Врз основа на член 11 од Законот за катастар на недвижности („Службен весник на Република Македонија“ бр. 55/2013, 41/2014, 115/2014, 116/2015, 153/2015, 192/2015, 61/2016 и 172/16) и член 13 од Статутот на Агенцијата за катастар на недвижности („Службен весник на Република Македонија“ бр. 77/13 и 30/15), а во врска со член 10 став (2) алинеја 2 и став (3) од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр. 38/09 и 158/10), Управниот одбор на Агенцијата за катастар на недвижности донесе

П Р А В И Л Н И К

ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ПРАВИЛНИКОТ ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО АГЕНЦИЈАТА ЗА КАТАСТАР НА НЕДВИЖНОСТИ

Член 1

Во Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, заведен под бр.01-17486/1 од 28.12.2011 година, по членот 2 се додаваат два нови члена 2-а и 2-б кои гласат:

„Член 2-а

Контролорот ја евидентира и ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.

Член 2-б

Одредбите од овој правилник се применуваат за:

-целосно и делумно автоматизирана обработка на личните податоци и

-друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на личните податоци.“

Член 2

По членот 6 се додаваат два нови члена 6-а и 6-б, кои гласат:

„Член 6-а

Контролорот треба да обезбеди соодветни технички мерки за тајност и заштита на обработката на личните податоци и тоа:

1. единствено корисничко име;

2. лозинка креирана од секое овластено лице, составена од комбинација од најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;

3. корисничко име и лозинка од точките 1 и 2 од овој член треба да овозможат пристап на овластеното лице до информацискиот систем во целина, на поединечни апикациии/или поединечна збирка на лични податоци потребни за извршување на неговата работа;

4. автоматизирано одјавување од информацискиот систем после изминување на одреден период на неактивност (не подолго од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничко име и лозинката;

5. автоматизирано отфрлање на информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да побара инструкција од администраторот на информацискиот систем;

6. инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол“) или рутер помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;

7. ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;

8. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и

9. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Член 6-б

(1) Контролорот треба да обезбеди соодветни организациски мерки за тајност и заштита на обработката на личните податоци и тоа:

1. ограничен пристап или идентификација за пристап до личните податоци;
2. организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување или снимање на документи преземени од електронска пошта и други извори;
3. уништивање на документи по истекот на рокот за нивно чување;
4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема на која се обработуваат личните податоци;

(2) Секторот за човечки ресурси кај контролорот, го известува Секторот за информатички технологии за вработувањето или ангажирањето на секое овластено 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 биде избришано корисничкото име и лозинката, односно заклучена за понатамошниот пристап.

(3) Известувањето од ставот (2) на овој член се врши и при било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем."

Член 3

По членот 12 се додава нов член 12-а кој гласи:

„Член 12-а

(1) Обврските и одговорностите на администраторот на информацискиот систем, Контролорот ги дефинира и ги утврдува во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

(2) Офицерот за заштита на личните податоци задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

(3) Во извештајот од ставот (2) на овој член треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности."

Член 4

По членот 15 се додаваат два нови члена 15-а и 15-б кои гласат:

„Член 15-а

(1) Лицата кои се вработуваат или се ангажираат кај Контролорот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организиациски мерки.

(2) За лицата кои се ангажираат за извршување на работа кај Контролорот во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Контролорот пред непосредно започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Лицата кои се вработуваат или се ангажираат кај Контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

(5) Во изјавата од ставот (4) на овој член особено треба да биде содржано дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од Контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи лични податоци, како и мерки за нивната заштита.

(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај Контролорот.

(7) Контролорот врши задолжително информирање на овластените лица за непсредните обврски и одговорности за заштита на личните податоци.

Член 15 б

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, Контролорот ги дефинира и утврдува во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.

(2) Контролорот задолжително го информира овластеното лице од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности. “

Член 5

Членот 16 се менува и гласи:

„ (1) Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, се физички лоцирани, хостирани и администрирани од страна на Контролорот.

(2) Физички пристап до просторијата во која се сместени серверите имаат само лица посебно овластени од директорот на Контролорот.

(3) Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице ќе биде придружувано и надгледувано од лицето од ставот (2) на овој член.

(4) Просторијата во која се сместени серверите се заштитува 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.

(5) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверските програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на Контролорот.

(6) Во случајот од ставот (5) на овој член, меѓусебните права и обврски на Контролорот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да се уредат со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.“

Член 6

Во членот 19, став (1), точката се заменува со запирка и се додаваат зборовите “или на хостирана околина надвор од просториите на Контролорот”.

Во ставот (2), точката се заменува со запирка и се додаваат зборовите “или на хостирана околина надвор од просториите на Контролорот”.

Член 7

По членот 19 се додаваат два нови члена 19-а и 19-б кои гласат:

„Член 19-а

(1) Контролорот задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

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

(3) Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци на начин утврден со овој Правилник.

Член 19-б

(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.

(2) Контролорот 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.

(3) Во евиденцијата на овластените лица утврдена во член 19-а став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

(4) Администраторот на информацискиот систем кој е овластен согласно Правилникот 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 комуникациската опрема само во согласност со критериумите кои се утврдени од страна на Контролорот."

Член 8

По членот 27 се додаваат два нови члена 27-а и 27-б кои гласат:

„Член 27-а

(1) Со медиумите од член 27 на овој правилник треба да се овозможи идентификација и евидентирање на категориите на лични податоци и истите треба да се чуваат на локација до која пристап имаат само овластени лица утврдени во овој Правилник.

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

(3) Контролорот воспоставува систем за евидентирање на медиумите кои се примаат со цел да овозможи 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.

(4) Одредбите од ставот (3) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на Контролорот .

(5) За пренесените медиуми надвор од работните простории на Контролорот, се преземаат неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив. Медиумите можат да се пренесуваат надвор од работните простории само со претходно писмено овластување од страна на директорот на Контролорот и 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.

Член 27-б

(1) По пренесувањето 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.

(2) Уништувањето на медиумот се врши со механичко разделување на неговите составни делови, при што истиот повторно да не може да биде употреблив.

(3) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

(4) За случаите од ставовите (2) и (3) на овој член комисиски се составува записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.“

Член 9

По членот 30 се додава седум нови члена 30-а, 30-б, 30-в, 30-г, 30-д, 30-ѓ и 30-е кои гласат:

„Член 30-а

(1) Пристапот до документите е ограничен само за овластените лица на Контролорот.

(2) За пристапувањето до документите задолжително се воспоставуватат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

(3) Доколку е потребен пристап на друго лице до документите тогаш се воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Член 30-б

Контролорот 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 30-в

Чувањето на документите се врши на начин на кој ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Член 30-г

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

(2) Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документите како и за категориите на личните податоци содржани во истите.

Член 30-д

Плакарите (орманите), картотеките или другата опрема за чување на документи се сместени во простории заклучени со соодветни заштитни механизми. Просториите се заклучени и за периодот кога документите не се обработуваат од овластените лица.

Член 30-ѓ

(1) Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на Контролорот.

(2) Уништувањето на копиите или умножените документи се врши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Член 30-е

Во случај на физички пренос на документите, Контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат.“

Член 10

Членот 31 се брише.

Член 11

Овој правилник влегува во сила со денот на неговото донесување и објавување на огласна табла и на веб-страницата на Агенцијата за катастар на недвижности.

Управен одбор

Претседател,

[illegible]та Јорданова, с.р