Република Македонија
Универзитет СВ. КИРИЛ И МЕТОДИЈ
Институт за социолошки и политичко-правни истражувања
Бр. 02-1505/11
21.12. 2015 год.
СКОПЈЕ

Бр. 02-1505/11
21.12.2015 година

Врз основа на член 23 став 5 од Законот за заштита на личните податоци („Службен весник на Република Македонија" бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014 и 153/2015), директорот на Институтот за социолошки и политичко-правни истражувања во состав на Универзитетот „Св. Кирил и Методиј" во Скопје 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 Институтот за социолошки и политичко-правни истражувања-Скопје во состав на Универзитетот „Св. Кирил и Методиј" во Скопје (во понатамошниот текст: Контролор).

Поимник
Член 2

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. **Идентификација** е постапка за идентификување на овластеното лице 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 може да 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 овластеното лице;
9. **Овластено лице** 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 множество на карактери кои се користат за проверка на овластеното лице;
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 контролорот за самостојно и независно вршење на работите во смисла на член 26-а од 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

Одредбите од овој Правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Одредбите од членот 20 на овој Правилник соодветно се применуваат и при проверката на постапувањето на обработувачот при обработката на личните податоци во смисла на член 26, став 3 од Законот за заштита на личните податоци.

Обработка на личните податоци

Член 4

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) Контролорот ќе 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 Збирката на лични податоци – Матична евиденција на вработени кај Контролорот (МЕВ) ќе се применуваат технички и организациски мерки од основно, средно и високо ниво.
(3) За Збирката на лични податоци – Матична евиденција на студенти кај Контролорот (МЕС) ќе се применуваат технички и организациски мерки од основно, средно и високо ниво.
(4) За Збирката на лични податоци – Евиденција за плати на вработени во Институтот за социолошки и политичко-правни истражувања при Универзитетот „Св. Кирил и Методиј" во Скопје ќе се применуваат технички и организациски мерки од основно и средно ниво.
(5) За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или 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 ќе 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 ја евидентира и 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 ќе ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

(2) Одредбите од ставот (1) на овој член ќе 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 овластените лица 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;
- Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;
- Правилник за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;
- Правилник за пријавување, реакција и санирање на инциденти;
- Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
- Правилник 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 ќе ја менува и дополнува кога ќе се направат промени на информацискиот систем.

Технички мерки
Член 11

Контролорот ќе 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 најмалку осум 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. автоматизирано 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 инифомацискиот 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 ќе 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;
      a. документите кои содржат лични податоци и кои овластените лица поради утврдениот начин на нивното добивање или испраќање, треба да ги транспортираат со електронска пошта, треба да бидат избришани од системот за електронска пошта веднаш кога ќе бидат преземени од него или испратени преку него.
      b. Треба да се води сметка ваквите документи да не остануваат во системот за електронска пошта преку нивно сместување во папките за испратена пошта односно избришана пошта
   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, ќе 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 13

(1) Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, се физички лоцирани, хостирани и администрирани од страна на Контролорот.

(2) Физички пристап до просторијата во која се сместени серверите 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 секогаш ќе 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 влијанија, 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 администрирани и 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 кое врши администрирање на серверите, ќе 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 14

(1) Лицата кои се вработуваат или се ангажираат кај Контролорот, пред нивното отпочнување со работа ќе бидат запознаени 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) Изјавата 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.

(8) Обврските и одговорностите на администраторот на информацискиот систем, се дефинирани и утврдени во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникацискаата опрема.

(9) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, се дефинирани и утврдени во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникацискаата опрема.

Евидентирање на инциденти

Член 15

Во Правилникот за пријавување, реакција и санирање на инциденти, се определени начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавило, кому е пријавен и мерките кои се преземени за негово санирање.

Идентификација и проверка

Член 16

(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, како и да се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

Контрола на пристап

Член 17

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

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

(3) Во евиденцијата на овластените лица утврдена во член 16 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 Правилникот 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 комуникацискаата опрема само во согласност со критериумите кои се утврдени од страна на Контролорот.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 18

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

(2) Во Правилникот 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 се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Начин на чување на сигурносните копии

Член 19

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.

Глава III. Средно ниво на технички и организациски мерки

Дополнителни правила за технички и организациски мерки
Контрола на информацискиот систем и информатичката инфраструктура

Член 20

(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 правно 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 офицерот 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.

(8) Образецот на извештајот од ставот (4) на овој член е составен дел на овој Правилник.

Идентификација и проверка

Член 21

Контролорот треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице.

Евидентирање на авторизираниот пристап *(логови)*

Член 22

(1) Контролорот води евиденција за секој авторизиран пристап која треба да ги содржи особено следните 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 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 офицерот за заштита на личните податоци и истите не може да се деактивираат.

(4) Евиденцијата од ставот (1) на овој член се чува најмалку една година.

Контрола на физички пристап

Член 23

Информацискиот систем се наоѓа во компјутерскиот центар на Контролорот во специјално за таа намена изготвена систем-сала во која имаат физички пристап само вработеното/те лице/а кое има статус на овластено лице.

Контролата на физички пристап е обезбедена со двојна врата со клуч.

Управување со медиуми

Член 24

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 25

(1) Во Правилникот 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 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, Контролорот издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 26

Меѓусебните права и обврски на Контролорот и правното, односно физичкото лице каде се чуваат сигурносните копии, ќе 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.

Тестирање на информацискиот систем

Член 27

(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 правно лице.

Глава IV. Високо ниво на технички и организациски мерки

Сертификациони постапки

Член 28

Контролорот ќе 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 29

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 електро комуникациска мрежа

Член 30

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

Глава IV – а. Друга рачна обработка на личните податоци

1. Основно ниво на технички и организациски мерки

Примена

Член 31

Одредбите од членовите 3, 5, 6, 7, 10, 12 и 14 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 32

(1) Пристапот до документите е ограничен само за овластени лица на Контролорот.
(2) За пристапувањето до документите задолжително ќе се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

Правило „чисто биро“

Член 33

Контролорот задолжително ќе 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 34

(1) Чувањето на документите 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 ќе примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Уништување на документи

Член 35

(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно 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. Средно ниво на технички и организациски мерки

Контрола
Член 36

Одредбите од членот 20 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.

Начин на чување на документите
Член 37

(1) Плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

3. Високо ниво на технички и организациски мерки

Копирање или умножување на документите
Член 38

(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 39

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 е пренесуваат.

Влегување во сила
Член 40

Овој Правилник влегува во сила со денот на донесувањето.

Директор

Проф. д-р Мирјана Борота Поповска

Образец

Извештај од извршената _____ (внатрешна или надворешна) контрола на информацискиот систем и информатичката инфраструктура

1. **Назив и седиште/име и презиме и адреса на живеење на контролорот**

---

2. **Информации за збирката на лични податоци врз која е извршена контролата**

_____

Назив на збирка/и на личните податоци	
Ниво на технички и организациски мерки:	
Начин на обработка на личните податоци:	

3. **Идентификација на контролата**

Датум на започнување:	
Датум на завршување:	
Спроведено од страна на (назив и седиште на правното лице кое врши надворешна контрола):	

4. **Резултати од контролата**

I. Целосно и делумно автоматизирана обработка на личните податоци

Ниво	Мерка на усогласеност	Степен на усогласеност	Констатирани недостатоци	Предложени корективни или дополнителни мерки за отстранување на констатираните недостатоци
Основно	Документација за технички и организациски мерки (член 10)			
Основно	Технички мерки (член 11)			
Основно	Организациски мерки (член 12)			
Основно	Физичка сигурност на информацискиот систем (член 13)			
Основно	Информирање за заштитата на личните податоци (член 14)			
Основно	Обврски и одговорности на администраторот на информацискиот систем (член 14-а)			
Основно	Обврски и одговорности на овластените лица (член 15)			
Основно	Евидентирање на инциденти (член 16)			
Основно	Идентификација и проверка, како и законска обработка на личните податоци (член 17)			
Основно	Контрола на пристап (член 18)			
Основно	Управување со медиуми (член 19)			
Основно	Уништување, бришење или чистење на медиумот (член 20)			
Основно	Сигурносни копии и повторно враќање на			

	зачуваните лични податоци (член 21)			
Основно	Начин на чување на сигурносните копии (член 22)			
Средно	Дополнителни правила за технички и организациски мерки (член 23)			
Средно	Контрола на информацискиот систем и информатичката инфраструктура (член 25)			
Средно	Идентификација и проверка (член 26)			
Средно	Евидентирање на авторизираниот пристап и законска обработка на личните податоци (член 27)			
Средно	Контрола на физички пристап (член 28)			
Средно	Управување со медиуми (член 29)			
Средно	Евидентирање на инциденти (член 30)			
Средно	Сигурносни копии (член 31)			
Средно	Тестирање на информацискиот систем (член 32)			
Високо	Сертификациони постапки (член 33)			
Високо	Пренесување на медиуми (член 34)			
Високо	Пренесување на личните податоци преку електронско комуникациска мрежа (член 35)			

II. Друга рачна обработка на лични податоци што се дел од посебна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци

Ниво	Мерка на усогласеност	Степен на усогласеност	Констатирани недостатоци	Предложени корективни или дополнителни мерки за отстранување на констатираните недостатоци
Основно	Документација за технички и организациски мерки (член 10)			
Основно	Организациски мерки (член 12)			
Основно	Информирање за заштитата на личните податоци (член 14)			
Основно	Обврски и одговорности на овластените лица (член 15)			
Основно	Евидентирање на инциденти (член 16)			
Основно	Пристап до документи и законска обработка на личните податоци (член 35-б)			
Основно	Правило „чисто биро“ (член 35-в)			
Основно	Чување на документи (член 35-г)			
Основно	Уништување на документи (член 35-д)			
Средно	Дополнителни правила за технички и организациски мерки (член 23)			
Средно	Контрола на информацискиот систем и информатичката инфраструктура (член 25)			
Средно	Начин на чување на документите (член 35-е)			

Високо	Копирање или умножување на документите (член 35-ж)			
Високо	Пренесување на документи (член 35-з)			

III. Податоци и факти врз основа на кои е изготвен извештајот и се предложени мерките за отстранување на констатираните недостатоци

➢ ➢

IV. Тим кој ја вршел контролата:

Име и презиме	Работно место	Потпис

V. Офицер за заштита на личните податоци кој го примил и ја потврдил содржината на извештајот (и)

Име и презиме	Потпис

VI. Одговорно лице, односно функционер на контролорот, кој е запознаен со содржината на извештајот

Име и презиме	Потпис

_____, _____, 20___ година М.П.
(место) (датум)