ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

КЉУЧНА ПОРУКА: У складу са **Законом о тајности података, Законом о информационој безбедности, Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима, Уредбом о посебним мерама физичко-техничке заштите тајних података** и другим прописима којима се уређује заштита тајних података, строго је забрањено креирање, обрада, анализа, чување или пренос тајних података (степена тајности **„ДРЖАВНА ТАЈНА“, „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ и „ИНТЕРНО“**) употребом јавних, бесплатних или неакредитованих алата заснованих на вештачкој интелигенцији (AI), јавних cloud сервиса, као и других неакредитованих информационо-комуникационих система (ИКТ система) и дигиталних платформи. **Тајни подаци могу се креирати, обрађивати, чувати и преносити искључиво у акредитованим ИКТ системима у којима су примењене прописане организационе, техничке, физичке и криптографске мере заштите.**

Под **акредитованим ИКТ** системом подразумева се информационо-комуникациони систем који је прошао поступак процене ризика и безбедносне акредитације у складу са прописима којима се уређују заштита тајних података и информациона безбедност, у којем су примењене прописане организационе, кадровске, физичке, техничке и криптографске мере заштите.

1. ШТА ЈЕ КОНКРЕТНО ЗАБРАЊЕНО?

Сваки од наведених поступака представља повреду прописа о заштити тајних података и информационој безбедности и може довести до безбедносних, кривичних, прекршајних и дисциплинских последица.

- **Унос текста и података у јавне AI алате** – куцање, копирање или уношење (copy-paste) тајних података у бесплатне или јавно доступне AI платформе (нпр. ChatGPT, Claude, Gemini, Copilot и друге) ради превођења, сажимања, анализе, генерисања или дораде текста.
- **Отпремање (upload) датотека** – слање PDF, Word, Excel докумената, фотографија, скенираних докумената, аудио и видео записа или других датотека у јавне AI системе или cloud сервисе ради OCR-а, анализе, превођења, издвајања података, генерисања садржаја или било које друге обраде.
- **Коришћење јавних cloud сервиса** – чување, синхронизација или дељење тајних података путем сервиса као што су Google Drive, Dropbox, OneDrive, iCloud, WeTransfer или других неакредитованих cloud платформи.
- **Коришћење неакредитованих ИКТ система** – рад са тајним подацима на рачунарима, серверима, таблетима, мобилним телефонима или другим уређајима који нису акредитовани за рад са тајним подацима.
- **Коришћење приватне ИКТ опреме** – употреба приватних лаптопова, мобилних телефона, USB меморија, спољних дискова и других приватних уређаја за обраду, чување или пренос тајних података.

ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

• **Повезивање акредитованих ИКТ система са јавним мрежама или неовлашћеним сервисима**, супротно прописаним мерама безбедности.
• **Коришћење неакредитованих локалних AI система**: Забрањена је употреба локално инсталираних, open-source, експерименталних или комерцијалних AI модела који нису прошли поступак безбедносне процене и акредитације, без обзира на то да ли су повезани на интернет.
• **Самостално инсталирање AI алата (Shadow AI)**: Забрањено је самостално инсталирање, конфигурисање или коришћење било ког система заснованог на вештачкој интелигенцији без претходног одобрења и спроведеног поступка безбедносне процене.

Напомена: Забрана се односи и на делимичне уносе, изводе, резимее, анонимизоване верзије, тестне примере, фотографије, табеле, шеме, метаподатке и друге сегменте докумената који, самостално или у комбинацији са другим информацијама, могу омогућити идентификацију, реконструкцију или откривање тајног податка.

2. ЗАШТО ЈЕ ТО БЕЗБЕДНОСНИ РИЗИК?

• **Губитак контроле над подацима.** Тајни подаци напуштају безбедносно контролисано окружење органа јавне власти и могу се обрађивати на серверима трећих лица, често ван Републике Србије.
• **Губитак суверенитета над информацијама.** Орган јавне власти губи контролу над местом чувања, начином обраде, даљим коришћењем и брисањем података.
• **Непостојање безбедносних гаранција.** Јавни AI алати и cloud сервиси не обезбеђују законом прописане гаранције поверљивости, интегритета, аутентичности, расположивости и непорецивости података.
• **Ризик од нарушавања интегритета података и аналитичког процеса.** Генеративни системи вештачке интелигенције могу произвести нетачне, непотпуне или измишљене информације (тзв. „AI халуцинације“), као и резултате настале манипулацијом улазних података или модела, што може довести до погрешних аналитичких, оперативних или стратешких процена и одлука.
• **Цурење метаподатака.** Отпремањем докумената, фотографија или других датотека у јавне AI системе могу се открити скривени метаподаци (нпр. аутор документа, назив институције, време креирања, историја измена, геолокација, техничке карактеристике уређаја и други идентификациони подаци), чиме се могу компромитовати додатне информације од значаја за безбедност, иако нису непосредно видљиве у самом садржају документа.
• **Ризик од секундарне анализе података (aggregation risk).** Јавни AI системи могу повезивати унете податке са другим јавно доступним или претходно обрађеним информацијама и реконструисати чињенице, односе или обрасце који нису непосредно откривени у самом документу.

ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

• **Недостатак прописаних мера заштите.** Неакредитовани ИКТ системи не обезбеђују прописану контролу приступа, ревизијски траг, евидентирање активности, криптозаштиту, управљање криптоматеријалима и друге мере информационе безбедности.
• **Угрожавање националне безбедности.** Компромитација тајних података може угрозити националну безбедност, одбрану, спољнополитичке интересе, рад државних органа и друге законом заштићене интересе Републике Србије.
• **Ризик од компромитације интегритета података:** Јавни AI системи могу генерисати нетачне, непотпуне или измишљене информације („AI халуцинације“), што може довести до погрешних аналитичких процена, оперативних закључака или доношења погрешних одлука.
• **Ризик од откривања метаподатака:** Отпремањем докумената могу се открити скривени метаподаци (аутор, време израде, историја измена, локација, технички подаци уређаја и др.), који могу представљати осетљиве информације иако нису видљиви у самом документу.

3. ОСНОВНИ БЕЗБЕДНОСНИ ЗАХТЕВИ

У складу са Законом о информационој безбедности и прописима којима се уређује заштита тајних података, рад са тајним подацима дозвољен је искључиво у акредитованим ИКТ системима у којима су:

• спроведена процена ризика и поступак акредитације;
• примењене организационе, техничке и физичке мере заштите;
• примењене мере криптобезбедности и криптозаштите ради обезбеђивања поверљивости, интегритета, аутентичности и непорецивости података;
• употребљени искључиво верификовани и одобрени криптографски производи, када је то прописано законом;
• обезбеђено безбедно управљање криптоматеријалима;
• примењене мере заштите од компромитујућег електромагнетног зрачења (КЕМЗ), када је то прописано;
• успостављени контрола приступа, ревизијски траг, безбедносни надзор и евидентирање активности.

Јавни AI алати, јавни cloud сервиси и други неакредитовани ИКТ системи не испуњавају наведене услове и не могу се користити за рад са тајним подацима.

ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

4. ПРАВНЕ ПОСЛЕДИЦЕ

Поступање супротно прописима о заштити тајних података и информационој безбедности може представљати кривично дело, прекршај и основ за дисциплинску и безбедносну одговорност.

Кривична одговорност: Чланом 98. Закона о тајности података прописано је да неовлашћено саопштавање, предаја, чињење доступним или прибављање тајних података непозваном лицу представља кривично дело. У зависности од степена тајности податка прописане су казне затвора:

- „ИНТЕРНО“ и „ПОВЕРЉИВО“ – од три месеца до три године;
- „СТРОГО ПОВЕРЉИВО“ – од шест месеци до пет година;
- „ДРЖАВНА ТАЈНА“ – од једне до десет година.

Кривична одговорност постоји и када је дело учињено из нехата, ако је услед непажљивог поступања тајни податак постао доступан непозваном лицу.

Прекршајна одговорност: Законом о тајности података прописана је прекршајна одговорност:

- одговорног лица у органу јавне власти (члан 99.);
- руковаоца тајним подацима (члан 100.), ако не предузима прописане мере заштите тајних података.

Поред тога, Законом о информационој безбедности прописане су обавезе у области управљања ризицима, примене мера информационе безбедности и поступања у случају безбедносних инцидената.

Дисциплинске и безбедносне последице: Повреда прописа може довести до:

- покретања дисциплинског поступка;
- престанка испуњености услова за приступ тајним подацима, односно престанка важења безбедносног сертификата;
- покретања поступка поводом безбедносног инцидента;
- предузимања других мера у складу са законом.

ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

5. ПРАВИЛНО ПОСТУПАЊЕ

1. Користите искључиво акредитоване ИКТ системе.
2. За пренос и чување тајних података користите искључиво одобрене криптографске производе и мере криптозаштите, у складу са Законом о информационој безбедности и прописима донетим на основу тог закона.
3. Пре увођења било ког AI система, софтвера или дигиталне платформе мора бити спроведена процена ризика, примењене мере информационе безбедности и окончан поступак акредитације.
4. Ова забрана не односи се на локално инсталиране и акредитоване AI системе који су прошли прописану безбедносну процену и налазе се под потпуном техничком и административном контролом органа јавне власти.
5. Пре употребе било ког новог AI алата или дигиталне платформе обавезно се консултујте са руковаоцем тајним подацима у органу јавне власти, службеником за безбедност или надлежном организационом јединицом за информациону безбедност.
6. Ако је тајни податак случајно унет у јавни AI систем или cloud сервис, одмах прекините рад. Не искључујте уређај насилно, не бришите историју рада, датотеке, логове или друге дигиталне трагове и не покушавајте самостално да отклоните последице. Без одлагања пријавите безбедносни инцидент ради спровођења прописаних процедура, процене настале штете и очувања форензичких трагова.

Напомена о криптобезбедности: Приликом рада са тајним подацима примењују се мере криптобезбедности и криптозаштите у складу са Законом о информационој безбедности. За заштиту преноса и чувања тајних података могу се користити искључиво верификовани и одобрени криптографски производи, у складу са законом и прописима донетим на основу закона.

6. **НАПОМЕНА: У тренутку израде овог инфолиста Република Србија нема посебан закон којим се свеобухватно уређује развој, стављање на тржиште и употреба система вештачке интелигенције. До доношења таквог закона, употреба система вештачке интелигенције у органима јавне власти, а нарочито приликом рада са тајним подацима, процењује се и дозвољава искључиво у складу са Законом о тајности података, Законом о информационој безбедности, прописима којима се уређује заштита тајних података, заштита података о личности и другим прописима од значаја за информациону и националну безбедност.**

ЗАШТИТА ТАЈНИХ ПОДАТАКА ПРИ КОРИШЋЕЊУ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

7. ПРАВНИ ОСНОВ

Овај инфолист заснива се на:

- Закону о тајности података;
- Закону о информационој безбедности;
- Закону о заштити података о личности;
- Уредби о посебним мерама заштите тајних података у информационо-телекомуникационим системима;
- Уредби о посебним мерама физичко-техничке заштите тајних података;
- другим прописима којима се уређују заштита тајних података, информациона безбедност и безбедност ИКТ система.

8. КОНТАКТ

За сва питања у вези са применом прописа о заштити тајних података, акредитацијом ИКТ система, криптозаштитом и поступањем у случају безбедносних инцидената обратите се: **Канцеларији Савета за националну безбедност и заштиту тајних података www.nsa.gov.rs**

ЗАПАМТИТЕ: Ако постоји и најмања сумња да ли је одређени систем, апликација или алат дозвољен за рад са тајним подацима, сматрајте да није дозвољен док не добијете писмену потврду од руковаоца тајним подацима у органу јавне власти.

Никада не претпостављајте да је неки AI алат, cloud сервис или дигитална платформа безбедна само зато што је широко доступна или се користи у пословне сврхе. Код рада са тајним подацима дозвољено је искључиво оно што је законом прописано, безбедносно процењено, криптографски заштићено и званично акредитовано.