



КО ЈЕ ОДГОВОРАН ЗА ЗАШТИТУ ПОДАТАКА?

Упоредни преглед према Закону о тајности података (ЗТП), Закону о заштити података о личности (ЗЗПЛ) и Закону о информационој безбедности (ЗИБ)

У свакодневном раду органа јавне власти заштита информација заснива се на три различита правна оквира. Иако се поједини појмови као тајни податак, лични податак и дигитална информација често погрешно користе као синоними, свака улога има другачији предмет заштите, другачији правни основ и различите обавезе.

Разумевање ових разлика представља први корак ка ефикасној, законитој и усклађеној заштити информација.

1. КЉУЧНЕ РАЗЛИКЕ: ТАБЕЛА УЛОГА

Улога	Правни основ	Ко је то?	Шта штити? (Фокус)	Главна обавеза
Руковалац тајним подацима	ЗТП (Закон о тајности података)	Физичко лице или организациона јединица органа јавне власти.	Тајне податке, односно податке од интереса за Републику Србију који су, у складу са Законом о тајности података, одређени и означени одговарајућим степеном тајности.	Контрола приступа и руковања: обезбеђује да тајним подацима приступају искључиво овлашћена лица са потребом да знају („need-to-know“), води прописане евиденције, контролише умножавање, достављање, чување и уништавање тајних података.
Руковалац података о личности	ЗЗПЛ (Закон о заштити података о личности)	Физичко или правно лице, односно орган власти.	Права појединца (приватност и законитост обраде).	Одређивање сврхе: одређује зашто и како се подаци обрађују и мора бити у стању да докаже усклађеност (начело одговорности).
Оператор ИКТ система	ЗИБ (Закон о информационој безбедности, „Службени гласник РС“, бр. 91/2025)	Правно лице, предузетник или орган јавне власти који користи ИКТ систем у обављању својих надлежности.	Инфраструктура и средства (сервери, мреже, рачунари, софтвер).	Физичка и техничка заштита: спроводи организационе, физичке и техничке мере ради обезбеђивања поверљивости, интегритета, расположивости и аутентичности ИКТ система и података.

Напомена о пословној тајни: Поред три основна стуба заштите (тајни подаци, подаци о личности и ИКТ системи), у правном систему постоји и четврти концепт – **пословна тајна**. Она се односи на информације које имају економску вредност и чије откривање би нанело штету привредном субјекту. Регулисана је Законом о заштити пословне тајне и Законом о привредним друштвима, а у пракси је најчешће релевантна у сарадњи јавних органа са приватним компанијама (нпр. тендери, уговори, техничка документација). За разлику од три стуба који су директно везани за јавне органе, пословна тајна је пре свега инструмент **заштите интелектуалне својине**, али је важно да органи јавне власти буду свесни њеног постојања и да у уговорним односима обезбеде адекватне мере заштите поверљивости.



КО ЈЕ ОДГОВОРАН ЗА ЗАШТИТУ ПОДАТАКА?

Упоредни преглед према Закону о тајности података (ЗТП),
Закону о заштити података о личности (ЗЗПЛ) и
Закону о информационој безбедности (ЗИБ)

2. КЉУЧНЕ СЛИЧНОСТИ: ЗАЈЕДНИЧКИ ИМЕНИТЕЉ

Иако су фокуси различити, сва три закона захтевају од организације да испуни иста три фундаментална принципа:

1. **Процена ризика:** Сваки од ових актера мора да процени ризике (безбедносне, по приватност или по ИКТ систем) и да примени мере које су сразмерне том ризику.
2. **Документовање:** Ниједна заштита не постоји ако није записана. То су, између осталог, План заштите тајних података или прописане евиденције и процедуре о руковању тајним подацима (ЗТП), евиденција активности обраде (ЗЗПЛ) и акти и документација о безбедности ИКТ система (ЗИБ).
3. **Људски фактор:** Сва три прописа захтевају да лица која обављају ове послове буду поуздана, обучена и да имају јасно дефинисана овлашћења и одговорности.

3. ПРАКТИЧНИ ИЗАЗОВ: КАДА СЕ УЛОГЕ ПРЕКЛАПАЈУ?

У пракси, један исти орган јавне власти (а често и исти људи) истовремено обавља све три улоге. На пример, приликом запошљавања новог државног службеника:

- Као **орган јавне власти**, покреће поступак за издавање сертификата за приступ тајним подацима, када је то законом прописано.
- Као **руководилац података о личности**, орган мора законито да обради податке о личности, укључујући посебне врсте података, када је то законом дозвољено.
- Као **оператор ИКТ система**, орган мора да осигура да се ти подаци чувају у ИКТ систему, уз примену одговарајућих криптографских и других мера заштите.

Златно правило: Ове функције не смеју да раде у изолацији („силосима“). Неопходна је координација између безбедносног менаџера, ИТ администратора и лица за заштиту података о личности.



КО ЈЕ ОДГОВОРАН ЗА ЗАШТИТУ ПОДАТАКА?

Упоредни преглед према Закону о тајности података (ЗТП),
Закону о заштити података о личности (ЗЗПЛ) и
Закону о информационој безбедности (ЗИБ)

4. УСЛАЂИВАЊЕ СА ЕУ, НАТО И МЕЂУНАРОДНИМ СТАНДАРДИМА

Да би систем заштите био модеран, отпоран и међународно препознатљив, ова три стуба треба да буду усклађена са следећим стандардима и добром праксом:

- **NIS2 директива (ЕУ):** Захтева да оператор ИКТ система (посебно ако је „од посебног значаја“) успостави јасне процедуре за управљање ризицима, примени одговарајуће организационе и техничке мере заштите и обезбеди рано обавештавање о значајним инцидентима у року од 24 часа, након чега следе детаљнија обавештења, у складу са NIS2.
- **ISO/IEC 27001:** Представља међународни стандард за успостављање, примену, одржавање и континуирано унапређивање система управљања информационом безбедношћу (ISMS). Заснива се на процени ризика, примени одговарајућих безбедносних контрола и континуираном побољшању организационих, техничких и физичких мера заштите.
- **НАТО стандарди:** Захтевају да се тајним подацима рукује у складу са националним прописима и међународним безбедносним стандардима, уз примену принципа „need-to-know“, физичке, организационе и техничке заштите, као и модела Zero Trust (нула поверења), где је то применљиво.

5. БРЗА КОНТРОЛНА ЛИСТА ЗА РУКОВОДИОЦЕ

Да ли је ваш орган јавне власти усклађен? Проверите ове четири тачке:

- **Јасноћа улога:** Да ли су у интерним актима јасно именована лица за све три улоге (или је дефинисана њихова међусобна координација)?
- **Документација:** Да ли постоје важећи Акт о процени ризика (ЗИБ) и План заштите тајних података, односно прописане евиденције и процедуре о руковању тајним подацима (ЗТП)?
- **Трећа лица:** Да ли уговори са добављачима услуга у облаку (cloud) и одржавања прописују одговарајуће уговорне, организационе и техничке мере заштите података, укључујући контролу приступа и евидентирање активности?
- **Едукација:** Да ли запослени знају разлику између тајног податка и податка о личности и коме да пријаве сумњив догађај?

За сва питања у вези са применом прописа о заштити тајних података обратите се:

Канцеларији Савета за националну безбедност и заштиту тајних података