15 мин, се врши автоматско одјавување на корисникот. Докололку постојат три неуспешни обиди за влегување во системот, корисникот автоматски се отфрла од системот и треба да побара инструкција од систем администраторот.

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

Контролорот води евиденција и воспоставува постапки за идентификација и проверка на авторизираниот пристап за корисниците кои имаат авторизиран пристап до системот. Информациониот систем/софтвер треба да овозможи пристап само на лицата со корисничкои име и лозинка и да овозможи начин на следење за да се знае кој пристапил, кога пристапил и до кои податоци пристапил. Наведената постапка ќе овозможи да се утврди дали личните податоци се користеле со несоодветна причина и кој е одговорен за тоа.

6. Напуштање на работното место

При напуштање на работното место корисникот задолжително се одјавува.

7. Заштита на информациониот систем

Информациониот систем треба да биде заштитен од недозволени и злонамерни обиди за пристап преку надворешни мрежи преку инсталирње на хардверска/софтверска заштитна мрежна бариера или рутер помеѓу информацискиот систем и интернет. Исто така системот треба да биде заштитен од непознати закани и од нови вируси и спајвер со ефективен и сигурен антивирус и антиспајвер.
Контролорот обезбедува ефективна и сигурна антиспам заштита која постојано ќе се ажурира заради превентивна заштита од спамови.

8. Физичка сигурност на информатичкиот систем и работните простории

Софтверските програми за обработка на личните податоци се инсталирани на сервер кој е хостиран и администриран од систем администраторот. Физички пристап до просторијата во која се сместени серверите име само лице кое е овластено од страна на контролорот. Доколку друго лице има потреба од пристап до просторијата во која се сместени серверите тогаш тоа лице задолжително треба да биде придружувано од овластеното лице. Просторијата во која се сместени серверите е заштитена од пожар, експлозии, прашина, вода, кражба, пречки во напојување со електрична енергија, електромагнетно зрачење. Во случај на прекин со напојување на систмот со електрична енергија, системот треба да биде обезбеден со УПС како секундарен механизам.

9.Објава

Овој план влегува во сила од денот на неговото донесување и истиот се објавува на ВЕБ страната на Агенцијата.

ДИРЕКТОР

м-р Борис Гунцев