ИНДУСТРИЈСКА БЕЗБЕДНОСТ

- СКРИПТА -

www.nsa.gov.rs

Београд, 2024. године

С А Д Р Ж А Ј

НЕОПХОДНИ КОРАЦИ

*за у**спостављање одговарајућег нивоа Система заштите тајних података у правном лицу (организациона безбедност)*

1. Процена стања и безбедности
2. Доношење нормативе за рад са тајним подацима
3. Израда Упутства о мерама заштите тајних података и одређивање одговорног лица задуженог за спровођење мера заштите
4. Процес сертификације правног лица и акредитација простора, опреме и процедура (акредитацију спроводи Канцеларија Савета за националну безбедност и заштиту тајних података), сертификација законског заступника наведеног правног лица и конкретних запослених за које постоји потреба приступа тајним подацима
5. Успостављање општих и посебних мера заштите тајних података
6. Инспекцијски надзор Министарства правде

НЕОПХОДНИ КОРАЦИ

за добијање сертификата правних лица

1. Формално писмо-обраћање правног лица органу јавне власти о намери учешћа на набавци која садржи тајне податке
2. Састанак са представницима органа јавне власти око безбедносних питања пре покретања поступка
3. Попуњавање одговарајућих безбедносних упитника за физичка лица и за правно лице
4. Прослеђивање безбедносних упитника за физичка лица и за правно лице органу јавне власти
5. Достављање безбедносног упитника са захтевом органа јавне власти Канцеларији Савета за националну безбедност и заштиту тајних података на даљи поступак
6. Припремни састанак законског заступника правног лица са Канцеларијом Савета за националну безбедност и заштиту тајних података око поступка издавања сертификата правном лицу
7. Покретање поступка безбедносне провере
8. Доношење решења за физичка лица
9. Акредитација простора, опреме и организационих услова за чување тајних података
10. Издавање сертификата правном лицу

ПРИРУЧНИЦИ И СКРИПТЕ:

1. **ОСНОВЕ ОБРАДЕ И ЗАШТИТЕ ПОДАТАКА** (https://nsa.gov.rs/extfile/sr/1424/Osnove_obrade_i_zastite_podataka-prirucnik.pdf)
2. **СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА** (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf)
3. **ПОСТУПАК ИЗДАВАЊА БЕЗБЕДНОСНОГ СЕРТИФИКАТА** (https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja__BS-skripta.pdf)
4. **УМАЊИВАЊЕ ИНСАЈДЕРСКЕ ПРЕТЊЕ** (https://nsa.gov.rs/extfile/sr/1485/Umanjivanje_insajderske_pretnje-skripta_.pdf)

1. Појам органа јавне власти и правног лица у смислу Закона о тајности података

Законом о тајности података (чл. 2. т. 7. наведеног закона) утврђено је да је „**орган јавне власти** државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује». **Појам правног лица** у смислу поступања са тајним подацима негативно се одређује, на посредан начин, у односу на наведени појам органа јавне власти; чиме се закључује да је правно лице у смислу позитивноправних одредби о заштити тајних података у Републици Србији свако правно лице које нема статус органа јавне власти, а које има потребу да поступа са тајним подацима Републике Србије или страним тајним подацима. Тиме је појам правног лица у смислу поступања са тајним подацима сужен у односу на класичан појам правног лица.

Ако постоји недоумица да ли је конкретно правно лице у класичном смислу те речи орган јавне власти/правно лице у смислу Закона о тајности података, постоји могућност обраћања Министарству правде одговарајућим захтевом за давање мишљења наведеног министарства. Образац наведеног захтева налази се на сајту Канцеларије Савета за националну безбедност и заштиту тајних података (www.nsa.gov.rs).

2. СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Приказ број 1: Систем заштите тајних података-елементи

Систем заштите тајних података, као вишеслојни систем заштите, служи циљу обезбеђења и усаглашеност са законским и институционалним захтевима, реализовања концепта заштите националне безбедности и успостављање међународне сарадње, као и високих стандарда квалитета корпоративног управљања и адекватног понашања, али и осигурања стварне одговорности и доброг система заштите тајних података.

СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА ОБУХВАТА:

1. РЕГИСТАРСКИ СИСТЕМ;
2. ПЕРСОНАЛНУ БЕЗБЕДНОСТ;
3. АДМИНИСТРАТИВНУ БЕЗБЕДНОСТ;
4. ФИЗИЧКУ БЕЗБЕДНОСТ;
5. ИНФОРМАЦИОНУ БЕЗБЕДНОСТ;
6. ИНДУСТРИЈСКУ БЕЗБЕДНОСТ;
7. КОНТРОЛУ И НАДЗОР.

РЕГИСТАРСКИ СИСТЕМ предвиђа руковање тајним подацима само у уређеном систему који мора бити успостављен у складу са прописима и стандардима из области заштите тајних података.

ПЕРСОНАЛНА БЕЗБЕДНОСТ обухвата низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за националну безбедност.

АДМИНИСТРАТИВНА БЕЗБЕДНОСТ је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.

ФИЗИЧКА БЕЗБЕДНОСТ представља примену физичких и техничких мера заштите ради спречавања неовлашћеног приступа тајним подацима и у суштини представља комбинацију безбедносних процедура и техничких стандарда који се заснивају на препорукама, процени и пракси.

ИНФОРМАЦИОНА БЕЗБЕДНОСТ представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ(ИКТ- информационо комуникационе технологије) система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

ИНДУСТРИЈСКА БЕЗБЕДНОСТ представља примену мера ради обезбеђења заштите тајних података од стране извођача или подизвођача у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора. Извршење поверљивог уговора подразумева све радње предузете након његовог закључења до извршења уговорних обавеза, односно до престанка његовог важења.

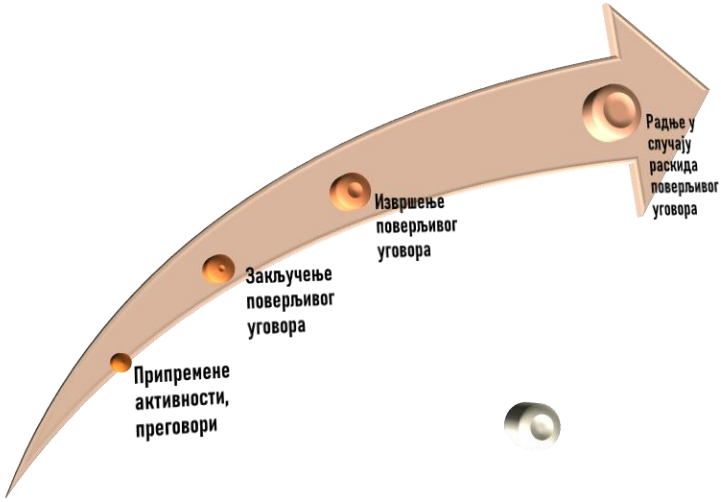
КОНТРОЛА И НАДЗОР – подразумева посебне мере надзора над поступањем са тајним подацима у органу јавне власти. Посебне мере надзора обухватају непосредан

увид, одговарајуће провере и разматрање поднетих извештаја у вези са спровођењем свих мера заштите тајних података или једне, односно одређених мера заштите тајних података и спроводе се у оквиру унутрашње контроле органа јавне власти.

- **УНУТРАШЊА КОНТРОЛА** – руководилац органа јавне власти а у случају потребе систематизује се посебно радно место или се задужује посебна организациона јединица у саставу органа јавне власти
- **КОНТРОЛА И СТРУЧНИ НАДЗОР** – Канцеларија Савета за националну безбедност и заштиту тајних података
- **КОНТРОЛА И ИНСПЕКЦИЈСКИ НАДЗОР** - Министарство надлежно за послове правосуђа

2.1. Индустријска безбедност

Индустријска безбедност представља примену мера ради обезбеђења заштите тајних података, од стране извођача или подизвођача, у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора.



Преговори се одржавају у просторији за чување тајних података. Просторија за чување тајних података мора да испуњава посебне физичко-техничке мере заштите тајних података.

Пре закључења поверљивог уговора са правним лицем овлашћено лице органа јавне власти врши проверу испуњености *организационих* и *техничких* услова за чување тајних података (за степене тајности П, СП, ДТ). О резултатима провере овлашћено лице органа јавне власти обавештава руководиоца органа јавне власти. Такође, пре закључења поверљивог уговора који садржи тајне податке степена тајности П, СП или ДТ правно лице или физичко лице које закључује поверљиви уговор, као прилог уговору, израђује *Упутство о мерама заштите тајних података*.

Извршење поверљивог уговора подразумева *све радње* предузете након његовог закључења до извршења уговорних обавеза, односно до престанка његовог важења.

У случају **раскида** поверљивог уговора правно лице обавезно је *да без одлагања врати документа и друге материјале који садрже тајне податке* и да предузме мере у вези са затварањем свог регистра, осим ако тај регистар не води по неком другом основу.

Из наведеног можемо закључити да се поступак закључења и извршења поверљивог уговора састоји, поред саме садржине поверљивог уговора, и из следећих фаза:

1. **Припремне активности, преговори**
2. **Закључење поверљивог уговора**
3. **Извршење поверљивог уговора**

3.1.* Радње у случају раскида.

Мора се напоменути да не само извршење поверљивог уговора, већ и претходне фазе наведеног поступка подразумевају имплементацију Закона о тајности података од стране правног лица. Имајући наведено у виду, исто поткрепљујемо следећим чињеницама:

а) Фаза 1: овлашћено лице органа јавне власти вршењем провере испуњености организационих и техничких услова за чување тајних података (П, СП, ДТ) управо врши проверу конкретних седамнаест питања[1] из сфера персоналне безбедности, административне безбедности, физичке безбедности, информационе безбедности...Такође, јако битан моменат за правна лица (који је у фази 1) представља израда Упутства о мерама заштите тајних података[2], којег је правно лице дужно да се држи у току рада са тајним подацима.

б) Фаза 2: Уговор подразумева **посебне мере заштите**[3] које се примењују на одговорајуће (организационе и техничке) **услове за чување** тајних података.

[1] Види: Прилог број 1.

[2] Види: Прилог број 4.

[3] Посебне мере заштите тајних података, сходно чл. 33. Закона о тајности података, утврђују се актом Владе Републике Србије и циљ њиховог утврђивања јесте управо ефикаснија примена општих мера заштите тајних података. Такође, поједине посебне мере заштите могу се ближе уредити актом надлежног

Довољно је имати у виду наводе из следеће табеле и схватити значај обавезе имплементације Закона о тајности података:

Организациони услови **нарочито се односе на:**	1) организацију процеса рада; 2) заштиту приступа тајним подацима; 3) заштиту од неовлашћеног коришћења тајних података; 4) одређивање одговорног лица задуженог за спровођење мера заштите; 5) утврђивање поступка у случају ванредних и хитних околности.
Технички услови **нарочито се односе на:**	1) физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци; 2) противпожарну заштиту; 3) заштиту тајних података приликом преношења и достављања изван просторија у којима се чувају; 4) транспорт тајних података; 5) обезбеђивање и заштита информационо-телекомуникационих средстава којима се врши преношење и достављање тајних података; 6) спровођење прописаних мера крипто-заштите.

Табела број 1: Организациони и технички услови за чување тајних података

Правно лице у смислу Закона о тајности података, као што се може видети, има обавезу успостављања одговарајућег нивоа Система заштите тајних података. Оптималан ниво у сваком појединачном случају је управо одговарајући ниво. Упознавши се Приказом број 1. са елементима Система заштите тајних података остаје нам да у даљем тексту наведемо основне моменте сваког елемента Система заштите тајних података, осим Индустријске безбедности-почетне теме овог водича.

министра, односно руководиоца посебне организације, у складу са актом Владе којим су утврђене посебне мере заштите.

2.2. Физичка безбедност

Физичка безбедност подразумева примену мера физичке заштите и техничке заштите на појединачним локацијама, у зградама или на отвореним просторима у којима се налазе или чувају тајни подаци који захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења. Избор мера које ће се користити за физичку безбедност тајних података зависи од специфичности објекта, броја тајних података, степена тајности. На основу ових параметара ради се општа процена ризика на основу које се примењују мере физичко-техничке заштите и чија је сврха координиција и оптимизација коришћење ресурса и надгледање, контролисање и умањење претње које могу да угрозе безбедност.

Мере физичког и техничког обезбеђења треба да се заснивају на принципу **„одбрана по дубини“**. Руковање и чување тајних података врши се у **безбедносним и административним зонама**. Простор или просторије у којима се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА“, „СТРОГО ПОВЕРЉИВО“, и „ПОВЕРЉИВО“ успостављене су као безбедносне зоне првог и/или другог степена. Простор или просторије у којима се обрађују и чувају тајни подаци степена тајности „ИНТЕРНО“ успостављају се као административне зоне. Просторије у којима се чувају, користе, обрађују и уништавају тајни подаци обезбеђују се **противпровалним и противпожарним системом**. Једна од мера је и успостављање ефикасне **контроле приступа**. Простор **око** просторија у којима се чувају, користе, обрађују или уништавају тајни подаци, као **и пут до њих**, по правилу, се обезбеђују **видео-надзором**. Ако просторије имају прозоре, ради предузимања мера одговарајуће техничке заштите, уграђују се **средства за противпровалну заштиту (детектори покрета и лома стакла)**, **сигурносне металне решетке** чији положај онемогућава отварање прозора, као и **специјална стакла** која онемогућавају поглед у унутрашњост просторије. Безбедносно техничка опрема, односно одговарајућа средства техничке заштите у којој се чувају тајни подаци су: **противпожарна метална каса са уграђеном бравом** за степен тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО” и/или **канцеларијски или метални ормар** за степен тајности „ИНТЕРНО”. Касе или просторије у којој се та каса налази, опремљене су системом јављања и морају испуњавати одговарајуће СРПС/ЕН техничке стандарде.

* Детаљније погледати скрипту Систем заштите тајних података (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf)

* Приручник Основе обраде и заштите података (https://nsa.gov.rs/extfile/sr/1424/Osnove_obrade_i_zastite_podataka-prirucnik.pdf)

2.3. Административна безбедност

Административна безбедност представља скуп мера, политика, процедура и пракси које су усмерене на очување безбедности информација, ресурса и операција унутар организације или система. Ова област се односи на управљање ризицима, заштиту података и информација, управљање приступом, обуку запослених и сличне активности које имају за циљ очување поверљивости, интегритета и доступности информација.

Мора се напоменути да *правно лице нема право креирања тајног податка*-правно лице може имати само право приступа тајним подацима до одговарајућег степена тајности и то након успешног окончања процеса сертификације.

Примери мера и активности из сфере административне безбедност тајних података који се предузимају се са циљем обезбеђења заштите и законитог поступања са тајним подацима јесу:

- пријем и евидентирање у књиге евиденције;
- обезбеђивање правилног чувања;
- правилна дистрибуција, припрема копија, превода и извода из тајног податка и реализација контроле дистрибуције до крајњих корисника по принципу „ПОТРЕБНО ДА ЗНА“;
- спречавање сваког покушаја неовлашћеног приступа и руковања од стране неовлашћених лица;
- правилан одабир архивске грађе, као и правилно издвајање и уништавање одабране непотребне архивске грађе.

Правилном применом административних безбедносних мера и активности у великој мери се омогућава смањење ризика од неовлашћеног приступа тајним подацима, као и лакше откривање нарушавања безбедности тајних података.

* Детаљније погледати скрипту Систем заштите тајних података (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf

2.4. Персонална безбедност

Мере и активности које се спроводе у домену персоналне безбедности обухватају низ процедура чији је основни циљ да се утврди да ли неко правно, односно физичко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за националну безбедност. Лица чије дужности предвиђају приступ тајним подацима претходно морају бити подвргнута

одговарајућој безбедносној провери пре него што им се изда одређени безбедносни сретификат/дозвола који ће важити током одобреног трајања тог приступа.

Подвлачимо неопходност поседовања како безбедносног сертификата за приступ тајним подацима одговарајућег степена тајности за правно лице, тако и за законског заступника правног лица и за конкретна физичка лица за која постоји потреба приступа тајним подацима. Поседовање безбедносног сертификата јесте први корак и нужан услов за приступ тајним подацима. Услови за издавање сертификата утврђују се кроз безбедносну проверу коју врше надлежне службе на захтев органа јавне власти, а преко Канцеларије Савета за националну безбедност и заштиту тајних података. У оквиру безбедносне провере надлежни орган са аспекта безбедности оцењује наводе из попуњеног безбедносног упитника. Безбедносни упитник попуњава се лично од стране лица на које се односи на начин утврђен Упутством за попуњавање безбедносних упитника. Законски заступник правног лица лично попуњава безбедносни упитник за правно лице и лично попуњава безбедносни упитник за себе као физичко лице.

Канцеларија Савета за националну безбедност и заштиту тајних података издаје правном лицу сертификат за приступ тајним подацима, који поред провере бонитета и пословања запослених у правном лицу подразумева и проверу простора, опреме и процедура. Ради заштите тајних података приликом реализације поверљивих уговора неопходно је да учесници у реализацији уговора претходно обезбеде поседовање одговарајућих безбедносних сертификата за правно лице и за физичка лица, односно да имају акредитован простор, опрему и процедуре, који обавља Канцеларија Савета за националну безбедност и заштиту тајних података.

Поседовање решења без издатог сертификата не значи могућност приступу тајном податку. Непреузимање сертификата подразумева угожавање националне безбедности Републике Србије, што уједно може представљати и безбедносну сметњу приликом нове провере.

Подвлачимо да правна лица немају право директног обраћања захтевом за сертификацију правног лица и физичких лица запослених у правном лицу, већ искључиво преко органа јавне власти са којим постоји уговорна сарадња која потребује приступ тајном податку.


СЕРТИФИКАТ ЗА ПРАВНА ЛИЦА
(подношење захтева)
уговорни однос
ПРАВНО ЛИЦЕ
ЗАХТЕВ И УПИТНИК
ОРГАН ЈАВНЕ ВЛАСТИ
ПРАВНО ЛИЦЕ=ОРГАН ЈАВНЕ ВЛАСТИ


Канцеларија Савета за националну безбедност и заштиту тајних података
ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА
ЗАКОНСКИ ЗАСТУПНИК ПРАВНОГ ЛИЦА
ЗАХТЕВ
РУКОВОДИЛАЦ ОРГАНА ЈАВНЕ ВЛАСТИ
ПРОПРАТНИ АКТ
Канцеларија Савета за националну безбедност и заштиту тајних података

2.5. Информациона безбедност

Информациона безбедност тајних података обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних података које се обрађују у ИКТ системима (ИКТ- информационо комуникационе технологије). Процесом безбедносне акредитације ИКТ система утврђује се да ли је систем постигао адекватан ниво заштите тајних података.

Безбедносна верификација ИКТ система обезбеђује:

- потврду да ли су планиране мере безбедности ИКТ система правилно спроведене;
- потврду да је одговарајућим тестирањем постигнут захтевани ниво безбедности;
- документовање резултата верификације безбедносне имплементације ИКТ система; ово потврђује да су испоштовани минимални безбедносни стандарди ИКТ система за обраду, чување и размену тајних података.

Проценом могућег нарушавања безбедности тајних података и безбедности ИКТ система, односно проценом безбедносног ризика, утврђује се вероватноћа да ће одређена рањивост тог система бити искоришћена и довести до нарушавања безбедности система.

Процена безбедносног ризика служи за утврђивање безбедносних ризика, тј. претњи и рањивости ИКТ система, утврђивање њихове величине, како би се идентификовале области у којима је потребна заштита тајних података у ИКТ систему.

Применом мера безбедности ради заштите ИКТ система постижу се следећи ефекти:

- идентификација особа које приступају систему;
- контрола и евиденција приступа на основу датог права приступа из дефинисане базе података;
- обезбеђивање поузданог начина да се укаже на степен тајности;
- идентификација корисника и поуздана евиденција одштампаног, копираног, модификованог или избрисаног тајног податка;
- заштита важних техничких и програмских елемената и функционалност система;
- контрола и управљање руковањем и преносом носача података на којима се чувају тајни подаци;
- планирање, конфигурисање, управљање и контрола мрежних уређаја.

Ове мере заједно чине основу за заштиту ИКТ система од различитих претњи, али је важно континуирано пратити нове трендове и технологије како би се осигурало да су системи увек заштићени од најновијих претњи.

* Детаљније погледати скрипту Систем заштите тајних података (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf)

* Приручник Основе обраде и заштите података (https://nsa.gov.rs/extfile/sr/1424/Osnove_obrade_i_zastite_podataka-prirucnik.pdf)

2.6. Контрола и надзор

Приликом рада са тајним подацима мора се имати у виду постојање следећих врста контрола и надзора:

Табела број 2: Врсте контроле и надзора

Врста контроле и надзора	Напомене
Инспекцијски надзор	Инспекцијски надзор врши министарство надлежно за послове правосуђа.
Стручни надзор	Стручни надзор је у надлежности Канцеларије Савета за националну безбедност и зашиту тајних података.
Унутрашња контрола	Правно лице има обавезу успостављања унутрашње контроле рада са тајним подацима у правном лицу (види Прилог број 5.). У случају недоношења одговарајуће одлуке законски заступник правног лица је надлежан за унутрашњу контролу рада са тајним подацима у правном лицу.

Облици унутрашње контроле[4]	**Најављена**	**Потпуна**
	Ненајављена	**Делимична**

2.7. Додатне напомене

2.7.1. Одговорно лице за спровођење мера заштите тајних података у правном лицу

Као што се и могло видети из досадашњег дела водича, правно лице има обавезу именовања одговорног лица за спровођење мера заштите тајних података у правном лицу. Именује се посебном одлуком (види: Прилог број), а такође је, сходно уредби из сфере индустријске безбедности, назначење конкретног лица које је одговорно за спровођење мера зашите тајних података у правном лицу обавезан део Упутства о

[4] Види детаљније: Додатне напомене 2.7.3.

мерама заштите тајних података, који је саставни део сваког појединачног поверљивог уговора.

Одговорно лице за спровођење мера заштите тајних података у правном лицу:

- има обавезу успостављања и одржавања на оптималном нивоу Система заштите тајних података у правном лицу;
- овлашћено је да прати примену Закона о тајности података и подзаконских аката из области заштите тајних података и међународних споразума чији је потписник Република Србија;
- особа је за контакт између Канцеларије Савета за националну безбедност и заштиту тајних података, наручиоца посла и правног лица у коме је запослено (које је у конкретном послу извођач или подизвођач);
- мора поседовати сертификат најмање оног степена тајности који је највиши у раду са тајним подацима у конкретном правном лицу.

Треба напоменути да се, у случају недоношења одговорајуће одлуке о именовању одговорног лица за спровођење мера заштите тајних података у правном лицу, истим сматра законски заступник правног лица.

2.7.2. Законски заступник

У сфери поступања са тајним подацима, мора се нагласити значај законског заступника. Наиме, треба имати у виду следеће:

- сертификација правног лица директно је везана за сертификацију законског заступника-законски заступник преузима сертификат за правно лице и сертификат за себе као законског заступника;
- у случају промене законског заступника који је преузео сертификат за правно лице, престаје да важи сертификат за правно лице;
- у случају да је законски заступник страни држављанин, примат има чињеница да ли Република Србија има потписан споразум из области размене и заштите тајних података са државом чији је држављанин законски заступник-и у том случају треба имати у виду следеће:
  - ако је законски заступник држављанин државе са којом Република Србија има потписан споразум из области размене и заштите тајних података може се, сходно Закону о тајности података и конкретном међународном споразуму, ући у поступак сертификације конкретног правног лица и конкретног законског заступника (ако је резултат наведеног поступка позитиван издаје се безбедносна дозвола за страно физичко лице за

законског заступника, док се правном лицу издаје сертификат за правно лице);

- ако законски заступник није држављанин државе са којом Република Србија има потписан споразум из области размене и заштите тајних података не постоји могућност сертификације тог законског заступника.

- у случају недоношења одговорајуће одлуке о именовању одговорног лица за спровођење мера заштите тајних података у правном лицу, истим се сматра законски заступник правног лица (законски заступник мора поседовати сертификат, односно безбедносну дозволу);
- у случају недоношења одговорајуће одлуке о унутрашњој контроли рада са тајним подацима у правном лицу, истим се сматра законски заступник правног лица (законски заступник мора поседовати сертификат, односно безбедносну дозволу).

2.7.3. Унутрашња контрола

Унутрашња контрола се може јавити у облику најављене, ненајављене, потпуне и делимичне унутрашње контроле.

Најављена контрола је редовна и врши се на основу Годишњег плана унутрашње контроле. Годишњи план унутрашње контроле, на основу одређених параметара, утврђује лице одређено за вршење послова унутрашње контроле (контролор), односно законски заступник правног лица у случају да контролор није одређен-а законски заступник у сваком случају даје своје писмено одобрење на сами утврђени Годишњи план рада унутрашње контроле. Контролор мора поседовати сертификат за приступ тајним подацима најмање оног степена тајности који је највиши у раду у конкретном правном лицу.

Ненајављена контрола је изненадна и врши се на основу Одлуке законског заступника правног лица. Законски застпуник наведену одлуку доноси на основу сопствене процене или на иницијативу контролора.

Потпуна контрола јесте контрола примене свих прописаних мера заштите тајних података. Делимична контрола је контрола примене само једне или више мера заштите тајних података (узорак).

О извршеној унутрашњој контроли контролор сачињава Извештај о извршеној унутрашњој контроли. Исти се доставља законском заступнику правног лица. Ако је унутрашњом контролом утврђено постојање конкретне/конкретних неправилности, саставни део извештаја јесте и Предлог мера за отклањање неправилности.

2.7.4. Ангажована лица која нису запослена у правном лицу

Уколико правно лице има потребу за ангажовањем лица која нису запослена код правног лица, а за које постоји потреба приступа тајним подацима у сврху извршења поверљивог уговора, неопходно је да та лица успешно прођу процес сертификације издавањем одговарајућег сертификата за приступ тајним подацима.

2.7.5. Правна лица као извођачи и подизвођачи

Уз констатацију постојања обавезе успостављања одговарајућег нивоа Система заштите тајних података од стране правног лица, што је и предмет овог водича, подвлачимо и следеће:

- подизвођач, у смислу поседовања одговарајућег безбедносног сертификата и примењивања одговарајућих мера заштите тајних података, мора испуњавати услове као и извођач;
- извођач и подизвођач и физичка лица која су запослена, односно радно ангажована од стране правног лица, а која морају приступати тајним подацима ради извршења поверљивог уговора, морају поседовати сертификат најмање оног степена тајности који је највиши у извршењу поверљивог уговора;
- и извођач и подизвођач поверљивог уговора именују одговорно лице за спровођење мера заштите тајних података у правном лицу, што је детаљније приказано у 2.7.1.-у ситуацији када то није урађено, законски заступник обавља послове одговорног лица за спровођење мера заштите тајних података у правном лицу;
- и извођач и подизвођач поверљивог уговора одређују унутрашњу контролу рада са тајним подацима, што је детаљније приказано у 2.6.-у ситуацији када то није урађено, законски заступник обавља послове унутрашње контроле рада са тајним подацима;
- извођач има обавезу сачињавања Списка правних лица са којим је склопљен поверљиви уговор са подизвођачем (види: Прилог број:) и достављања исто органу јавне власти који је наручилац посла.

2.7.6. Страни држављани

У ситуацији када је у правном лицу запослен, односно радно ангажован, страни држављанин на радном месту које захтева приступ тајним подацима правно лице има обавезу да преко органа јавне власти који је наручилац посла захтева издавање безбедносне дозволе, у складу са Законом о тајности података и потписаним

међународним споразумом Републике Србије у области размене и заштите тајних података са државом чији је држављанин то физичко лице. У ситуацији када наведено лице није држављанин државе која има потписан споразум са Републиком Србијом у области размене и заштите тајних података не постоји могућност уласка наведеног лица у процедуру издавање безбедносне дозволе.

2.7.7. Транспорт тајних података

Транспорт тајних података у свим фазама закључења и извршења поверљивог уговора подразумева превоз тајних података од места поласка до крајњег одредишта, превозним средством наручиоца, извођача, подизвођача или ангажовањем превозника који поседује сертификат за приступ тајним подацима. Превозно средство којим се врши транспорт тајних података мора поседовати заштиту адекватну степену тајности података који се транспортују. Транспорт се врши у пратњи курира и/или лица које врши обезбеђење, а које има сертификат за приступ тајним подацима, у складу са Законом о тајности података. Транспорт тајних података врши се према Плану транспорта тајних података, који утврђују наручилац и извођач. Ако се врши транспорт два или више тајних података, сваки од њих се посебно идентификује и предузимају се мере заштите тих тајних података према највећем степену тајности који се транспортује. Није дозвољена промена степена тајности тајног податка у току транспорта, осим у крајње оправданим околностима. У ванредним ситуацијама курир и/или лице које врши обезбеђење има дужност непрекидног чувања тајних података на за то одређеном месту.

Овлашћено лице које је одредило степен тајности податка/одговорно лице за спровођење мера заштите тајних података у правном лицу, односно законски заступник правног лица доставља тајни податак кориснику који има сертификат за приступ тајним подацима најмање оног степена тајности податка који се доставља. Тајни податак се доставља на коришћење кориснику, преко лица које преноси тајне податке-курира. Курир мора поседовати сертификат за приступ тајним подацима одговарајућег степена тајности. На захтев лица којем предаје или од кога преузима тајни податак, курир је дужан да покаже курирско уверење.

2.7.8. Стандарди физичке и техничке заштите

- ***Јасно дефинисане и видљиво означене просторије безбедносног подручја/зоне (периметри) или „рестриктивни простори“***

- ***Просторије (зидови, подови, плафони)-грађевинске мере заштите***

Плафони, зидови и подови морају бити израђени од армираног бетона или чврстог незапаљивог материјала. Ако су просторије међусобно повезане размаком између плафона и крова морају бити одвојени чврстим незапаљивим материјалом.

- ***Прозори (EN 356) - Прозори заштићени решеткама, непровидним завесама или сигурносним фолијама***

Прозор се у принципу не сме инсталирати. Када је неизбежна уградња прозора, они морају бити ограничени на минимум и опремљени гвозденим шипкама пречника 13мм или више и интервалима од 10 цм или више, у складу са SRPS EN стандардима. Прозорско стакло мора бити непрозирно са слојем жичане мреже или једноставно непрозирно, са заштитом од провале. Овим стандардом се утврђују захтеви и методе испитивања за сигурносно стакло које је пројектовано да издржи примену силе одлагањем приступа објекту и/или особама у заштићено подручје на кратак временски период. Стандард класификује производе од сигурносног стакла у категорије отпорности према примени силе.

- ***Вентилацијски, канализациони или други отвори заштићени металним решеткама***

Да би се спречио улазак, осматрање или прислушкивање, канали, плафонски прозори, одводи, тунели и остали отвори морају бити затворени жичаном мрежом или гвозденим шипкама пречника од 13 mm или више, са интервалима мањим од 10 cm, у складу са SRPS EN стандардима.

- ***Физичко осигурање/чувар, стража + тим за хитне интервенције*;** (подзаконски акти, интерни прописи или SRPS A.L2.002)

Овим српским стандардом утврђују се захтеви за услуге приватног обезбеђења. Овај стандард из гране истражних делатности обухвата само категорију детективских услуга. Коришћење овог стандарда помаже организацијама да успоставе или провере квалитет процеса којима се пружају и користе услуге приватног обезбеђења.

- ***Посебна улазна врата***... (EN 1627)

Овим стандардом утврђују се захтеви и класификација система за карактеристике отпорности на провалу пешачких врата, прозора, зид-завеса, гриља и застора. Стандард се може применити за следеће начине отварања: окретања, нагињања, клизања, окретно-нагибна, одозго или одоздо висећа, клизна (хоризонтално и вертикално), као и фиксне конструкције. Стандард такође обухвата производе који садрже ставке као што су писма-плоче или вентилационе гриље. Стандард утврђује захтеве за отпорност на провалу грађевинског производа.

- ***Кључеви и комбинације*** (EN 1300)

Овим документом се утврђују захтеви за браве високе сигурности (HSL) за поузданост, отпорност на провале и неовлашћено отварање са методама испитивања. Он такође пружа шему за класификацију HSL према њиховој отпорности на провале и неовлашћено отварање. Применљив је на механичке и електронске HSL. За електронске браве које се користе у дистрибуираном систему, упућује се на EN 17646 за даље информације. Браве могу да садрже следеће карактеристике као опције, али оне нису обавезне:

а) препознат код за спречавање промене кода и/или омогућавање/оне-могућавање паралелних кодова;
б) препознат код за онемогућавање времена подешавања;
в) интеграција алармних компоненти или функција;
г) отпорност на разарање киселинама;
д) отпорност на Х- зраке;
ђ) отпорност на експлозиве;
е) време функционисања;

- ***Контрола приступа*** (EN 50133-1 и EN 50133-1/A1)

Овим стандардом специфицирају се захтеви за аутоматске системе и компоненте контроле приступа у околини зграда.

- ***Противпровални систем осигурања*** /IDS (EN 50131-1)

Овим стандардом специфицирају се захтеви за противпровалне и противпрепадне алармне системе који су инсталирани у зградама и користе специфична или неспецифична повезивања са проводником или без проводника.

- ***Алармни систем*** (EN 50134-1)

Овим стандардом специфицира се минимум захтева за друштвене алармне системе. Овом серијом стандарда нису обухваћени додатни захтеви за особе са инвалидитетом (са оштећењем вида и слуха).

- ***Резервно напајање електричном енергијом, клима уређај***

- ***Противпожарни систем, детектори дима*** (EN 54-1, EN 54-2, EN 54-3, EN 54-4, EN 54-5, EN 54-11)

Овај документ се примењује на системе за детекцију пожара и пожарне алармне системе у и око зграда. Документ се не примењује на уређаје за алармирање дима, који су обухваћени стандардом EN 14604.

- ***Видео надзор*** (SRPS EN 62676-1-1:2015)

Стандард IEC 62676-1-1:2013 специфицира минимум захтева и даје препоруке за системе видео-надзора (VSS) (до скора називани CCTV системи) који се инсталирају због сигурности. Овај стандард специфицира минимум захтева за перформансе и функционалне захтеве који ће бити уговорени између корисника, правних лица и добављача, али не укључују захтеве за пројектовање, планирање, инсталисање, испитивање, рад или одржавање.

- ***Обележени телефони, рачунари, принтери и сл.***

- ***Резач папира – Шредер*** (DIN 66399)

Сигурно одлагање, у овом контексту, значи да уређаји за складиштење података, који садрже осетљиве податке, могу уништавати на такав начин да репродукција тих података није могућа или је што теже могућа.

- ***Металне касе – сефови*** (EN 1143-1)

Овим стандардом успостављају се основе за испитивање и класификација слободностојећих каса, уграђених каса (у под или зид), АТМ каса и АТМ основа, врата трезорских просторија, као и трезорских просторија (са вратима или без њих), у зависности од њихове отпорности према провали. Овај стандард не обухвата испитивање и класификацију система депозита и АТМ система.

- ***Системи менаџмента безбедношћу информација*** SRPS/СРПС ISO/IEC 27001:2022

ISO/IEC 27001 обезбеђује референтни скуп контрола безбедности информација, сајбер безбедности и заштите приватности, укључујући упутства за имплементацију заснована на међународно признатим најбољим праксама.

- ***Chain of supply*** – Листа сертификовне опреме која се уграђује у систем физичко-техничке заштите, односно инсталациони материјал за наведену опрему мора бити у складу са декларацијом произвођача опреме која се инсталира ради заштите тајних података.

2.7.9. Приватно обезбеђење, минимални технички услови код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама, детективска делатност-упућивање на одговарајуће прописе

Законом о приватном обезбеђењу уређено је обавезно обезбеђење и заштита одређених објеката, послови и рад правних и физичких лица у области приватног обезбеђења, услови за њихово лиценцирање, начин вршења послова и остваривање надзора над њиховим радом. Такође, напомињемо да је Влада Републике Србије донела Уредбу о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама, у складу са чл. 33. став 1. Закона о приватном обезбеђењу. Наведеном уредбом уређени су минимални технички услови код обавезне уградње система техничке заштите у банкама, пословницама банака платним институцијама, пословницама јавног поштанског оператора и у другим финансијским организацијама. Одредбе ове уредбе не примењују се на пословнице банака и финансијских организација које се налазе у објектима које обезбеђују организационе јединице војске, полиције или правосудне страже или код којих су минимални услови за техничку заштиту уређени посебним законом или прописом донетим на основу закона.

Министар унутрашњих послова је 2015. године донео Правилник о начину вршења послова техничке заштите и коришћења техничких средстава. Наведеним правилником ближе је прописан начин вршења послова техничке заштите и коришћења техничких средстава у обављању послова приватног обезбеђења.

Министар унутрашњих послова је 2019. године донео Правилник о просторно-техничким условима за обављање детективске делатности. Наведеним правилником прописани су ближи услови који се односе на пословни простор за обављање детективске делатности и на физичко-техничке мере за чување збирки података и других евиденција.

❖ Детаљније погледати скрипту Посебне мере физичко-техничке заштите тајних података (https://nsa.gov.rs/extfile/sr/3915/Posebne_mere_fizicko_tehnicke_zastita1.pdf)

2.7.10. Неопходни кораци за добијање сертификата правних лица

1. Формално писмо-обраћање правног лица органу јавне власти о намери учешћа на набавци која садржи тајне податке

2. Састанак са представницима органа јавне власти око безбедносних питања пре покретања поступка

3. Попуњавање одговарајућих безбедносних упитника за физичка лица и за правно лице

4. Прослеђивање безбедносних упитника за физичка лица и за правно лице органу јавне власти

Сходно чл. 51. ст. 3. Закона о тајности података **законски заступник правног лица подноси захтев за издавање сертификата** за правно лице, за себе као физичко лице и за конкретне запослене у правном лицу (ако постоји потреба приступа тајним подацима од стране тих конкретних запослених) **органу јавне власти са којим има уговорни однос** који потребује приступ тајним подацима правном лицу и конкретним запосленим у истом. У прилогу захтева достављају се попуњени безбедносни упитник за правно лице, безбедносни упитник за физичко лице (за законског заступника) и, ако постоји потреба приступа тајним подацима од стране конкретних запослених у том правном лицу, и безбедносни упитник за физичко лице -за сваког конкретног запосленог за којег постоји потреба приступа тајним подацима. Безбедносни упитници попуњавају се на начин прописан Упутством за попуњавање безбедносних упитника-од стране лица на које се односе, с тим да безбедносни упитник за правно лице попуњава лично законски заступник правног лица.

5. Достављање безбедносног упитника са захтевом органа јавне власти Канцеларији Савета за националну безбедност и заштиту тајних података на даљи поступак

Орган јавне власти који има уговорни однос са правним лицем подноси захтев за сертификацију правног лица, законског заступника правног лица и конкретних запослених за које постоји потреба приступа тајним подацима Канцеларији Савета-у прилогу наведеног захтева налазе се безбедносни упитници који су достављени органу јавне власти од стране правног лица.

6. Припремни састанак законског заступника правног лица са Канцеларијом Савета за националну безбедност и заштиту тајних података око поступка издавања сертификата правном лицу

7. Покретање поступка безбедносне провере

Канцеларија Савета, ако су безбедносни упитници попуњени у складу са Упутством за попуњавање безбедносних упитника, исте доставља органу надлежном за вршење безбедносне провере (за правна лица и за цивиле надлежан је МУП, односно БИА (зависно од степена тајности)) на даљу надлежност. У случају да безбедносни упитници нису попуњени у складу са Упутством за попуњавање безбедносних упитника исти се враћају органу јавне власти који је подносилац захтева.

8. Доношење решења за правно лице и за физичка лица

На основу извештаја са препоруком (које орган надлежан за вршење безбедносне провере доставља Канцеларији Савета) и извршене провере простора, опреме и процедура код правног лица Канцеларија Савета доноси одговарајуће решење.

9. Акредитација простора, опреме и организационих услова за чување тајних података

Канцеларија Савета врши проверу простора, опреме и процедура код правног лица.

10. Издавање сертификата правном лицу

Ако је Канцеларија Савета донела решење којим се утврђује право приступа тајним подацима до одређеног степена тајности, Канцеларија Савета издаје правном лицу сертификат за приступ тајним подацима, који поред провере бонитета и пословања запослених у правном лицу подразумева и проверу простора, опреме и процедура.

П Р И Л О З И

Прилог број 1: Формално писмо-обраћање правног лица органу јавне власти о намери учешћа у набавци која садржи тајне податке-образац

Прилог број 2: Седамнаест питања из разних сфера Система заштите тајних података које проверава овлашћено лице органа јавне власти пре закључења поверљивог уговора са правним лицем

Прилог број 3: Списак правних лица са којим је склопљен поверљиви уговор са подизвођачем-образац

Прилог број 4: Списак правних лица са којима је склопљен поверљив уговор-образац

Прилог број 5: Упутство о мерама заштите-образац

Прилог број 6: Одлука о одређивању одговорног лица за спровођење мера заштите тајних података у правном лицу-образац

Прилог број 7: Одлука о одређивању унутрашње контроле у правном лицу-образац

Прилог број 8: Изјава о заштити тајних података из тендерске документације-образац

Прилог број 9: ПЕРСОНАЛНА ЕВИДЕНЦИЈА-евиденција запослених који поседују сертификат за приступ тајним подацима-образац

Прилог број 10: Евиденција запослених који имају сертификат, а који ће да учествују у извршењу поверљивог уговора-образац

Прилог број 11: Неопходни кораци за добијање сертификата правних лица

Прилог број 12: Садржина Плана транспорта

Прилог број 13: План заштите тајних података за ванредне и хитне случајеве-образац

Прилог број 14: Појмовник о раду са тајним подацима

Прилог број 15: Каталог прописа за рад са тајним подацима

ФОРМАЛНО ПИСМО-ОБРАЋАЊЕ ПРАВНОГ ЛИЦА ОРГАНУ ЈАВНЕ ВЛАСТИ О НАМЕРИ УЧЕШЋА У НАБАВЦИ КОЈА САДРЖИ ТАЈНЕ ПОДАТКЕ

ОБРАЗАЦ

_____

(Назив правног лица)

Седиште правног лица:

Број:

НАЗИВ ОРГАНА ЈАВНЕ ВЛАСТИ

М Е С Т О

А д р е с а

Предмет: Формално писмено обраћање о намери учешћа у набавци која садржи тајне податке

Поштовани,

Овим путем изражавамо намеру учешћа у набавци која садржи тајне податке _____ (назив набавке).

Напомињемо следеће (заокружити):

1. Спремни смо да опремимо простор у седишту нашег правног лица

2. Немамо могућност опремања просторија нашег правног лица.

Гарантујемо да ћемо поступати са тајним подацима у складу са Законом о тајности података, како у поступку преговора, тако и у реализацији поверљивог уговора (ако до истог дође).

_____

(Печат и потпис законског заступника)

Дана _____20____ У _____

ПРЕ ЗАКЉУЧЕЊА ПОВЕРЉИВОГ УГОВОРА СА ПРАВНИМ ЛИЦЕМ
овлашћено лице органа јавне власти проверава:

1) Да ли је ради реализације послова који се предвиђају уговором неопходан приступ тајним подацима физичким лицима која ће да обављају уговорене послове;
2) Да ли правно лице поседује сертификат који одговара најмање оном степену тајности којим су означени тајни подаци који се правном лицу достављају;
3) Да ли су за физичка лица која обављају уговорене послове издати сертификати, односно дозволе;
4) Да ли је простор, односно просторија правног лица или физичког лица у којој ће да се чувају тајни подаци, опремљена у складу са прописом који уређује посебне мере физичко-техничке заштите ТП;
5) Начин евидентирања, чувања и архивирања тајних података;
6) Да ли постоји акт правног лица о поступању са тајним подацима, мерама заштите тајних података, као и о поступању са тајним подацима у случају ванредних ситуација;
7) Означавање ормара и каса у којима се чувају и депонују тајни подаци;
8) Начин коришћења и приступа тајном податку, вођење прописаних евиденција, а посебно евиденције о приступу тајном податку, као и чување тих евиденција;
9) Начин вршења умножавања тајних података;
10) Паковање и достављање тајних података унутар и ван безбедносне зоне;
11) Поступак уништавања тајних података;
12) Евиденцију улаза и излаза лица и возила, коришћење безбедносних пропусница и посебних безбедносних пропусница, функционисање физичког и електронског система за обезбеђење објекта и простора;
13) Чување сертификата;
14) Пријем, обраду, пренос, чување, архивирање и уништавање тајних података у електронској форми;
15) Чување средстава крипто-заштите;
16) Начин чувања поверљивог уговора који садржи тајне податке;
17) Предузимање осталих мера заштите тајних података.

СПИСАК ПРАВНИХ ЛИЦА СА КОЈИМ ЈЕ СКЛОПЉЕН ПОВЕРЉИВИ УГОВОР СА ПОДИЗВОЂАЧЕМ

Од: _____ (Датум)

(назив правног лица)

За: _____

(назив органа јавне власти-носиоца пројекта)

У склопу пројекта

_____ (назив пројекта)

_____ (назив правног лица)

склопио је поверљиви уговор са подизвођачем са следећим правним лицима:

Табела број 1: Списак правних лица са којима је склопљен поверљиви уговор са подизвођачем

Р. бр.	Назив и адреса правног лица	Име и презиме и контакт законског заступника правног лица	Име и презиме и контакт одговорног лица за спровођење мера заштите тајних података у правном лицу	Степен тајности поверљивог уговора са подизвођачем

Сачинио: Одобрио:

_____ _____

Одговорно лице за спровођење мера заштите тајних података у правном лицу

Законски заступник правног лица

СПИСАК ПРАВНИХ ЛИЦА СА КОЈИМА ЈЕ СКЛОПЉЕН ПОВЕРЉИВИ УГОВОР[5]

Од: _____ (Датум)

(назив органа јавне власти) Контакт телефон руковаоца тајним подацима:

За: Канцеларију Савета за националну безбедност и заштиту тајних података

У склопу пројекта

_____ (назив пројекта)

_____ (назив органа)

склопио је поверљиве уговоре са следећим правним лицима:

Табела број 1: Списак правних лица са којима је склопљен поверљиви уговор

Р. бр.	Назив и адреса правног лица	Име и презиме и контакт законског заступника правног лица	Име и презиме и контакт одговорног лица за спровођење мера заштите тајних података у правном лицу	Степен тајности поверљивог уговора

Сачинио: Одобрио:

(руковалац тајним подацима) Руководилац органа

[5] У случају постојања уговора са подизвођачем, приложити овом списку копију Списка правних лица са којима је склопљен поверљиви уговор са подизвођачем (коју је орган јавне власти добио од правног лица са којим има склопљен поверљиви уговор).

јавне власти

УПУТСТВО О МЕРАМА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

1. Овим упутством прописују се обавезе правног лица _____ (назив правног лица) које ће да закључи поверљиви уговор.
2. За одговорно лице за спровођење мера заштите тајних података у правном лицу _____(назив правног лица) именује се _____(име и презиме физичког лица).
3. Правно лице _____ (назив правног лица) одржава непрекидну везу са овлашћеним лицем или другим лицем органа јавне власти који је одговоран за надзор над извршењем поверљивог уговора.
4. Правно лице _____(назив правног лица) дужно је да омогући органу јавне власти да за време извршења поверљивог уговора изврши контролу о предузетим мерама заштите тајних података из тог уговора.
5. Правно лице _____ (назив правног лица) дужно је да одмах обавести орган јавне власти о уоченим неправилностима у вези са заштитом тајног податка или његовом откривању неовлашћеном лицу.
6. Правно лице _____ (назив правног лица) дужно је да обезбеди податке о лицима који ће да имају приступ тајним подацима из поверљивог уговора.
7. Правно лице _____(назив правног лица) дужно је да води евиденцију запослених који имају сертификат, а који ће да учествују у извршењу поверљивог уговора.
8. Правно лице _____(назив правног лица) дужно је да обезбеди да се запослени упознају са мерама заштите тајних података и да се придржавају тих мера.
9. Правно лице _____(назив правног лица) дужно је да изради списак тајних података и области у којима могу да настану ти тајни подаци.
10. Правно лице _____(назив правног лица) дужно је да упозна подуговарача са мерама заштите тајних података које је дужан да спроведе.
11. Правно лице _____(назив правног лица) дужно је да користи тајне податке којима има приступ по основу поверљивог уговора, само у сврхе одређене тим уговором, односно подуговором.
12. Правно лице _____(назив правног лица) дужно је да по извршењу поверљивог уговора, односно подуговора све тајне податке врати органу јавне власти.
13. Правно лице _____(назив правног лица) дужно је да обезбеди уништавање тајних података у складу са прописом којим су уређене посебне мере физичко-техничке мере заштите тајних података.

Правно лице _____ (назив правног лица) дужно је да се у току извршења поверљивог уговора, односно подуговора придржава обавеза садржаних у Упутству о мерама заштите тајних података.

На основу члана 2. Уредбе о посебним мерама заштите тајних података који се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа (Службени гласник Републике Србије“, број: 63/2013) *законски заступник правног лица* доноси

ОДЛУКУ
о одређивању одговорног лица за спровођење мера заштите тајних података у правном лицу

1. Овом одлуком одређује се одговорно лице за спровођење мера заштите тајних података у правном лицу (у даљем тексту: Одговорно лице).

2. За одговорно лице *у правном лицу* одређује се _____.

3. Са овом одлуком упознати запослене који раде на пословима руковања тајним подацима у *правном лицу.*

4. Ова одлука ступа на снагу даном доношења.

Број:

Датум:

ЗАКОНСКИ ЗАСТУПНИК

_____

На основу члана 85. Закона о тајности података („Службени гласник РС”, број 104/09) законски заступник доноси:

ОДЛУКУ
о одређивању унутрашње контроле *у правном лицу*

1. Овом одлуком одређује се унутрашња контрола за рад са тајним подацима *у правном лицу.*

2. За унутрашњу котролу (контролоре) за рад са тајним подацима у правном лицу одређује се _____.

3. Са овом одлуком упознати запослене који раде на пословима руковања тајним подацима у *правном лицу.*

4. Ова одлука ступа на снагу даном доношења.

Број:

Датум:

ЗАКОНСКИ ЗАСТУПНИК
ПРАВНОГ ЛИЦА

_____

И З Ј А В А
О ЗАШТИТИ ТАЈНИХ ПОДАТАКА ИЗ ТЕНДЕРСКЕ ДОКУМЕНТАЦИЈЕ

За чување и коришћење тајних података из документације са ознаком тајности, насталих или уступљених током тендерског поступка везаног уз

_____

(назив поверљивог уговора, програма или пројекта)

Потврђујем да:

- Сам упознат/а са прописима који уређују заштиту тајних података и обавезујем се да ћу уступљени тајни податак са којим се упознам или на било који други начин дођем до њега чувати и штитити, као и да ћу са истим поступати у складу са одредбама Закона о тајности података („Службени гласник РС“ број 104/2009) и другим подзаконским актима из области заштите тајних података, као из члана 27. Уредбе о јавним набавкама у области одбране и безбедности („Службени гласник РС“ број 93/2020) у вези Закона о јавним набавкама („Службени гласник РС“ број 91/2019 и 92/2023).
- Увид у тајне податке из тендерске документације могу остварити само они запослени којима је то потребно у обављању послова и дужности, који су упознати са прописима о тајности података и који имају одговарајући сертификат за приступ тајним подацима.
-

Обавезујем се:

- Испунићу све прописане мере и стандарде за заштиту тајних података у складу са Законом о тајности података и подзаконским актима усаглашеним са Законом;
- Нећу умножавати и копирати примљене тајне податке, нити их давати на увид или уступити трећој страни без одговарајућег одобрења;
- Тајне податке из тендерске документације вратићу до истека рока за достављање понуде по позиву за закључење поверљивог уговора или подуговора.

У_____,

дана_____

(Овлашћено лице у правном лицу)

ПЕРСОНАЛНА ЕВИДЕНЦИЈА

-евиденција запослених који поседују сертификат за приступ тајним подацима [6]

Назив правног лица Датум сачињавања/ажурирања Евиденције: _____

Име и презиме законског заступника правног лица

Потпис-одобрење законског заступника правног лица на Евиденцију

Табела број 1: Списак лица која поседују сертификат за приступ тајним подацима

Р. бр	Име и презиме	ЈМБГ	Степен тајности	Датум издавања сертификата	Датум важења сертификата

Сачинио Евиденцију:

Одговорно лице за спровођење мера заштите тајних података у правном лицу

[6] Персоналну евиденцију-евиденцију запослених који поседују сертификат за приступ тајним подацима води правно лице. Одговорно лице за спровођење мера заштите тајних података у правном лицу води и редовно ажурира сваку промену. Законски заступник потписом на Евиденцији одобрава наводе из исте.

Евиденција запослених који имају сертификат, а који ће да учествују у извршењу поверљивог уговора [7]

Назив правног лица Датум сачињавања/ажурирања Евиденције: _____

Име и презиме законског заступника правног лица

Потпис-одобрење законског заступника правног лица на Евиденцију

Табела број 1: Евиденција запослених који имају сертификат, а који ће да учествују у извршењу поверљивог уговора

Р. бр	Име и презиме	ЈМБГ	Степен тајности	Датум издавања сертификата	Датум важења сертификата

Сачинио Евиденцију:

_____

Одговорно лице за спровођење мера заштите тајних података у правном лицу

[7] Евиденцију запослених који имају сертификат, а који ће да учествују у извршењу поверљивог уговора води правно лице. Одговорно лице за спровођење мера заштите тајних података у правном лицу води и редовно ажурира сваку промену. Законски заступник потписом на Евиденцији одобрава наводе из исте.

Неопходни кораци за добијање сертификата правних лица

1. Формално писмо-обраћање правног лица органу јавне власти о намери учешћа на набавци која садржи тајне податке

2. Састанак са представницима органа јавне власти око безбедносних питања пре покретања поступка

3. Попуњавање одговарајућих безбедносних упитника за физичка лица и за правно лице

4. Прослеђивање безбедносних упитника за физичка лица и за правно лице органу јавне власти

5. Достављање безбедносног упитника са захтевом органа јавне власти Канцеларији Савета за националну безбедност и заштиту тајних података на даљи поступак

6. Припремни састанак законског заступника правног лица са Канцеларијом Савета за националну безбедност и заштиту тајних података око поступка издавања сертификата правном лицу

7. Покретање поступка безбедносне провере

8. Доношење решења за физичка лица

9. Акредитација простора, опреме и организационих услова за чување тајних података

10. Издавање сертификата правном лицу

ПЛАН ТРАНСПОРТА-САДРЖИНА

План транспорта, утврђен од стране наручиоца и извођача, мора садржати:

- Утврђивање мера заштите тајних података, према највећем степену тајности који се транспортује;
- Одређивање маршуте пута којим ће се обавити транспорт, уколико је то могуће, директно и у најкраћем року;
- Одређивање процедура за заустављањање;
- Одређивање начина комуникације приликом транспорта.

број копије.

Евиденциони број.:

О д о б р е н о

……дана…….месеца……године

……
(име,положај)

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА ЗА ВАНРЕДНЕ И ХИТНЕ СЛУЧАЈЕВЕ

У случају ако дође до нарушавања или компромитовања тајних података

План заштите тајних података (у даљем тексту – података) за ванредне и хитне случајеве обухвата све процедуре, задатке и активности које законски заступник правног лица..... треба да усвоји, а који се користи у ванредним и хитним случајевима, када неовлашћено лице приступи подацима или у случају када дође до уништења ових података.

У случају било какве компромитације података, одговорно лице за спровођење мера заштите тајних података у правном лицу (у даљем тексту: Одговорно лице) треба одмах да преда извештај о томе законском заступнику.

1. Нарушавање или компромитовање безбедности података:

а) Одговорно лице треба да провери у којој мери је дошло до нарушавања или компромитовања података.

б) Одговорно лице треба да оформи комисију за испитивање спорних околности. Само лица која имају адекватно искуство у овим пословима, која су независна од оних који су укључени директно у случај и која имају дозволу приступа (сертификат) за ниво компромитованих података, могу бити чланови ове комисије.

в) Комисија треба да припреми записник са детаљним извештајем и да га презентује руковаоцу тајних података који подноси извештај законском заступнику.

г) Законски заступник сачињава коначан извештај о компромитовању безбедности и наређује даље поступање у складу са безбедносним политикама правног лица. У извештају о компромитовању безбедности података, који сачињава Одговорно лице, требало би обухватити следеће:

- податке неопходне за препознавање и идентификацију података
- назив оргизационе целине код кога се налази податак и датум пријема
- степен тајности и период важења
- евиденциони број додељен оригиналу потписан од примаоца
- предмет, број страница и серијски број копија
- околности компромитовања и нарушавања безбедности
- утврђивање временског периода компромитовања или нарушавања (познато или претпостављено на почетку/на крају поступка испитивања спорних околности)
- место компромитовања или нарушавања

- примарне узроке развоја ситуације компромитовања или нарушавања безбедности – утврђивање узрока
- име одговорне особе за компромитацију или нарушавање безбедности (уколико је познато)
- списак предузетих мера и активности

- Одговорно лице требало би да заведе следеће:
- редни број одређеног случаја
- датум одређеног случаја
- место одређеног случаја
- кратак опис одређеног случаја
- узбуњивање
- неовлашћени продор
- провале
- пожар
- пуцање водоводних цеви
- експлозија бомбе, итд.

д) редни број записника комисије састављеног за одређени случај

ђ) Записник о компромитовању и нарушавању безбедности чува се 5 година.

Уколико податак нестане, треба предузети мере које би разјасниле степен тајности, а организациона целина у чијем поседу се налазе ови подаци, може их наредне године уклонити из регистра према ставкама за контролу.

2. Потребне мере када је лице које има овлашћени приступ документима одсутно без одобрења

У случају када је Одговорно лице одсутно без одобрења

Након утврђивања разлога недоласка Одговорног лица, законски заступник треба да предузме мере у складу са следећим:

- У зависности од тога у која документа је Одговорно лице имало увид, врши се целокупни или делимични преглед докумената;
- Уколико се приликом прегледа утврди недостатак докумената, извршавају се задаци који су дефинисани у Плану заштите података за ванредне и хитне случајеве, наведено под тачком бр. 1.

3. Поступак у случају оправданог и неоправданог активирања електронског система безбедности

Ова ситуација се може десити само ван радног времена, јер је тада безбедносни систем активиран.

Када се кутија за кључеве у којој се налазе кључеви од привременог регистра/регистра врати, Одговорно лице..... ће бити обавештен о активирању алармног система и функционалности система за узбуњивање. Одговорно лице..... треба то да провери на дисплеју који се налази у привременом регистру/регистру.

У случају оправданог активирања аларма (праве узбуне)

а) Након алармирања два лица из обезбеђења, тим за реаговање треба да оде на то место и провери узрок узбуњивања. Служба обезбеђења не треба да отвара врата привременог регистра/регистра. Само лица са одговарајућим безбедносним сертификатом могу ући у просторију за чување података.

Могућ упад се може проверити непосредим надзором (увидом).

Истовремено Одговорно лице треба да оде да искључи аларм и да извести законског заступника.

б) У случају откривања упада, уколико је то могуће, снаге за реаговање ће зауставити или ухватити уљезе, пријавити Одговорно лице који о томе обавештава законског заступника и службу обезбеђења.

в) Обезбедити место због даље истраге.

г) У периоду истраге алармни систем мора да буде неактиван.

У случају неоправданог активирања аларма (лажна узбуна)

а) Након алармирања два лица из обезбеђења, Одговорно лице треба да оде на то место и провери узрок узбуњивања. Истовремено аларм треба да се искључи и да се извести законски заступник.

б) Након утврђивања узрока узбуњивања, систем треба да се врати у првобитно стање.

Рад алармног система треба да буде контролисан сваког месеца путем теста за узбуњивање, а запажања са теста уписују се у дневник рада. Одговорно лице ће предузети мере за кориговање рада система узбуњивања уколико се утврди нека неправилност у раду система.

4. Задаци који треба да се изврше у случају приступа документима

У случају алармирања електронског система безбедности треба поступати како је наведено у одељку под редним бројем 3.

Уколико систем за узбуну не указује на упад, а патрола нађе доказе о упаду, такође треба поступати како је наведено у одељку под редним бројем. 3.

5. Правила која се односе на руковање сигурносним кључевима и њиховим копијама заједно са запечаћеним ковертама где се налазе шифре

а) Коришћене копије сигурносних кључева са списком просторија, треба да се доставе обезбеђењу и да након радног времена буду закључани у металној кутији за кључеве. Одговорно лице свако јутро пре почетка радног времена проверава просторије и узима кључеве из кутије. Обезбеђење нема овлашћење да без посебног одобрења рукује кључевима који су закључани у кутији;

б) Узимање и повраћај кључева из сигурносне кутије треба да буде евидентиран преко адекватне регистрационе књижице;

в) Дупле кључеве од привременог регистра/регистра треба чувати означене, у запечаћеним ковертама које су у надлежности Одговорног лица;

г) Уколико постоји више копија кључева (копија бр. 3, 4...) оне се такође чувају у запечаћеним ковертама које су у надлежности Одговорног лица или у сигурносној кутији;

д) Коришћење било које копије кључа се евидентира у регистрациону књижицу, а Одговорно лице потврђује његову употребу својим потписом;

ђ) ЗАБРАЊЕНО је држање сигурносних кључева у џепу и њихово копирање. У случају нестанка кључа брава може бити замењена, а у случају оштећења кључа може се направити копија;

е) Безбедносне шифре сигурносних врата (катанаца), сефова и система приступа треба да буду запечаћеној коверти која је у надлежности Одговорног лица. Замена ових шифара треба да буде евидентирана у "књижицу за замену шифара".

6. Безбедносне шифре се мењају у следећим случајевима:

- Најмање једном на сваких 6 месеци
- Након неовлашћеног приступа шифри било које врсте
- Након одласка или промене запослених у привременом регистру/регистру (било који запослени)

7. Задаци који се извршавају при отклањању последица од пожара, елементарних непогода, као и за уклањање оштећења уколико их има

Током оснивања привременог регистра/регистра, Одговорно лице треба да захтева уградњу адекватног система за заштиту од пожара у административној зони или безбедносној категорију заштите.

Електронски сензори своје сигнале шаљу обезбеђењу.

а) Уколико дође до пожара током радног времена

- Централни прекидач треба да буде направљен тако да је безбедан и када је угрожен рестриктиван простор.
- Ватрогасну службу треба одмах обавестити и истовремено започети гашење пожара. Приликом гашења пожара треба посветити додатну пажњу како неовлашћена лица не би приступила документима.
- Документа треба извадити из угрожених просторија и однети у собу бр……. Током транспорта докумената Одговорно лице надлежно је за правилно чување докумената. У случају привременог чувања докумената од стране једног или два лица из обезбеђења, особе коме су ова документа дата на чување морају да поседују одговарајући безбедносни сертификат одговарајућег нивоа.
- Ако приликом гашења пожара неовлашћено лице ипак приступи подацима, Одговорно лице заједно са одговарајућим лицима треба да сачини одговарајући записник.
- Треба обавестити Одговорно лице да треба да започне са обезбеђивањем места за чување и преношење докумената.
- Ако је пожар угрозио само једну просторију у административној зони, место евакуације треба да буде просторија бр…….. У случају да је пожар угрозио целу зграду……, место евакуације је…… (адреса) или регистар за податке.
- Током гашења пожара Одговорно лице треба да сарађује са руководиоцем ватрогасне службе, да му наведе која сигурносна места су најугроженија и које запаљиве материје се могу наћи тамо.
- Чланови ватрогасне службе у току пожара могу ући у безбедносну зону само уз одобрење руковаоца подацима.
- Након гашења пожара Одговорно лице треба да сачини записник о претрпљеном оштећењу или уништењу материјалних средстава и да тај записник преда законском заступнику.

б) У случају да дође до пожара ван радног времена

- Најмање две особе из обезбеђења треба одмах да оду на место пожара.

- Обезбеђење о пожару обавештава Одговорно лице.
- Даље поступање се врши како је наведено у одељку 7/а.

в) У случају пуцања водоводних цеви током радног времена
- Одговорно лице предузима мере како би блокирао централне чесме, као и секторе угроженог подручја
- Истовремено треба да се започне чување података који ће се преносити у просторију бр ……. Током преноса докумената, правилно чување података је у надлежности Овлашћеног лица.

г) У случају пуцања водоводних цеви ван радног времена
- Две патроле треба одмах да оду на место штете.
- Обезбеђење извештава Одговорно лице о догађају, који предузима мере блокирања централне чесме и угрожених подручја и одводи Одговорно лице на место штете.
- Након доласка Одговорног лица, даље поступати како је наведено у одељку 7/а.

8. Процедура поступања у случају природних катастрофа

У случају да дође до непредвиђених природних катастрофа (земљотреси, итд) на челу са Одговорним лицем треба проценити:

- физичку штету у рестрикривној зони;
- где се налазе оштећења безбедносних система који штите податке;
- утврдити да ли су подаци нестали или су уништени.

Након процене, Одговорно лице је дужно:
- да поднесе извештај законском заступнику;
- да обезбеди реконструкцију рестриктивних простора;
- да неоштећени подаци све време буду под заштитом Одговорног лица.

9. Процедура поступања у случају ванредног стања

Налог за евакуацију привременог регистра/регистра
- Ако се ванредно стање тиче само једне просторије, место евакуације је заштићена соба бр. …….. Током целог периода евакуације податке треба да чувају 2 чувара, а најмање један од чувара треба да поседује овлашћење законског заступника.

Уколико се ванредно стање тиче целе зграде ……..., податке треба одмах пренети у ……., или их однети у привремени регистар/регистар за податке. У сваком случају, Овлашћено лице прописује начин пратње приликом евакуације, тако да обезбеђење мора да поседује овлашћење законског заступника и лични безбедносни сертификат одговарајућег нивоа.

- Уколико ванредно стање не дозвољава евакуацију, користи се машина за уништавање докумената која мора да буде у могућности да уништи документа до њиховог непрепознавања и немогућности њиховог поновног склапања (2mm*15mm).
- После прекида ванредног стања потребно је направити посебан попис евакуисаних и уништених података.

10. Процедура поступања у случају непоштовања правила за руковање подацима

а) Када је документ привремено нестао, према нивоу тајности, се одмах подноси извештај законском заступнику (након разјашњења узрока нестанка и поновног прегледа)

б) Треба да се утврди да ли је неовлашћено лице имало приступ подацима.

в) Што се тиче ситуације дефинисане под одељком б), Овлашћено лице треба да сачини одговарајући записник о компромитовању безбедности без одлагања.

Одговорно лице у оквиру свог извештаја треба да предложи безбедносне мере, уколико је то потребно.

11. Остале мере безбедности

а) Сваку планирану промену рестриктивних простора, за разлику од акредитованих програма, треба да одобри законски заступник.

б) У привременом регистру/регистру ЗАБРАЊЕНО је уношење ватреног оружја, муниције и приватних мобилних телефона, чак и у искљученом режиму.

в) Брисање и чишћење административне зоне може се обављати једино у присуству особа које управљају објектима.

12. Информације о запосленима у привременом регистру/регистру

Одговорно лице/запослени у привременом регистру/регистру:
Име:
Положај:
Адреса:
Број мобилног телефона.:

Остали запослени:
Име:
Адреса:

Број телефона:
Број мобилног телефона:

Остали запослени:
Име:
Адреса:
Број телефона:
Број мобилног телефона:

Резервни план ступа на снагу дана његовог проглашења.

Направљено:…копија
Један примерак…..страна
Регистрациони бр.:
Администратор:
Прималац::

ПОЈМОВНИК О РАДУ СА ТАЈНИМ ПОДАЦИМА

1. **Административна безбедност** је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.
2. **Административна зона** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ИНТЕРНО".
3. **Алармни уређаји** су уређаји који служе за обезбеђивање објекта и предмета, тако што звучним или светлосним сигналом упозоравају на недозвољену активност. Могу бити механички, електрични и електронски.
4. **Аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио.
5. **Безбедносна зона I степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО". Самим уласком у ову зону сматра се да је остварен приступ тајним подацима.
6. **Безбедносна зона II степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО".
7. **Безбедносна култура** је безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности.
8. **Безбедносна провера** је поступак који пре издавања сертификата за приступ тајним подацима спроводи надлежни орган, у циљу прикупљања података о могућим безбедносним ризицима и сметњама у погледу поузданости за приступ тајним подацима.
9. **Безбедносна свест** подразумева знање и став који чланови организације имају у погледу заштите одређених вредности – националне безбедности, одбране, унутрашњих и спољних послова, људских слобода и права, као и физичке и интелектуалне имовине, а посебно информација и података којима располаже организација (орган јавне власти, правно лице или комапнија).
10. **Безбедносна сметња** представља чињеницу која онемогућава издавање сертификата.
11. **Безбедносне процедуре** су прописана правила за поступање лица у раду са тајним подацима.
12. **Безбедносни брифинг** представља упознавање са прописима којима се уређује тајност података и последицама неовлашћеног приступа и коришћења тајних података.
13. **Безбедносни инцидент** дешава се када постоји стварни или потенцијални ризик за штићене податке и даље категорисан као кривично дело или прекршај.

14. **Безбедносни ризик** је стварна могућност нарушавања безбедности тајних података.
15. **Безбедносни упитник** је саставни део документације у поступку издавања сертификата за приступ тајним подацима.
16. **Безбедност** означава стање неког субјекта (појединца, групе људи, заједнице, институције) које карактерише одсуство невоља, брига, несрећа, опасности и других зла.
17. **Дебрифинг** подразумева упознавање са прописима и обавезама по престанку потребе за приступом тајним подацима по различитим основама.
18. **Дата Бреацх/Компромитација података** је безбедносни инцидент у коме се осетљиви, заштићени или поверљиви подаци копирају, преносе, гледају, краду или користе од стране појединца који је неовлашћен за приступ тим подацима.
19. **Доставница** је потврда о томе да је лично или посредно достављање извршено која садржи лично име и адресу лица и податке којима се идентификује уручено писмено.
20. **Документ** је сваки носач податка (папир, магнетни или оптички медиј, дискета, УСБ меморија, смарт картица, компакт диск, микрофилм, видео и аудио запис и др.), на коме је записан или меморисан тајни податак.
21. **Евиденцију корисника тајних података** је евиденција коју води руковалац тајним подацима у органу јавне власти.
22. **Жалба** је правно средство у управном поступку које се може изјавити против управног акта тј. против првостепеног решења.
23. **Заштита података** је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације.
24. **Изјава** чини саставни део документације на основу које је издат сертификат за приступ тајним подацима, односно дозвола.
25. **Индустријска безбедност** представља примену мера ради обезбеђења заштите тајних података, од стране извођача или подизвођача, у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора.
26. **Инсајдер** (енг. инсидер - "неко унутра") је назив за особу која је припадник неке друштвене групе због чега располаже одређеним сазнањима недоступним широј јавности.
27. **Информанти** су лица која случајно и пригодно сазнају за планирана или извршена кривична дела и њихове учиниоце.
28. **Информатори** (поузданик, вигилант и агент провокатор) су особе спремне да дуже време полицији пружају криминалистички и кривично правне релевантне информације, при чему се њихов идентитет чува у тајности.
29. **Информациона безбедност** представља скуп мера које омогућавају да подаци којима се рукује путем икт система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

30. **Информациона безбедност тајних података** обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних информација које се обрађују у информационо комуникационим системима (ИКТ).
31. **Информациона гаранција** представља гаранцију од стране органа јавне власти или правног лица да ће адекватно штитит податке од неовлашћеног приступа, коришћења, дељења или злоупотребе уз поштовање прописа и стандарда за заштиту података
32. **Интегритет** значи очуваност изворног садржаја и комплетности података;
33. **Интерна контрола** представља мере пажње усмерене на спречавање грешака, прекомерних трошкова и преваре, проверава и обезбеђује поузданост информација.
34. **ISO/SEC 27001** је међународни стандард за управљање безбедношћу информација. Детаљно описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ИСМС) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.
35. **Компромитација тајног податка** представља умишљајно, нехатно или немарно откривање тајних података непозваним и неовлашћеним лицима.
36. **Компромитујуће електромагнетно зрачење (КЕМЗ)** представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података.
37. **Контраобавештајна заштита** је посебан вид обавештајне активности чији је циљ заштита тајних података сопствене државе, заштита виталних државних органа и институција, спречавање деловања противничких обавештајних служби на територији своје земље и друго.
38. **Корисник тајног податка** је држављанин Републике Србије или правно лице са седиштем у Републици Србији, коме је издат сертификат од стране надлежног органа, односно страно физичко или правно лице коме је на основу закљученог међународног споразума издата безбедносна дозвола за приступ тајним подацима, као и функционер органа јавне власти који на основу овог закона има право приступа и коришћења тајних података без издавања сертификата.
39. **Кривично дело** је безбедносни инцидент који би разумно могао да доведе или јесте довео до губитка или компромитовање штићених података и захтева истрагу ради даље анализе и покретања кривичног поступка.
40. **Криптографски производ** је софтвер или уређај путем кога се врши криптозаштита.
41. **Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима.
42. **Листа "ПОТРЕБНО ДА ЗНА"** представља међународни принцип рада са тајним подацима који подразумева списак лица и радних места који имају приступ тајним подацима у оквиру органа јавне власти/ принцип двоструког кључа приступу тајним подацима.

43. **Листа "ПОТРЕБНО ПОДЕЛИТИ СА"** представља међународни принцип рада са тајним подацима који подразумева списак органа јавне власти који међусобно размењују тајне податке.
44. **Лојалност** је значење изведено преко синонима: оданост, верност, исправност, поданичка верност, честитост, часност, привржености, поверљивост, постојаност, непроменљивост, искреност,поштење.
45. **Мере заштите** су опште и посебне мере које се предузимају ради спречавања настанка штете, односно мере које се односе на остваривање административне, информатичко-телекомуникационе, персоналне и физичке безбедности тајних података и страних тајних података.
46. **Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.
47. **Непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.
48. **Надлежност** представља право и дужност доношења одлука које се односе на управљање делегираним ресурсима (људским, буџетским, техником и тајним подацима) да би се остварили циљеви националне и организационе безбедности, односно система зштите тајних података.
49. **Обезбеђење** је планска примена и коришћење оперативно-тактичких метода, мера, радњи, средства и снага ради заштите од угрожавања одређених личности, људи, масовних скупова, имовине, отвореног-затвореног простора, фабричких хала, магацина или других објеката.
50. **Обрада података** је генерално, "прикупљање и употреба података ради стварања смислене информације".
51. **Овлашћено лице за одређивање тајности података (произвођач)** подразумева да креатор тајних података може бити свако лице које има одговарајући безбедносни сертификат и које према својим дужностима и задацима треба да креира, тј. рукује тајним подацима - информацијама.
52. **Одлука о одређивању тајних података у органу јавне власти** је одлука којом се одређују се тајни подаци у органу јавне власти, што укључује и утврђивање степена и рока тајности.
53. **Одређивање тајних података** је поступак којим се податак, у складу са овим законом, одређује као тајни и за који се утврђује степен и рок тајности.
54. **Одлука о одређивању руковаоца тајним подацима у органу јавне власти** је одлука којом се одређује се руковалац тајним подацима у органу јавне власти.
55. **Одговорност** када је у питању систем заштите тајних података и организациона безбедност, представља обавезу да се даваоцу овлашћења одговара за испуњавање тих овлашћења (обавеза поступања). Одговорност обухвата и давање информација и образложења за спровођење одређених поступака, активности или одлука, када је у питању рад са тајним подацима.
56. **Означавање степена тајности** је означавање тајног податка ознакама: "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО", "ПОВЕРЉИВО" или "ИНТЕРНО".

57. **Орган јавне власти** је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује.
58. **Организационе мере заштите** представљају организацију заштите процеса рада и функционисања информационо-комуникационог система у редовним околностима и ванредним ситуацијама.
59. **Организациони услови** односе се нарочито на организацију процеса рада, заштиту приступа тајним подацима, заштиту од неовлашћеног коришћења тајних података, одређивање одговорног лица задуженог за спровођење мера заштите, као и утврђивање поступка у случају ванредних и хитних околности.
60. **Патролирање** је услуга обезбеђења коју врше службеници обезбеђења крећући се у одређено време између више међусобно раздвојених места/објеката.
61. **Периметар је део физичке безбедности** који се мора поставити око објеката у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.
62. **Персонална безбедност** представља низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за безбедност.
63. **Податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и суверености, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове.
64. **Податак о личности** је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.
65. **Правно лице** има регистровано седиште на територији Републике Србије;обављање делатности у вези са интересима из члана 8. овог закона; постојање одговарајуће безбедносне провере; ако није у поступку ликвидације или стечаја; није кажњавано мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мере безбедности забране обављања одређених регистрованих делатности или послова,уредно измирење пореских обавеза и доприноса;
66. **Прекршај** је безбедносни инцидент који не доводи до губитка, компромитовања или сумње да је дошло до безбедносни инцидент.
67. **Процена ризика** је одређивање квантитативних и квалитативних вредности ризика који се односе на конкретну ситуацију и уочене претње.
68. **Регистарски систем** представља уређен систем који мора да буде реализован у складу са прописима и стандардима из области ЗТП.
69. **Решење** представља управни акт надлежног органа којим је решена управна ствар која је била предмет управног поступка.

70. **Ризик информационо-комуникационог система** подразумева могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
71. **Руковалац тајним податком** је физичко лице или организациона јединица органа јавне власти, који предузима мере заштите тајних података у складу са одредбама овог закона.
72. **Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
73. **Саботажа** описује намерне радње којима се наноси штета физичкој или виртуелној инфраструктури организације, укључујући непоштовање процедура одржавања или ИТ, контаминирање чистих простора, физичко оштећење објеката или брисање кода ради спречавања редовних операција.
74. **Сецуриту бреацхес/кршење безбедности** представља неовлашћени приступ информацијама на мрежама, серверима или уређајима, заобилажење сигурности на тим системима, што на крају резултира отицањем или компромитацијом података.
75. **Сајбер безбедност** представља примену технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.
76. **Сајбер претња** укључује крађу, шпијунажу, насиље и саботажу свега што је повезано са технологијом, виртуелном стварношћу, рачунарима, уређајима или интернетом.
77. **Сертификат за приступ тајним подацима** је документ који потврђује да лице има право приступа и коришћења тајних података у одговарајућој мери по принципу „потреба да зна“.
78. **Сертификовање привредних субјеката** омогућава њихово учешће на расписаним тендерима у државама са којима Република Србија има закључене и ратификоване међународне споразуме о размени и узајамној заштити тајних података.
79. **Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије.
80. **Страни тајни податак** је податак који Републици Србији повери страна држава или међународна организација уз обавезу да га чува као тајни, као и тајни податак који настане у сарадњи Републике Србије са другим државама, међународним организацијама и другим међународним субјектима, у складу са закљученим међународним споразумом који је са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија;
81. **Тајност** је својство које значи да податак није доступан неовлашћеним лицима.
82. **Тајни податак** је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности.

83. **Техничка заштита** је обезбеђење лица и имовине које се врши техничким средствима и уређајима, њиховим планирањем, пројектовањем, уградњом и одржавањем.
84. **Техничке мере заштите** представљају обезбеђење и заштиту података и информација и других елемената информационо-комуникационог система, који се остварују применом посебних техничко-технолошких процеса рада и/или спровођењем физичко-манипулативних мера заштите у било којој процедури у оквиру рада ИКТ система.
85. **Уговор** је документ који подразумева посебне мере заштите тајних података које се примењују на све организационе и техничке услове за чување тајних података у поступку закључења уговора између органа јавне власти и правног или физичког лица на основу којег се тајни подаци достављају овим лицима.
86. **Унутрашња контрола** је процес установљен и спровођен од стране руководиоца органа јавне власти, организационе јединице или овлашћеног појединца.
87. **Управни поступак** је поступак доношења управних аката. Под управним поступком подразумевају се процедурална правна правила која се примењују у вези са доношењем одлука у управним стварима.
88. **Физичка безбедност/сигурност** представља примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима се налазе или чувају тајни подаци који захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.
89. **Физичка заштита** је услуга обезбеђења која се пружа првенствено личним присуством и непосредном активношћу службеника обезбеђења у одређеном простору и времену у складу са планом обезбеђења, применом мера и овлашћења службеника обезбеђења;
90. **Физичко-техничка заштита** је обезбеђење лица и имовине применом физичке заштите и коришћењем средстава техничке заштите.
91. **Тајни податак означен степеном тајности „ДРЖАВНА ТАЈНА“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије.
92. **Тајни податак означен степеном тајности „СТРОГО ПОВЕРЉИВО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала тешка штета по интересе Републике Србије.
93. **Тајни податак означен степеном тајности „ПОВЕРЉИВО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по интересе Републике Србије.
94. **Тајни податак означен степеном тајности „ИНТЕРНО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по рад, односно обављање задатака и послова органа јавне власти.
95. **Технички услови** односе се нарочито на физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци, противпожарну заштиту, заштиту тајних података приликом преношења и достављања изван просторија

у којој се чувају, транспорт тајних података, обезбеђивање и заштиту информационо-телекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера крипто-заштите.

96. **Шифра** је пресликавање (трансформација, правило) којим се тајна порука пресликава у неразумљив низ знакова (слова, бројеве...)
97. **Шпијун** је ухода, доушник, достављач, потказивач, вребач, жбир...
98. **Шпијунажа** је прикривена или недозвољена пракса шпијунирања за потребе стране владе, организације, субјекта или особе ради добијања поверљивих информација ради војне, политичке, стратешке или финансијске користи.
99. **Штета** је нарушавање интереса Републике Србије настала као последица неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последица друге радње обраде тајних података и страних тајних података.
100. **Штићени простор** је објекат или простор на којем се врше услуге обезбеђења.

КАТАЛОГ ПРОПИСА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

- Закон о тајности података
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА” и „СТРОГО ПОВЕРЉИВО” - "Службени гласник РС", број 46 од 24. маја 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у органима јавне власти - "Службени гласник РС", број 79 од 29. јула 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству одбране - "Службени гласник РС", број 66 од 29. јуна 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству унутрашњих послова "Службени гласник РС", број 105 од 29. новембра 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Безбедносно-информативној агенцији "Службени гласник РС", број 70 од 7. августа 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Канцеларији Савета за националну безбедност и заштиту тајних података "Службени гласник РС", број 86 од 30. септембра 2013.
- УРЕДБА о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа "Службени гласник РС", број 63 од 19. јула 2013.
- УРЕДБА о посебним мерама физичко-техничке заштите тајних података "Службени гласник РС", број 97 од 21. децембра 2011.
- УРЕДБА о посебним мерама надзора над поступањем са тајним подацима „Службени гласник РС“, број 90 од 30. новембра 2011.
- УРЕДБА о посебним мерама заштите тајних података у информационо-телекомуникационим системима "Службени гласник РС", број 53 од 20. јула 2011.
- УРЕДБА о начину и поступку означавања тајности података, односно докумената "Службени гласник РС", број 8 од 11. фебруара 2011.
- УРЕДБА о садржини, облику и начину вођења евиденција за приступ тајним подацима "Службени гласник РС", број 89 од 29. новембра 2010.
- УРЕДБА о садржини, облику и начину достављања сертификата за приступ тајним подацима „Службени гласник РС“, број 54 од 4. августа 2010.
- УРЕДБА о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну

безбедност и заштиту тајних података и Министарству правде "Службени гласник РС", број 79 од 29. октобра 2010.

- УРЕДБА о обрасцима безбедносних упитника "Службени гласник РС", број 30 од 07. маја 2010.
- -ПРАВИЛНИК о службеној легитимацији и начину рада лица овлашћених за вршење надзора "Службени гласник РС", бр. 85 од 27. септембра 2013, 71 од 11. јула 2014.

ОСТАЛИ ПРОПИСИ

- Стратегија националне безбедности
- Стратегија одбране
- Закон о основама уређења служби безбедности
- Закон о одбрани и Закон о Војсци Србије
- Закон о полицији
- Закон о спољним пословима
- Закон о Безбедносно-информативној агенцији
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији
- Законик о кривичном поступку и Кривични законик
- Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
- Закон о државним службеницима
- Закон о информационој безбедности
- Закон о јавним набавкама и Уредба о јавним набавкама у области одбране и безбедности "Службени гласник РС", број 93 од 1. јула 2020.
- Закон о електронским комуникацијама
- Закон о пореском поступку и пореској администрацији
- Закон о заштити узбуњивача
- Закон о приватном обезбеђењу

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ

И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

Адреса електронске поште за заказивање онлине консултација:
online.konsultacije@nsa.gov.rs

Адреса електронске поште за заказивање брифинга:
termini.sertifikati@nsa.gov.rs

веб: www.nsa.gov.rs