ЗАНАЕТЧИСКА КОМОРА СКОПЈЕ
Бр. 0202-181/12
04.12.2025 год.
СКОПЈЕ

Во врска: Работ. знак: 0202-181/12
Рок на чување: трајно
04.12.2025 год.
СКОПЈЕ

Врз основа на член од Статутот (бр.0101-343/14 од 06.07.2016 година), а во врска со член 66 став 6 од Законот за заштита на личните податоци (Службен весник на РСМ, бр. 42/20 и 294/21) и Правилникот за безбедност на обработката на личните податоци (Сл. весник бр. 266/2024), Управниот одбор на Занаетчиска комора Скопје на одржаната седница на ден 03.12.2025 година, донесе:

ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ ВО ЗАНАЕТЧИСКА КОМОРА СКОПЈЕ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој Правилник се утврдуваат техничките и организациските мерки за обезбедување тајност и заштита при обработката на личните податоци, согласно Законот за заштита на личните податоци и Правилникот за безбедност на обработката на личните податоци (Сл. весник бр. 266/2024) што се применуваат во Занаетчиска комора Скопје“(во натамошниот текст: комора).

Член 2

Одредбите од овој правилник се применуваат за:
- целосно и делумно автоматизирана обработка на личните податоци;
- 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;
- обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Категориите на лични податоци кои се обработуваат се:

1. ***Евиденција на занаетчии и вршители на занаетчиска дејност***
   - Име и презиме
   - Адреса
   - Ден, месец и година на раѓање
   - ЕМБГ
   - Име на родител

2. ***Евиденција на вработени***
   - Име и презиме на вработениот
   - Единствен матичен број на вработениот
   - Адреса на живеење
   - Извод од државјанство
   - Дипломи и уверенија за стекнато образование

3. ***Евиденција на плати на вработени***
   - Име и презиме
   - Број на лична карта
   - Матичен број
   - Адреса
   - Број на трансакциона сметка
   - Износ на месечни приходи

Член 3

Комората ќе применува технички и организациски мерки кои се класифицираат во три нивоа:
- основно ниво
- средно ниво и
- високо ниво.

Член 4

За сите документи задолжително ќе се применуваат технички и организациски мерки класифицирани на основно ниво.

За документи кои содржат матичен број на граѓанинот задолжително се применуваат техничките и организациските кои се класифицираат на основно и средно ниво.

За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на личните податоци и/или матичен број на граѓанинот задолжително се применуваат техничките организациските мерки кои се класифицираат на основно, средно и високо ниво

II. СИСТЕМ ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ

Член 5

Комората воспоставува и одржува систем за заштита на лични податоци, кој вклучува политики, процедури, насоки и работни упатства. Системот е усогласен со обемот, природата и сложеноста на обработката и ризиците по правата и слободите на субјектите на податоци.

Член 6

Комората:
- определува цели на обработка;
- идентификува и опишува информациски систем;
- обезбедува документација со опис на технички/организациски мерки;
- води евиденција за обработка;
- ги утврдува релациите со други системи и активности;
- врши проценка на ризик согласно Методологијата за проценка (Прилог 1).

III. УПРАВУВАЊЕ СО РИЗИК

Член 7

Комората спроведува процес на управување со ризик кој опфаќа:

1. Преглед на информацискиот систем (системи, услуги, податоци);
2. Проценка на ризици (идентификација на влијанија, закани, извори на ризик, носители);
3. Спроведување и проверка на мерки;
4. Периодични безбедносни проверки и акциски планови.

Проценката на ризик ги разгледува следниве цели: минимизација, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање. Ризиците се проценуваат по веројатност, влијание и сериозност.

IV. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 8

Комората обезбедува мерки во три нивоа: основно, средно и високо. Изборот зависи од категоријата на податоци и начинот на обработка.

Мерките вклучуваат:

- Автентикација на корисници (корисничко име, лозинка);
- Ограничен пристап и логирање на пристапи;
- Автоматско одјавување;
- Антивирусна, анти-спам, фајервол заштита;
- Физичка заштита на сервери;
- Бекап, архивирање, криптирање;
- Едукација и изјави за тајност.

Член 9

Комората врши евидентирање и ја чува целокупната документација за за обработка на личните податоци и сите негови промени.

Член 10

Регистраторот за занаетчискиот регистар во комората за запишување на податоците во регистарот согласно документацијата за техничките и организациските мерки.

Член 11

Во комората се обезбедуваат следните технички мерки за тајност и заштита при обработката на личните податоци:

1. Единствено корисничко име за секој вработен;
2. Лозинка креирана за секој вработен посебно, составена од комбинација на најмалку 8 (осум) алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. Автоматизирано одјавување од информацискиот систем после изминување на 15 минути на неактивност и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинка;
4. 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;

5. Автоматизирано отфрлање од информативниот систем после три неуспешни обиди (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на корисникот дека треба да побара инструкции од администраторот на информацискиот систем;
6. Инсталирана е хардверска/софтверска заштита мрежна бариера ("фајервол"), како и рутер помеѓу информацискиот систем и интерна конекција;
7. Инсталирана е ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем заштита, која постојано ќе се ажурира заради превентивна од непознати и непланирани закани од нови вируси и спајвери;
8. Инсталирана е ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и
9. Серверите во комора се приклучени на енергетска мрежа преку уред за непрекинато напојување.

Член 12

Документите кои содржат лични податоци по истекот на рокот на чување согласно прописите за архивска граѓа се уништуваат. Документите во хартиена форма кои содржат лични податоци по истекот на рокот на нивното чување се уништуваат со горење на документацијата при што истите повторно не можат да бидат употребливи и читливи.

Личните податоци на вработените во коморато како и личните податоци на учениците во секое време се чуваат во заклучени шкафови и пристап до нив имаат вработените кои се овластени за водење на тековните работи согласно Правилниците за систематизирање и оранизација на работните места во коморато.

Вработеното лице кое ги врши работите за човечки ресурси во комората, го известува администраторот на информацискиот систем за вработување или ангажирањето на корисник со право на пристап до информацискиот систем, за да му биде доделено корисничкото име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката.

Член 13

Серверите кои содржат лични податоци се физички лоцирани и хостирани во комората во посебна просторија до која пристап има само наставникот по информатика кој е задолжен за одржување на информацискиот систем.

Доколку е потребен пристап на друго лице до просторијата во кои се наоѓаат серверите, тогаш тоа лице треба да биде придружувано и надгледувано од наставникот од ставот 1 на овој член.

За просторијата во која се наоѓаат серверите се преземаат мерки за заштита од потенцијални закани како што се кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Член 14

Лицата кои се вработуваат или се ангажираат во коморато пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со документацијата за техничките и организациските мерки.

За лицата кои се ангажираат за извршување на работа во коморато во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

Комората пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

Лицата кои се вработуваат или ангажираат во комората, пред нивното отпочнување со работа своерачно потпишуваат Изјава за тајност и заштита на обработка на личните податоци.

Изјавата на тајност и заштита на обработка на личните податоци 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 документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на коморато, освен ако со закон поинаку не е уредено и дека истите ќе ги чуваат како доверливи лични податоци .

Изјавата за тајност и заштита на обработката на личните податоци задолжително се чува во персоналните досиеја на лицата кои се вработуваат или ангажираат.

Изјавата за тајност и заштита на обработката на личните податоци е составен дел од овој правилник (прилог 2).

Официрот за заштита на личните податоци задолжително врши континуирано информирање на вработените за непосредните обврски и одговорности за заштита на личните податоци.

Член 15

Пристап до документите во хартиена форма кои содржат лични податоци имаат вработените во комората и други овластени лица во согласност со работните должности утврдени во Правилниците за систематизација и организација на работните места во коморато.

За пристапувањето до документите задолжително се воспоставуваат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува, како и за пристапот на другите лица до документите.

Овластените лица во коморато задолжително го применуваат правилото „чисто биро„ при обработка на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап.

Копирањето и умножувањето на документите го вршат единствено вработените лица во коморато согласно овластувањата во Правилниците за систематизација и организација на работните места во коморато.

За документите кои се пренесуваат надвор од работните простории на коморато задолжително се применуваат соодветни мерки така што личните податоци содржани во истите нема да бидат видливи и достапни за трети лица или други неовластени лица.

Член 16

Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и 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.

Член 17

Начинот на евидентирање на секој инцидент, времето кога се појавил, корисникот кој го пријавил, на кого е пријавен и превземените мери се уредени со Правилата за пријавување, реакција и санирање на инциденти.

Член 18

Постапките и процедурите за управувањето, уништувањето како и за бришењето или чистењето на медиумот се определни со Правила на начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.

Член 19

Постапките и процедурите за правење на сигурности копии како и начинот на чување се регулирани во Правила за начинот на правење на сигурносна копија,архивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Член 20

Комората врши надворешна контрола на секои три години и внатрешна контрола секоја година на информатичкиот систем и информатичката структура во комората согласно прописите за заштита на личните податоци.

Надворешната конторла се врши од страна на независно трето правно лице.

Член 22

Личните податоци кои ќе се пренесуваат преку електронско комуникациска мрежа од комората до Управата за јавни приходи, а кои содржат и единствен матичен број на вработените во комората се криптирани односно заштитени со соодветни мерки кои гарантираат дека податоците нема да бидат читливи при преносот.

V. ЗАВРШНА ОДРЕДБА

Член 23

Со денот на влегувањето во сила на овој Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци во ЗКСкопје престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци во ЗКСкопје“ Скопје 0302-144/1 од 04.08.2021 година

Член 24

Овој правилник влегува во сила со денот на неговото донесување и се применува од 10 декември 2025 година.

Претседател на
Занаетчиска комора Скопје
Горан Ристовски

Прилог 1

МЕТОДОЛОГИЈА ЗА ПРОЦЕНКА НА РИЗИК

Контролор: Занаетчиска комора Скопје

Вовед

Една од клучните обврски која произлегува од Законот за заштита на личните податоци (во натамошниот текст „ЗЗЛП“) е обезебедување на безбедноста на обработката на личните податоци. Имено, согласно ЗЗЛП безбедноста подеднакво ги опфаќа минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање [1] на личните податоци, и истите треба да се согледуваат од пристап базиран на ризик, при што од нивото на ризик зависи и сетот на технички и организациски мерки кои контролорот мора да ги преземе за да управува со ризикот.

Опфат и цел

Целта на оваа анализа е да овозможи идентификација и проценка на безбедносните ризици на сите активности за обработка на личните податоци кај контролорот Занаетчиска комора Скопје. Ова анализа се користи и за утврдување на нивото на ризикот при појавување на безбедносни инциденти, при што Тимот за одговор на безбедносни инциденти е должен да го утврди нивото на ризик во согласност со оваа анализа на ризик и методологијата за управување со ризици.
Оваа анализа има за цел да овозможи:

- едноставен пристап кој овозможува разбирање на контекстот на активностите на обработка на личните податоци и последователно да се проценат поврзаните безбедносни ризици,
- предлагање на соодветни организациски и технички мерки за безбедност на личните податоци, а кои се соодветни на утврдениот ризик.

Управување со ризици на активностите на обработка на личните податоци

Анализата на ризик и управувањето со безбедносните ризици е од суштинско значење за безбедноста на обработка на личните податоци, што води кон донесување на соодветни безбедносни мерки.

Во контекст на оваа анализа:
Поимот влијание се дефинира како влијание во однос на слободите и правата на поединците. Односно, анализата на влијанието е насочена кон можните негативни ефекти што може да ги претрпи поединецот, како што е кражба на идентитет, измама, финансиска загуба, физичка или психолошка штета, понижување, оштетување на угледот, дискриминација, закана по живот. Иако еден од критериумите на мерење претставува и бројот на засегнати лица, во одредени случаи тоа може да не е релевантно, бидејќи влијанието може да донесе сериозни негативни последици и само за едно лице.

---

[1] минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање, како главни столбови на безбедноста на личните податоци, се дефинирани во член 2 од Правилникот за безбедност на обработката на личните податоци.

Процедурата за управувањето со ризици е составена од четири фази и тоа:

- Анализа на ризик – ни дава слика за тековните ризици за безбедноста на податоците. Ризикот се дефинира како веројатност да се појави негативен исход (закана) помножена со влијанието на негативниот исход (доколку се појави). Анализата на ризикот почнува со идентификација на ризици, проследено со одредување на релеватната веројатност на појавување и влијанието на секоја закана. За правилно оценување на ризикот, мора подеднакво да се земат предвид веројатноста и влијанието на заканата.
- Третман на ризик – врз основа на оценката на ризикот, во оваа фаза контролорот избира соодветни безбедносни мерки за третирање на ризиците. Мерките може да имаат различни ефекти, како што се: ублажување, пренос, избегнување, бришење. За третирање на ризиците треба да се користат повеќе видови на безбедносни мерки.
- Прифаќање на ризици – дури и кога ризиците се управувани, можно е ризикот до одредено ниво да остане. Овие ризици кои не се класифицирани како висок ризик, може да се сметаат за прифатливи, а таа одлука ја носи менаџментот.
- Комуникација на ризици – сите засегнати страни треба да бидат информирани за усвоените контроли на ризици како и за прифатените ризици.

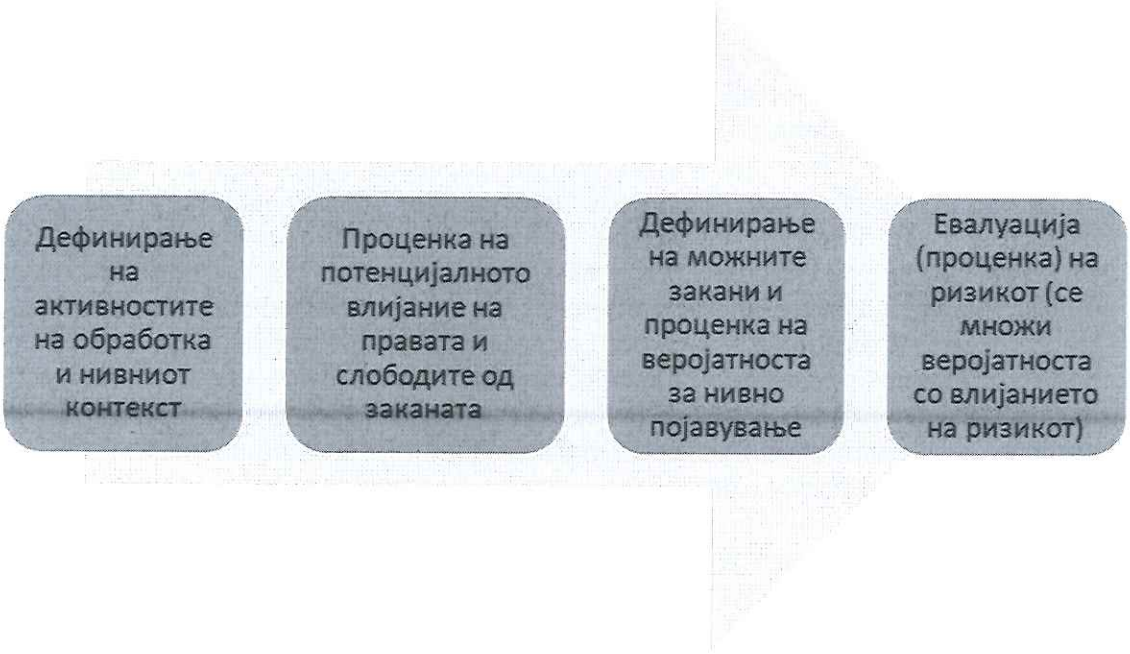
При управување со безбедносни ризици многу е битно да се дефинира општиот контекст на обработката (т.е. категории на личните податоци, цел на обработка, примачи на податоците...), што понатаму ќе води кон дефинирање на можните закани и ризици врз основа на влијанието на поединците.

Слика 1: фази на управување со ризици

Како што може да се види на слика 1, процедурата за управување со ризици започнува во прва фаза со дефинирање на контекстот на личните податоци, врз основа на што понатаму се дефинираат ризиците, истите се проценуваат и врз основа на проценката се дефинираат соодветни технички и организациски мерки, а во завршната фаза се применуваат и се мониторираат мерките што се преземени со цел да се согледа нивната ефикасност.

Анализирање на безбедносните ризици на активностите за обработка на личните податоци

Анализирањето на безбедносните ризици се заснова на четири чекори и тоа:



1. *Прв чекор* – Дефинирање на активностите на обработка и нивниот контекст

Првиот чекор е почетната точка на оваа анализа и од суштинско значење за успешно извршена анализа е да се дефинира опфатот на системот за обработка на личните податоци и неговиот релевантен контекст. Во овој чекор, контролорот мора да ги земе предвид различните фази на обработка на личните податоци, како што се собирање, складирање, чување, употреба, отстранување, итн., како и нивните последователни параметри.

Во оваа фаза при вршење на анализата треба да одговориме најмалку на следниве прашања:

а) За која активност на обработка станува збор?

Во оваа фаза се дефинира дека анализа на ризик се врши за секоја активност на обработка на личните податоци, без разлика што тие се обработуваат преку истите технички средства (ИТ мрежа, системи, апликации). При вршење на анализата на ризик треба да се има предвид

дека активностите на обработка вклучуваат различни податоци од различна категорија на чувствителност и на тој начин претставуваат различни нивоа на ризици спрема субјектот на личните податоци.

b) Кои категории на лични податоци се обработуваат?

Директно поврзано со првото прашање, категориите на личните податоци кои се обработуваат, од една страна ни помагаат при дефинирање на активноста на обработката, а од друга страна ни даваат почетна индикација за можното ниво на ризик.

c) Која е целта на обработка?

Целта на обработка, исто така, е директно поврзана со активноста на обработка и му помага на контролорот да ја дефинира обемноста на обработка на личните податоци (тука мора да се има предвид кој добива пристап до податоците, начинот на кој се обезбедува пристап итн.). Во текот на проценката на ризикот е неопходно да се разликуваат активностите на обработка на податоци врз основа на целта на обработка, дури и кога се работи за обработка на иста категорија на лични податоци.

d) Кои средства се користат за обработка на личните податоци?

Активностите на обработка на личните податоци можат да се вршат на автоматизиран или неавтоматизиран начин, односно хартиена обработка на личните податоци, или пак и на двата начина. Кај автоматизираниот начин се вклучени, пред се, информатичка инфраструктура, системи, апликации или пак рачна обработка на податоци. При вршење на анализата е многу битно добро да се дефинираат и сфатат средствата со кои се врши обработка на податоците, имајќи го предвид фактот дека истите може да се менуваат во различни фази на обработката (собирање, складирање, употреба, пренос, уништување на податоци).

e) Каде се врши обработка на личните податоци (локација)?

Локацијата каде се врши обработка на личните податоци е многу важен фактор при утврдување на ризикот. Доколку личните податоци се пренесуваат во трета земја, дополнителни мерки за заштита треба да бидат преземени согласно ЗЗЛП. Ова посебно треба да се има предвид кога се ангажира обработувач на личните податоци.

f) Кои се категориите на субјектите на личните податоци?

Категориите на субјектите на личните податоци треба да бидат јасно и недвосмислено дефинирани, со цел подобро разбирање на активностите за обработка. Треба да се има предвид дека во одредени случаи категоријата на субјектите на личните податоци може да биде индикатор за потенцијално ниво на ризик кое може да се утврди уште во оваа прва фаза (на пример, обработка на податоци за деца).

g) Кои се примателите на личните податоци?

Дефинирањето на примателите на личните податоци е со цел да се разбере преносот на личните податоци, како и условите при преносот на податоци. Одредени преноси на податоци може да сносат одредено ниво на ризик кое контролорот треба да го утврди уште во оваа фаза на анализата.

Наспроти сите овие прашања, како главен елемент кој мора да се има предвид е правниот основ за обработка на личните податоци, кој мора да биде добро утврден уште пред започнување на оваа анализа, а со анализата дополнително да се провери.

2. *Втор чекор* – Проценка на потенцијалното влијание над правата и слободите на поединците

Во овој чекор, контролорот треба да го процени потенцијалното влијание што заканата може да го има над правата и слободите на поединецот. Заканата може да биде поврзана со било кое нарушување на доверливоста, интегритетот или достапноста на личните податоци.

- *Ниво на влијание*

Ниво на влијание	*Опис*
ниско	Субјектот може да наиде на мали непријатности, кои ќе бидат надминати без никаков проблем (време изгубено за повторно внесување на податоци, нервози, иритации, и друго)
средно	Субјектите може да наидат на значителни непријатности, кои ќе можат да бидат надминати и покрај неколкуте потешкотии (дополнителни трошоци, одбивање на пристап до деловни услуги, страв, недостаток на разбирање, стрес, итн.)
високо	Субјектите може да наидат на значајни последици, кои би требало да бидат способни да ги надминат, иако со сериозни потешкотии (злоупотреба на средствата, црна листа од финансиски институции, оштетување на имотот, губење работа, влошување на здравјето)
Многу високо	Субјектите може да наидат на значајни, па дури и неповратни последици, кои можеби нема да ги надминат (неспособност за работа, долгорочни психолошки или физички заболувања, итн.)

Табела 1- опис на нивоа на влијание

- *Како да се процени влијанието*

Проценката на влијанието може да се направи само во квалитативни параметри, имајќи ја предвид конкретната активност на обработка на личните податоци.

Параметрите кои треба да бидат внимателно земени предвид се:

- Категории на лични податоци: Овој параметар, по природа, може веднаш да го намали нивото на влијанието, врз основа на чувствителноста на податоците. На пример, кога податоците вкулучуваат медицински досиеја или информации за политички убедувања (или други посебни категории на лични податоци), влијанието на нарушување на безбедноста може да биде сериозно за поединците. Сепак, мора да се има предвид дека проценката не може да се базира само на разликување на податоците помеѓу посебни категории на лични податоци и „обични“ категории на лични податоци. И

личните податоци кои не спаѓаат во посебни категории на лични податоци можат да откријат многу критични податоци за субјектот (на пример: локација, навики, финансиски информации) и, на тој начин, да причинат катастрофални ефекти врз субјектот во случај на нарушување.

- Критичноста на активноста за обработка на личните податоци: со овој параметар е важно да се процени целокупната критичност на обработката. Посебно внимание треба да се посвети на обработката на личните податоци кои се базираат или може да доведат до систематско следење или надзор над поединци.
- Обем на обработени лични податоци: овој параметар се однесува на обемот на личните податоци кои се обработуваат за еден поединец: колку повеќе податоци, толку повеќе потенцијални негативни ефекти. Обемот треба да се земе предвид и во однос на времето (на пример, иста категорија на лични податоци во одреден временски период) и содржината (дополнување на податоци од иста категорија на лични податоци).
- Посебните карактеристики на контролорот: овој параметар се однесува на полето на работа и деловните активности на контролорот, што може да откријат дополнителни информации за одредена категорија на лични податоци.
- Посебните карактеристики на субјектите на личните податоци: влијанието, исто така, може да се зголеми во случај субјектите на личните податоци да спаѓаат во одредена група (ранливи категории, малолетници, итн.).

Покрај параметрите споменети погоре, друг важен аспект што треба да се земе предвид е препознатливоста на субјектите на личните податоци, односно колку е лесно за корисникот кој има пристап до сетот на податоци да го идентификува субјектот на личните податоци. Во таа насока, битно е да се земат предвид техничките мерки што би можеле да ја намалат препознатливоста на субјектот (на пример, енкрипција), со што се намалува можноста за неовластено откривање на личните податоци.

Додека се оценува влијанието, треба се земат предвид и можните секундарни ефекти врз правата и слободите на поединците.

- *Проценка на влијанието*

Проценка на влијанието се врши врз основа на анализата од претходната секција и нивоата на влијание во табела 1. Како што може да се види во табела број 2, влијанието треба да биде проценето одвоено за доверливоста, интегритетот и достапноста. Многу е важно да се имаат предвид сите случаи на неовластено откривање, промена или уништување на податоците и да се изврши проценка врз основа на најлошото можно сценарио.

бр.	Прашање	Проценка
1	Влијанието што неовластеното откривање може да го има врз личните податоци на поединецот (губење доверливост) – во контекст на деловната активност – и впишете соодветно проценка Примери на губење доверливост - Досие со документи или лаптоп е изгубен	☐Ниско ☐Средно ☐Високо ☐Многу високо

бр.	Прашање	Проценка
	при пренесување - Опремата е фрлена без да се уништат податоците - Личните податоци се погрешно испратени до неовластени примателиКлиенти можат да пристапат до туѓи податоци - Личните податоци се објавуваат преку интеренет, или на друг начин се прават достапни - Усб со личните податоци е украден од просториите - Погрешно конфигурирана веб-страница ги прави јавно достапни податоците на интерент од внатрешните корисници	
2	Влијанието што неовластеното менување на податоците може да го има врз личните податоци на поединецот (губење на интегритет) – во контекст на деловната активност – и впишете соодветна проценка Примери на губење на интегритет - Регистрацијата која е неопходна за добивање на одредена онлајн услуга претпела неовластена промена и поединците мора да ја побараат услугата офлајн - Податоците кои се битни за точноста на податоците на субјектите на личните податоци се сменети.	☐Ниско ☐Средно ☐Високо ☐Многу високо
3	Влијанието што неовластеното уништување или губење на личните податоци може да го има врз личните податоци на поединецот (губење на достапноста) - во контекст на деловната активност – и впишете соодветна проценка Примери за губење на достапноста - Датабазата со личните податоците е компромитирана и потребно е преземаање на активности за врќање на податоците на интернет, - Досието на вработениот е изгубено и поединецот мора да ги достави податоците повторно кај контролорот, - Датотека/датабаза е корумпирана и нема копија (back-up) од истите податоци, односно нема начин за враќање на податоците - Критичен сервис е во прекин е не може брзо да се врати во функција.	☐Ниско ☐Средно ☐Високо ☐Многу високо

Табела 2: прашања за проценка на влијанието

По спроведување на гореспоменатата проценка, можно е да се добијат три различни нивоа на влијание. Највисокото од овие нивоа треба да се смета за конечен резултат на влијанието, поврзано со целокупната обработка на личните податоци.

3. *Трет чекор* – дефинирање на можните закани и проценка на веројатноста за нивно појавување

Во овој чекор, единствена цел ни е да ги дефинираме и разбереме заканите за целокупната обработка на личните податоци кај контролорот (внатрешни и надворешни) и да ја процениме веројатноста за нивно појавување (веројатноста за појавување на закана).

Оваа проценка се врши во четири главни области, и тоа:

- Средства на контролорот (хардвер и софтвер)
- Постапки/процедури поврзани со обработката на личните податоци
- Различни страни и поединци вклучени во обработката на личните податоци
- Деловниот процес и обемот на обработка.

Табела 3 подолу ги сумира прашањата поврзани со проценката на веројатноста за појава на закана.

А) средства на контролорот (хардвер и софтвер)		
1.	Дали некој дел од обработката на личните податоци се врши преку интернет?	Кога обработката на личните податоци се изведува целосно или делумно преку интернет, се зголемуваат можните закани од надворешни напаѓачи преку интернет, особено кога услугата е достапна за сите корсиници на интернет.
2.	Дали е овозможено да се пристапи до внатрешниот систем за обработка на личните податоци преку интернет?	Кога се обезедува пристап до внатрешен систем преку интернет, веројатноста за надворешни закани се зголемува. Во исто време се зголемува и веројатноста за случајна или намерна злоупотреба од страна на корисниците.
3.	Дали системот за обработка на личните податоци е поврзан со друг внатрешен или надворешен ИТ систем или услуга?	Поврзување со надворешни ИТ системи може да доведе до дополнителни закани поради ризиците и потенцијалните безбедносни пропусти кои се својствени

		за тие системи. Истото важи и за внатрешните системи, имајќи предвид дека ако не се соодветно конфигурирани, таквите врски може да овозможат пристап до личните податоци на повеќе лица кај контролорот.
4.	Дали неовластени лица можат лесно да пристапат до средствата за обработка на личните податоци?	Иако фокусот е ставен на електронските системи и услуги, физичката безбедност е важен аспект, кој доколку не е соодветно заштитен, може сериозно да ја загрози безбедноста.
5.	Дали системот за обработка на личните податоци е дизајниран, имплементиран или одржуван без да се следат најдобрите практики?	Лошо дизајнираните, имплементирани и/или одржувани хардверски и софтверски компоненти може да претставуваат сериозни ризици за безбедноста на личните податоци. За таа цел, најдобрите практики го акумулираат искуството од претходните настани и може да се сметаат за практични упатства како да се избегне изложување и да се постигнат одредени нивоа на издржливост.
Б) Постапки/процедури поврзани со обработка на личните податоци		
6.	Дали улогите и одговорностите на вработените за заштита на личните податоци се нејасни или не се јасно дефинирани?	Во случај кога улогите и одговорностите не се јасно дефинирани, пристапот па и другиот вид на обработка на личните податоци може да биде неконтролиран, што може да резултира со неовластено пристапување и користење на ресурсите и загрозување на целокупната безбедност на системот.
7.	Дали е јасно дефинирана употребата на интернет, системот и физичките ресурси кај самиот контролор?	Кога употребата на ресурсите не е јасно дефинирана, може да настанат безбедносни закани поради недоразбирање или намерна злоупотреба. Јасната

		дефиниција за мрежна инфраструктура, информатичкиот систем и физичките ресурси може да ги намали потенцијалните ризици.
8.	Дали на вработените им е дозволено да користат свои медиуми (усб, лаптоп...) за да се поврзат со системот за заштита на личните податоци?	Вработените што ги користат нивните лични уреди во рамки на контролорот може да го зголемат ризикот од истекување на податоци или неовластен пристап до информатичкиот систем. Покрај тоа, бидејќи уредите не се централно контролорирани, тие може да доведат вируси и други закани во системот.
9.	Дали на вработените им е дозволено да пренесуваат, складираат или на друг начин да ги обработуваат личните податоци надвор од просториите на контролорот?	Обработката на личните податоци надвор од просториите на контролорот може да понуди поголема флескибилност, но во исто време воведува дополнителни ризици, посебно со пренесување на податоци преку несигурни мрежи (пр. отворени WI-FI мрежи) и со тоа се зголемува ризикот од неовластен пристап и употреба на овие податоци.
10.	Дали е возможно да се обработат личните податоци без притоа за истото да се зачува лог (запис)?	Недостаток на соодветни механизми за мониторирање и запишување на логови може да ја зголеми злоупотребата на процесите/процедурите и ресурсите, што резултира со злупотреба на личните податоци.
В) Различни страни и поединци вклучени во обработката на личните податоци		
11.	Дали обработката на личните податоци се врши од недефиниран број на вработени?	Кога пристапот (и понатамошната обработка) на личните податоци е отворен за голем број на вработени, се зголемуваат можностите за злоупотреба од човечки фактор. Јасно дефинирање на пристап до

		личните податоци и ограничување на пристапот само на тие лица може да придонесе за безбедноста на личните податоци.
12.	Дали некој дел од активностите на обработка на личните податоци се врши од трета страна (обработувач)?	Кога обработката се врши од страна на обработувачи, контролорот може делумно да ја загуби контролата врз овие податоци. Контролорот мора да подготви соодветна процедура за избор на обработувачи, кои можат да понудат високо ниво на безбедност и јасно да се дефинира кој дел од обработката им е доделен, одржувајќи колку што е можно повисоко ниво на контрола.
13.	Дали страните/поединците кои се вклучени во обработката на личните податоци се јасно информирани за нивните обврски?	Кога вработените не се јасно информирани за нивните обврски, заканите од случајна злоупотреба, како што се откривање или уништување на податоците значително се зголемуваат.
14.	Дали вработените кои се вклучени во обработката на личните податоци се обучени, односно имаат знаење од областа на осигурување на безбедност на активностите на обработка?	Кога вработените не се свесни за потребата од примената на безбедносни мерки, тие случајно можат да претставуваат дополнителни закани за системот. Обуката во голема мера ќе придонесе за освестување на вработените, како за нивнтие обврски за заштита на личните пдоатоци, така и за примена на специфични мерки.
15.	Дали страните/поединците кои се вклучени во обработката на личните податоци го занемаруваат безбедното складирање/чување на податоците, како и уништувањето на личните податоци?	Многу нарушувања на личните податоци се случуваат поради недостаток на мерки за физичка заштита, како што се брави и безбедносни системи за уништување. Датотеките базирани на хартија обично се дел од влезот или излезот на

Слика 2: Конечна евалуација (проценка) на ризик

Матрицата на ризик прикажана во табела 6 подолу се пополнува врз основа на најлошото можно влијание (највисоко влијание врз поединецот). Следствено на тоа, нивото на влијание е проценето на ниво повисоко од нивото на можната појава на заканата, и само две полиња се предвидени за низок ризик, две за среден ризик, високиот и многу високиот ризик се споени во едно и завземаат четири полиња обоени со црвено.

Табела 6 Евалуација (проценка на ризик)

Независно од резултатот добиен од извршената анализа на ризик, конторлорот може слободно да го приспособи добиеното ниво на ризик, земјќи ги предвид специфичните карактеристики на активноста на обработката на личните податоци и секако документирање и обезбедување на соодветната оправданост за ова приспособување.

5. *Петти чекор* – Технички и организациски мерки за заштита на обработката на личните податоци

По оценување на нивото на ризик, контролорот треба да предложи соодветни безбедносни мерки за заштита на личните податоци. Безбедносните мерки се поделени во две категории и тоа технички и организациски мерки. Безбедносните мерки треба да бидат во корелација со Правилникот за безбедност на обработката на личните податоци (Сл. весник бр. 266/2024).

Прилог 2 - Изјава за обезбедување тајност и заштита на обработката на личните податоци Врз основа на одредбите од Законот за заштита на личните податоци (Службен весник на Република Северна Македонија бр 42/2020) и член 31 став (4) од Правилникот за безбедност на обработката на личните податоци (Службен весник на РСМ бр. 266/2024).
на 04.12.2025 година, ја давам следната

И З Ј А В А

за обезбедување тајност и заштита на обработката ка личните податоци

Јас долупотпишаниот/ната, _____ (име и презиме), _____
(работно место), во Занаетчиска комора Скопје“, согласно со Правилникот за безбедност на обработката на личните податоци и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во Занаетчиска комора Скопје се обврзувам дека:

- ќе ги почитувам начелата за заштита на личните податоци;
- ќе ги применувам техничките и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци и ќе ги чувам како доверливи личните податоци. како и мерките за нивна заштита:
- ќе вршам обработка на личните податоци согласно упатствата добиени од Занаетчиска комора Скопје“;
- на трети лица надвор од Занаетчиска комора Скопје“ и на други лица од Занаетчиска комора Скопје нема да издавам каков било податок од збирките на лични податоци или каков било друг личен податок кој ми е достапен и кој сум го дознал/а или ќе го дознаам при вршењето на работата, освен ако со закон не е предвидено поинаку.

Потпис: