Врз основа на член 23 став 5 од Законот за заштита на личните податоци („Службен весник на Република Македонија" бр. 7/05, 103/08 и 124/10), министерот за образование и наука 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

Октомври, 2011

10. „**Лозинка**" е доверлива информација составена од множество на знаци кои се користат за автентицирање на овластеното лице преку употреба на неговата корисничка сметка;

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. „**Офицер за заштита на личните податоци**" е лице овластено од Министерството за самостојно и независно вршење на работите во смисла на Законот за заштита на личните податоци;

13. „**Проверка**" е постапка за верификација на идентитетот на овластеното лице 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

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

(2) Одредбите од членот 26 на овој правилник соодветно се применуваат и при проверката на постапувањето на обработувачот при обработката на личните податоци во смисла на Законот за заштита на личните податоци.

Обработка на личните податоци

Член 4

(1) Одредбите од овој 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) Министерството 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:

Одржување на информацискиот систем

Член 9

(1) Физичките или правните лица кои вршат одржување на информацискиот систем на Министерството 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 Министерството.

Пренос на лични податоци во други држави

Член 10

(1) 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. Основно ниво на технички и организациски мерки

Документација за технички и организациски мерки

Член 11

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

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

1. План за создавање систем на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;

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

3. Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;

4. Правила за пријавување, реакција и санирање на инциденти;

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

6. 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, Министерството веднаш ја менува и дополнува кога ќе се направат промени во информацискиот систем.

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 Министерството, 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) Известувањето 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) Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички во работните простории на Министерството .

(2) Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се хостирани и администрирани од страна на овластени лица во Министерството.

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

(4) Доколку е потребен пристап на друго лице до просторијата во која се сместени серверите и личните податоци зачувани на нив, тогаш тоа лице треба да биде придружувано и надгледувано од лицето од ставот (3) на овој член, за што се води посебен дневник за пристап на други лица во кој обавезно се запишува почетокот и крајот на пристапот, неговото име и презиме, бројот на личната карта, од кое овластено лице е придружувано и која била целта на неговиот престој во просторијата.

(5) 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.

податоци.

Обврски и одговорности на администраторот на информацискиот систем

Член 16

(1) Обврските и одговорностите на администраторот на информацискиот систем, Министерството 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) Министерството 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, Министерството 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) Министерството 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

(1) Во Правилата за пријавување, реакција и санирање на инциденти, Министерството 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) Министерството 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, Министерството 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

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 23

(1) Министерството е одговорно 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 и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

(4) 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.

(5) Министерството задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци согласно ставот (4) на овој член.

Начин на чување на сигурносните копии

Член 24

(1) 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. Средно ниво на технички и организациски мерки

Дополнителни правила за технички и организациски мерки

Член 25

(1) Во документацијата за технички и организациски мерки утврдена во член 11 од овој правилник, задолжително треба да се содржани постапките за вршење периодични контроли, заради следење на усогласеноста на работењето на Министерството 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.

Контрола на информацискиот систем и информатичката инфраструктура

Член 26

(1) Информацискиот систем и информатичката инфраструктура на Министерството 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.

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

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

(5) Офицерот 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 29

(1) Во документацијата за технички и организациски мерки, Министерството треба да определи критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Член 30

(1) Министерството 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 Министерството.

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

Евидентирање на инциденти

Член 31

(1) Во Правилата за пријавување, реакција и санирање на инциденти, Министерството ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица 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, Министерството издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 32

(1) 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.

V. Друга рачна обработка на личните податоци

1. Основно ниво на технички и организациски мерки

Примена

Член 37

(1) Одредбите од членовите 3, 5, 6, 7, 11, 13, 15, 16, 17 и 18 соодветно се применуваат и при друга рачна обработка на 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 38

(1) Пристапот до документите треба биде ограничен само за овластени лица на Министерството.

(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 39

(1) Министерството 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.

Чување на документи

Член 40

(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, Министерството 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 Министерството треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени

презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат".

VI. Завршни одредби

Член 46

(1) Овој правилник влегува во сила наредниот ден од денот на неговото донесување

Бр. 13-4841/1
17.08. .2011 година

Министер,

м-р Панче Кралев