20090380693

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ

Врз основа на член 23 став 5 од Законот за заштита на личните податоци („Службен весник на Република Македонија" бр. 7/05 и 103/08), директорот на Дирекцијата за заштита на личните податоци донесе

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА 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 контролорот на збирка на лични податоци.

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. **Авторизиран пристап** е овластување доделено на корисникот 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 телекомуникациска мрежа;
4. **Идентификација** е постапка за идентификување на корисникот на информацискиот систем;
5. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;
6. **Информациски систем** е систем со кој се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;
7. **Инцидент** е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;
8. **Контрола на пристап** е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на корисникот;
9. **Корисник** е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема;
10. **Лозинка** е доверлива информација составена од збир на карактери кои се користат за проверка на корисникот;

11. **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;

12. **Одговорно лице за заштита на личните податоци** е лице овластено од контролорот за координирање и контрола на техничките и организациските мерки кои се применуваат за тајност и заштита на обработката на личните податоци;

13. **Проверка** е постапка за верификација на идентитетот на корисникот на информацискиот систем;

14. **Сигурносна копија** е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.

Обработувач на збирка на лични податоци

Член 3

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 овој правилник се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци и
- друга 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 три нивоа:

- основно;
- средно и
- високо.

Примена на нивоа

Член 6

(1) За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на основно ниво.

(2) За документите кои содржат лични податоци што се однесуваат на: кривични дела, изречени казни, алтернативни мерки и мерки на безбедност за извршени кривични дела, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(3) За документи кои содржат: посебни категории на лични податоци, лични податоци кои се обработуваат за полициски цели и лични податоци кои се обработуваат заради заштита на интересите на државната безбедност и одбраната на Република Македонија, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

(4) За документите кои содржат матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(5) За документите кои се пренесуваат преку телекомуникациска мрежа, а содржат посебни категории на лични податоци и матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

(6) Со документацијата за технички и организациски мерки, контролорот треба да пропише и обезбеди соодветен степен на заштита на личните податоци, согласно на нивоата кои се определени во овој член.

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.

II. Основно ниво на технички и организациски мерки

Документација за технички и организациски мерки

Член 10

(1) Контролорот задолжително донесува и применува документација за технички и организациски мерки за корисниците кои имаат пристап до личните податоци и до информацискиот систем.

(2) Документацијата од ставот (1) на овој член особено содржи:

- План за создавање систем на технички 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 корисниците при користење на документите и информатичко 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 медиумите.

(3) Документацијата од ставот (2) на овој член, контролорот веднаш ја менува и дополнува кога ќе се направат промени во организационата поставеност на информацискиот систем.

Технички мерки

Член 11

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 секој корисник, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. корисничко име и лозинка која овозможува пристап на корисникот 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. 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 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 сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
9. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Организациски мерки

Член 12

(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 корисниците 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 чување;

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

Физичка сигурност на информацискиот систем

Член 13

(1) Серверите 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 овластени лица 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 овластено лице 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 влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Информирање за заштитата на личните податоци

Член 14

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

Обврски и одговорности на корисниците

Член 15

(1) Обврските и одговорностите на секој корисник кој има пристап до личните податоци и до информацискиот систем, контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема.

(2) Контролорот задолжително ги информира корисниците 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 16

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

Идентификација и проверка

Член 17

(1) Контролорот задолжително води евиденција за корисниците 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 18

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

(2) Контролорот воспоставува механизми за да се оневозможи пристап на корисниците до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

(3) Во евиденцијата на корисниците утврдена во член 17 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секој корисник.

(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 19

(1) Со медиумите 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 корисници утврдени во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

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

Уништување, бришење или чистење на медиумот

Член 20

(1) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

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

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

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

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 21

(1) Контролорот е одговорен за проверка на примената на Правилата за начинот на правење на сигурносна копија, архивирање и чување, како и за повторното враќање на зачуваните лични податоци.

(2) Во Правилата од ставот (1) на овој член, задолжително треба да се содржани постапките за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

(3) Сигурносни копии задолжително се прават секој работен ден, на крајот од работната седмица и секој последен работен ден во месецот.

Начин на чување на сигурносните копии

Член 22

(1) Сигурносните копии се чуваат во просторија која се наоѓа надвор од објектот во кој е сместен информацискиот систем.

(2) Сигурносните копии треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

Глава III. Средно ниво на технички и организациски мерки

Дополнителни правила за технички и организациски мерки

Член 23

Во документацијата за технички и организациски мерки утврдена во член 10 од овој правилник, задолжително треба да се содржани постапките за овластување на одговорно лице за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки, како и за мерките кои треба да се преземат при користење на медиумите.

Одговорно лице за заштита на личните податоци

Член 24

Контролорот задолжително овластува едно или повеќе лица за заштита на личните податоци кои ќе бидат одговорни за координација и контрола на постапките и упатствата утврдени во документацијата за техничките и организациските мерки.

Контрола на информацискиот систем и информатичката инфраструктура

Член 25

(1) Информацискиот систем и информатичката инфраструктура на контролорот задолжително подлежат 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.

(2) Контролорот врши надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

(3) Надворешната контрола од став (1) на овој член се врши преку обработка на документи од страна на независно трето лице.

(4) Во извештајот од извршената контрола од ставот (1) на овој член 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 корективни или дополнителни мерки за нивно отстранување.

(5) Во извештајот од ставот (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.

(6) Извештајот од ставот (4) на овој член 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, за отстранување на констатираните недостатоци.

(7) Извештајот од ставот (4) на овој член треба да биде достапен за увид на Дирекцијата за заштита на личните податоци.

Идентификација и проверка

Член 26

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

Евидентирање на авторизираниот пристап

Член 27

(1) Контролорот води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци: име и презиме на корисникот, 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 за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

(2) Во евиденцијата од ставот (1) на овој член 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.

(3) Операциите кои овозможуваат евидентирање на податоците од ставовите (1) и (2) на овој член треба да бидат контролирани од страна на одговорното лице за заштита на личните податоци и истите не може да се деактивираат.

(4) Евиденцијата од ставот (1) на овој член се чува најмалку десет години.

(5) Одговорното лице за заштита на личните податоци врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Контрола на физички пристап

Член 28

Во документацијата за технички и организациски мерки, контролорот треба да определи критериуми за корисниците кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Член 29

(1) Контролорот треба да воспостави систем за евидентирање на медиумите кои се примаат со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.

(2) Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на контролорот.

(3) За пренесените медиуми надвор од работните простории на контролорот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Евидентирање на инциденти

Член 30

(1) Во Правилата за пријавување, реакција и санирање на инциденти, контролорот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на корисниците кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени и кои биле рачно внесени при враќањето.

(2) За повторно враќање на личните податоци, контролорот издава писмено овластување на корисниците за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 31

Сигурносните копии задолжително треба да бидат чувани на друга оддалечена локација од местото каде е сместен информацискиот систем и истата треба да биде обезбедена со соодветни технички и организациски мерки согласно документацијата за технички и организациски мерки.

Тестирање на информацискиот систем

Член 32

(1) 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.

(2) Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето лице.

Глава IV. Високо ниво на технички и организациски мерки

Сертификациони постапки

Член 33

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 во електронски облик и електронски потпис.

Пренесување на медиуми

Член 34

Медиумите можат 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 телекомуникациска мрежа

Член 35

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

Глава V. Преодни и завршни одредби

Престанување на важење

Член 36

Со денот на отпочнувањето на примената на овој правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр. 111/05).

Влегување во сила

Член 37

Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Македонија“, а ќе се применува од 1 јуни 2009 година.

Бр. 01-339/1
10 март 2009 година
Скопје

Директор,
Маријана Марушиќ, с.р.