ОПШТИНА КАРПОШ
ГРАДОНАЧАЛНИК

МКД СЕРТИФИКАТ
МКС ISO 9001:2015
МКС ISO 14001:2015
МКС ISO 45001:2018

Број: 11 - 7790/3
Датум:25.11.2021
Скопје

Врз основа на член 6 од Правилникот за безбедност и обработка на личните податоци („Службен весник на Република Северна Македонија бр.122/2020), Градоначалникот на Општина Карпош донесе

ПРАВИЛНИК
ЗА ТЕХНИЧКИТЕ Н ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ Н ЗАШТИТА НА ОВРАВОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ
Предмет на уредување

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува Општина Карпош (во натамошниот текст - контролорот) на збирки на лични податоци.

Значење на изразите

Член 2

(1) Одделни изрази употребени во овој правилник го имаат следново значење:
1.Авторизиран пристап е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на контролорот;
2. Администратор на информацискиот систем е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;
3. Документ е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникациска мрежа.
4. Информатичка инфраструктура е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;

ул.Радика бр.9 бараки бр.1 и бр.2 тел. 023055 -903, факс: 3062-925
www.karpos.gov.mk; gradonacalnik@karpos.gov.mk

5. Информациски систем е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;
6. Инцидент е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;
7. Контрола на пристап е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;
8. Овластено лице е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема на кои се обработуваат лични податоци
9. Лозинка е доверлива информација составена од множество на карактери кои се користат за проверка и автентикација на овластеното лице;
10. Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени;
11.Сигурносна копија е копија на личните податоци содржани во електронските документи, кои се зачувани na медиум за да се овозможи нивно повторно враќање.
(2) Останатите изрази употребени во овој правилник ro имаат значењето согласно одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија" бр.42/2020)

Обработувач на збирка на лични податоци

Член 3

(1)Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Обработка на личните податоци

Член 4

Одредбите од 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 лични податоци.

Нивоа на технички и организациски мерки

Член 5

(1)Контролорот треба да применува технички и организациски мерки, кои обезбедуваат тајност и заштита на обработката на личните податоци, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка.
(2)Техничките и организациските мерки од ставот (1) на овој член се класифицираат во две нивоа:
- стандардно и
- високо.

Примена на нивоа

Член 6

(1)За сите документи задолжително се применуваат технички и организациски мерки за безбедност на обработка на личните податоци вклучувајќи зашита од неовластена или незаконска обработка, како и зашита од нивно губење, уништување или оштетување
(2)Контролорот ја демонстрира примената на мерките според барањата утврдени во ставот (1) на овој член, вклучувајќи ги причините и основите за изборот на примената на стандарднот, односно високото ниво.

Правила за обработка на личните податоци надвор од работните простории на контролорот

Член 7

Обработката на личните податоци надвор од работните простории на контролорот се врши врз основа на обезбедено писмено овластување од страна на контролорот и во согласност со соодветното ниво на технички и организациски мерки кои се применувале за обработка на податоците содржани во документите.

Евидентирање и чување на документација за софтверски програми

Член 8

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

Одржување на информацискиот систем

Член 9

(1)Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

(2)Одредбите од ставот (1) на овој член се применуваат и ако физичките или правните лица вршат обработка на личните податоци на контролорот.

Пренос на лични податоци во други држави

Член 10

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во други држави само согласно условите утврдени во прописите за заштита на личните податоци.

II. СТАНДАРДНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Документација за технички и организациски мерки

Член 11

Документацијата за технички и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем на контролорот содржи:

-План за создавање систем на текнички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;

-Акт за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;

-Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатицко комуникациската опрема;

- Правила за пријавување, реакција и санирање на инциденти;

-Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;

-Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на уредите за електронски записи

- Правилник за начинот на вршење на видео надзор

ул.Радика бр.9 бараки бр.1 и бр.2 тел. 023055 -903, факс: 3062-925
www.karpos.gov.mk; gradonacalnik@karpos.gov.mk

- Упатство за начинот на водење евиденција за лица овластени за вршење на обработка на личните податоци.

Технички мерки

Член 12

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 на најмалкуосум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;

3.корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, на поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;

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

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

Организациски мерки

Член 13

(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 и снимање на документи преземени од електронската пошта и други извори;
3.уништување на документи по истекот на рокот за нивно цување;
4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и
5.почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.

(2) Вработеното лице кое ги врши работите за човечки ресурси кај контролорот, го известува администраторот на информацискиот систем 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 бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.

(3) Известцвањето 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.

Физичка сигурност на информацискиот систем

Член 14

(1)Çерверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани, хостирани и администрирани од страна на контролорот.

(2) Физички пристап до просторијата во која се сместени серверите може да имаат само лица посебно овластени од контролорот.

(3) Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице треба да 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 примени на мерки и контроли со кои се намалува ризикот од потенцијални закани вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски вли}анија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

(5)По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски 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 бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Информирање за заштитата на личните податоци

Член 15

(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 организациски 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 непосредното 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) Изјавата од ставот (4) на овој член особено 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.
(6) Изіавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.
(7)Контролорот задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Обврски и одговорности на администраторот на информацискиот систем

Член 16

(1)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 и информатичко комуникациската опрема.

(2)Контролорот 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.

Обврски и одговорности на овластените лица

Член 17

(1)Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до 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 и информатичко комуникациската опрема.

(2) Контролорот задолжително ги информира овластените лица од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Евидентирање на инциденти

Член 18

Во Правилата за пријавување, реакција и санирање на инциденти, контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кој го пријавил, на кого е пријавен и мерките кои се преземени за негово санирање.

Идентификација и проверка

Член 19

(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 утврден во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и да се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

Контрола на пристап

Член 20

(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 наовластените 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 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.
(4) 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.

Управување со медиуми

Член 21

(1)Со електронска евиденција 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 овластените лица утврдени во актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

(2)Пренесувањето на уредите за електронски записи надвор од работните простории се врши само со претходно писмено овластување од страна на контролорот.

Уништување, бришење или чистење на медиумот

Член 22

(1)По пренесувањето на личните податоци од електронска евиденција или по истекот на определениот рок за чување, уредите за електронски записи и електронската евиденција треба да се уништат, избришат или да се исчистат од снимените лични податоци.
(2) Уништувањето на уредите за електронски записи се врши со механичко разделување на составните делови на уредите на кои е снимена, при што истите повторно да не може да бидат употребливи.
(3) Бришењето или чистењето на електронска евиденција 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 електронска евиденција, идентификација на уредите за електронски записи, како и за категориите на лични податоци снимени на истите.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 23

(1) Контролорот е одговорен за проверка на примената на Правилата за начинот на правење на сигурносна копија, архивирање и чуваг-ve, како и за повторното враќање на зачуваните лични податоци.
(2)Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.
(3)Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.
(4) Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци согласно ставот (3) на овој член.

Начин на чување на сигурносните копии

Член 24

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

III. ВНСОКО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Сертификациони постапки

Член 25

Контролорот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите за податоците ио електронски облик и електронски потпис.

Пренесување на медиуми

Член 26

Уредите за електронски записи и електронската евиденција може да се пренесуваат надвор од работните простории само 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.

Пренесување на личните податоци преку електронско комуникациска мрежа

Член 27

Личните податоци можат да се пренесуваат преку електронско комуникациска мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

IV . ДРУГА РАЧНА ОВРАВОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

1. СТАНДАРДНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Примена

Член 28

Одредбите од членовите 3, 5, 6, 7, 11, 13, 15, 17 и 18 соодветно се применуваат и при друга рачна обработка па личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Пристап до документите

Член 29

(1)Пристапот до документите е ограничен само за овластени лица на контролорот.
(2) За пристапувањето до документите задолжително треба да се воспостават 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 треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро"

Член 30

Контролорот задолжително го применува правилото „чисто биро" при обработката на личните податоци содрхсани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Чување на документи

Член 31

(1) Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.
(2)Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.
(3) Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 32

(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 документот како и за категориите на личните податоци содржани во истиот.

2. ВИСОКО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Копирање или умножување на документите

Член 33

(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 треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 34

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.

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Примена

Член 35

За се што не е регулирано со овој Правилник се применуваат одредбите од Законот за заштита на лични податоци.

Влегување во сила

Член 36

Овој правилник влегува во сила со денот на неговото потпишување.

ГРАДОНАЧАЛНИК
НА ОПШТИНА КАРПОШ
Стевчо Јакимовски