Врз основа на член 50 од Законот за локалната самоуправа („Службен весник на Република Македонија“ бр. 5/02) и член 23, став 4 од Законот за заштита на личните податоци („Службен весник на Република Македонија“ 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 Република Македонија“ бр. 38/09, 158/2010), Градоначалникот на општината Пробиштип донесе

ПРАВИЛНИК 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 Пробиштип 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 Пробиштип 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 доверливости 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 органзациски 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:

- единствено корисничко име;
- лозинка креирана од секое овластено лице, која е составена од комбинација на најмалку осум алфанумерички карактери (најмалку една голема буква) и специјални знаци;

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;

- 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;
- 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;
- 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;
- инсталирана хардверска и софтверска заштитна мрежна бариера (“firewall”) 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;
- 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;
- инсталирана ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и

-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 Пробиштип 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:

-целосна доверливост и сигурност на лозинките и на останатите форми на и-ограничен пристап, односно идентификација за пристап до личните податоци, преку дентификација;

-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;
-бришење или уништување на документи по истекување на рокот на нивно чување согласно прописите за архивска граѓа;
-издавање на писмено овластување при секое изнесување на било кој медиум кој е носител на лични податоци (преносен компјутер, мемори стик, CD-диск, флопи дискета, преносен тврд диск и слично) надвор од работните простории, со цел да не дојде до нивно губење или незаконско користење;
-воспоставување и примена на мерки за физичка сигурност на работните простории и инфоматичко – комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци;
-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 воспстави 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 задолжителон треба да има мислење за тоа во колкава мера постапките и упатствата содржани во 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 се 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 секојнеовластен 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 Пробиштип“.

Општина Пробиштип
Градоначалник
Тони Тоневски

Прилог: 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._____ , во својство на вработено лице во Општина Штип, отстапено преку АПВ или времено ангажирано лице-волонтер

ИЗЈАВУВАМ дека:

- ќе ги почитувам начелата за заштита на личните податоци;
- ќе вршам обработка на личните податоци согласно упатствата добиени од Општина Штип 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.

_____ година

Изјавил

_____