Врз основа на член 34 од Законот за Судскиот совет на Република Македонија („Службен весник на Република Македонија“ бр. 60/06,бр.150/10, 100/2011,бр.20/2015 и бр.61/2015, бр.61/2015, бр.197/17 и бр.83/18) и член 23 од Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр.7/05, 103/08, 124/08 и 124/10), а во врска со член 10 став 2 алинеја 1 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, Судскиот совет на Република Македонија на седницата одржана на ден 18.09.2018 година, 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

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 Судскиот совет на Република Македонија (во натамошниот текст: Советот)во својство на контролор согласно Законот за заштита на личните податоци.

Значење на употребените изрази

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 во Советот;
2. **Администратор** на информацискиот систем е административен службеник-информатичар во Советот кој е овластен 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. Документот во смисла на овој правилник е секој спис од предмет и друг документ содржан во евиденциите, уписниците и евидентните книги што се водат во Советот;

4. **Идентификација** е постапка за идентификување на овластеното лице на информацискиот систем;
5. **Информатичка инфраструктура** е целата информатичко комуникациска опрема на Советот, 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 во Советот 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 во Советот, 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 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 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) Судскиот совет на Република Македонија 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 на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

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

(4) 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.

(5) Со документацијата за технички и организациски мерки, Советот ќе 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 Советот 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

Советот 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 Советот 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 во Судскиот совет на Република Македонија.

II. Основно ниво на технички и организациски мерки

Документација за технички и организациски мерки

Член 10

(1) Судскиот совет на Република Македонија 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;
- Акт за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;
- Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и 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, Советот ја менува и дополнува веднаш кога ќе се направат промени во информацискиот систем.

(4)

Технички мерки

Член 11

Советот обезбедува соодветни технички мерки за тајност и заштита на обработката на личните податоци, преку дефинирање на правилата кои се однесуваат на следните барања:

- Единствено корисничко име на ниво на оперативен систем;
- Лозинка креирана од овластено лице, која корисникот може да ја промени;
- Лозинката е потребно да има минимум 8 алфа-нумерички карактери од кои минимум една голема буква и специјални знаци;
- Лозинката на администраторот – информатичар треба да има 12 карактери
- Промената на лозинката е на временски период кој не може да биде подолг од 3 месеци;
- Автоматизирано одјавување од информацискиот систем се врши после изминување на 15 минути неактивност и за повторно активирање на системот потребно е повторно внесување на корисничко име и лозинка;
- Автоматизирано отфрлање од информацискиот систем настанува после 3 неуспешни обиди за најавување и потребно е барање инструкции од администраторот на информацискиот систем;
- Корисничко име и лозинка која овозможува пристап на овластеното лице до информацискиот систем во целина, до поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;
- Инсталирана хардверска/софтверска заштитна мрежна бариера (“firewall”) 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;

- Ефективна и сигурна анти-вирусна, анти-спајвер и анти-спам заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси, спајвери и спамови;
- Приклучување на информацискиот систем (серверот и компјутерска опрема во судниците) на енергетска мрежа преку уред за непрекинато напојување;

Во случај на инцидент, пристап до информацискиот систем има овластено правно лице за одржување и сервисирање на информацискиот систем (во понатамошниот текст "Овластеното правно лице") исклучиво по барање и во присуство на информатичарот кој го администрира информацискиот систем, а врз основа на претходно овластување од страна на претседателот на Советот.

Организациски мерки
Член 12

(1) Советот обезбедува соодветни организациски мерки за тајност и заштита на обработката на личните податоции и тоа:

1. Ограничен пристап или идентификација за пристап на личните податоци ,

2.организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори.

3. уништување на документи по истекот на рокот за нивно чување,

4. мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат,обработуваат и чуваат личните податоци ,

5.почитување на техничките упатства при инсталирање и користење на информатичко комуникациска опрема на која се обработуваат личните податоци.

(2)Во насока на обезбедување тајност и заштита на обработката на личните податоци, Советот склучува договор со овластеното правно лице со кој се регулираат обврските и одговорностите на овластеното правно лице и на вработените кај овластеното правно лице, а во поглед на примената на Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на директорот на Дирекцијата за заштита на личните податоци.

Физичка сигурност на информацискиот систем

Член 13

(1)Серверите на кои се инсталирани софтверски програми за обработка на личните податоци, треба да се физички лоцирани ,хостирани и администрирани од страна на Советот .

(2)физички пристап до просторијата во која се сместени серверите може да имаат само лица овластени од Советот.

(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 став 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 елекромагнетно зрачење.

Информирање за заштитата на личните податоци

Член 14

(1) Лицата кои се вработуваат или се ангажираат кај Советот , 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 во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Советот 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 ангажираатво во Советот, 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 .

Член 15

(1) Обврските и одговорностите на администраторот на информацискиот систем, Советот 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) Советот задолжително врши периодична контрола над работата на администраторот-информатичар 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 16

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, Советот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем- информатичарот кој го администрира информацискиот систем на Советот и на овластените лица при пристапувањето до судските предмети, другите документите и информатичко-комуникациската опрема.

(2) Советот 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 17

Начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кое го пријавил, на кого е пријавен и мерките кои се преземени за негово санирање се уредени со Правилникот за пријавување, реакција и санирање на инциденти.

Идентификација и проверка

Член 18

(1)Советот 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,Советот 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 овој правилник ,како да се чуваат заштитени со соодветни методи , така што нема да бидат разбирливи додека се валидни.

Контрола на пристап

Член 19

(1)Заради идентификација и проверка на авторизираниот пристап, Советот задолжително води евиденција за овластените

лица кои имаат авторизиран пристап до документите и информатичкиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

(2)Советот врши проверка на авторизираниот пристап преку кој се овозможува:

- евидентирање на работната станица и корисничкото име за овластените лица кои пристапуваат до информацискиот систем, заедно со нивото на авторизиран пристап, времето и датумот на пристап, како и снимање на овие податоци;
- идентификување на компјутерскиот систем од кој се врши надворешен обид за пристап во оперативните функции или податоци без потребното ниво на авторизација и генерирање извештај за секој чекор од неавторизираните пристапи.

(3)Врз основа на механизмите наведени во претходните ставови од овој член, Советот е во можност да врши идентификација и проверка на авторизираниот пристап, односно контрола на пристапот до личните податоци и информатичко–комуникациската опрема од страна на овластените лица со обезбеден постојан увид во моменталниот и минатиот пристап, како и преземените операции од страна на овластените лица.

(4)Врз основа на механизмите предвидени во оваа точка се овозможува секое овластено лице да има авторизиран пристап само до личните податоци и информатичко-комуникациската опрема кои се неопходни за извршување на нивните задачи, како и се оневозможува пристап до лични податоци и информатичко–комуникациската опрема со права различни од тие за кои е овластено.

(5)При вршење на проверката, Советот се грижи за примена на воспоставените правила за заштита на доверливоста и интегритетот на лозинките при нивно пријавување, доделување и чување.

(6)Информатичарот кој го администрира информацискиот систем е овластен да го доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко - комуникациската опрема врз основа на насоките на претседателот на Советот. Притоа, како критериум за авторизиран пристап до личните податоци и информатичко-комуникациската опрема, информатичарот се раководи од работното место на секое овластено лице, од што зависи и нивото на пристап до личните податоци што е задолжен да ги обработува.

Управување со медиуми ,уништување, бришење и чистење на медиуми

Член 20

(1)Со медиумите се овозможува идентификација и евидентирање на категориите на лични податоци и истите 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 СС на РМ.

(3)Уништувањето, бришењето и чистењето на медиумите е уредено со Правилникот за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 21

Постапката за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени е уредена со Правилникот за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци

Глава III. Средно ниво на технички и организациски мерки

Дополнителни правила за технички и организациони мерки

Член 22

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

Одговорно лице за заштита на личните податоци

Член 23

Советот 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 организационите мерки.

Контрола на информацискиот систем и информатичката инфраструктура

Член 24

(1)Информацискиот систем и информатичката инфраструктура на Советот 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)Надворешна контрола на информацискиот систем и информатичката инфраструктура на Советот се врши секои три години, а внатрешна контрола секоја година.

(3)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.

(4)Во извештајот од ставот (3) 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.

(5)Извештајот од ставот (3) на овој член се анализира од страна на Офицерот за заштита на личните податоци, кој доставува предлози на Советот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

(6)Извештајот од ставот (5) на овој член треба да биде достапен за увид на Дирекцијата за заштита на личните податоци.

Идентификација и проверка

Член 25

Советот воспоставува 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 авторизиран пристап

Член 26

(1) Советот 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. Оваа евиденција се чува најмалку 5 години.

(2)Во оваа евиденцијата 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, се контролираат од страна на одговорното лице за заштита на личните податоци и истите не може да се деактивираат.

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

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

Контрола на физички пристап

Член 27

Во документацијата за технички и организациони мерки Советот определува критериуми за овластените лица кои можат да имаат пристап до просториите каде е сместен информацискиот систем.

Управување со медиуми

Член 28

(1)Советот воспоставува систем за евидентираање 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 применi,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 став 1 на овој член , се применуваат и за евидентирање на медиумите кои се испраќаат од страна на Советот.

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

Евидентираање на инциденти

Член 29

(1)Советот во Правилата за пријавување,реакција и санирање на инциденти, 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 лични податоци кои се вратени и кои биле рачно внесени при враќањето.

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

Тестирање на информацискиот систем

Член 30

(1)Советот 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 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 31

Советот 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 32

Медиумите можат да се пренесуваат надвор од работните простории на Советот само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само административниот службеник-информатичар кој го администрира информацискиот систем може да ги декриптира или лице овластено од претседателот на советот.

Пренесување на личните податоци преку електронско комуникациска мрежа

Член 33

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. Ова се однесува на документи што содржат матичен број на граѓанинот или посебни категории на лични податоци.

.....

Глава IV -а.

РАЧНА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Основно ниво на техничи и организациски мерки

Примена

Член 34

Советот врши рачна обработка на личните податоци содржани во документите во хартиена форма. Тие се чуваат во физички заштитени ормани до кои имаат пристап само овластени лица .Плакарите, ормарите или друга опрема за чување на документи се сместени во простории кои имаат соодветни заштитни механизми. Просториите се заклучени и во периодот кога документите не се обработуваат од овластените лица.

Пристап до предмети и другите документи во хартиена форма

Член 35

Пристапот до документите во хартиена форма треба биде ограничен само на овластените лица во Советот преку механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува и за сите документи во хартиена форма кои што содржат лични податоци се применува основното ниво на технички и организациски мерки.

Правило „чисто биро“

Член 36

Во Советот задолжително се применува правилото „чисто биро“ при обработката на личните податоци содржани во документите, заради нивна заштита од пристап на неовластени лица, за време на целиот процес на обработка.

1.3 Чување на документи

Член 37

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Уништување на документи

Член 38

(1)Уништувањето на документите се врши во согласност со прописите за архивски материјал со ситнење или на друг начин, на начин што истите повторно да не можат да бидат употребливи.

(2) Во случајот од став 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 39

За документите во хартиена форма коишто содржат матичен број на граѓанинот, се применуваат дополнителни правила – средно ниво на технички и организациски мерки

Начин на чување на документите

Член 40

(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.

(2)Кога физичките карактеристики на просториите не дозволуваат примена на наведените мерки, Советот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

3. Високо ниво на технички и организациски мерки

Член 41

За документите во хартиена форма коишто содржат посебни категории на лични податоци се применуваат дополнителни правила – високо ниво на технички и организациски мерки.

Копирање или умножување на документите

Член 42

(1)Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување на Советот.

(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 43

Во случај на физички пренос на документи, Советот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат.

V.ЗАВРШНИ ОДРЕДБИ

Член 44

Овој правилник влегува во сила на денот на неговото донесување.

СУДСКИ СОВЕТ
НА РЕПУБЛИКА МАКЕДОНИЈА
Претседател,
Зоран Караџовски

Прилог 1

Врз основа на член 14 став 4 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија" бр. 38/09 и 158/10) и член 7 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на Судскиот совет на Република Македонија, поднесувам

И З Ј А В А
за обезбедување тајност и заштита на обработката на личните податоци

Јас долупотпишаниот/та, ----------
- _____.
име и презиме)

(вработен-а во Судски совет на Република Македонија на работно место со звање _____
_____
изјавувам дека:

- ќе ги почитувам начелата за заштита на личните податоци;
- ќе вршам обработка на личните податоци според упатствата добиени од Судскиот совет на Република Македонија кој согласно Законот за заштита на личните податоци се јавува во својство на контролор на лични податоци;
- ќе се придржувам кон документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци усвоена од страна на Судскиот совет на Република Македонија;
- ќе ја чувам тајноста на личните податоци кои што ќе ги обработувам;
- ќе ги чувам како доверливи мерките за заштита на личните податоци.

Датум, Изјавил,

_____

(потпис)

Прилог 2 – од Упатството и Правилникот за технички и организациски мерки на ДЗЛП

I. Целосно и делумно автоматизирана обработка на личните податоци[1]

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 (член 17)			

[1] Во извешатајот се посочени членови од Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на Дирекцијата за заштита на личните податоци („Службен весник на Република Македонија“ бр.28/09 и 158/10)

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 (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 обработка на лични податоци што се дел од посебна збирка на лични податоци или се намети 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	Идентификација и проверка (член 17)			
Основно	Контрола на пристап (член 18)			
Основно	Чување на документи (член 35-б)			
Основно	Уништување на документи (член 35-в)			
Средно	Дополнителни правила за технички и организациски мерки (член 23)			
Средно	Контрола на информацискиот систем и информатичката инфраструктура (член 25)			
Средно	Примена на правилото „чисто биро“ (член 35-д)			
Високо	Начин на чување на документите (член 35 - ѓ)			
Високо	Копирање или умножување на документите (член 35 - е)			

Високо	Пристап до 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

_____
_____
_____
_____
_____
_____

_____, _____, 20_____ година
(место) (датум)

М.П. _____(потпис на одговорното лице)

_____