Број 08-401/1
08.06.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 1 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

П Л А Н
ЗА СОЗДАВАЊЕ СИСТЕМ НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. Цел на планот

Со овој План се предвидува создавање на соодветен систем за технички и организациски мерки што Општина Демир Капија во својство на контролор ги применува за обезбедување тајност и заштита на обработката на личните податоци.

II. Нивоа на технички и организациски мерки

На сите документи во Општина Демир Капија задолжително се применуваат технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци класифицирани во две нивоа:

- основно ниво и
- средно ниво

III. Документација за технички и организациски мерки

Системот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во Општина Демир Капија се состои од следните механизми:

1. Донесување на Правилник за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;
2. Донесување на Правила за определување на обврските и одговорностите на овластените лица при користење на документите и информатичко комуникациската опрема;
3. Донесување на Правила за пријавување, реакција и санирање на инциденти;
4. Донесување на Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
5. Донесување на Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите;

Вработените и ангажираните лица во Општина Демир Капија се должни секој во рамките на своите работни задачи да ги почитуваат и применуваат овие интерни акти.

Општина Демир Капија овластува едно или повеќе лица за заштита на личните податоци во Општина Демир Капија коешто ќе се грижи за правилната примена на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Општина Демир Капија со посебен акт определува офицер за заштита на личните податоци којшто е овластен од контролорот за самостојно вршење на работите во смисла на член 26 - а од Законот за заштита на личните податоци.

Офицерот за заштита на личните податоци во Општина Демир Капија врши редовна проценка на потребата за изготвување и донесување на нови интерни акти или промена на старите од аспект на нивно усогласување со прописите за заштита на личните податоци.

IV. Периодични контроли

Офицерот за заштита на личните податоци во Општина Демир Капија најмалку еднаш месечно ги вршат следните контроли и за тоа изготвува извештај:

- Контрола на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци,

- Контрола на евиденција за секој авторизиран/неавторизиран пристап до информацискиот систем,
- Контрола на доверливоста и сигурноста на лозинките и на останатите форми на идентификација,
- Контрола на начинот за пристап на вработените и ангажираните лица во Општина Демир Капија до интернет кои се однесуваат на симнување и снимање на документи преземени од електронска пошта и други извори,
- Контрола на уништување на документи кои содржат лични податоци по истекување на рокот за чување, како и за начинот на уништување, бришење и чистење на медиумите,
- Контрола на начинот на управување со медиуми кои се носители на лични податоци,
- Контрола на писмените овластувања и работни задачи издадени од страна на градоначалникот на Општина за вршење на обработка на личните податоци и за пренесување на медиуми надвор од работните простории на Општина Демир Капија
- Контрола на начинот на воспоставување физичка сигурност на работните простории и опремата каде што се обработуваат и чуваат личните податоци,
- Контрола на начинот на пристап до целиот информациски систем преку персоналните компјутери,
- Контрола на начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци,
- Контрола на евиденцијата за физички пристап до просторијата во која се сместени серверите,
- Контрола на постапката за потпишување на изјави за тајност и заштита на обработката на личните податоци од страна на вработените и ангажираните лица во Општина Демир Капија

V. Категории на лични податоци кои се обработуваат

Контролорот Општина Демир Капија при своето тековно работење ги обработува следниве категории на лични податоци:

- Име и презиме
- Дата и место на раѓање
- ЕМБГ
- Број на лична карта
- Адреса
- Контакт информации - електронски (пр. број на телефон или факс)
- Број на сметка во банка
- Број на здравствена легитимација.

Од посебните категории на податоци (чувствителни податоци), контролорот согласно Законот за заштита на лични податоци ги обработува податоците коишто се однесуваат на припадност на заедниците.

VI. Завршна одредба

Овој План влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/1
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 2 од Правилникот за техничките и организациските мерки за обезбедување

тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

П Р А В И Л Н И К ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој Правилник се пропишуваат техничките и организациските мерки што Општина Демир Капија во својство на контролор ги применува за обезбедување тајност и заштита на обработката на личните податоци.

Член 2

Техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци кај контролорот се класифицираат во две нивоа:

- основно ниво и
- средно ниво.

Член 3

За обезбедување тајност и заштита на обработката на личните податоци, со правното лице кое го одржува информацискиот систем, Општината задолжително склучува писмен договор за регулирање на неговите обврски и одговорности во однос на примената на прописите за заштита на личните податоци и на донесената документација за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци од контролорот.

II. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 4

Контролорот овластува едно или повеќе лица за заштита на личните податоци (офицер за заштита на личните податоци) кои ќе бидат одговорни за координација и контрола на постапките утврдени во донесената документација за техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци (во натамошниот текст: одговорно лице за заштита на личните податоци).

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

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.

Член 5

Овластеното лице кое ги врши работите за човечки ресурси кај контролорот ќе го известува администраторот на информацискиот систем за вработувањето или ангажирањето по друг основ на секое овластено лице со право на пристап до информацискиот систем, заради доделување корисничко име и лозинка, како и во случај на престанок на вработувањето, заради бришење на корисничкото име и лозинката, односно исклучување за натамошен пристап.

Соодветно известување ќе се врши и при било кои други промени во работниот или статусот на ангажирањето на овластеното лице, доколку таквите промени имаат влијание врз нивото или обемот на дозволениот пристап до збирките на лични податоци преку информацискиот систем.

Член 6

Овластените лица пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

За лицата кои склучуваат договор за вработување, задолжително нивниот договор содржи одредби за обврските и одговорностите за заштита на личните податоци.

Контролорот пред непосредното започнување со работа на корисниците, дополнително ги информира за нивните обврски и одговорности за заштита на личните податоци.

Контролорот задолжително врши континуирано информирање на овластените лица за непосредните обврски и

одговорности за заштита на личните податоци.

Овластените лица пред нивното отпочнување со работа своерачно потпишуваат Изјава за тајност и заштита на обработката на личните податоци која 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 упатствата добиени од контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита. Изјавата задолжително се чува во досиејата на овластените лица.

Составен дел на овој правилник е образецот на Изјавата за тајност и заштита на обработката на личните податоци.

Член 7

Контролорот врши целосна и делумна автоматизирана или пак друга рачна обработка на личните податоци со примена на технички мерки за обезбедување тајност и заштита и тоа:

1. единствено корисничко име;
2. лозинка креирана од секое овластено лице, која е составена од комбинација на најмалку осум алфанумерички карактери (најмалку една голема буква) и специјални знаци;
3. корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, како и до поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговите работни задачи;
4. автоматизирана промена на лозинката по изминат утврден временски период што не може да биде подолг од 60 дена, при што се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни;
5. автоматизирано одјавување од информацискиот систем по изминување на определен период на неактивност (не подолго од 15 минути), по што за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
6. автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на корисникот дека треба да се побара инструкција од администраторот на информацискиот систем;
7. инсталирана хардверска и софтверска заштитна мрежна бариера 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;
8. инсталирана ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
9. инсталирана ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
10. приклучување на информацискиот систем (компјутери и сервери) на енергетска мрежа преку уред за непрекинато напојување.

Член 8

Контролорот обезбедува организациски мерки за тајност и заштита на обработката на личните податоци, во однос на информирањето на овластените лица, физичката заштита на работните простории и опремата и заштита на информацискиот систем како целина, вклучувајќи го и собирањето, обработувањето и чувањето на податоците.

За спроведување на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и за следење на прописите за заштита на личните податоци од страна на градоначалникот на Општина Демир Капија се определува администратор на информацискиот систем.

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

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. Во евиденцијата на корисниците на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

Администраторот на информацискиот систем кој е овластен со Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци 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.

Обврските и одговорностите на администраторот на информацискиот систем контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите на информатичко комуникациската опрема.

Контролорот задолжително врши периодична контрола, на секои три месеци над работата на администраторот на информацискиот систем и изготвува извештај за извршената контрола во којшто се содржани констатираните неправилности и предложените мерки за отстранување на истите.

Член 9

Контролорот при автоматизираната обработка на личните податоци ги применува следните организациски мерки за тајност и заштита на обработката на личните податоци:

1. ограничен пристап, односно идентификација за пристап до личните податоци, преку целосна доверливост и сигурност на лозинките и на останатите форми на идентификација;
2. воспоставување и примена на организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;
3. бришење или уништување на документи по истекување на рокот на нивно чување согласно прописите за архивска граѓа;
4. издавање на писмено овластување при секое изнесување на било кој медиум кој е носител на лични податоци (преносен компјутер, мемори стик, ОР-диск, флопи дискета, преносен тврд диск и слично) надвор од работните простории со цел да не дојде до нивно губење или незаконско користење;
5. воспоставување и примена на мерки за физичка сигурност на работните простории и инфоматичко - комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци;
6. почитување на техничките упатства при инсталирање и користење на информатичко - комуникациската опрема на која се обработуваат лични податоци.

Член 10

Контролорот воспоставува и применува мерки за физичка сигурност на информацискиот систем преку физичко обезбедување на работните простории и информатичко - комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци.

Одредбите од овој правилник целосно се применуваат и при друга рачна обработка на личните податоци што се дел од постојана збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Заради обезбедување на физичка сигурност, серверите на кои се инсталирани софтверските програми за обработка на личните податоци се физички лоцирани, хостирани и администрирани од страна на контролорот.

Физички пристап до просторијата во која се сместени серверите (информациониот систем) може да имаат само лица кои имаат добиено посебно писмено овластување од страна на контролорот во кое се образложени причините за нивниот пристап до просторијата.

Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите (информациониот систем), тогаш тоа лице задолжително ќе биде придружувано и надгледувано од овластено лице од став 3 на овој член.

По исклучок серверите на кои се инсталирани софтверски програми за

обработка на лични податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот. Во овој случај меѓусебните права и обврски на контролорот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, ќе 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.

Просторијата во која се сместени серверите (информациониот систем), контролорот ја 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 електромагнетско зрачење.

Контролорот треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секој корисник кој пристапил до информацискиот систем и можноста за проверка на авторизацијата на секој корисник.

Контролорот води евиденција за секој авторизиран пристап која треба да го содржи особено следниве 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 на авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Во погоренаведената 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 од треба да бидат контролирани од страна на офицерот за заштита на личните податоци и истите не може да се деактивираат. Евиденцијата се чува најмалку пет години. офицерот за заштита за заштита на личните податоци врши периодична проверка на податоците, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Член 11

Контролорот задолжително 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.

Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето лице. Информацискиот систем и информатичката инфраструктура на контролорот задолжително подложи на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци. Контролорот врши надворешна контрола на информацискиот систем и на информатичката инфраструктура на секои три години, а внатрешна контрола на секоја година. Надворешната контрола се врши преку обработка на документи од страна на независно трето лице.

Во извештајот од извршената контрола задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни мерки за отстранување на констатираните недостатоци. Извештајот се анализира од страна на одговорното лице за заштита на личните податоци кој доставува предлози на контролорот за преземање на потребните корективни или

дополнителни мерки. Извештајот треба да биде достапен за увид на Дирекцијата за заштита на личните податоци.

Член 12

Со медиумите треба да се овозможи идентификација и евидентирање на категориите на лични податоци и истите треба да се чуваат на локација до која имаат пристап само овластени лица.

Заради евидентирање на медиумите кои се примаат за да се овозможи директна или индиректна идентификација на видот на медиумот кој е примен, информацискиот систем што се применува кај контролорот содржи систем во кој се евидентирани следните податоци за секој медиум кој е примен:

- Датум и време на примање;
- Испраќач;
- Број на примени медиуми;
- Вид на документот кој е снимен на медиумот;
- Начин на испраќање на медиумот и
- Име и презиме на лицето овластено за прием на медиумот.

Системот од став 1 на овој член се применува и за евидентирање на медиумите кои се испраќаат од страна на контролорот. Медиумите пред изнесување односно пред испраќање од страна на контролорот се предмет на посебни информатички мерки - скремблирање/криптирање, со што се обезбедува заштита од неовластено обработување на личните податоци што се снимени на ваквите медиуми.

Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на контролорот.

Член 13

Пристап до документите е ограничен само за овластени лица од страна на контролорот и за која цел ќе се воспостават механизми за идентификација на овластените лица и за категориите на лични податоци до кои се пристапува.

Освен овластеното лице пристап на друго лице до документите е дозволен само со посебно овластување дадено од страна на контролорот.

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.

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отварање. Во случај кога поради физичките карактеристики на документите тоа не е можно контролорот ќе примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Плакарите картотеките и другата опрема за чување документи задолжително треба да бидат сместени во простории заклучени со соодветни механизми и истите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

Доколку поради физичките карактеристики на просториите не е можна примената на овие мерки контролорот ќе примени други мерки за да се спречи секој неовластен пристап до документите.

III. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 14

Овој Правилник влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/2
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Образец 1

И З Ј А В А
за тајност и заштита на личните податоци

Јас долупотпишаниот / та,
....., со живеалиште во ..... на ул. ..... бр. ....., со ЕМБГ ..... и л.к. рег. бр. ..... издадена од ....., во својство на вработено/ангажирано лице во општина Демир Капија,

ИЗЈАВУВАМ дека:

- ќе ги почитувам начелата за заштита на личните податоци;

- ќе вршам обработка на личните податоци согласно упатствата добиени од општина Демир Капија во својство на контролор, освен ако со закон поинаку не е уредено;

- ќе ги чувам како доверливи личните податоци кои ќе ги обработувам;

- ќе ја применувам донесената документација за технички и организациски мерки од контролорот, и

- ќе ги чувам како доверливи мерките за заштита на личните податоци.

Изјавува,

_____
.....

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 3 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

П Р А В И Л Н И К ЗА ОПРЕДЕЛУВАЊЕ НА ОБВРСКИТЕ И ОДГОВОРНОСТИТЕ НА ОВЛАСТЕНИТЕ ЛИЦА ПРИ КОРИСТЕЊЕ НА ДОКУМЕНТИТЕ И ИНФОРМАТИЧКО КОМУНИКАЦИСКАТА ОПРЕМА

Член 1

Со овој правилник се пропишуваат обврските и одговорностите на овластените лица при користење на документите и информатичко коминикацискатa опрема што Општина Демир Капија во својство на контролор ги применува за обезбедување тајност и заштита на обработката на личните податоци.

Секое овластено лице кое има пристап до личните податоци и до информатичко комуникацискатa опрема кај контролорот, ги има следните обврски и одговорности:

- Да ги применува сите правила и процедури воспоставени со донесените интерни акти од страна на контролорот за обезбедување тајност и заштита на обработката на личните податоци;
- Да ги применува сите мерки за физичка сигурност на просториите каде се наоѓа информацискиот систем на контролорот;
- Веднаш да ги пријави кај администраторот на информацискиот систем секакво сознание, било директно или индиректно, до кое ќе дојде, а може да укажува дека постои ризик од нарушување на системот за тајност и заштита на обработката на личните податоци кај контролорот, било да се работи за надворешен или за внатрешен ризик;
- Не смее да ги прекршува преземените обврски за доверливост, со кои се обврзува дека секој податок до кој ќе дојде во текот на работењето кај контролорот, а кој спаѓа во категоријата на личен податок согласно Законот за заштита на личните податоци, ќе го чува како доверлив и нема да го пренесува, оддава, ниту на друг начин ќе го стави на располагање на било кое друго лице и во било која форма, надвор од системот на пропишани и воспоставени технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;
- Не смее да превзема содржини од непознати, неавторизирани, непроверени,сомнителни или забранети интернет страници;
- Да ја чува доверливоста на својата лозинка;
- Не смее да врши неавторизирано пренесување и/или користење на интерни документи и делови од нив или друга комуникација надвор од Општина Демир Капија.

Член 3

Секое овластено лице е одговорно за соодветна примена на интерните акти кај контролорот со кои се уредува заштитата на личните податоци, како и е одговорен

доколку, како последица на прекршување или непочитување на некои од воспоставените мерки, биде загрозена тајноста на личните податоци што се обработуваат кај Контролорот или пак доколку дојде до нивна злоупотреба.

Под загрозување на тајноста на личните податоци се подразбира случајно или намерно постапување, непостапување или пропуштање од страна на овластените лица, како резултат на што се создаваат услови или можност да дојде до злоупотреба на личните податоци што се обработуваат кај Контролорот.

Член 4

Во случај на било какво прекршување или непочитување на било кој пропис или интерен акт од страна на овластеното лице, контролорот задолжително спроведува постапка за испитување на причините, начинот и последиците од таквото прекршување, односно непочитување, заради спречување на настанување на слично прекршување или непочитување во иднина.

Во случаите од став 1 на овој член, конторолорот спроведува и постапка за утврдување на одговорноста на овластеното лице согласно закон.

Член 5

Администраторот на информацискиот систем ги има следниве обврски и одговорности:

- учествува во подготовка на стратегија на техничка платформа на информациски систем на Општината;
- учествува во изготвување на план и стандарди за подобрување, развој и надоградување на информациско-комуникациска инфраструктура (хардвер, софтвер, мрежна, комуникациска опрема и информатички проекти);
- учествува во планирање и координација на активностите во врска со оптимално функционирање и користење на расположливите технички и програмски ресурси;
- организира, подготвува услови и ја врши инсталацијата на ИТ опремата и нејзино вградување во ИТ платформата;
- врши системско администрирање на информатичка и комуникациска инфраструктура;
- врши обезбедување и управување со системот за безбедност и заштита на податоци, документи и информации на ИС на Општината од неовластен пристап и користење, како и пристап и организација на системска сала;
- разработува методи и спроведува процедури за заштита и сигурност на информацискиот систем, заштита на податоци, електронско архивирање на податоци и документи;
- систематски ги следи и ги проучува новите технологии и софтвер од областа на информатиката (во хардвер и софтвер) и ги оценува можностите за нивна примена во ИС;
- активно учествува во работата на проектни тимови и учествува во изготвување на стручно- аналитичките материјали од областа на информациските системи.

Член 6

Овој Правилник влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/3
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 4 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

ПРАВИЛНИК ЗА ПРИЈАВУВАЊЕ , РЕАКЦИЈА И САНИРАЊЕ НА ИНЦИДЕНТИ

Член 1

Со овој правилник се пропишува начинот на пријавување, реакција и

санирање на инциденти кои влијаат или можат да влијаат на тајноста и заштитата на личните податоци кои се обработуваат во Општина Демир Капија во својство на контролор.

Член 2

Секое овластено лице е должно веднаш да го пријави на администраторот на информацискиот систем секој инцидент што ќе настане во процесот на обработување на личните податоци.

Пријавувањето на инцидентот од став 1 на овој член се врши во електронска форма, а доколку тоа не е возможно, пријавувањето се врши во писмена форма, при што се наведуваат следните податоци за инцидентот:

- Време на настанување на инцидентот;
- Траење и престанок на инцидентот;
- Место во информацискиот систем каде се појавил инцидентот;
- Податок или проценка за обемот, односно опсегот на инцидентот;
- Име и презиме на овластеното лице кое го пријавило инцидентот;
- Име и презиме на овластените лица до кои е доставена пријавата за инцидентот.

Член 3

По приемот на пријавата за инцидент, администраторот на информацискиот систем веднаш започнува да врши проценка на причините за појавување на инцидентот, како и за тоа дали и кои мерки треба да се преземат за негово санирање и за спречување на негово повторување во иднина.

Доколку се работи за инцидент кој се повторува, администраторот на информацискиот систем е должен да преземе мерки кои ќе гарантираат трајно отстранување на ризикот од негово повторување.

Член 4

Доколку како последица на инцидент дојде до губење или бришење на дел или сите лични податоци содржани во информацискиот систем, истите ќе бидат повторно внесени - вратени во информацискиот систем, со користење на сигурносните копии кои што се чуваат кај контролорот.

Постапката од став 1 на овој член ќе се примени и доколку бришењето или губењето на дел или сите лични податоци содржани во информацискиот систем е неопходно заради отстранување на последиците од инцидентот или за преземање на мерки за спречување на негово повторување во иднина.

Член 5

При повторното внесување - враќање на личните податоци во системот, задолжително и во електронска форма се врши евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на податоците, категориите на лични податоци кои биле вратени и кои биле рачно внесени при враќањето.

Повторното враќање на личните податоци во информацискиот систем се врши од страна лицата врз основа на претходно издадено писмено овластување од страна на градоначалникот на Општина Демир Капија.

Член 6

Овој Правилник влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/4
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 5 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

ПРАВИЛНИК ЗА НАЧИНОТ НА ПРАВЕЊЕ НА СИГУРНОСНА КОПИЈА, АРХИВИРАЊЕ И ЧУВАЊЕ, КАКО И ЗА ПОВТОРНО ВРАЌАЊЕ НА ЗАЧУВАНИТЕ ЛИЧНИ ПОДАТОЦИ

Член 1

Со овој Правилник се пропишува начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци кои се обработуваат во Општина Демир Капија во својство на контролор.

Член 2

Контролорот задолжително врши редовно снимање на сигурносна копија и архивирање на податоците во информацискиот систем за да се спречи нивно губење или уништување.

За правење на сигурносна копија од став 1 на овој член, контролорот располага со сервер за поддршка во кој секој работен ден се меморираат внесените податоци така што, во случај на пад на информацискиот систем, или негово оштетување од каква било причина, сите податоци остануваат сочувани во серверот за поддршка.

Член 3

Заради заштита од неовластен пристап, серверот за поддршка кој претставува сигурносна копија на сите снимени податоци е сместен во безбедна просторија заштитена со сигурносна брава до која имаат пристап само овластени лица од контролорот.

Член 4

Контролорот задолжително прави сигуроносни копии секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

Контролорот задолжително ја проверува функционалноста на сигуроносните копии за вршење реконструкција на личните податоци.

Задолжително прави дополнителна сигурносна копија на податоците од серверот за поддршка на медиум, на крајот од работната недела и секој последен работен ден во месецот.

Направената сигурносна копија од став 1 на овој член, подлежи на физичка и криптографска заштита, со што се оневозможува каква било модификација на содржината на истата.

По извршеното копирање на личните податоци содржани во електронските документи, сигурносната копија се носи на друга оддалечена безбедна локација која се наоѓа надвор од просторијата во која се чуваат серверите или персоналните компјутери во кои се сместени збирките на личните податоци за кои се прави сигуроносна копија.

Сигуроносните копии коишто се чуваат на друга одалечена локација од местото каде е сместен информацискиот систем ќе бидат заштитени со соодветни технички и организациски мерки.

Меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде се чуваат сигуроносните копии ќе се уредат со писмен договор во којшто задолжително ќе бидат содржани техничките и организациските мерки за обезбедување тајност и заштита на личните податоци.

Пристап до оддалечената безбедна локација каде се чува медиумот имаат само овластени лица од контролорот, при што медиумот се чува затворен во сеф со безбедносна брава и кој е обезбеден од физички влијанија (кражба, пожар, поплава и други влијанија).

Обезбедувањето на безбедната локација од став 3 на овој член го врши Градоначалникот на Општина Демир Капија.

Член 5

При повторно враќање на зачуваните лични податоци, се врши евидентирање на корисникот кој е овластен за извршување на операциите за повторно враќање на податоците, датумот на враќањето на податоците, категориите на податоците кои се вратени и кои биле рачно внесени при враќањето.

Член 6

Овој Правилник влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/5
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.

Градоначалникот на Општина Демир Капија врз основа на член 50 став 1 точка 16 од Законот за локалната самоуправа ("Службен весник на РМ" бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци ("Службен весник на РМ" бр. 7/05, 103/08 и 124/10), а во врска со член 10, став 2, алинеја 6 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на РМ" бр. 38/09, 158/2010), донесе

ПРАВИЛНИК
ЗА НАЧИНОТ НА УНИШТУВАЊЕ НА ДОКУМЕНТИТЕ, КАКО И ЗА НАЧИНОТ НА УНИШТУВАЊЕ, БРИШЕЊЕ И ЧИСТЕЊЕ НА МЕДИУМИТЕ

Член 1

Со овој Правилник се пропишува начинот на уништување, бришење и чистење на документите и на медиумите што се користат за обработување на личните податоци од страна на Општина Демир Капија во својство на контролор.

Член 2

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

За уништувањето на документите во хартиена форма кои содржат лични податоци се формира Комисија која составува записник кој ги содржи сите податоци за целосна идентификација на документацијата, како и за категориите на лични податоци содржани во истата.

Член 3

По пренесувањето на личните податоци од медиумот или по истекот на определниот рок за чување, медиумот се уништува, се брише или пак се чисти од личните податоци кои се снимени на него.

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

Бришењето или чистењето на медиумот се врши на начин што оневозможува понатамошно обновување на снимените лични податоци.

За случаите од ставовите 1 и 3 на овој член се составува записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Член 4

Овој Правилник влегува во сила со денот на донесувањето, а ќе се објави во "Службен гласник на Општина Демир Капија".

Број 08-492/6
26.07.2012 година
Демир Капија

Градоначалник на
Општина Демир Капија,
Трајче Димитриев с.р.