ОПШТИНА ВЕЛЕС
MUNICIPALITY OF VELES

Врз основа на чл.50 став 1 точка 15 од Законот за локалната самоуправа („Службен весник на Република Македонија" бр. 5/02) и член 32 став (3) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 42/20 и 294/21), а во врска со одредбите од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Северна Македонија" бр. 122/20), Градоначалникот на Општина Велес на ден 24.07.2023 година, донесе:

ПРАВИЛНИК
ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

1. ОПШТИ ОДРЕДБИ

Член 1

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

Член 2

Изразите употребени во овој Правилник го имаат следното значење:

1. Авторизиран пристап е овластување доделено на корисникот за обработка на лични податоци, користење н одредена информатичко комуникациска опрема или пристап до одредени работни простории на контролорот.
2. Идентификација е постапка за идентификување на корисникот на информацискиот систем.
3. Контрола на пристап е операција за доделување пристап до личните ПОДАТОЦИ или до информатичко комуникациската опрема со цел проверка на корисникот.
4. Лозинка е доверлива информација составена од збир на карактери кои се користат за проверка на корисникот.
5. Корисник е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и , информатичко комуникациската опрема.
6. Проверка е постапка за верификација на идентитетот на корисникот на информацискиот систем.
7. Информациски систем е систем со кој се обработуваат личните податоци со цел да бидат достапни и употребли за секој што има право и потреба да ги користи.
8. Информатичка инфраструктура е целата информатичко комуникациска опрема во чии рамки се собираа обработуваат и чуваат личните податоци.
9. Администратор на информацискиот систем е лице овластено за планирање и применување на техничките организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на лични податоци.
10. Одговорно лице за заштита на личните податоци е лице овластено од контролорот за координирање и контро на техничките и организациските мерки кои се применуваат за тајност и заштита на обработката на лични податоци.
11. Документ е секој запис во хартиена или електронска форма кој може: да содржи лични податоци, да се чува медиум во рамки информатичко комуникациската спрема која се користи за обработка на податоците, да доставува преку пошта или да се пренесува преку телекомуникациската мрежа.
12. Инцидент е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци.
13. Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на податоците можат да бидат снимени или од кој истите молчат да бидат повторно вратени.
14. Сигурносна копија е копија на личните податоци содржани во електронските документи, кои се зачувани медиум на начин кој овозможува нивно повторно враќање.

Член 3

Соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка, техничките и организациските мерки се класифицирани на основно, средно и високо ниво.

Член 4

За обезбедување тајност и заштита на обработката на личните податоци, со правните лица кои вршат одржување и надградби на соодветните апликативни решенија во Општина Велес, задолжително се склучува писмен договор за регулирање на нивните 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.

2. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 5

Контролорот овластува лице за заштита на личните податоци кое ќе биде одговорно за координација и контрола на постапките и упатствата утврдени во донесената документација за техничките и организациските мерки за обезбедување безбедност на обработка на личните податоци (во натамошниот текст: одговорно лице за заштита на личните податоци).

Член 6

Корисникот кој ги врши работите за човечки ресурси кај контролорот ќе го известува администраторот на информацискиот систем за вработувањето или ангажирањето по друг основ на секој корисник 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 однос или статусот на ангажирањето на корисникот, доколку таквите промени имаат влијание врз нивото или обемот на дозволениот пристап до збирките на лични податоци преку инфомацискиот систем.

Член 7

За корисниците 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.

Корисниците 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 корисниците.

Изјавата од став 4 на овој член претставува составен дел на овој правилник (Образец 1).

Член 8

Контролорот врши автоматизирана обработка на личните податоци со примена на технички мерки за обезбедување тајност и заштита и тоа: единствено корисничко име; лозинка креирана од секој корисник, 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 корисникот 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 и во 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 од приклучување на информацискиот систем (компјутери и сервери) на енергетска мрежа преку уред за непрекинато напојување.

Член 9

Контролорот обезбедува организациски мерки за тајност и заштита на обработката на личните податоци, во однос на информирањето на корисниците, физичката заштита на работните простории и опремата за 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 Велес се определува администратор на информацискиот систем.

Член 10

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

- ограничен пристап, односно идентификација за пристап до личните податоци, преку целосна доверливост и сигурност на лозинките и на останатите форми на идентификација;
- воспоставување и примена на организациски правила за пристап на корисниците 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 граба;
- издавање на писмено овластуванње при секое изнесување на било кој медиум кој е носител на лични податоци 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 личните податоци.

Член 11

Контролорот воспоставува и применува мерки за физичка сигурност на информацискиот систем преку физичко обезбедување на работните простории и инфоматичко - комуникациската опрема каде што се собираат, обработуваат и чуваат личните 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 може да имаат само корисници кои имаат добиено 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, тогаш тоа лице задолжително ќе биде придружувано и надгледувано од овластено лице од став 3 на овој член.

Просторијата во која се сместени серверите, 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.

Член 12

Контролорот води евиденција за корисниците кои имаат авторизиран пристап до информацискиот систем која содржи: Име и презиме на корисникот; Работната станица и корисничкото име за сите корисници кога пристапуваат до информацискиот систем, заедно со нивото на авторизиран пристап за секој корисник, датумот и времето на пристапување, како и лични податоци кон кои е пристапено; Видот на пристапот со операциите кои се преземени при обработка на податоците; Запис за авторизација за секое пристапување; Запис за секој неавторизиран пристап; Запис за автоматизирано отфрлање од информацискиот систем и Идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Евиденцијата од став 1 на овој член се чува најмалку десет години.

Одговорно лице за заштита на личните податоци врши периодична проверка на податоците од став 1 на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Врз основа на механизмите наведени во став 1 на овој член, контролорот е во можност да врши идентификација и проверка на авторизираниот пристап, односно контрола на пристапот до личните податоци и информатичко комуникациската опрема од страна на корисниците, со обезбеден постојан увид во моменталниот и минатиот пристап и преземени операции во информацискиот систем од страна на сите корисници.

Врз основа на механизмите наведени во став 1 на овој член се овозможува секој од корисниците да има авторизиран пристап само до личните податоци и информатичко - комуникациската опрема кои се неопходни за извршување на нивните задачи, како и се оневозможува пристап на корисниците до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се овластени корисниците.

При вршење на проверката врз основа на корисничко име и лозинка, контролорот секогаш ги применува воспоставените правила за заштита на нивната доверливост и интегритет при пријавување, доделување и чување на истите.

Администраторот на информацискиот систем е овластен да го доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко - комуникациската опрема само врз основа на работното место на секој од корисниците од што зависи и нивото на пристап на секој од корисниците до личните податоци што е задолжен да ги обработува.

Член 13

Заради евидентирање на медиумиге 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.

Член 14

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 донесената документација за технички и организациски мерки и прописите за заштита на личните податоци. Тестирањето се врши преку обработката на документи кои содржат имагинарни лични податоци од страна на независно трето лице.

Член 15

Информацискиот систем и информатичката структура на контролорот задожително подлежат на внатрешна и надворешна контрола, со цел да се провери дали постапките и упатствата содржани во донесената документација 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 информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

Надворешната контрола се врши преку обработка на документи од страна на независно трето лице.

Во извештајот од извршената контрола од став 1 на овој член задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во донесената документација 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 корективни или дополнителни мерки за нивно отстранување.

Во извештајот од став 4 на овој член треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

Извештајот од став 4 на овој член се анализира од страна на одговорното лице за заштита на личните податоци, кој доставува предлози до градоначалникот на Општина Велес за преземање на потребните корективни или дополнителни мерки за отстранување на констатираните недостатоци.

Извештајот од став 4 на овој член треба да биде достапен за увид на Агенцијата за заштита на личните податоци на Република Северна Македонија.

3. ЗАВРШНИ ОДРЕДБИ

Овој Правилник влегува во сила со денот на неговото потпишување.

Бр.08-1104/6
24.07.2023 година
Велес

Градоначалник на
Општина Велес
Марко Колев

Изготвил: Надица Габерова
Одобрил:Марија Чатмова

Образец 1

ИЗЈАВА

за тајност и заштита на личните податоци дадена од:

Име и презиме: ______________________________

ЕМБГ: ______________________________

Лична карта број: ______________________________

Издадена од: ______________________________

Улица и адреса на живеење: ______________________________

во својство на:

вработено ангажирано лице во Општина Велес,

ИЗЈАВУВАМ дека:

_ Ќе ги почитувам начелата за заштита на личните податоци;
_ Ќе вршам обработка на личните податоци согласно упатствата добиени од општината во својство на контролор, освен ако со закон поинаку не е уредено;
_ Ќе ги чувам како доверливи личните податоци кои 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,

____

име и презиме/потпис

____