Врз основа на член 23 став 1 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, 153/2015, 99/2016 и 64/2018) и член 16 став 1 алинеја 3 од Законот за поштенските услуги („Службен весник на Република Македонија” број 158/2010, 27/2014, 42/2014, 187/2014, 146/2015,31/2016, 190/2016, 64/2018 и 27/2019) Комисијата на Агенцијата за пошти, на состанокот одржан на 15.10.2019 година, го донесе следниот

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

## I. ОПШТИ ОДРЕДБИ

### Предмет на уредување и значење на изразите

### Член 1

Со овој Правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува Агенцијата за пошти (во натамошниот текст – контролорот) на збирка на лични податоци.

(1) Одделни изрази употребени во овој Правилник го имаат следново значење:

1. Автозиран пристап е овластување доделено на овластено 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 податоции 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 овластено 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 тајност и заштита на личните податоци;
8. Контрола на пристап е операција за доделување на пристап до личните податоци или до информатичко комуникациска опрема со цел проверка на овластено 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 овластено 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 вратено;
12. Офицер за заштита на личните податоци е лице овластено од контролорот за самостојно и независно вршење на работата 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 која на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.

(2) Останати изрази употребени во овој Правилник го имаат значењето согласно одредбите 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, 153/2015, 99/2016 и 64/2018).

Обработувач на збирка на лични податоци

Член 2

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

(2) Одредбите од членот 25 на овој Правилник соодветно се применуваат и при проверка на постапувањето на обработувачот при обработка на личните податоци во смисла на член 26 став 3 од Законот за заштита на личните податоци.

Обработка на личните податоци

Член 3

Одредбите од овој Правилник се применуваат за:

- Целосна и делумно автоматизирана обработка на личните податоци и
- Друга рачна обработка на личните податоци што се дел од постојана збирка на лични податоци или се наменети да бидат дел од збирката на лични податоци.

Нивоа на техничките и организациски мерки

Член 4

(1) Контролорот треба да се 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 нивна обработка.

(2) Техничките и организациските мерки од ставот (1) на овој член се класифицираат на три ниво:

- основно;

- средно и

- високо.

Примена на нивоа

Член 5

(1) За сите документи задолжително се применуваат техничките и организациските мерки кои се класифицираат на основно ниво.

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

(4) За документите кои содржат матичен број на граѓанинот задолжително се применуваат техничките и организациски мерки кои се класифицираат на 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 техничките и организациски мерки кои се класифицираат на основно, средно и високо ниво.

(6) Со документацијата за технички и организациски мерки, контролорот треба да пропише и обезбеди соодветен степен за 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 6

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

Член 7

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

Одржување на информацискиот систем

Член 8

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

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

Пренос на личните податоци

Член 9

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

## II. ОСНОВНО НИВО НА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ

Документација за техничките и организациските мерки

Член 10

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

- План за создавање систем на техничките и организациските 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 уредите за елекронски записи;
- Упатство за начинот на водење евиденција за лица овластени за вршење на обработка на личните податоци.

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 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 овластено 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 на информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластено лице дека треба да побара инструкција од администраторот на информацискиот 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 незадоволени или злонамерни обиди за влез или пробивање на системот;

7. Ефективна и сигурна анти-вирусна и анти-спајдер заштита на информацискиот систем, која постојано ќе се ажурира заради превентира од непознати и непланирање закани од нови вируси и спајвери;
8. Ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамнови и
9. Приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Организациони мерки

Член 12

(1) Контролорот треба да обезбеди соодветни организациски мерки за тајност и заштита на обработка на личните податоци и тоа:

1. Ограничен пристап или идентификација за пристап до личните податоци;
2. Организациски правила за пристап на овластени лица до интернет кои се однесуваат на симнување и снимање на документи превземени од електронска 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 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 на 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 овластено лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.

Физичка сигурност на информацискиот систем

Член 13

(1) Серверите на кое се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани, хостирани и администратирани 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 ризици во опкружување преку примени на мерки и контроли со кои се намалува ризикот од потенцијални закани вклучувајки кражба, пожар, екплозии, чад, вода, прашина, вибрации, хемиски влијаниа, пречки во снабувањето 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 случај од ставот (5) на овој член, меѓусебните права и обврски на контролорот и правно, односно физичко 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 14

(1) Лицата кои се вработени 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 техничките и организациските мерки.

(2) За лицата кои се ангажираат за извршување на работа кај контролорот во договор за нивото ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.
(3) Контролорот пред непосредно 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 ангажираат кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработка 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.

Обврски и одговорности на администраторот на информавискиот систем

Член 15

(1) Обврските и одговорностите на администраторот на информацискиот систем, контролорот ги дефинира и утврдува во Правилникот 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 над администраторот на информацискиот систем и изработува извештај за завршената контрола.
(3) Во извештајот од ставот (2) на овој член треба да се содржани констатираните неправилности и предложени мерки за отстранување на тие неправилности.

## Обврски и одговорности на овластени лица

### Член 16

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, контролорот ги дефинира и утврдува во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластени лица при користење на документите и информатичко комуникациската опрема.

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

## Евидентирање на инциденти

### Член 17

Во Правилникот 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 превземени за негово санирање.

## Идентификација и проверка

### Член 18

(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 основ 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 Правилникот 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 19

(1) Овластените лица задолжително имаат автоматизиран 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 овластените 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 Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработка 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 20

(1) Со електронска евиденција треба да се овозможи идентификација и евидентирање на категориите на личните податоци и истите треба да се чуваат на локација до која пристап имаат само овластените лица утврдени со Правилникот за техничките и организациските мерки за обезбедување тајност и зашита на обработката на личните податоци.
(2) Пренесувањето на уредите за електронски записи надвор од работните простории се вршат само со претходно писмено овластување на страна на контролорот.

Уништување, бришење или чистење на медиумот

Член 21

(1) По пренесување 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 избрши 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 22

(1) Контролорот е одговорен за проверка на примената на Правилникот за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните податоци.
(2) Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седница, 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 реконструкцијата на личните податоци согласно ставот (3) на овој член.

Начин на чување на сигурносни копии

Член 23

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

## III. СРЕДНО НИВО НА ТЕХНИЧКИТЕ МЕРКИ

### Дополнителни правила за технички и организациски мерки

Член 24

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 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 уредите за електронски записи и за електронска евиденција.

### Контрола на информацискиот систем и информатичката структура

Член 25

(1) Информацискиот систем и информатичката структура 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 констатирани 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

превземање 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 извештај од ставот (4) на овој член е составен дел на овој правилник.

Идентификација и проверка

Член 26

Контролорот обезбедува механизми кои ќе овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизација за секое овластено лице.

Евидентирање на авторизираниот пристап (логови)

Член 27

(1) Контролорот води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци: име и презиме на овластено 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 превземени 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 евиденција 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 потребно ниво на авторизација.

(3) Операциите кои овозможуваат евидентирање на податоците на 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 5 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 28

Физичкиот пристап и контролата на физички пристап до просториите каде е сместен информацискиот систем се спроведува во согласност со документацијата за технички и организациски мерки и Законот за заштита на личните податоци.

## Управување со медиуми

### Член 29

(1) Контролорот треба да воспостави системи за водење за електронска евиденција кои се примаат со цел да овозможи директна или индиректна идентификација на видот на електронска евиденција која е примена, датум и време на примање, испраќач, број на електронски евиденции кои се применти, вид на документ кој е снимен, начин на испраќање на електронска евиденција, име и презиме на лицето овластено за прием на електронска евиденција.

(2) Одредбите од ставот (1) на овој член се применуваат и за електронско евидентирање кои се испраќаат од страна на контролорот, како и за уредите за електронски записи.

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

## Евидентирање на инциденти

### Член 30

(1) Во Правилникот за пријавување, реакција и санирање на инциденти се определени 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 лица за да ги извршат операциите за враќање на податоците.

Сигурносни копии

Член 31

(1) Сигурносните копии задолжително се прават секој работен ден, на крајот од работната седница и секој последен работен ден во месецот.
(2) Сигурносните копии се чуваат надвор од објектот во кој се наоѓаат серверите или персоналните компјутери во кои се сместени збирките на лични податоци за кои се прави сигурносна копија.
(3) Сигурносните копии кои се чуваат на другата оддалечена локација од сместото каде е сместен информацискиот систем треба да бидат обезбедени со соодветни технички и организациски мерки, согласно документацијата за технички и организациски мерки.
(4) Во случајот (3) на овој член, меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде се чуваат сигурносните копии, треба да бидат уредени со договор во писмена форма, кој задолжително ќе ги содржи техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

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 правно лице.

## IV. ВИСОКО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Сертификациони постапки

Член 33

Контролорот може да применува и други технички мерки за тајност 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

Уредите за електронски записи и електронската евиденција може да се пренесуваат надвор од работните простории само ако личните податоци се криптирани или ако се заштитани 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 35

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 – А. ДРУГА РАЧНА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

### 1. ОСНОВНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Примена

Член 36

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

Пристап до документите

Член 37

(1) Пристапот до документите е ограничен само за овластени лица на контролорот.

(2) За пристапување до документите задолжително треба да се воспостави механизми за идентификација на овластени 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 прооцедури за таа цел во документацијата за техничките и организациските мерки.

Правило „Чисто биро"

Член 38

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

Чување документи

Член 39

(1) Чувањето на документи треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.
(2) Кога физичките карактеристики на документи не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки кои што ќе 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 40

(1) Уништувањето на документи се врши со ситнење или со друг начин, при што истите повторно не можат да бидат употребливи.
(2) Во случајот (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 ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ

### Контрола

### Член 41

Одредбите од членовите 25 и 26 соодветно да се применуваат и при друга рачна обработка на личните податоци што се дел од постојана збирка на лични податоци или се наменети да бидат дел на збирка на личните податоци.

### Начин на чување на документите

### Член 42

(1) Плакарите (орманите), картотеките или друга 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 овластени лица.
(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи неовластен пристап до документите.

## 3. ВИСОКО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

### Копирање или умножување документи

### Член 43

(1) Копирањето или умножувањето на документи може да се врши едноставно со контрола на овластени лица определени со претходно писмено овластување од страна на контролорот.
(2) Уништувањето на копиите или умножувањето документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 44

Во случај на физички пренос на документи 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 45

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

Влегување во сила

Член 46

Овој Правилник влегува во сила со денот на неговото потпишување, а истиот ќе се објави на веб страницата на Агенцијата за пошти.

Агенција за пошти
Комисија
Борче Груевски, претседател