ШТИЋЕНИ ПОДАЦИ У РЕПУБЛИЦИ СРБИЈИ

СКРИПТА

Проф.др Горан Д. Матић

Београд, 2025. година

Уводна разматрања о проблематици штићених података у Републици Србији

У Републици Србији, заштита података, као и права и обавезе у вези са њима, регулисана је широким спектром законодавних аката који покривају различите аспекте штићених података. Класификација и адекватна заштита ових података играју кључну улогу у контексту националне безбедности, економске стабилности, јавног здравља и поштовања људских права. Иако је створен солидан правни оквир, имплементација и надзор у овој области остају значајан изазов.

Историјски контекст и правна еволуција

Материја штићених података у Србији прошла је јасну правну еволуцију, која се може пратити још од настанка модерне српске државе у 19. веку до данас. У почетку су штићени подаци били регулисани кроз појединачне акте и подзаконске прописе из области војске, полиције и судства, где је поверљивост информација третирана као питање од виталног значаја. Временом, ова регулатива прелази у шире оквире, обухватајући и јавну управу и здравство.

У периоду од 1815. године, када је започела модерна државна организација у Србији, започела је и потреба за регулисањем тајности у војним и административним питањима. Постојале су разне одредбе које су се односиле на поверљивост података, али су биле ограничене на војну и дипломатску сферу. У овом периоду, тајност је била изузетно важна за одржавање стабилности и независности земље, те је у контексту војних и дипломатских односа било неопходно заштитити важне информације.

Након Првог светског рата и уласка Србије у Краљевину Југославију, састављена су уредба и закони који су регулисали појам тајности у новој држави. Ова законска решења, иако нису била усмерена директно на заштиту пословних тајни у савременом смислу, поставила су основу за даље развијање правног система који ће се касније фокусирати и на приватни сектор. Са формирањем Краљевине Југославије 1918. године, законодавни оквир заштите података, укључујући тајне податке, пословне и личне податке, претрпео је значајне промене. У овом периоду, већ је постојала потреба да се обавезно чувају тајне које су се односиле на војне, политичке и економске интересе земље, али и на чување података који су били од значаја за функционисање државних институција и јавног сектора.

Након Другог светског рата, у социјалистичкој Југославији заштита података добила је нови импулс и регулативе су постале чвршће. Влада је креирала специфичне прописе који су се односили на заштиту тајних података, али и на чување пословних и професионалних тајни као важан аспект економске и државне сигурности. У овом периоду, осим војних и политичких тајни, посебну пажњу добијали су и подаци који су се односили на економске интересе земље. Податке који су имали посебну економску вредност често су чинили и подаци о важним индустријама, стратешким ресурсима и капацитетима унутрашње привреде.

Социјалистичка Југославија такође је поставила велике нагласке на заштиту података који су били од интереса за државу, али и на одржавање тајности података који су се односили на личне информације грађана и радну снагу, што је обухватало и податке о запосленима, као и о њиховим правима и обавезама у систему социјалистичког самоуправљања. У овом периоду, постојала је регулатива која је налагала да предузећа

чувају тајне податке од конкуренције, као и од страних власти које су могле угрозити економски суверенитет.

Држава је такође регулисала питање личних података у контексту безбедности, али није било у потпуности развијеној свести о правима појединаца у односу на њихове личне податке као што је то данас. Лични подаци су се често користили у различитим аспектима живота грађана, укључујући државну контролу над радним окружењем, али су истовремено били и штит зарад економских интереса.

После распада Социјалистичке Југославије и формирања нових држава, укључујући Републику Србију, заштита података добила је на значају у складу са глобалним трендовима и са усвајањем нових стандарда заштите информација. Закони који се односе на тајне податке и пословне тајне постали су значајнији, а регулисани су са све већом пажњом на правима појединаца, али и потреби да се штите пословни интереси у глобализованом економском окружењу.

Лични подаци - су првобитно били третирани као службена тајна, нарочито у здравству, где је поверљивост података пацијената имала изузетан значај. На нивоу бивше Југославије, донета је Уредба о заштити личних података, али она никада није у потпуности примењена. Поверљивост података у здравству истиче се као посебан сегмент који се кроз историју третирао под режимом службене тајне. Заштита медицинских података пацијената имала је дугу традицију, при чему је поверљивост била основни принцип у управљању овим подацима. Овај приступ је и даље веома значајан, али сада као личних података и професионалне медицинске тајне, посебно у контексту модерног здравственог система, где се велике количине осетљивих података обрађују у дигиталним форматима.

Први значајан корак у модерној регулацији личних података у Србији представља доношење Закона о заштити података о личности 2009. године. Овај закон је установио основне принципе заштите личних података и дефинисао права и обавезе у обради података. Нови Закон о заштити података о личности из 2018. године усклађен је са Општом уредбом о заштити података (GDPR) Европске уније, чиме је Србија усвојила савремене стандарде у овој области.

Тајни подаци - Пре доношења Закона о тајности података 2009. године, ова област је углавном била регулисана подзаконским актима из области одбране, који су се примењивали на све органе јавне власти као део наслеђа југословенског правног система. Ови прописи су обезбеђивали централизован и строг приступ управљању поверљивим информацијама.

Доношење Закона о тајности података 2009. године представља прекретницу у уређењу ове области, стварајући јединствени оквир за класификацију, обележавање и управљање поверљивим информацијама. Закон је увео јасне категорије тајности и процедуре које обезбеђују транспарентност и контролу над обрадом тајних података.

Пословна тајна - Историјат пословне тајне у Србији до данас показује континуирану еволуцију која је пратила политичке и економске промене у земљи. Од раних дана када је тајност била искључиво везана за војне и дипломатске интересе, до савременог периода који признаје важност пословне тајне за развој економије, Србија је унапредила своје правне механизме како би заштитила ове важне информације. Тиме се обезбеђује

не само заштита од спољних претњи већ и од неовлашћеног приступа који може угрозити конкурентност на тржишту и поверење у пословне односе.

Данас, законодавство Србије обухвата и прецизну дефиницију пословних и професионалних тајни, као и регулисање начина на који се чувају тајне информације у корпоративном сектору. Заштита личних података такође добија све већи значај у односу на прелазак на дигиталну економију и глобализацију информација. Пословна тајна се, у савременом контексту, разматра као важан фактор који доприноси конкурентности предузећа, као и економској сигурности земље у целини.

Кључни аспекти проблематике

Недовољно јасно дефинисање и обележавање података У пракси се често дешава да подаци од јавног значаја добијају ознаку поверљивости без одговарајуће анализе. Ово нарушава транспарентност и отежава јавни надзор.

Непотпуно усклађивање прописа Прелазак са подзаконских аката на законску материју доноси бројне изазове, укључујући колизију различитих закона, попут Закона о слободном приступу информацијама и Закона о тајности података.

Поглед из силоса Један од великих проблема у пракси је тзв. "поглед из силоса", где институције и организације делују изоловано, фокусирајући се искључиво на своје надлежности и не сарађујући са другим субјектима. Овај фрагментирани приступ доводи до недостатка координације, што угрожава ефикасност заштите података. На пример, различите институције могу имати конфликтне смернице за руковање истим подацима, чиме се отежава доследна примена прописа.

Ефекат четири мајмуна Прича о "четири мајмуна" илуструје укорењене праксе које опстају чак и када су нови прописи и препоруке доступни. У експерименту, група мајмуна је смештена у просторију са мердевинама које воде до банана. Када један мајмун покуша да дохвати банане, сви добијају електрошокове. Временом, мајмуни престају да покушавају. Када се замене новим мајмунима, они, иако никада нису били изложени шоковима, настављају да спречавају друге да дохвате банане. У пракси, ово означава понашање где институције и појединци одржавају застареле или погрешне праксе, игноришући нова правила и упутства.

Технолошки изазови Савремена технолошка решења, као што су криптографија и блокчејн, нису довољно примењена у Србији због недостатка ресурса и недовољне обуке запослених.

Балансирање безбедности и јавног интереса Злоупотреба класификације и означавања података са циљем ускраћивања информација јавног значаја представља озбиљан изазов за транспарентност и демократију (нпр. ознаком тајности или пословном тајном).

Препоруке за унапређење система

У циљу побољшања система заштите података, потребно је применити следеће мере:

Доношење и примена јединственог закона који ће интегрисати све аспекте управљања штићеним подацима.

Јачање институционалних капацитета за боље управљање и надзор.

Унапређење координације између органа јавне власти како би се превазишли проблеми изолованог деловања.

Примена савремених технолошких решења, посебно у области класификације и безбедног руковања подацима.

Подизање свести и едукација о значају заштите података међу запосленима и грађанима.

Препоруке за унапређење система

Доношење јединственог закона који обухвата све аспекте заштите података, укључујући личне, тајне и медицинске податке.

Јачање институционалних капацитета кроз едукацију стручњака и обезбеђивање адекватних ресурса.

Унапређење координације између институција ради превазилажења фрагментираног деловања.

Интензивније коришћење савремених технологија, попут блокчејна и криптографских метода.

Подизање свести јавности и организација о значају заштите података и поштовању законских обавеза.

У Србији, од периода формирања Краљевине Југославије до данас, законодавни оквир за заштиту података претрпео је значајне промене. Од заштите војних и политичких тајни, преко социјалистичког периода када су се додали и пословни и професионални аспекти, па до модерног доба када се пружа равномерна заштита свих врста података – од тајних и пословних до личних података. Србија је кренула путем усклађивања свог законодавства са међународним стандардима, што омогућава већу заштиту података и спречава злоупотребе, али и гарантује економску безбедност земље у глобализованом свету.

А У Т О Р

С а д р ж а ј

1. Класификација и заштита података у Републици Србији

Заштићени подаци представљају општи термин за податке који се не сматрају јавним и чија је заштита неопходна из различитих разлога, било на основу закона, уговора или ради очувања људских слобода и права, укључујући право на приватност. Процес класификације и заштите података омогућава њихово организовање, разврставање и контролисано руковање у складу са правним оквиром и специфичним захтевима.

Процес класификације података

Класификација података подразумева:

Разврставање и категоризацију података у различите врсте или класе, на основу њихове важности и осетљивости.

Омогућава одвајање података ради различитих државних, пословних или личних сврха.

Представља кључни аспект управљања подацима и дефинисања њихове доступности.

Основне категорије класификације у Републици Србији обухватају:

Подаци од интереса за Републику Србију (тајни подаци)

Лични подаци

Пословне тајне

Професионалне тајне

Јавни подаци

Архивска грађа

Штићени подаци у Републици Србији

Штићени подаци у Србији обухватају различите категорије информација које су законом, подзаконским актима или интерним прописима заштићене од неовлашћеног приступа, обраде, откривања или злоупотребе. Њихова заштита кључна је за очување безбедности, приватности и јавних интереса. Ове податке можемо поделити у две главне групе:

1. Подаци који су законом заштићени

Њихово откривање или злоупотреба носе кривичну или прекршајну одговорност.

2. Административни и осетљиви подаци

Иако нису формално означени као тајни, њихова обрада и приступ подлежу посебним правилима.

Категорије штићених података

I. Подаци који су законом заштићени:

Тајни подаци

Ознаке степена тајности: *Државна тајна*, *Строго поверљиво*, *Поверљиво*, *Интерно*.

Уређени Законом о тајности података.

Подаци о личности

Регулисани Законом о заштити података о личности.

Укључују идентификационе податке и информације о приватности грађана.

Пословна тајна

Дефинисана Законом о привредним друштвима.

Обухвата информације од тржишне вредности.

Банкарска и фискална тајна

Регулисана Законом о банкама и Законом о порезу на додату вредност.

Укључује податке о финансијским трансакцијама и обавезама.

Здравствени подаци

Заштићени Законом о здравственој заштити и Законом о правима пацијената.

Укључују медицинску документацију.

Судски, тужилачки и прекршајни подаци

Регулисани законима о судским поступцима.

Обухватају истраге, доказе, сведочења и пресуде.

Поверљиви подаци у јавним набавкама

Регулисани Законом о јавним набавкама.

Укључују осетљиве информације о понуђачима и процедурама.

Професионалне тајне

Адвокатске, лекарске, новинарске и друге професионалне поверљиве информације.

Подаци о малолетницима

Регулисани Кривичним закоником и Законом о заштити права детета.

Укључују личне податке и судске поступке.

Пореска тајна

Регулисана Законом о пореском поступку и администрацији.

II. Административни и осетљиви подаци:

Отворени подаци

Јавно доступни подаци објављени од стране државних органа.

Подаци за сарадњу са ЕУ

Регулисани споразумима са Европском унијом.

Подаци о безбедности инфраструктуре

Витална инфраструктура, енергетика и саобраћај.

Оперативни подаци полиције и јавне безбедности

Аналитички извештаји и процене.

Еколошки подаци

Податке о загађењу и заштити животне средине.

III. Архивска грађа:

Архивска грађа је део културног наслеђа и обухвата:

Јавну архивску грађу доступну након истека рокова (70 година од настанка, или 100 година од рођења лица).

Затворену грађу са ограниченим приступом (нпр. материјали служби безбедности, поверљиви документи).

Напомене:

Обухвата историјску, војну и културну документацију.

Дигитализација омогућава приступ осетљивим материјалима без угрожавања оригинала.

Надлежност: Државни архив Србије и Војни архив.

Класификација и заштита података, укључујући архивску грађу, од суштинског су значаја за очување историјског, културног и националног наслеђа Републике Србије. Док су неки подаци отворени за јавност, други подлежу строгим правилима и процедурама како би се осигурала њихова безбедност. Континуирана модернизација система и дигитализација архивске грађе од кључног су значаја за унапређење приступа и очување за будуће генерације.

2. Тајни подаци у Републици Србији
Правни основ, категорије и односи са другим штићеним подацима

Према **Закону о тајности података** („Службени гласник РС“, бр. 104/2009), **тајни податак** је дефинисан као:

"Подаци које је надлежни орган, у складу са овим законом, означио одговарајућим степеном тајности, а чије неовлашћено откривање, коришћење или приступ може настати или проузроковати штетне последице по интересе Републике Србије."

Ова дефиниција истиче да тајни подаци морају бити **званично означени** од стране надлежног органа и да њихово откривање може нанети **штетне последице** по државу.

Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја, односе се нарочито на:

1) националну безбедност Републике Србије, јавну безбедност, односно на одбрамбене, спољнополитичке, безбедносне и обавештајне послове органа јавне власти;

2) односе Републике Србије са другим државама, међународним организацијама и другим међународним субјектима;

3) системе, уређаје, пројекте, планове и структуре који су у вези са подацима из тач. 1) и 2) овог става;

4) научне, истраживачке, технолошке, економске и финансијске послове који су у вези са подацима из тач. 1) и 2) овог става.

Према одредбама Закона о одбрани (чл. 102) – мере заштите тајних података:

Тајни подаци који се односе на систем одбране означени као подаци од интереса за националну безбедност Републике Србије, као и тајни подаци настали у раду команди, јединица и установа Војске Србије, чијим би откривањем неовлашћеним лицима настала штета, штите се у складу са законом којим се уређује заштита тајности податка и не могу се учинити доступним јавности.

Тајним подацима значајним за систем одбране сматрају се:

1) подаци и документа од значаја за систем националне безбедности, чијим би откривањем неовлашћеним лицима могла настати штета по интересе и циљеве у области одбране;

2) подаци о плановима употребе Војске Србије, ратној организацији и формацији команди, јединица и установа Војске Србије, подаци о борбеним и другим материјалним средствима, односно врстама покретних ствари намењених потребама одбране, чијим би откривањем неовлашћеним лицима могла настати штета по оперативну и функционалну способност Војске Србије;

3) подаци о патентима значајним за одбрану земље и средствима и уређајима намењеним одбрани који су у процесу усвајања и испитивања;

4) подаци о војним објектима и другим непокретностима значајним за одбрану земље, изузев података који су према прописима о заштити животне средине неопходни за процену утицаја на животну средину;

5) подаци о предузетим мерама, радњама и поступцима садржани у одлукама, наређењима, саопштењима и другим актима у области одбране земље, чије би откривање нанело штету интересима снага одбране.

Систем заштите тајних података у Републици Србији

У Републици Србији, систем заштите тајних података регулисан је свеобухватним законским и подзаконским актима, са примарним фокусом на Закону о тајности података („Службени гласник РС“, бр. 104/2009), који дефинише поступке одређивања, обраде, чувања и заштите података од значаја за националну безбедност. Поред овог закона, значајну улогу играју и Закон о одбрани, Закон о информационој безбедности, подзаконски акти, као и међународни споразуми о заштити тајних података.

Основни концепти заштите тајних података

Систем заштите тајних података обухвата неколико кључних области:

Регистарски систем – Вођење евиденције о тајним подацима је обавезно и спроводи га надлежни орган у складу са законским и подзаконским актима. Евиденција обухвата означавање, приступ, дистрибуцију и архивирање тајних података, уз примену важећих стандарда како би се осигурала њихова потпуна контрола и праћење.

Персонална безбедност – Обухвата спровођење безбедносних провера за лица која рукују тајним подацима, укључујући издавање безбедносних сертификата.

Административна безбедност – Укључује процедуре означавања степена тајности, евидентирање приступа, процедуре декласификације и уништавања тајних података.

Физичка безбедност – Обухвата мере заштите објеката, докумената и просторија у којима се чувају тајни подаци, као што су контролисани приступ, алармни системи и видео надзор.

Информациона безбедност – Обухвата заштиту електронских система, комуникација и база података који садрже тајне податке, укључујући криптографску заштиту (на пример, коришћење алгоритама AES-256 и RSA) и управљање приступом путем мултифакторске аутентификације, контроле приступних листа и система детекције упада.

Индустријска безбедност – Примењује се на привредне субјекте који обрађују или чувају тајне податке у оквиру пословних активности од значаја за државу.

Контрола и надзор – Спроводи се унутрашња и спољашња ревизија како би се утврдило поштовање прописа и идентификовале слабости у систему заштите тајних података.

Степени тајности података

Према Закону о тајности података, тајни подаци се означавају у складу са потенцијалном штетом која би могла настати у случају њиховог неовлашћеног откривања. Разликују се четири степена тајности:

Државна тајна – Откривање може изазвати тешке последице по суверенитет, уставни поредак или безбедност Републике Србије.

Строго поверљиво – Откривање може значајно угрозити виталне интересе државе.

Поверљиво – Откривање би могло нанети штету институцијама или њиховим функцијама.

Интерно – Подразумева најнижи степен осетљивости, намењен за службену употребу.

Означавање степена тајности

Сваком тајном податку мора бити додељен одговарајући степен тајности, који се јасно означава на документима или електронским записима. Ово омогућава лакше руковање и примену одговарајућих безбедносних мера.

Преклапање са другим категоријама штићених података

Поред тајних података, постоје и друге категорије штићених података, као што су:

Лични подаци – регулисани Законом о заштити података о личности,

Пословна тајна – дефинисана Законом о привредним друштвима,

Професионалне тајне – односе се на поверљиве податке у правосуђу, медицини и другим професијама.

Када податак припада више категорија, примењују се најстроже мере заштите које важе за било коју од категорија.

Практична примена и изазови

Систем заштите тајних података у Србији суочава се са бројним изазовима:

Прекомерно означавање података као тајних – доводи до оптерећења система заштите.

Недовољна усклађеност између институција – различити стандарди примене безбедносних мера.

Ограничена улагања у информациону безбедност – повећава ризик од сајбер напада.

Недовољна контрола приступа – може довести до неовлашћеног коришћења тајних података.

Континуирана едукација запослених, ажурирање безбедносних мера и јачање система надзора су кључни за даље унапређење система заштите тајних података у Републици Србији. У том контексту, примењују се постојећи програми обуке који обухватају безбедносне протоколе, поступке руковања тајним подацима и стандардизоване методологије заштите информација у складу са домаћим и међународним прописима.

3. Подаци о личности или лични подаци

Лични подаци представљају било коју информацију која се односи на идентификовану или идентификујућу физичку особу (субјекта података). У складу са Општом уредбом о заштити података (GDPR) и Законом о заштити података о личности ("Службени гласник РС", број 87/2018), идентификујућа физичка особа је она која се може директно или индиректно идентификовати помоћу идентификатора као што су: име, идентификациони број, подаци о локацији, онлајн идентификатор или један или више

фактора специфичних за физички, физиолошки, генетски, ментални, економски, културни или социјални идентитет те особе.

Правни оквир за заштиту личних података у Републици Србији

Основни правни оквир

Обрада личних података у Републици Србији регулисана је различитим прописима који се примењују у различитим областима, укључујући општу заштиту личних података, полицијске прописе, прописе из области одбране и кривичне прописе.

Основни правни оквир чине:

Закон о заштити података о личности (Службени гласник РС број 87/18) – главни правни акт који усклађује домаће законодавство са Општом уредбом о заштити података (GDPR) и прописује начела обраде личних података, права субјеката и обавезе руковалаца и обрађивача података.

Закон о евиденцијама и обради података у области унутрашњих послова (Службени гласник РС број 47/18) – регулише начин вођења, коришћења и заштите евиденција унутрашњих послова, укључујући личне податке грађана.

Закон о полицији (Службени гласник РС број 6/16, 24/18, 87/18, 86/19) – уређује обраду личних података од стране полицијских органа у сврху очувања јавног реда и безбедности, спречавања и откривања кривичних дела и идентификације починилаца.

Закон о одбрани (Службени гласник РС број 116/07, 88/09, 104/09, 10/15, 36/18) – дефинише обраду личних података у контексту националне безбедности, мобилизације и функционисања система одбране.

Кривични законик Републике Србије (Службени гласник РС број 85/05, 88/05, 107/05... 35/19, 118/21) – предвиђа кривичне санкције за неовлашћену обраду, злоупотребу или незаконито прикупљање и откривање личних података.

Закон о приватном обезбеђењу (Службени гласник РС број 104/13, 42/15, 87/18) – уређује начин обраде личних података у области приватног обезбеђења.

Закон о детективској делатности (Службени гласник РС број 104/13) – регулише обраду личних података у оквиру детективских услуга.

Закон о информационој безбедности (Службени гласник РС број 6/16, 94/17, 77/19) – регулише мере техничке и организационе заштите података у ИТ системима.

Закон о електронским комуникацијама (Службени гласник РС број 44/10, 60/13, 62/14, 95/18, 86/19) – садржи одредбе које се тичу заштите приватности у електронској комуникацији и заштите корисничких података.

Закон о праву на приступ информацијама од јавног значаја и заштити података о личности (Службени гласник РС број 120/04, 54/07, 104/09, 36/10, 105/21) – уређује баланс између транспарентности јавних органа и заштите личних података.

Закон о електронској управи (Службени гласник РС број 27/18, 25/20, 44/21) – регулише поступање са личним подацима у оквиру јавних електронских услуга.

Међународни инструменти

Поред домаћег законодавства, заштита личних података у Србији је усклађена са међународним стандардима, укључујући:

Општу уредбу о заштити података (GDPR) – примењује се у прекограничним трансакцијама и размени података са државама ЕУ.

Конвенцију Савета Европе 108+ – најстарији међународни уговор о заштити података, који Србија примењује као потписница.

Права субјеката података

Грађани Србије имају следећа права у вези са својим личним подацима:

Право на приступ – могу захтевати копију својих података.

Право на исправку – ако су подаци нетачни или непотпуни.

Право на брисање („право на заборав“) – могу тражити брисање података под одређеним условима.

Право на ограничење обраде – уколико је тачност података спорна или је обрада незаконита.

Право на преносивост података – могу захтевати пренос података другом руковаоцу.

Практични примери примене прописа

Примери како се прописи примењују у пракси:

Банке – обавезне су да штите податке клијената и примењују сигурносне мере против злоупотребе.

Здравствене установе – чувају медицинске податке пацијената у складу са Законом о правима пацијената.

Образовни систем – школе и универзитети морају поштовати правила о заштити података ученика и студената.

Унапређење заштите у ИТ сектору

Како би се побољшала заштита личних података у дигиталном окружењу, препоручују се следеће мере:

Шифровање података – како би се онемогућио неовлашћени приступ.

Сигурносне копије – редовно прављење резервних копија података.

Аутентификација корисника – коришћење двофакторске аутентификације.

Мониторинг система – праћење и превенција сајбер-напада.

Унапређење правног оквира и доследна примена прописа о заштити личних података у Србији је од суштинског значаја за заштиту приватности грађана, спречавање злоупотребе и унапређење безбедности у дигиталном окружењу. Институције, правна лица и организације које рукују личним подацима морају се придржавати строгих

правила, уз сталну едукацију и надзор ради очувања правне сигурности и заштите људских права.

4. Пословна тајна

Пословна тајна представља виталан елемент заштите осетљивих пословних информација које омогућавају компанијама да задрже своју конкурентску предност. Њена заштита је незаобилазна за очување поверења клијената, пословних партнера и интегритета унутрашњих процеса. Такође, пословна тајна често кореспондира са професионалном тајном у областима као што су ревизорски и саветнички послови.

Пословна тајна у Србији регулисана је следећим прописима:

Закон о заштити пословне тајне („Службени гласник РС”, бр. 53/2021):

Прописује услове за идентификацију пословне тајне.

Одређује мере заштите и санкције за неовлашћено прибављање или откривање.

Закон о привредним друштвима („Службени гласник РС”, бр. 36/2011):

Уређује обавезе друштава у погледу очувања пословне тајне, посебно у управљању и кадровима.

Закон о тајности података („Службени гласник РС”, бр. 72/2009):

Дефинише услове под којима пословне информације могу бити означене као тајни подаци.

Закон о заштити података о личности:

Допуњује заштиту у случајевима када пословна тајна обухвата личне податке.

Пословна тајна vs. Тајни податак: Пословна тајна није аутоматски тајни податак у смислу Закона о тајности података. Ипак, одређени документи, попут уговора у одбрамбеној индустрији, могу бити означени одговарајућим степеном тајности ако њихово откривање угрожава безбедност или економске интересе државе.

Категорије пословних тајни и примери

Финансијски подаци:

Пример: План реорганизације компаније у случају финансијске кризе.

Технолошки детаљи:

Пример: Формула за производњу производа или алгоритам за иновације у софтверу.

Маркетиншке стратегије:

Пример: План освајања новог тржишта са анализом конкуренције.

Клијентске базе података:

Пример: Листа клијената са детаљима о њиховим уговорима и преференцијама.

Производни процеси:

Пример: Јединствена метода израде производа која смањује трошкове и повећава квалитет.

Примери из праксе и злоупотребе

Ревизорски послови:

Пример: Ревизор открива податке о финансијским неправилностима компаније конкуренцији.

Последице: Компанија може поднети тужбу за накнаду штете и покренути кривични поступак.

Саветничке услуге:

Пример: Консултант неовлашћено користи податке о стратегији клијента за сопствену корист.

Последице: Одузимање лиценце и обавеза накнаде штете клијенту.

IT консалтинг:

Пример: IT консултант продаје алгоритам развијен за клијента конкурентској фирми.

Последице: Покретање судског поступка због повреде пословне тајне и захтев за надокнаду губитака.

Заштита пословне тајне представља правну, етичку и стратешку обавезу сваке компаније. Посебна пажња мора бити посвећена примени интерних правила, као што су уговори о поверљивости и евиденција приступа осетљивим информацијама. Иако пословна тајна није аутоматски тајни податак, неке информације могу добити овај статус ако испуњавају критеријуме Закона о тајности података, нарочито у осетљивим индустријама попут одбране. Улога контролних механизама и придржавање закона кључни су за очување поверења и избегавање злоупотреба.

5. Заштита поверљивих података у јавним набавкама

Заштита поверљивих података у јавним набавкама је неопходна како би се осигурао интегритет процеса набавке и спречиле злоупотребе. Непотребно означавање података као поверљивих може угрозити транспарентност и довести до злоупотреба. Овај текст разматра две правне ситуације у вези са заштитом података: поверљиве информације које нису тајни подаци и јавне набавке на које се не примењује Закон о јавним набавкама, уз укључивање одредби Закона о заштити пословне тајне.

Главни прописи који регулишу заштиту поверљивих података:

Закон о јавним набавкама („Службени гласник РС”, бр. 91/2019),

Закон о тајности података („Службени гласник РС”, бр. 72/2009, 36/2011),

Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018),

Закон о заштити пословне тајне („Службени гласник РС”, бр. 53/2021).

Закон о заштити пословне тајне уводи детаљну регулативу о заштити информација које представљају пословну тајну, дефинишући критеријуме за њихову идентификацију и правну заштиту у случају неовлашћеног откривања или коришћења.

Поверљиви подаци који нису тајни - Поверљиви подаци у јавним набавкама укључују осетљиве информације које нису формално класификоване као тајни подаци по Закону о тајности података. Ове информације обухватају:

Пословне тајне понуђача: финансијске податке, тржишне стратегије и производне поступке заштићене Законом о заштити пословне тајне.

Личне податке: податке о појединим лицима укљученим у поступак.

Техничке спецификације: детаље значајне за конкурентску предност понуђача.

Информације о стратешким набавкама: процене које могу утицати на тржишну равнотежу.

Напомена: Наручилац је обавезан да образложи одлуке о поверљивости, осигуравајући да не дође до злоупотребе института поверљивости ради избегавања транспарентности.

Јавне набавке на које се не примењује Закон о јавним набавкама - У случајевима када Закон о јавним набавкама није примењив, као што су набавке у области националне безбедности и мање вредности, и даље постоје обавезе у погледу заштите поверљивих података:

Закон о тајности података и **Закон о заштити података о личности** остају обавезујући.

Закон о заштити пословне тајне такође се примењује како би се обезбедила заштита пословних информација које испуњавају критеријуме за пословну тајну.

Наручиоци морају осигурати да се поверљивост не користи за прикривање незаконитости или неправилности у поступку.

Мере заштите и надзор - Кључне мере за спречавање злоупотреба поверљивости укључују:

Обавезно образложење одлука о поверљивости – свака одлука мора бити заснована на законским основама.

Ограничење приступа поверљивим информацијама – само овлашћена лица смеју имати увид.

Евиденција и контрола приступа – одржавање електронских система за праћење.

Обучавање службеника – едукација о заштити поверљивих и пословних тајни.

Надзор независних органа – Државна ревизорска институција и Агенција за спречавање корупције.

Заштита поверљивих података у јавним набавкама, укључујући пословне тајне, мора бити у складу са принципима законитости, транспарентности и пропорционалности. Закон о заштити пословне тајне обезбеђује додатни ниво заштите за осетљиве информације понуђача. Јачање контролних механизама и примена законских обавеза могу допринети већој ефикасности и транспарентности у јавним набавкама.

6. Заштита фискалних и банкарских података у Србији

Фискални и банкарски подаци представљају кључну категорију за осигурање финансијске безбедности и приватности појединаца и правних лица. Ови подаци укључују информације о финансијским трансакцијама, стањима на рачунима, кредитима, депозитима и другим финансијским аспектима који се обрађују у оквиру банкарског и фискалног система.

Правни оквир

Заштита фискалних и банкарских података у Србији регулисана је следећим прописима:

Закон о банкама („Службени гласник РС“, бр. 107/2005, 91/2010, 14/2015, 44/2018, 91/2019 и 122/2021): Утврђује обавезу банака да чувају податке о клијентима и дефинише појам „банкарске тајне“, укључујући изузетке када се подаци могу доставити државним органима.

Закон о заштити података о личности („Службени гласник РС“, бр. 87/2018): Прописује стандарде заштите личних података, укључујући оне који се односе на финансијске информације физичких лица.

Закон о платним услугама („Службени гласник РС“, бр. 44/2018 и 139/2022): Регулише електронска плаћања и заштиту података корисника платних услуга.

Закон о спречавању прања новца и финансирања тероризма („Службени гласник РС“, бр. 113/2017, 91/2019 и 153/2020): Предвиђа обавезу финансијских институција да прикупљају, обрађују и чувају одређене финансијске податке ради спречавања прања новца и тероризма. Овај закон такође регулише обавезу идентификације клијената и пријављивања сумњивих трансакција надлежним органима.

Закон о информационој безбедности („Службени гласник РС“, бр. 6/2016, 94/2017 и 77/2019): Уређује мере заштите информационих система који обрађују осетљиве податке.

Закон о тржишту капитала („Службени гласник РС“, бр. 31/2011, 112/2015 и 108/2016): Уводи мере против инсајдерске трговине и регулише обавезе пружалаца финансијских услуга у спречавању злоупотребе информација.

Европски контекст

Србија као кандидат за чланство у ЕУ постепено усклађује своје прописе са европским стандардима. Нарочито, **Општа уредба о заштити података (GDPR)** значајно утиче на

законодавни оквир Србије у области заштите личних података. Усвајањем **Закона о заштити података о личности из 2018. године**, Србија је направила важан корак у приближавању европским стандардима заштите приватности у финансијском сектору.

Категорије података под заштитом

Фискални и банкарски подаци могу обухватати:

Основне податке о рачуну – број рачуна, стање, историју трансакција.

Информације о кредитима – износ кредита, каматне стопе, услове отплате.

Личне податке клијената – име, адресу, јединствени матични број грађана (ЈМБГ), идентификационе податке правних лица.

Инвестиционе и осигуравајуће податке – податке о улагањима, полисама осигурања, тржишним трансакцијама.

Интерне анализе банака – процене ризика, кредитне рејтинге, извештаје о финансијском понашању клијената.

Утицај дигитализације на заштиту података

Са убрзаном дигитализацијом банкарских услуга, укључујући електронско банкарство, мобилне апликације и дигиталне трансакције, потреба за заштитом података је значајно порасла. Финансијске институције све више користе напредне методе заштите, попут:

Двофакторске аутентификације (2FA) за приступ рачунима.

Биометријске идентификације (отисак прста, препознавање лица).

Блокчејн технологије за осигурање интегритета трансакција.

Напредних алгоритама за детекцију превара у реалном времену.

Мере заштите банкарских и фискалних података

Финансијске институције у Србији примењују низ мера заштите, укључујући:

Шифровање података и употребу безбедносних сертификата.

Ограничење приступа осетљивим информацијама на принципу „потребе да се зна“.

Строге процедуре аутентификације за кориснике електронског банкарства.

Континуирано унапређивање безбедносних технологија и система.

Практични примери заштите и злоупотребе података

Постоје бројни случајеви злоупотребе банкарских података у свету, укључујући хакерске нападе на банке и финансијске институције. У Србији, најчешћи облици злоупотребе обухватају:

Фишинг нападе, где корисници несвесно откривају приступне податке преварантима.

Злоупотребу платних картица, где криминалци копирају податке са картице и користе их за неовлашћене трансакције.

Неовлашћено откривање података, где банкарски службеници незаконито прослеђују информације трећим лицима.

С друге стране, успешно спроведене мере заштите, као што су биометријска идентификација и напредни системи за детекцију превара, значајно су смањили ризик од оваквих злоупотреба.

Инсајдерска трговина

Инсајдерска трговина представља незаконито коришћење повлашћених информација које нису јавно доступне, а које могу утицати на тржишну цену финансијских инструмената. Закон о тржишту капитала захтева од свих институција да спрече овакву злоупотребу путем:

Строгих интерних процедура за контролу приступа повлашћеним информацијама.

Обавезе пријављивања сумњивих активности регулаторним органима.

Спровођења едукације запослених у вези са спречавањем инсајдерских активности.

Пример добре праксе је коришћење дигиталних система за праћење комуникација и трансакција запослених, чиме се минимизира ризик од злоупотребе.

Надзор и регулација

Главне институције које надгледају и регулишу заштиту фискалних и банкарских података у Србији су:

Народна банка Србије (НБС) – врши супервизију над банкама и финансијским институцијама у вези са применом закона о банкарству и заштити клијената.

Повереник за информације од јавног значаја и заштиту података о личности – надгледа примену закона о заштити података о личности и поступа у случају повреде права на приватност.

Управа за спречавање прања новца – прати сумњиве финансијске трансакције и спречава злоупотребу банкарског система у сврху финансирања криминалних активности.

Статус тајности фискалних и банкарских података

Банкарски подаци нису означени степеном тајности у смислу **Закона о тајности података („Службени гласник РС“, бр. 72/2009)**, али су заштићени као **банкарска тајна, пословна тајна и професионална тајна**, у складу са релевантним законима.

7. Здравствени подаци као категорија штићених података

Здравствени подаци представљају једну од најосетљивијих категорија штићених података, јер се односе на физичко и ментално здравље појединаца. Некада је коришћен термин службена тајна у здравству за њих. Њихова обрада и заштита регулисани су строгим правним оквирима како би се обезбедила приватност и спречила злоупотреба.

Поред заштите права појединаца, здравствени подаци имају значајну улогу у очувању националне безбедности, стабилности јавног здравља, као и заштити пословних и привредних интереса.

Важно је напоменути да здравствени подаци нису класификовани као тајни подаци у складу са Законом о тајности података, већ припадају категорији посебно осетљивих личних података у складу са Законом о заштити података о личности, и заштићени су као професионална тајна здравствених радника.

Правни основ - Обрада здравствених података у Србији регулисана је кроз неколико кључних закона који дефинишу оквире за њихово прикупљање, чување и обраду:

Закон о заштити података о личности (Сл. гласник РС бр. 87/2018) - утврђује принципе обраде личних података, укључујући здравствене податке, који су класификовани као осетљива категорија.

Закон о правима пацијената (Сл. гласник РС бр. 25/2013) - гарантује право пацијената на приватност и заштиту њихових података у здравственим установама.

Закон о здравственој заштити (Сл. гласник РС бр. 25/2019) - прописује обавезе здравствених радника у вези са чувањем професионалне тајне.

Закон о електронској управи (Сл. гласник РС бр. 27/2018) - регулише сигурност информационих система који обрађују електронске здравствене податке.

Закон о информационој безбедности (Сл. гласник РС бр. 6/2016) - осигурава заштиту критичних информационих система од сајбер напада.

Уредба о заштити одређених лица и објеката (Сл. гласник РС бр. 72/2011) – утврђује мере безбедносне заштите за највише државне функционере од значаја за националну безбедност. Она обухвата и мере превентивно-медицинске заштите, што подразумева и специфичну обраду здравствених података ових лица у оквиру безбедносних процедура.

Етички кодекс Лекарске коморе Србије - дефинише обавезе лекара у погледу чувања поверљивости података о пацијенту и задовољења етичких стандарда у професионалном раду.

Етички кодекс Медицинских сестара и техничара Србије - регулише обавезу медицинских сестара и техничара да чувају поверљивост здравствених података и поступају са поштовањем према правима пацијената.

Кључни војни, полицијски и за припаднике БИА прописи који регулишу заштиту медицинских података:

1. За припаднике Војске Србије:

• **Закон о Војсци Србије (Сл. гласник РС бр. 116/2007, 88/2009, 101/2010, 10/2015, 36/2018, 88/2019 и 153/2020)** – предвиђа здравствену заштиту припадника ВС, укључујући поверљивост медицинских података.
• **Закон о одбрани (Сл. гласник РС бр. 116/2007, 88/2009, 104/2009, 10/2015, 36/2018, 88/2019 и 153/2020)** – регулише заштиту података од значаја за одбрану, што може обухватати и здравствене податке војних лица у контексту оперативне способности.
• **Правилник о здравственој способности за војну службу (Сл. гласник РС, број**

82/2014) – дефинише критеријуме за оцену здравствене способности и чување медицинске документације војних лица.
• **Правилник о војној евиденцији (Сл. гласник РС бр. 46/2019)** – садржи одредбе о вођењу здравствених података регрутованих и активних припадника ВС.
• **Упутство о вођењу медицинске документације у војноздравственим установама** – интерни акт који уређује евидентирање, чување и приступ здравственим подацима припадника ВС.

2. За припаднике Министарства унутрашњих послова (МУП) и Безбедносно-информативен агенције (БИА):

• **Закон о полицији (Сл. гласник РС бр. 6/2016, 24/2018, 87/2018 и 86/2019)** – уређује здравствену заштиту и мере заштите података о здравственом стању полицијских службеника.

• **Закон о безбедносно-информативној агенцији (Сл. гласник РС бр. 42/2002, 111/2009, 65/2014, 66/2014, 36/2018, 80/2021)** – садржи одредбе о заштити здравствених података припадника БИА у оквиру безбедносних мера.

• **Правилник о медицинским прегледима припадника МУП-а (Сл. гласник РС бр. 61/2016)** – утврђује процедуре за обављање систематских прегледа и поверљивост медицинске документације.

• **Правилник о медицинско-психолошким критеријумима за пријем у МУП (Сл. гласник РС бр. 37/2018)** – уређује критеријуме за здравствену и психолошку процену полицијских службеника.

• **Упутство о вођењу здравствених картона припадника МУП-а** – интерни акт који дефинише процедуре за прикупљање, обраду и чување медицинских података.

Ови прописи осигуравају да здравствени подаци припадника Војске Србије и МУП-а буду заштићени у складу са законом и процедурама о заштити тајних података.

Категорије здравствених података

Индивидуални медицински подаци: Обухватају податке о историји болести, дијагнозама, терапијама, лабораторијским налазима и лечењима.

Генетски подаци: Посебно осетљиви подаци који се односе на генетске карактеристике појединца.

Подаци о јавном здрављу: Анонимизоване информације које се користе за креирање политика јавног здравља.

Електронски здравствени картони (EHR): Дигитализоване медицинске информације пацијената, које омогућавају бржи и сигурнији приступ подацима.

Електронски рецепти: Дигитални записи о прописаним терапијама, који доприносе ефикаснијој комуникацији између здравствених радника и апотека.

Примери из праксе

Електронски здравствени картони (EHR): Ови записи омогућавају здравственим радницима брз приступ подацима пацијента, чиме се смањује могућност грешака и убрзава лечење.

Електронски рецепти: Пацијенти могу добити прописане терапије без папирних докумената, што убрзава процес лечења и чини га транспарентнијим.

Јавно здравље: Током пандемије COVID-19, агрегирани подаци о броју оболелих и вакцинацији коришћени су за планирање и праћење мера, уз строго чување поверљивости индивидуалних података.

Научна истраживања: Анонимизовани здравствени подаци коришћени су у истраживањима уз сагласност пацијената, како би се испоштовала њихова приватност.

Корелација са личним подацима и професионалном тајном - Здравствени подаци су неодвојиви од личних података (име, презиме, ЈМБГ) и подлежу строгим правилима заштите. Поред тога, они су заштићени професионалном тајном коју су здравствени радници дужни да чувају. Свако неовлашћено откривање или злоупотреба представља тежак прекршај са прописаним санкцијама.

Корелација са отвореним подацима - Иако су здравствени подаци личне природе строго поверљиви, агрегирани и анонимизовани подаци могу се представити као отворени подаци. На пример, статистика о вакцинацијама или стопама оболевања може бити доступна јавности ради информисања и планирања.

Здравствени подаци као тајни подаци и категорија штићених података - Здравствени подаци представљају једну од најосетљивијих категорија штићених података, јер се односе на физичко и ментално здравље појединаца. Ови подаци нису означени као тајни подаци према Закону о тајности података (Сл. гласник РС бр. 104/2009), али су посебно осетљиви лични подаци у складу са Законом о заштити података о личности (Сл. гласник РС бр. 87/2018). Поред тога, у одређеним случајевима здравствени подаци могу добити статус тајних података ако њихово откривање може угрозити националну безбедност, одбрану, јавну безбедност, пословне или безбедносне интересе. Због своје осетљивости, они захтевају висок ниво заштите како би се обезбедила приватност појединаца и спречила евентуална злоупотреба.

Основ за означавање степена тајности здравствених података припадника Војске Србије, Министарства унутрашњих послова (полиције) и безбедносних служби (БИА, ВБА и ВОА), налази се у више војних, полицијских и других прописа, а који могу бити означени као тајни подаци у складу са Законом о тајности података. Степен тајности зависи од потенцијалног ризика који би настао откривањем ових података:

Интерно: Податке о лечењу или здравственом стању који нису од директног значаја за националну безбедност, али су важни за интерну употребу.

Поверљиво: Податке чије откривање може нанети штету припадницима војске, полиције, служби безбедности или нарушити интегритет институције.

Строго поверљиво: Информације које могу угрозити оперативне активности служби безбедности или безбедност припадника војске и полиције.

Државна тајна: Здравствени подаци од критичног значаја за националну безбедност, попут података који се односе на стратегијске мисије или највише државне званичнике.

Означавањем степеном тајности података врше надлежни органи у складу са процедурама и прописима о тајности података, осигуравајући њихову безбедност и ограничен приступ.

Здравствени подаци највиших државних руководилаца

Здравствени подаци највиших државних руководилаца, укључујући председника Републике, председника Владе, председника Народне скупштине и министара, добијају посебан третман због њиховог значаја за националну безбедност и стабилност државе. У таквим случајевима, ти подаци могу бити означени степеном тајности као строго поверљиви или чак државна тајна, у зависности од њихове природе и потенцијалног ризика од откривања. Циљ овакве заштите је да се спречи злоупотреба података за подривање стабилности или уцењивање руководилаца.

Примери из праксе

Припадници специјалних јединица: Здравствени картони припадника јединица попут САЈ-а или војних специјалних снага обележени су као поверљиви, како би се осигурала заштита њихове сигурности.

Највиши државни руководиоци: У случају лечења или здравствених интервенција председника Републике, подаци се означавају као строго поверљиви, с обзиром на њихов утицај на функционисање државе.

Оперативне мисије у војсци: Епидемиолошки подаци припадника војске у борбеним задацима и мисијама често су означени као тајни како би се спречило да противник искористи информације о здравственом стању јединица.

Заштита и обрада здравствених података са ознаком тајности - Приступ здравственим подацима са ознаком тајности је строго ограничен на овлашћена лица и установе. Њихова обрада мора бити у складу са прописаним стандардима информационе безбедности и етичким кодексима који регулишу рад здравствених радника, као и са Законом о тајности података.

Коришћење електронских система за обраду: Обрада здравствених података означених степеном тајности мора бити у складу са прописаним стандардима информационе безбедности и заштите тајних података, уз примену мера које обезбеђују заштиту од неовлашћеног приступа или злоупотребе.

Неовлашћено откривање: Свако неовлашћено откривање или злоупотреба здравствених података означених степеном тајности подлеже озбиљним санкцијама, укључујући дисциплинске мере и санкције за прекршаје и кривична дела.

Здравствени подаци представљају критичну категорију штићених података, јер обједињују приватност појединаца, професионалну етику здравствених радника и јавни интерес. Иако нису класификовани као тајни подаци у складу са Законом о тајности података, они имају статус посебно осетљивих личних података и професионалне тајне. Баланс између поверљивости и транспарентности, уз употребу савремених технологија

и унапређење законских оквира, кључан је за јачање поверења у систем здравствене заштите и ефикасно управљање овим подацима у складу са највишим стандардима.

Здравствени подаци могу бити означени степеном тајнсоти поверљиво или строго поверљиви или чак као државна тајна у случајевима када је њихова заштита неопходна за очување националне безбедности и интереса државе. Посебан третман добијају подаци припадника безбедносних структура и највиших државних руководилаца. Баланс између заштите приватности и јавног интереса постиже се применом строгих процедура означавања степена тајности и усклађивањем са законом, што омогућава очување сигурности државе и појединаца.

8. Судски, тужилачки, прекршајни и управни подаци у Србији

Судски, тужилачки, прекршајни и управни подаци у Србији представљају категорије осетљивих информација које подлежу строгим правним регулацијама у складу са Законом о заштити података о личности, као и другим домаћим и међународним прописима. Ови подаци обухватају информације настале у разним правним и административним поступцима, укључујући судске процесе, јавне набавке, прекршајне поступке и конкурсе за запошљавање у државној управи. Њихова обрада, размена и чување морају бити усклађени са принципима заштите приватности, поверљивости, дигиталне безбедности и транспарентности у јавном интересу.

Правни основ

Закон о заштити података о личности (Сл. гласник РС, бр. 87/2018): Основни пропис који дефинише заштиту осетљивих података, укључујући судске, тужилачке, прекршајне и управне информације.

Закон о поступку пред судовима (Сл. гласник РС, бр. 72/2011): Обезбеђује равнотежу између јавности и поверљивости судских поступака.

Закон о јавном тужилаштву (Сл. гласник РС, бр. 116/2008): Осигурава заштиту поверљивих података током истрага и подизања оптужница.

Прекршајни законик (Сл. гласник РС, бр. 65/2013): Уређује податке о прекршајима, казнама и поступцима.

Закон о јавним набавкама (Сл. гласник РС, бр. 91/2019): Прописује транспарентност јавних набавки и заштиту пословних тајни.

Закон о тајности података (Сл. гласник РС, бр. 104/2009): Уређује категоризацију и заштиту тајних података.

Европски стандард GDPR: Утиче на поступке обраде података у Србији, усклађујући их са захтевима за заштиту података у ЕУ.

Категорије података

Судски подаци: Пресуде, доказни материјали, записници. *Пример:* Пресуде се објављују јавности, али лични подаци жртава остају поверљиви.

Тужилачки подаци: Информације о истрагама и оптужницама. *Пример:* Подаци истраге доступни су тек по завршетку поступка.

Прекршајни подаци: Казне, решења о прекршајима. *Пример:* Записи о саобраћајним прекршајима доступни су само странкама у поступку.

Управни подаци: Одлуке и акти јавних органа.

Подаци у јавним набавкама: Финансијски извештаји, понуде.

Пословна тајна: Уговори и стратешке информације компанија.

Професионална тајна: Медицинске и адвокатске информације подложне поверљивости.

Тајни подаци: Информације означене степеном тајности, попут националне или државне безбедности, одбране или спољних послова и слично.

Електронска обрада података

Са растућом дигитализацијом, системи електронске обраде података у судству и администрацији пружају значајне предности, али и изазове:

Предности: Бржи приступ информацијама и ефикасније руковање подацима. *Пример:* Електронске платформе омогућавају већу доступност судских одлука у јавним базама.

Изазови: Ризик од сајбер напада или неовлашћене обраде података. Употреба јаке енкрипције и сајбер-безбедносних стандарда постаје неопходна.

Сарадња са европским и међународним стандардима

Примена Опште регулативе о заштити података (GDPR) у Србији побољшава усклађеност са европским стандардима. Србија је такође потписница међународних конвенција попут Конвенције о заштити људских права и Конвенције о борби против корупције, које доприносе интегритету и сигурности обраде података.

Примери из праксе

- **Судски поступци**: У случају кривичног дела, суд објављује пресуду на својој интернет страници како би се обезбедила јавна доступност одлука. Међутим, из пресуде се уклањају лични подаци жртава и сведока, као што су имена, адресе и други идентификациони подаци, како би се заштитила њихова приватност у складу са законима о заштити података.

- **Судски поступци са малолетницима**: У случају када је малолетник жртва кривичног дела, судске пресуде које су доступне јавности обавезно укључују мере заштите идентитета жртве. То значи да се уместо имена користе иницијали, а сви лични подаци жртве уклањају из документа. Такође, јавност може бити искључена из суђења како би се малолетнику омогућила додатна заштита. У случају када је малолетник извршилац кривичног дела, суђење се одвија по посебним процедурама за малолетнике. Циљ је ресоцијализација, па се пресуде често фокусирају на мере као што су васпитне препоруке, обавезни програми едукације или праћење од стране стручних служби, уместо строгих казнених мера. Лични подаци малолетника такође остају заштићени како би се избегла стигматизација.

- **Јавне набавке**: Приликом спровођења конкурса за изградњу јавне инфраструктуре, на пример, мостова или болница, јавна управа објављује списак понуђача и њихове понуде. Истовремено, поверљиви подаци, као што су детаљне финансијске стратегије или технички детаљи који би могли да дају конкурентску предност, остају доступни само комисији задуженој за избор.

- **Конкурси за запошљавање**: Када се расписује конкурс за запошљавање у државној институцији, објављује се ранг листа кандидата и њихови резултати на тестирањима. Међутим, сам садржај тестова и детаљни одговори кандидата доступни су искључиво члановима комисије која врши оцену, како би се обезбедила фер процена и спречиле манипулације.

- **Управни поступци**: У случајевима административних поступака, као што је издавање грађевинске дозволе, надлежни орган објављује коначну одлуку, али поједини елементи поступка, као што су детаљи приватних споразума или финансијски подаци подносилаца захтева, остају заштићени. Ово омогућава транспарентност самог процеса одлучивања, док истовремено обезбеђује заштиту осетљивих података појединаца и организација.

Препоруке за унапређење

Увођење додатних обука за стручно особље у области заштите података.

Унапређење технолошке инфраструктуре ради боље заштите дигитализованих података.

Јачање сарадње са међународним организацијама ради усаглашавања са глобалним стандардима.

Судски, тужилачки, прекршајни и управни подаци, као и подаци који се односе на заштиту тајности самих поступака, укључујући тајне податке, личне податке, пословне и професионалне тајне, као и пореске тајне, представљају основу за очување правног поретка и функционисање административног система Србије. Поред тога, заштита националне безбедности, привредних интереса и пословања компанија од посебног је значаја како би се осигурала стабилност и конкурентност земље, истовремено спречавајући злоупотребу осетљивих информација које могу угрозити интересе државе, појединаца или привреде.

Пружање транспарентности у раду органа власти уз истовремену заштиту осетљивих података представља изазов који изискује пажљиво осмишљене мере, непристрасну примену закона и стално унапређивање регулаторних оквира. Овај процес мора бити заснован на принципима правде и одговорности, где се транспарентност не користи на уштрб приватности и безбедности, већ као средство за јачање поверења у институције.

Успешно балансирање између отворености и приватности није само предуслов ефикасног и модерног друштва, већ и кључни механизам у борби против корупције, спречавању недозвољеног утицаја на поступке и јачању правне сигурности. Овај баланс је основа која омогућава истинску демократију и осигурава да сваки грађанин буде заштићен од злоупотреба, а држава и њене институције функционално и одговорно обављају своје задатке.

Посебан акценат треба ставити на адекватну заштиту података који су од критичног значаја за безбедност државе, грађана и привреде, како би се избегле злоупотребе,

осигурала правична примена закона и истовремено обезбедила транспарентност која гради поверење у институције. Такав приступ не само да одржава стабилност правног система, већ и доприноси одрживом развоју друштва као целине.

Овај баланс није само основа модерног правног система, већ и гарант очувања демократских вредности и одговорног управљања, што је кључно за будућност и напредак Србије.

9. Професионалне тајне као категорија заштићених података

Професионалне тајне обухватају податке који се односе на одређене професије, где је поверљивост од пресудног значаја за обављање посла и заштиту интереса клијената, пацијената или других лица. У Републици Србији, ове тајне су регулисане низом закона и представљају значајну категорију заштићених података.

Правни основ

Закон о адвокатури (Сл. гласник РС, бр. 31/2011, 24/2012) Адвокати су обавезни да чувају као тајну све што им клијент повери у оквиру заступања, у складу са правилима адвокатске етике.

Закон о здравственој заштити (Сл. гласник РС, бр. 25/2019) Обавезује лекаре и друго медицинско особље да чувају лекарску тајну, која укључује све информације које се односе на здравље пацијента и пружање здравствених услуга.

Закон о јавним бележницима (Сл. гласник РС, бр. 31/2011, 85/2012, 19/2013) Нотари су дужни да чувају тајност свих података из докумената које састављају или оверавају.

Закон о јавном информисању и медијима (Сл. гласник РС, бр. 83/2014) Новинари су дужни да заштите идентитет извора информација, уколико су подаци поверљиви.

Закони цркава и верских заједница Свештеници су обавезни да чувају исповедаоницу и друге поверљиве информације које добију током свог верског рада.

Категорије података

Адвокатска тајна: Информације које клијент саопшти адвокату, укључујући документа, сведочења или податке о случају.

Лекарска тајна: Медицинска документација, дијагнозе, историја болести и здравствени подаци.

Новинарска тајна: Идентитет извора и информације које нису за јавност.

Нотарска тајна: Подаци и документи које нотару поверавају клијенти.

Свештеничка тајна: Информације добијене током верских обреда, попут исповести.

Пракса

Строга поверљивост: Професионалци у овим областима морају применити мере заштите како би обезбедили сигурност података.

Казнене мере: Повреде професионалне тајне могу довести до дисциплинских, кривичних или грађанских санкција.

Ограничено откривање: Под одређеним условима, попут судског налога, тајни подаци могу бити откривени, али само у складу са законом.

Судски вештаци и професионална тајна - Судски вештаци имају посебан статус у контексту заштите података јер се њихова улога често преклапа са различитим категоријама заштићених података, укључујући професионалне тајне. Њихова дужност укључује коришћење, обраду и анализу информација које могу бити од суштинског значаја за судски поступак.

Правни основ

Закон о парничном поступку (Сл. гласник РС, бр. 72/2011, 49/2013) регулише улогу и обавезе судских вештака у грађанским поступцима, укључујући обавезу да поступају с пуном поверљивошћу.

Кривични законик (Сл. гласник РС, бр. 85/2005) обавезује вештаке у кривичним поступцима да чувају поверљивост података до којих дођу током рада.

Закон о заштити података о личности (Сл. гласник РС, бр. 87/2018) поставља оквир заштите личних података које судски вештаци обрађују.

Категорије података са којима раде судски вештаци

Лични подаци: Име, адреса, здравствени подаци, финансијске информације.

Професионалне тајне: Информације добијене од адвоката, лекара или других професионалаца укључених у поступак.

Пословна тајна: У привредним споровима, могу укључивати анализу пословних података.

Подаци из судских поступака: Подаци достављени током судског процеса који су често поверљиви.

Пракса

Одржавање неутралности: Судски вештаци морају бити независни и непристрасни у обради података.

Поверљивост података: Информације до којих дођу могу се користити само у оквиру задатог поступка, а извештаји се чувају као део поверљиве судске документације.

Правила откривања података: У случају потребе за објављивањем извештаја или података, то се врши искључиво у складу са одредбама закона.

Корелација са професионалном тајном - Судски вештаци често сарађују са професионалцима чији подаци подлежу професионалној тајни (на пример, адвокатским или лекарским). У таквим случајевима, вештак је обавезан да те податке обради уз пуну поверљивост и у складу са релевантним законима.

Професионална тајна представља један од темеља поверења између професионалаца и лица са којима сарађују, било да су то клијенти, пацијенти, странке или извори

информација. У Републици Србији, овај концепт је чврсто утемељен у законским прописима који обезбеђују да се поверљиви подаци штите од злоупотребе и откривања. Међутим, у свету брзог напредовања технологије и дигитализације, одржавање и заштита професионалних тајни постају све сложенији задатак који захтева сталну прилагодбу новим правним и технолошким условима.

Професионална тајна обухвата широк спектар података — од адвокатских поверљивих комуникација, преко здравствених информација, до новинарских извора и верских исповести. Она чини основе поверења које клијенти и друштво полажу у различите професионалне службе. Уз строг правни оквир, поштивање ових тајни представља не само законску обавезу, већ и моралну одговорност професионалаца који су их дужни чувати.

У исто време, с обзиром на све већу међусобну повезаност и интеракцију између различитих категорија заштићених података, као што су лични подаци, пословне тајне или подаци од значаја за безбедност, важно је наставити развијати свеобухватне и прецизне приступе њиховој заштити. Ово је од изузетне важности за очување интегритета професија, као и за одржавање поверења у институције које обезбеђују ову заштиту.

Заштита професионалних тајни остаје витална за одржавање сигурности, приватности и етичког деловања у друштву, те се њена заштита мора стално усаглашавати са новим правним, технолошким и друштвеним изазовима. Заједно са применом дисциплинских и кривичних мера у случају повреде поверљивости, овај оквир обезбеђује одржавање високе етичке и правне одговорности у свим професијама које се ослањају на поверљивост и тајност.

10. Подаци о малолетним лицима или малолетницима

У Републици Србији, подаци о малолетницима представљају изузетно осетљиву категорију података која захтева посебну заштиту. Ови подаци су регулисани низом закона који пружају правни оквир за њихову обраду и заштиту.

Правни основ

Закон о заштити података о личности (Сл. гласник РС, бр. 87/2018): Овај закон прописује опште услове за прикупљање, обраду, чување и пренос података о личности. Посебно наглашава потребу за већом заштитом података о малолетницима, јер су деца као посебна група рањива на злоупотребу својих личних података.

Породични закон (Сл. гласник РС, бр. 18/2005, 72/2011, 6/2015, 44/2018): Регулише права и обавезе родитеља и старатеља у погледу заштите личних података малолетних лица, као и прописује који су подаци о малолетницима потребни за обављање родитељских дужности и заштите права деце.

Кривични законик Републике Србије (Сл. гласник РС, бр. 85/2005, 88/2009, 121/2012, 104/2013, 108/2014, 94/2016): Кривични законик садржи одредбе које се односе на заштиту малолетника од злоупотребе њихових личних података. Посебно се

наглашава кривична одговорност у случају злоупотребе или неовлашћеног откривања података о малолетницима.

Закон о основама система образовања и васпитања (Сл. гласник РС, бр. 88/2009, 52/2013, 55/2017): Регулише обавезу образовних институција да штите податке о ученицима, укључујући и податке који се односе на малолетнике. Школе и други васпитно-образовни системи морају осигурати да су подаци ученика заштићени и да се не деле без одговарајуће сагласности родитеља или старатеља.

Закон о заштити деце од насиља и занемаривања (Сл. гласник РС, бр. 106/2006): Овај закон регулише поступке заштите деце у ситуацијама насиља, као и обавезу пријављивања и заштите података о деца која су жртве насиља. Он укључује и забрану објављивања података који могу открити идентитет деце која су жртве кривичних дела.

Закон о јавним информацијама и медијима (Сл. гласник РС, бр. 83/2014, 58/2015, 12/2016, 50/2018): Овај закон забрањује објављивање података који могу открити идентитет малолетника у осетљивим ситуацијама, као што су судски поступци, кривична дела или насиље.

Закон о социјалној заштити (Сл. гласник РС, бр. 24/2011): Уређује обраду и заштиту података о деци која се налазе у систему социјалне заштите, укључујући децу без родитељског старања.

Закон о спречавању дискриминације (Сл. гласник РС, бр. 22/2009): Садржи одредбе које осигуравају да подаци о малолетницима не смеју бити коришћени на дискриминаторан начин или за кршење њихових права.

Закони и прописи који регулишу рад са посебним категоријама деце: На пример, законски акти који се односе на децу са инвалидитетом или специфичним потребама често укључују мере заштите података који су везани за њихове здравствене или образовне потребе.

Категорије података

Идентификациони подаци:

Име, презиме

Датум рођења

Адреса пребивалишта

ЈМБГ (јединствени матични број грађана)

Образовни подаци:

Оцена

Присуство настави

Дисциплински поступци

Разредни успех

Резултати испита

Здравствени подаци:

Медицинска историја

Историја вакцинација

Лечење и дијагностички подаци

Психолошке оцене и подаци

Подаци о социјалном статусу:

Информације о породици, старатељству

Финансијска ситуација

Подаци о животним условима и статусу у друштву

Корелација са професионалним тајнама и личним подацима - Корелација између **професионалних тајни** и **личних података** о малолетницима представља важан аспект који мора бити пажљиво регулисан како би се осигурала адекватна заштита права деце. **Професионалне тајне** малолетника укључују информације које се односе на њихову активност у професионалним и радним сферама, као што су учешће у стручним, научним или образовним програмима, као и било какве информације повезане са њиховим радним искуствима (ако су укључени у радне активности). Ове информације морају бити обрађиване у складу са прописима о заштити података, поштујући принципе поверљивости, и не смеју бити делене без сагласности родитеља или старатеља.

Лични подаци малолетника, као што су име, презиме, датум рођења, адреса и други подаци који могу идентификовати дете, морају се такође третирати са истим нивоом заштите. Посебно је важно да професионални подаци малолетника буду пажљиво раздвојени од личних података, како би се спречила могућност њихове злоупотребе. У пракси, то подразумева да информације о активности малолетника, као што су у образовању или волонтирању, не смеју бити повезане са подацима који могу довести до њихове личне идентификације, без одговарајуће сагласности родитеља или старатеља.

На овај начин, потребно је обезбедити да се **професионалне тајне** и **лични подаци** малолетника обрађују са највишим степеном поверљивости и у складу са прописима који регулишу заштиту података о деци.

Пракса

Образовне институције: Школе, вртићи и друге образовне установе имају законску обавезу да чувају податке о ученицима у складу са прописима, као и да их не деле без сагласности родитеља или законског старатеља. Ове институције такође морају спроводити мјере заштите података у складу са прописима Закона о заштити података о личности.

Здравствене установе: Медицински подаци малолетника, укључујући податке о здрављу, вакцинацијама и другим медицинским интервенцијама, морају се обрађивати у складу са прописима о заштити података. Ове информације се третирају као строго поверљиве и не смеју бити откривене без одговарајуће сагласности.

Судови и полиција: Подаци о малолетним учиниоцима кривичних дела обрађују се уз посебне мере заштите, како би се спречила њихова злоупотреба. Малолетници који су учинили кривична дела имају права на посебну заштиту и третман, како би се спречила додатна штета по њихов лични и друштвени статус. Такође, у складу са законом, подаци о малолетним учиниоцима не смеју се објављивати.

Медијска пракса: Медији су у обавези да обезбеде да у извештајима о осетљивим темама не дође до идентификације малолетника. Ово укључује коришћење иницијала уместо пуних имена и замагљивање слика на којима се могу препознати.

Сарадња институција: Када је потребно разменити информације о малолетницима између различитих институција, као што су школе и социјалне службе, то се мора радити уз посебне мере поверљивости и уз сагласност родитеља или старатеља.

Заштита података о малолетницима у Републици Србији је регулисана низом правних акта који обезбеђују безбедност и приватност деце. Посебна пажња се посвећује правима деце и спречавању злоупотребе личних података, као и заштити њихове приватности у различитим контекстима. Важно је да сви учесници у процесу обраде података о малолетницима, било да су то образовне институције, здравствене установе или органи власти, поступају у складу са законским прописима како би осигурали поштовање права и безбедност малолетних лица.

11. Отворени подаци у Републици Србији Правни основ, категорије, пракса и информационе технологије

1. Правни основ:

Отворени подаци су у Србији регулисани низом закона и подзаконских аката који имају за циљ да осигурају приступ информацијама од јавног интереса, као и да подстакну транспарентност, отвореност и ефикасност рада јавних органа. Главни правни оквири су:

Закон о слободи приступа информацијама од јавног значаја (Службени гласник РС, бр. 120/2004 и касније измене): Овај закон представља основни оквир за приступ информацијама од јавног значаја. Он прописује право грађана на приступ информацијама које државни органи поседују, под условом да те информације нису класификоване као поверљиве.

Закон о електронској управи (Службени гласник РС, бр. 27/2018): Овај закон регулише употребу информационих технологија у јавном сектору, укључујући принципе отворених података и промовисање електронских услуга које омогућавају лакши приступ подацима.

Закон о заштити података о личности (Службени гласник РС, бр. 87/2018): Овај закон регулише обраду личних података и има значајан утицај на управљање и доступност

отворених података, посебно када се ради о личним подацима који се односе на физичке особе.

Закон о информационој безбедности (Службени гласник РС, бр. 6/2016): Регулише аспекте безбедности података који се користе и размењују унутар јавних и приватних институција, укључујући заштиту отворених података од злоупотреба.

Стратегија развоја електронске управе Републике Србије: Стратегија која указује на значај развоја отворених података и њихове интеграције у јавну управу, како би се омогућила боља сарадња између државних органа и грађана.

Корелација отворених података са другим тајним подацима: Отворени подаци и подаци од јавног значаја морају бити пажљиво одвојени од тајних података. Закон о слободи приступа информацијама од јавног значаја пружа право на приступ информацијама, али одређује да се информације које су класификоване као поверљиве или тајне, не могу објавити као отворени подаци. Тајни подаци, укључујући војне, дипломатске и економске тајне, подлеже посебним прописима и обезбеђени су строгим мерама заштите. Овај разликан приступ осигурава да се јавни интерес не угрози, док истовремено омогућава транспарентност у другим областима.

Категорије отворених података:

Отворени подаци у Србији могу обухватити различите категорије информација, које су доступне јавности и које државни органи, јавне институције или друга тела могу објавити у складу са прописима о отвореним подацима. Неке од најважнијих категорија су:

Државни и локални регистри: Ово укључује податке о јавним службеницима, правним субјектима, земљишним парцелама, податке о правима и обавезама предузећа, као и информације о власничким правима и транзакцијама.

Податке о јавним финансијама: Овде се укључују подаци о буџетима, јавним набавкама, јавним уговорима и обавезама јавних органа према јавности.

Податке о животној средини: Ови подаци обухватају информације о квалитету ваздуха, воде, земљишта, као и податке о климатским условима и природним катастрофама.

Подаци о образовању и здравству: У ову категорију спадају статистике у вези са образовним институцијама, здравственим установама, бројем пацијената, здравственим услугама и другим релевантним подацима.

Транспорт и инфраструктура: Подаци који се односе на јавни транспорт, саобраћајне површине, изградњу и одржавање инфраструктуре.

Подаци о безбедности и правди: Статистике о криминалитету, правосудним поступцима, као и јавни подаци који се односе на безбедност грађана.

Отворени подаци и заштита осетљивих информација:

Од велике важности је управљање подацима који могу да садрже деликатне или осетљиве информације. Заштита приватности и безбедности података о личности мора бити усклађена са свим законским обавезама које се односе на управљање и размену

отворених података. Примена принципа минималне обраде података и контроле приступа подацима од важности омогућава избегавање неовлашћеног откривања информација које су класификоване као тајне, било да су у питању војни, безбедносни или економски подаци.

Практична примена и пракса:

У Србији постоји низ примера где је употреба отворених података довела до побољшања јавних услуга и повећане транспарентности:

Платформе за отворене податке: На нивоу Републике Србије и локалних самоуправа, бројне платформе су развијене које омогућавају грађанима и стручним круговима да приступе различитим базама података, као што је Портал отворених података који је доступан на сајту Владе Републике Србије.

Пример отворених података у јавним набавкама: Одређени подаци у вези са јавним набавкама су објављени у складу са Законом о јавним набавкама и слободом приступа информацијама. Ово је омогућило већу транспарентност у одлучивању и смањење ризика од корупције.

Примена у образовању и здравству: Податке који се односе на резултате испита, статистике у вези са здравственим установама и њиховим услугама користе образовне и здравствене установе како би побољшали своје услуге и комуникацију са јавностима.

Управљање подацима који су истовремено отворени и тајни: Могуће је извршити одређене комбинације између отворених података и тајних информација, али само уз примену строгих мера контроле. Подаци који имају комерцијалну вредност, као што су јавне набавке, понуде и уговори, могу бити доступни као отворени подаци након одређених проверених рокова, али увек уз одвојену класификацију за заштиту осетљивих информација.

Информационе технологије и будућност отворених података:

Информационе технологије играју кључну улогу у развоју и примени отворених података у Србији. Неколико важних аспеката укључује:

Интеграција са електронским управама: Примена система за електронску размену података и платформи за отворене податке омогућава бржи и лакши приступ информацијама од јавног значаја.

Употреба великих података (Big Data): Увођење аналитике великих података може значајно побољшати управљање и коришћење отворених података, као и унапредити предвиђање и управљање јавним политкама.

Блокчејн технологија: Блокчејн може обезбедити већи ниво безбедности и транспарентности у управљању отвореним подацима, посебно када се ради о документима који захтевају верификацију и проверу идентитета.

Примена вештачке интелигенције: Вештачка интелигенција може помоћи у анализи и интерпретацији отворених података, као и у креирању бољих услова за јавне политике и сервисе.

Отворени подаци у Републици Србији су кључни за подстицање транспарентности, повећање јавне одговорности и побољшање услуга јавних институција. Правни оквири и напори у примени савремених информационих технологија значајно доприносе развоју овог сектора. Будућност отворених података у Србији зависи од даљег усмеравања на развој ефикасних и сигурних платформи које омогућавају већи приступ подацима уз поштовање права на приватност и заштиту података, као и усклађивање са строгим правним и безбедносним оквирима који регулишу тајне податке.

12. Пореска тајна
Правни основи, категорије података и примери из праксе

Правни основи

Закон о пореском поступку и пореској администрацији ("Службени гласник РС", бр. 80/2002 и касније измене):

Чланови овог закона дефинишу појам пореске тајне и обавезу чувања података који се односе на пореске обвезнике.

Пореска тајна обухвата све информације које порески органи прикупе током обављања својих дужности, осим ако је законом другачије прописано.

Закон о тајности података ("Службени гласник РС", бр. 104/2009):

Према овом закону, пореска тајна није аутоматски класификована као тајни податак. Она се сматра **штићеним податком**, али може бити класификована као тајни податак ако њено откривање угрожава јавни или национални интерес.

Закон о заштити података о личности ("Службени гласник РС", бр. 87/2018):

У случајевима када пореска тајна укључује личне податке, примењују се одредбе овог закона, укључујући принципе транспарентности и ограничења приступа.

Интеграција других врста тајни:

Пословна тајна: Ако у оквиру пореског поступка буду прикупљени подаци попут пословних планова, стратегија или финансијских извештаја, они ће се сматрати делом пореске тајне.

Банкарска тајна: Подаци о банковним рачунима или трансакцијама који су прикупљени током пореске контроле такође могу бити укључени у пореску тајну.

Категорије података које спадају у пореску тајну

Лични подаци пореских обвезника:

Име, презиме, ЈМБГ, адреса и други идентификатори.

Финансијски подаци:

Информације о приходима, пореским обавезама, плаћањима, дуговањима и субвенцијама.

Пословни подаци:

Финансијски извештаји, подаци о трансакцијама, добит и губици предузећа.

Банкарски подаци (као део пореске тајне):

Информације о банковним рачунима, плаћањима и кредитима.

Подаци о пореским контролама:

Извештаји инспекцијских надзора, анализе ризика и налази инспекција.

Подаци о пореским олакшицама и субвенцијама:

Информације о пореским подстицајима које користе обвезници.

Примери из праксе

Заштита пословних података:

Током пореских контрола често се прикупљају подаци о унутрашњем пословању предузећа. Ови подаци се чувају као пореска тајна, али могу садржати и елементе пословне тајне, попут стратегија за унапређење производње.

Банкарски подаци у контексту пореске тајне:

Порески органи могу приступити информацијама о банковним рачунима пореских обвезника како би проверили усклађеност са обавезама. Ови подаци се третирају као штићени подаци у складу са законом.

Кршење пореске тајне:

У пракси су забележени случајеви неовлашћеног откривања података о пореским обвезницима. Овакав прекршај повлачи новчане казне и друге санкције у складу са Законом о пореском поступку.

Интероперабилност са међународним системима:

У сарадњи са међународним организацијама попут OECD-а, подаци за размену морају се адекватно заштитити и пратити правила о повредама поверљивости.

Велике пореске афере:

У случајевима међународних пореских истрага, као што су прање новца или избегавање плаћања пореза, размена података између земаља подразумева високу заштиту пореске тајне.

Однос пореске тајне са отвореним подацима - Пореска тајна, као категорија заштићених података, у принципу није у складу са концептом отворених података, који подразумева јавну доступност информација. Међутим, одређене информације које су прикупљене у оквиру пореског поступка могу бити доступне јавности ако се не односе на тајне податке или ако је тако прописано законом.

Пример овога су подаци о пореским обавезницима који су изузети од пореске тајне и који се објављују у складу са Законом о слободи информација. Такви подаци обично не

укључују специфичне финансијске информације, већ више опште податке као што су износ пореза који је обавезник платио.

Неке земље имају законодавство које омогућава објављивање података о великим пореским обавезницима или о правним субјектима који су корисници јавних средстава. Ови подаци, иако нису увек у потпуности отворени, представљају вид транспарентности који може бити усклађен са принципима отворених података, али у оквиру ограничења која налаже пореска тајна.

Однос пореске тајне са личним подацима - Пореска тајна у већини случајева укључује личне податке пореских обвезника, као што су име, презиме, ЈМБГ и адреса. Ови подаци су заштићени од откривања, како би се осигурала приватност појединца.

Према Закону о заштити података о личности, ако пореска тајна садржи личне податке, они се морају обрадити у складу са прописима о заштити личних података, што подразумева стриктне мере у погледу прикупљања, обраде, чувања и размене ових података.

Са друге стране, ако лични подаци не спадају у категорију пореске тајне, онда могу бити доступни јавности у складу са прописима који регулишу обавештавање или уз захтев појединца. Међутим, такви подаци морају бити обрађени уз поштовање права на приватност и поштовање принципа као што су транспарентност и минимизација података.

Однос пореске тајне и личних података захтева пажљиво балансирање између права на приватност појединаца и потребе за транспарентношћу у пореском систему.

Утицај на права пореских обвезника

Права пореских обвезника укључују заштиту од неовлашћеног откривања података. У случајевима повреде, обвезници имају право да траже правну заштиту и накнаду.

Пореска администрација мора обезбедити транспарентност у обради података, као и правовремено обавештавање обвезника о свим активностима које укључују њихове податке.

Практичне мере заштите

Енкрипција података:

Сви подаци који се чувају и размењују морају бити шифровани ради спречавања приступа од стране неовлашћених лица.

Ограничење приступа:

Приступ пореским подацима је дозвољен само овлашћеним лицима уз коришћење вишефакторске аутентификације.

Ревизије безбедности:

Редовне ревизије и провере безбедносних процедура доприносе јачању интегритета података.

Интерна контрола и одговорност

Унутрашње контроле као што су праћење приступа подацима, евидентирање активности и извештавање о неправилностима играју кључну улогу у заштити пореске тајне.

У случају кршења, лица одговорна за злоупотребу података могу се суочити са санкцијама, укључујући разрешење и кривичну одговорност.

Будући правни развој

Увођење нових технологија као што су **вештачка интелигенција** и **blockchain** могло би побољшати обраду и заштиту података.

Очекује се развој правних оквира који ће боље регулисати размену осетљивих података у међународном контексту.

Сарадња са другим институцијама

Сарадња са финансијском полицијом, царинским службама и међународним организацијама као што су OECD и UNCTAD омогућава бољу заштиту од пореских превара.

Размена података између институција мора бити строго регулисана како би се осигурала поверљивост и интегритет.

Пореска тајна представља сложену категорију података која обухвата личне, пословне и банкарске информације. Њена заштита је кључна за очување поверења у порески систем. Увођење савремених технологија и побољшање сарадње са другим институцијама значајно ће допринети јачању система заштите података. Успостављање стриктних процедура и транспарентност у раду пореске администрације осигуравају ефикасно управљање овим осетљивим информацијама.

13. Подаци за ограничену употребу у сарадњи са Европском унијом (ЕУ)

Подаци за ограничену употребу у сарадњи са Европском унијом (ЕУ) представљају категорију података који нису означени као тајни, али су заштићени у складу са релевантним правним и стратешким оквирима.

Правни и стратешки основи

Закон о заштити података о личности ("Службени гласник РС", бр. 87/2018): Регулише обраду података о личности и обезбеђује заштиту права појединаца у вези са обрадом њихових података.

Закон о тајности података ("Службени гласник РС", бр. 104/2009, 36/2011, 104/2013): Утврђује правила заштите, обраде и приступа подацима који су означени одређеним степеном тајности.

Закон о слободном приступу информацијама од јавног значаја ("Службени гласник РС", бр. 120/2004, 54/2007, 104/2009, 36/2010, 105/2021): Утврђује правила приступа и ограничења у погледу одређених категорија података.

Споразум о стабилизацији и придруживању између Европских заједница и њихових држава чланица и Републике Србије ("Службени гласник РС – Међународни уговори", бр. 83/2008): Дефинише оквир за сарадњу Србије и ЕУ, укључујући и размену одређених података.

Национални програми за усвајање правних тековина ЕУ: Садрже мере за усклађивање са стандардима ЕУ у области заштите и размене података.

Општа уредба о заштити података (General Data Protection Regulation – GDPR, Уредба (ЕУ) 2016/679): Европски правни оквир који дефинише правила за заштиту података о личности, укључујући право на приступ подацима, право на заборав и транспарентност.

Споразум између Републике Србије и Европске уније о безбедносним процедурама за размену и заштиту тајних података ("Службени гласник РС – Међународни уговори", бр. 19/2019): Регулише размену тајних информација између Србије и ЕУ.

Директива Савета 2013/488/ЕУ: Дефинише правила безбедности за заштиту тајних података Европске уније.

Категорије података

Подаци о јавним службеницима: Информације о запосленима у јавним институцијама који учествују у програмима сарадње са ЕУ.

Подаци о пројектима финансираним из ЕУ фондова: Финансијски извештаји, планови и резултати пројеката подржаних из ЕУ средстава.

Подаци о међународној сарадњи: Информације о билатералним и мултилатералним споразумима и активностима.

Документација у процесу придруживања ЕУ: Извештаји о напретку, анализе усклађености, препоруке и записници са званичних састанака.

Економски и трговински подаци: Информације о трговинским односима и политикама усклађивања са ЕУ стандардима.

Тајни подаци: Информације означене као тајне, које се размењују у складу са Споразумом између Србије и ЕУ и Директивом Савета 2013/488/ЕУ.

Отворени подаци: Јавни подаци који су доступни јавности преко Портала отворених података Републике Србије и Портала европских података.

Примери из праксе

Програми прекограничне сарадње: Размена података о пројектима, учесницима и финансирању, уз поштовање правила о заштити података.

Електронска размена докумената: Користе се сигурне платформе за размену података између српских институција и органа ЕУ.

Преговарачки процеси: Србија размењује анализе, мишљења и препоруке са институцијама ЕУ у оквиру преговарачких кластера.

Размена тајних података: У складу са Споразумом о размени тајних података и Директивом Савета 2013/488/ЕУ, обезбеђују се строге мере безбедности за заштиту поверљивости.

Отворени подаци: Користе се за истраживање, анализу, креирање јавних политика и транспарентност, како на националном тако и на европском нивоу.

Мере заштите

Физичке мере:

Контрола приступа зградама и просторијама где се подаци обрађују, уз утврђивање нивоа овлашћења за приступ.

Употреба сигурносних ормана и сефова за чување података.

Видео надзор и присуство безбедносног особља за заштиту просторија.

Технолошке мере:

Шифровање података током преноса и складиштења како би се спречио неовлашћен приступ.

Коришћење виртуелних приватних мрежа (VPN) за сигурну размену података.

Мултифакторска аутентификација за проверу идентитета корисника.

Редовно ажурирање система и спровођење пентестова за откривање потенцијалних сајбер претњи.

Заштита података на крајњим уређајима, укључујући мобилне телефоне и лаптопове.

Организационе мере:

Обука запослених о правилном руковању подацима, препознавању безбедносних претњи и правилној реакцији на инциденте.

Успостављање процедура за класификацију, складиштење и уништавање осетљивих података.

Праћење и евидентирање безбедносних инцидената уз редовну ревизију политика.

Разрада планова за опоравак од инцидената (Disaster Recovery Plan) како би се минимизирале последице потенцијалних напада.

Подаци за ограничену употребу, тајни подаци и отворени подаци представљају кључне елементе за успешну сарадњу између Републике Србије и Европске уније. Њихова заштита захтева примену физичких, технолошких и организационих мера како би се обезбедила сигурност, транспарентност и ефикасност у размена података. Успостављање највиших стандарда безбедности не само да јача поверење између партнера, већ и доприноси укупном напретку процеса европских интеграција.

14. Правни и стратешки оквири за податке о безбедности инфраструктуре у Републици Србији

У Републици Србији, правни и стратешки оквири који се односе на безбедност инфраструктуре уређени су кроз различите законе и стратегије. Ови прописи имају за циљ заштиту критичне инфраструктуре, информациону безбедност и регулацију обраде података од јавног и личног значаја.

Правни оквири

Закон о критичној инфраструктури („Службени гласник РС“, бр. 87/2018):

Овај закон утврђује критеријуме за идентификацију и одређивање критичне инфраструктуре.

Регулише како националну, тако и европску критичну инфраструктуру, и прописује мере заштите и управљање ризицима.

Надлежни органи и власници критичне инфраструктуре имају одговорност за примену ових мера.

Закон о информационој безбедности („Службени гласник РС“, бр. 6/2016, 94/2017, 77/2019):

Дефинише мере заштите информационих система од значаја за државу, укључујући системе критичне инфраструктуре.

Прописује обавезе оператора ИКТ система у вези са превентивним и реактивним мерама заштите.

Усклађен је са европским регулативама, као што су НИС 2 директива и Акт о сајбер безбедности.

Закон о тајности података („Службени гласник РС“, бр. 104/2009, 36/2010):

Регулише класификацију података на „државну тајну“, „службену тајну“ и друге категорије.

Прописује мере заштите тајних података и приступ осетљивим информацијама од значаја за безбедност инфраструктуре.

Закон о слободном приступу информацијама од јавног значаја („Службени гласник РС“, бр. 120/2004, 54/2007, 104/2009, 36/2010, 105/2021):

Грађанима омогућава приступ информацијама које поседују државни органи, уз изузетке за информације које могу угрозити националну или јавну безбедност.

Податке о критичној инфраструктури штити од злоупотребе, чиме балансира транспарентност и безбедносне потребе.

Закон о заштити података о личности („Службени гласник РС“, бр. 87/2018):

Усклађен са европским GDPR стандардима, овај закон регулише обраду и заштиту личних података.

Посебно је значајан за системе који обрађују осетљиве личне податке, као што су здравствени и транспортни системи.

Стратегија развоја информационог друштва и информационе безбедности (2021–2026):

Поставља циљеве за унапређење информационе безбедности и заштиту критичне инфраструктуре.

Подржава развој система за управљање инцидентима и сарадњу између јавног и приватног сектора у области безбедности.

Категорије штићених података

Подаци у оквиру критичне инфраструктуре могу се поделити у неколико категорија:

Технички подаци:

Информације о структури, функционисању и одржавању инфраструктуре (нпр. планови објеката, техничке шеме).

Оперативни подаци:

Протоколи и процедуре који се односе на рад система (нпр. планови реаговања на инциденте, алгоритми управљања).

Безбедносни подаци:

Информације о мерама заштите, као што су конфигурације сајбер система и физичке мере (нпр. локације надзорних камера).

Подаци о корисницима:

Лични подаци корисника услуга инфраструктуре, попут информација о пацијентима или података електронских карата.

Пословна тајна:

Информације које се односе на унутрашње пословање субјеката критичне инфраструктуре, као што су финансијски извештаји, стратешки планови, уговори и информације о партнерима и добављачима.

Професионална тајна:

Подаци који су доступни одређеним професионалним групама у оквиру критичне инфраструктуре, као што су медицински, адвокатски и инжењерски подаци који су заштићени етичким и законским нормама.

Отворени подаци:

Информације које су јавно доступне и односе се на званичне презентације, као што су извештаји, статистике, анализе, истраживања и остали подаци од јавног интереса.

Електроенергетски системи:

Управљање електроенергетским мрежама подразумева заштиту SCADA система, који су често мета сајбер напада.

Здравствени системи:

Електронски здравствени картони садрже осетљиве податке пацијената, који су заштићени Законом о заштити података о личности.

Саобраћајна инфраструктура:

Интелигентни системи управљања саобраћајем (нпр. семафори, електронске карте) обрађују податке који су критични за безбедност и ефикасност транспорта.

Проблеми у пракси - Један од значајних проблема у области заштите података о безбедности инфраструктуре је преклапање између објеката који су обухваћени **Планом одбране** и оних који су дефинисани као **критична инфраструктура**.

Разлика у нивоу заштите података: Док су подаци у Плану одбране углавном означени као тајни (државна тајна или строго поверљиво), подаци који се односе на критичну инфраструктуру углавном су осетљиви или поверљиви, али не нужно класификовани као тајни.

Надлежности и регулаторни оквири: План одбране је у надлежности сектора одбране и безбедности, док је критична инфраструктура под управом више институција, укључујући цивилне и комерцијалне ентитете, што доводи до неслагања у примени мера заштите.

Проблеми у разграничавању објеката: Нека инфраструктура припада и једној и другој категорији (нпр. војни аеродроми који су истовремено део цивилног саобраћаја), што компликује примену прописа и одређивање степена заштите података.

Недоследност у приступу и безбедносним мерама: Иако критична инфраструктура није формално обухваћена регулативама о тајним подацима, неке информације о њој могу имати значајне безбедносне импликације, што захтева посебне процедуре заштите које нису увек довољно јасно дефинисане.

Правни и стратешки оквири у Србији обухватају разноврсне аспекте заштите података о инфраструктури, али изазови у разграничавању тајних, поверљивих и осетљивих података и даље постоје. Неопходно је прецизније дефинисати улоге надлежних институција и ускладити мере заштите како би се избегли конфликти у примени прописа и омогућило ефикасно управљање безбедносним ризицима.

15. Подаци у вези са одбраном (уколико нису означени као тајни)
Стратегијски и правни оквир, категорије података, примери из праксе

Подаци који се односе на одбрану Републике Србије, али нису означени као тајни, представљају важан сегмент у систему безбедности и одбране државе. Иако нису

класификовани као тајни, ови подаци имају висок ниво заштите и третирају се као штићени подаци, чиме се спречава њихово коришћење на начин који би могао наштетити националним интересима. У овом контексту потребно је размотрити примену правног и стратегијског оквира, категорије података и примере из праксе који илуструју значај њихове заштите.

1. Напомена о штићеним подацима у вези са одбраном који нису тајни

Иако већина података у вези са одбраном носи ознаку о тајности, постоје и одређени подаци који нису означени као тајни али су и даље штићени. Ови подаци нису класификовани као „тајни“ у стриктном смислу, али ипак подлежу строгим мерама контроле и заштите, како би се спречило давање информација које би могле наудити безбедности Републике Србије. Такав поступак се односи на информације које су од значаја за одбрану, али које не представљају непосредну претњу ако буду објављене. Пример таквих података могу бити неки технички подаци о одбрамбеној опреми која није од стратешке важности у тренутним условима.

2. Разлика између података са ознаком тајности и поверљивих података

Подаци са ознаком тајности: Пројекти, информације и подаци означени одговарајућим степеном тајнсоти у складу са прописима, који се односе на безбедносне, одбрамбене и војне стратегије, планове, операције и ресурсе. Њихова неовлашћена објава представља непосредну претњу националној безбедности. У ову категорију спадају документи, војне операције, тајни уговори о сарадњи и слично.

Поверљиви подаци: Информације које нису означене као тајне, али се и даље сматрају важним и подлежу заштити како би се спречила њихова злоупотреба. Поверљиви подаци укључују техничке детаље, логистичке информације, интерне организационе податке и слично. Иако њихова објава обично не угрожава безбедност, могу имати негативан утицај на функционисање система одбране.

3. Стратегијски и правни оквир

Правни и стратешки оквир у Републици Србији дефинише како се управља подацима са ознаком тајности и поверљивим подацима, укључујући њихово коришћење и заштиту. Овде су кључни закони и стратегије:

- **Закон о основама уређења служби безбедности** *Службени гласник Републике Србије, број 116/2007, 72/2012, 20/2015, 88/2018, 23/2022.*
- **Закон о одбрани** *Службени гласник Републике Србије, број 116/2007, 88/2009, 104/2009, 10/2015, 36/2018, 44/2021.*
- **Закон о Војсци Србије** *Службени гласник Републике Србије, број 116/2007, 88/2009, 10/2015, 44/2021.*
- **Закон о радној, материјалној и војној обавези** *Службени гласник Републике Србије, број 88/2009, 95/2010, 99/2011, 92/2015, 36/2018.*
- **Стратегија националне безбедности Републике Србије** *Службени гласник Републике Србије, број 94/2019.*

 Стратегија одбране Републике Србије *Службени гласник Републике Србије, број 94/2019.*

 Закон о јавним набавкама *Службени гласник Републике Србије, број 91/2019.*

 Закон о заштити пословне тајне *Службени гласник Републике Србије, број 53/2021.*

 Закон о заштити података о личности *Службени гласник Републике Србије, број 87/2018.*

 Закон о слободном приступу информацијама од јавног значаја *Службени гласник Републике Србије, број 120/2004, 54/2007, 104/2009, 36/2010, 105/2021.*

4. Категорије података

Јавни подаци: Информације које су доступне јавности, као што су извештаји о јавним набавкама или објаве које не укључују стратешке или поверљиве аспекте.

Интерни подаци: Ова категорија обухвата податке о дневним активностима, организацији и раду који нису осетљиве природе.

Поверљиви подаци: Логистички планови, техничке информације и детаљи који се не означавају као тајни, али су важни за несметано функционисање.

Пословне тајне: Уговори, планови сарадње, финансијске информације и остали елементи од пословног значаја.

Професионалне тајне: Ове тајне су регулисане етичким кодексима и односе се на релације стручњака и клијената, попут адвокатских, лекарских или новинарских тајни које се могу појавити у контексту одбране.

5. Примери из праксе

- **Подаци са ознаком тајности:**

Тајни планови о војним операцијама или складиштима оружја.

- **Поверљиви подаци:**

Логистички планови за транспорт ненасилне опреме или спецификације ресурса.

- **Јавни подаци:**

Објаве о јавним набавкама за опрему ниског ризика, попут канцеларијске опреме.

- **Пословне тајне:**

Уговори са компанијама које пружају логистичке услуге или опрему за Војску Србије.

- **Професионалне тајне:**

Адвокатска документација у процесима који укључују сектор одбране.

Лекарски подаци о здравственом стању припадника војске који су достављени у поверењу.

Новинарске тајне које укључују информације из истраживачког рада.

- **Отворени подаци:**

Извештаји, статистике, анализе и истраживања која су јавно доступна.

Податке од јавног интереса које институције објављују ради транспарентности.

Подаци у вези са одбраном Републике Србије, било да су са ознаком тајности или спадају у категорију штићених података, имају суштинску улогу у очувању безбедносних и стратешких интереса државе. Подаци са ознаком тајности подлежу примени мера и процедура у складу са Законом о тајности података, јер њихово неовлашћено коришћење и откривање може довести до тешке штете или штете интересима Републике Србије.

С друге стране, штићени подаци укључују информације које нису означене као тајне, али су од значаја за функционисање система одбране, као што су јавни, интерни и поверљиви подаци, као и пословне и професионалне тајне. Ови подаци, иако не представљају директну претњу уколико буду делимично објављени, захтевају одговарајуће управљање и заштиту како би се спречила њихова злоупотреба и обезбедила ефикасност у оперативним и организационим аспектима.

Закони, стратегије и етички кодекси служе као темељ за правилно управљање и заштиту ових података. Док подаци са ознаком тајности штите критичне аспекте националне безбедности, штићени подаци, укључујући поверљиве и осетљиве информације, омогућавају несметано функционисање система одбране и очување стратешке одрживости државе.

16. Подаци у вези са тероризмом који нису означени као тајни, али припадају осетљивој категорији, представљају важан аспект у контексту јавне и националне безбедности

Иако нису формално класификовани као тајни подаци, ови подаци имају потенцијал да значајно утичу на сигурност државе и њених грађана. Стога, њихово прикупљање, обрада и дистрибуција морају бити усклађени са строгим законским и регулаторним оквирима који штите интересе безбедности, али истовремено осигуравају поштовање основних људских права и приватности.

Када је реч о осетљивим подацима који се односе на тероризам, важно је напоменути да њихова злоупотреба може имати озбиљне последице, како по саму безбедност, тако и по правну сигурност грађана. Одговорност државних органа који управљају овим подацима јесте да успоставе ефикасне и транспарентне механизме који спречавају могућу злоупотребу, истовремено омогућавајући адекватну и правовремену реакцију на терористичке претње.

Поштујући принципе правде и транспарентности, одговорне институције морају обезбедити да сви подаци буду обрађени на начин који је у складу са постојећим правним оквирима, као што су Закон о заштити података о личности, Закон о заштити тајних података, као и међународне обавезе у области људских права. Уједно, свака

обрада и дељење ових података морају бити свесно и унапред регулисани, како би се избегле могуће злоупотребе и нарушавање права појединаца.

Стога, контекст правног оквира који обухвата осетљиве податке у борби против тероризма није само техничко питање, већ и изузетно важан изазов у складу са демократским принципима, који мора бити решаван у циљу обезбеђивања сигурности без угрожавања основних права и слобода.

Правни основи

Закон о полицији (*"Службени гласник РС", бр. 6/2016, 24/2018, 87/2018, 86/2019, 121/2021 и 127/2021 – др. закон*) – Уређује овлашћења полиције у прикупљању, обради и коришћењу података за потребе јавне безбедности, укључујући и борбу против тероризма.

Закон о безбедносно-информативној агенцији (*"Службени гласник РС", бр. 42/2002, 111/2009, 65/2014 и 66/2014 – др. закон*) – Дефинише надлежности БИА у прикупљању, обради и заштити података који су значајни за националну безбедност, укључујући тероризам.

Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији (*"Службени гласник РС", бр. 88/2009, 55/2012 – одлука УС, 17/2013 и 113/2017*) – Регулише надлежности војних безбедносних и обавештајних структура у заштити националне безбедности и сузбијању терористичких претњи.

Закон о тајности података (*"Службени гласник РС", бр. 104/2009, 36/2011 и 20/2015*) – Одређује који подаци могу бити означени степеном тајности и како се њима управља.

Закон о кривичном поступку (*"Службени гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019 и 27/2023*) – Регулише примену специјалних истражних мера, попут тајног надзора комуникација и прикривених истражитеља, у случајевима тероризма.

Закон о заштити података о личности (*"Службени гласник РС", бр. 87/2018*) – У случају да подаци садрже личне информације, њихова обрада мора бити у складу са принципима заштите приватности.

Закон о спречавању прања новца и финансирања тероризма (*"Службени гласник РС", бр. 113/2017, 91/2019 и 153/2020*) – Утврђује мере за праћење финансијских токова који могу бити повезани са терористичким активностима.

Међународни стандарди и споразуми – Србија је у обавези да примењује међународне конвенције, попут **Конвенције УН о сузбијању тероризма** и **Директиве ЕУ 2017/541 о борби против тероризма**, која дефинише мере превенције и криминализације терористичких активности.

Примери из праксе

Објављивање статистике и анализа ризика – Полицијске и безбедносне службе могу објављивати годишње извештаје о безбедносним претњама, укључујући тероризам.

Сарадња са међународним организацијама – Србија учествује у разменама података о терористичким претњама кроз Интерпол, Европол и друге међународне механизме.

Јавна упозорења и превенција – Када постоје индиције о потенцијалним нападима или ризичним догађајима, полиција може издати безбедносна упозорења грађанима.

Медијска комуникација – Објављивање података о ухапшеним лицима или сузбијању терористичких група мора бити уравнотежено између јавног интереса и потребе да се не угрози истрага.

Национална или јавна безбедност?

Подаци у вези са тероризмом спадају у оба домена:

Национална безбедност – У питању су подаци који се тичу заштите суверенитета, територијалног интегритета и стабилности државе. Они укључују анализе безбедносних претњи, информације о међународним терористичким мрежама и сарадњу са страним службама.

Јавна безбедност – Тероризам директно угрожава животе грађана и јавни поредак. Информације које се односе на потенцијалне претње по цивилно становништво припадају сфери јавне безбедности.

Стратегије и прописи

Национална безбедност и одбрана:

Стратегија националне безбедности Републике Србије (*"Службени гласник РС", бр. 94/2019*) – Дефинише основне претње, ризике и начине заштите националне безбедности, укључујући борбу против тероризма.

Стратегија одбране Републике Србије (*"Службени гласник РС", бр. 94/2019*) – Одређује мере заштите државе у случају оружаних претњи и угрожавања безбедности.

Финансирање тероризма и спречавање злоупотреба:

Стратегија спречавања прања новца и финансирања тероризма 2022–2026 – Дефинише институционалне мере за откривање и спречавање илегалних финансијских токова.

Правилник о методологији за израду процене ризика од прања новца и финансирања тероризма (*"Службени гласник РС", бр. 10/2019*) – Утврђује процедуре за финансијски надзор.

Законски и подзаконски акти за примену Стратегије – Уредбе и правилници који се односе на рад банкарског и финансијског сектора у контроли сумњивих трансакција.

Изазови у примени правног оквира - Иако Србија има свеобухватан правни оквир за заштиту и обраду података у вези са тероризмом, његова примена у пракси носи одређене изазове:

Координација између институција

Борба против тероризма захтева сарадњу више институција – полиције, Безбедносно-информативне агенције (БИА), Војнобезбедносне агенције (ВБА), Војнообавештајне агенције (ВОА), као и правосудних и финансијских органа.

Изазов је постићи ефикасну размену информација уз очување интегритета истрага и поштовање законских процедура.

Овде се посебно истиче потреба за усаглашеним приступом у праћењу финансијских токова који могу бити повезани са терористичким активностима.

Заштита приватности приликом обраде података

Закони о заштити података о личности налажу строге услове за прикупљање, чување и обраду осетљивих информација, укључујући оне које се односе на потенцијалне терористичке активности.

Баланс између безбедности и заштите основних права грађана представља континуирани изазов, посебно када је реч о праћењу комуникација и електронских података.

Неопходно је обезбедити да мере прикупљања и коришћења података буду пропорционалне и у складу са правним стандардима, како би се избегла злоупотреба.

Нове технологије и њихов утицај на анализу података

Развој вештачке интелигенције и великих података (Big Data) отвара могућности за напредну анализу претњи, али истовремено доноси и етичка и правна питања.

Алгоритми за препознавање образаца у подацима могу значајно унапредити откривање терористичких активности, али такође носе ризик од погрешних позитивних идентификација и могућег профилисања без довољних доказа.

Питање је како ускладити употребу ових технологија са правним оквиром који у Србији још увек није у потпуности прилагођен овим изазовима.

Примери добре праксе - Како би се побољшала ефикасност и законитост обраде података у области борбе против тероризма, корисно је размотрити примере позитивне праксе из других земаља:

Француски Центар за анализу терористичких претњи (CNRLT)

У Француској постоји интегрисани приступ у борби против тероризма, где специјализоване безбедносне агенције, финансијске институције и тужилаштва размењују информације у реалном времену.

Кључна предност овог система је унапређена координација и употреба алгоритама за рану детекцију сумњивих финансијских трансакција.

Систем FINCEN у САД

Амерички Финансијски центар за праћење криминалних активности (FINCEN) функционише као централна база за анализу и спречавање прања новца и финансирања тероризма.

Овај модел показује како се сарадња између финансијских институција и безбедносних служби може користити за рану идентификацију претњи.

Европска платформа за размену информација (EIS)

Европолова база података о тероризму омогућава брзу размену података између држава чланица ЕУ, чиме се смањује ризик од понављања грешака и омогућава координисан одговор на потенцијалне претње.

Србија, као кандидат за чланство у ЕУ, има приступ одређеним механизмима сарадње са Европолом, али ова сарадња може бити додатно унапређена.

Етички аспекти при обради података о грађанима у контексту тероризма - Обрада података о грађанима, чак и ако нису означени као тајни, увек носи етичке изазове, посебно у контексту тероризма. Проблеми који се јављају у овој области укључују:

Баланс између безбедности и људских права

Безбедносне агенције морају да воде рачуна да мере које примењују у борби против тероризма буду у складу са основним људским правима, као што су право на приватност и слободу изражавања.

Када се подаци прикупљају и обрађују, потребно је обезбедити да не дође до дискриминације или неоснованог профилисања по основу религије, расе или других осетљивих категорија.

Ризик од злоупотребе података

Постоји опасност да се подаци искористе изван законских оквира, што може довести до кршења људских права и поверења грађана у институције.

Тиме се могу нарушити основна начела демократског друштва, попут транспарентности и одговорности.

Приступ транспарентности у раду са осетљивим подацима - Док се борба против тероризма често повезује са високим нивоом тајности и ограниченим приступом информацијама, важно је развијати механизме који омогућавају транспарентност, а да се не угрози безбедност:

Информисање јавности уз уважавање безбедносних интереса

Грађани имају право да буду информисани о мерама које се предузимају ради њихове заштите, али не на начин који би открио критичне оперативне податке који могу угрозити ефективност тих мера.

Јавност може бити обавештена о постојању стратегија и закона који се примењују, али детаљи који би могли угрозити безбедност не би требало да буду откривени.

Регулисање приступа подацима у јавним институцијама

Како би се постигла транспарентност, неопходно је да постоје контроле које омогућавају јавним и независним институцијама (као што су омбудсман и судови) да прате како се подаци користе и да ли се поштују правни стандарди.

Потребно је успоставити механизме за независну надзорну контролу и ревизију рада безбедносних агенција.

Примена нових технологија у постојећем правном систему Србије

Иако нове технологије представљају значајан напредак у области борбе против тероризма, важно је осигурати да се њихова примена правилно усклади са постојећим правним оквиром. Овде су неки кораци који би могли бити остварив у кратком року:

Приступ "малим корацима" у примени технологија

За почетак, Србија може интегрисати мање инвазивне технологије, као што су системи за аутоматизовану размену података са другим земљама (попут Европола), како би се побољшала превенција тероризма.

Развој и имплементација алата за анализу великих података (Big Data) у реалном времену може се започети са пилот пројектима који се тестирају у ограниченим секторима, као што је анализа финасијских токова.

Реализација вештачке интелигенције у надзору

У будућности, увођење вештачке интелигенције за рану детекцију терористичких мрежа и претњи може бити кључно, али је важно да се ови системи користе у складу са правним оквиром и раде исправно, уз адекватну контролу.

Употреба "чистих" алгоритама, који не угрожавају основне принципе правде и приватности, била би важна тачка у процесу модернизације.

Уз увођење нових технологија и методологија у пракси, Србија ће морати да води рачуна о етичким и правним аспектима обраде података о грађанима. За успешну борбу против тероризма важно је одржати деликатан баланс између безбедности и поштовања људских права. Истовремено, транспарентност у раду са осетљивим подацима и развој примена нових технологија требају бити интегрисани у правни систем тако да не угрозе безбедносне интересе, али и да обезбеде стални надзор и поштовање демократских принципа.

Обрада и заштита осетљивих података у вези са тероризмом остаје изазов који захтева континуирану модернизацију правног оквира, унапређење међусекторске сарадње и примену савремених технологија у складу са најбољим међународним праксама.

17. Оперативни подаци полиције и јавне безбедности (уколико нису означени као тајни)

Оперативни подаци полиције и јавне безбедности представљају информације које се користе за планирање, анализу и реаговање на безбедносне изазове. Њихова обрада и доступност уређени су релевантним правним оквиром, укључујући **Закон о полицији („Службени гласник РС”, бр. 6/2016, 24/2018, 87/2018, 86/2019, 122/2021 и 124/2022)**, **Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018)** и **Закон о тајности података („Службени гласник РС”, бр. 104/2009, 10/2015 и 44/2018)**.

Категорије оперативних података

Општи подаци о безбедносним догађајима – укључују информације о нарушавању јавног реда и мира, кривичним делима, прекршајима и интервенцијама полиције.

Податке о локацијама криминалних активности – користе се за анализу и предвиђање безбедносних ризика.

Статистике о криминалу и безбедносним инцидентима – садрже податке о врстама кривичних дела и другим безбедносним показатељима.

Оперативне информације о јавним скуповима и манифестацијама – обухватају податке о безбедносним проценама и мерама за осигурање јавног реда.

Подаци о ухапшеним и задржаним лицима – воде се у складу са **Закоником о кривичном поступку**.

Информације о превентивним акцијама полиције – односе се на програме за смањење криминала.

Додатни сегменти

Технологија у раду полиције

Министарство унутрашњих послова користи савремене технолошке системе за побољшање ефикасности рада полиције, укључујући:

Системе за видео-надзор (нпр. „Паметни град“ са мрежом надзорних камера),

Системе за аутоматско препознавање регистарских таблица (ANPR),

Форензичке софтвере за анализу података и дигиталне доказе,

Биометријске системе идентификације у граничним прелазима,

Базе података повезане са међународним безбедносним системима, попут **ИНТЕРПОЛ-а и ЕУРОПОЛ-а**.

Евалуација рада полиције

Оцењивање рада полицијских службеника спроводи се кроз:

Интерне ревизије и надзор над радом полиције од стране **Сектора унутрашње контроле** у МУП-у,

Комисије за праћење рада полиције, укључујући и независна тела,

Извештаје о безбедности који садрже анализе и препоруке за унапређење рада,

Механизме за подношење жалби грађана на поступање полицијских службеника.

Специјализоване јединице

Поред стандардних полицијских јединица, постоје и специјализоване формације:

Специјална антитерористичка јединица (САЈ) – елитна јединица за борбу против тероризма и високоризичне интервенције.

Жандармерија – јединица за одржавање јавног реда и борбу против организованог криминала.

Хеликоптерска јединица – подршка операцијама из ваздуха.

Јединица за високотехнолошки криминал – истражује сајбер-криминал и дигиталне претње.

Сарадња са цивилним сектором

Полиција сарађује са невладиним организацијама и локалним заједницама кроз:

Превентивне програме у школама и локалним срединама,

Пројекте са цивилним сектором о људским правима и транспарентности,

Сарадњу са медијима на едукацији јавности о безбедносним ризицима.

Примери транспарентности

Министарство унутрашњих послова објављује:

Годишње извештаје о раду,

Јавне базе података (регистар несталих лица, статистике о безбедности),

Информације о јавним набавкама и буџетским средствима,

Јавне седнице и консултације са цивилним друштвом.

Кључни изазови у пракси:

Усклађивање различитих правних режима – Оперативни подаци полиције могу садржати осетљиве информације које потпадају под више правних режима, попут Закона о заштити података о личности, Закона о тајности података и Закона о кривичном поступку. Питање је како правилно означити податке тако да буду заштићени, али и доступни за рад надлежних органа.

Проблем превисоког или преniског означавања тајности – Неправилно означавање података може довести до две екстремне ситуације:

Прекомерно означавање („овер-класификација“) може ограничити приступ подацима који су потребни за рад различитих служби и успорити оперативне активности.

Недовољно означавање („андер-класификација“) може довести до откривања осетљивих информација неовлашћеним лицима и угрожавања безбедности истрага или сведока.

Сарадња и размена информација – Полиција често сарађује са другим институцијама, попут тужилаштва, судова, безбедносних агенција и међународних партнера. Питање је како осигурати да су подаци адекватно заштићени, али истовремено доступни релевантним службама без прекомерних бирократских ограничења.

Динамика ажурирања података – Оперативни подаци се мењају у реалном времену, што значи да се и ниво тајности можда мора ревидирати. Потребно је установити јасне процедуре за периодично преиспитивање степена тајности података, како би се избегле грешке у њиховој заштити.

Обученост кадрова – Често особе које раде са овим подацима немају довољно знања о законским захтевима и процедурама за правилно означавање тајности, што може довести до пропуста у примени прописа.

Проблем означавања оперативних података степеном тајности није само правно питање, већ и питање практичне примене у свакодневном раду полиције и служби безбедности. Потребно је унапређивање нормативног оквира, развој јасних упутстава и континуирана едукација кадрова како би се осигурала ефикасна заштита података, али и несметано функционисање система безбедности.

Оперативни подаци полиције и јавне безбедности играју кључну улогу у одржавању сигурности грађана и борби против криминала. Њихова обрада и размена морају бити усклађени са важећим законским прописима, уз поштовање принципа заштите података о личности и транспарентности у раду надлежних органа. Истовремено, коришћење савремених технологија, сарадња са домаћим и међународним безбедносним структурама, као и активна комуникација са јавности, представљају важне инструменте унапређења рада полиције. Континуирана евалуација и надзор над полицијским активностима доприносе јачању поверења грађана и унапређењу ефикасности институција.

У будућности, неопходно је наставити са унапређењем правног оквира, модернизацијом технолошких капацитета и јачањем сарадње са цивилним друштвом како би се осигурао одговоран, законит и ефикасан рад полицијских структура.

18. Штићени подаци о финансијским трансакцијама

Штићени подаци о финансијским трансакцијама, који нису означени степеном тајности, обухватају информације које се односе на финансијске трансакције, али нису формално класификоване као поверљиве или тајне. Ови подаци су под заштитом различитих закона и прописа, укључујући Закон о заштити података о личности, Закон о Народној банци Србије, Закон о платном промету и одредбе које се односе на пословну и професионалну тајну.

Правни основ:

Закон о заштити података о личности:

Регулише обраду личних података, укључујући податке о финансијским трансакцијама, и обезбеђује заштиту од неовлашћеног приступа и дељења личних информација.

Закон о Народној банци Србије:

Обавезује банке и финансијске институције да чувају поверљивост података клијената у оквиру концепта банкарске тајне.

Закон о платном промету:

Уређује начин спровођења финансијских трансакција, обраду података о платном промету и одговорности укључених страна.

Законски и уговорни оквири пословне и професионалне тајне:

Пословна тајна обухвата информације које имају економску вредност, као што су трговачке стратегије, подаци о клијентима, процеси и иновације.

Професионална тајна укључује поверљиве информације које су повезане са професионалним активностима, као што су финансијски извештаји, консултантски материјали, и слично.

Категорије података:

Информације о трансакцијама: износи, датуми, врсте трансакција, и примаоци.

Банкарски подаци: бројеви рачуна, подаци о банкама, стања на рачуну.

Лични подаци клијената: имена, адресе, идентификациони бројеви.

Подаци заштићени банкарском тајном: стање рачуна, трансакције, финансијски уговори и обавезе клијената.

Пословна и професионална тајна: трговачке стратегије, процеси, осетљиви уговори и други подаци који представљају конкурентску предност.

Банкарска, пословна и професионална тајна:

Банкарска тајна обавезује банке да заштите податке клијената, као што су подаци о рачунима, трансакцијама и кредитним обавезама.

Пословна и професионална тајна:

Укључује информације од стратешког или пословног значаја које нису доступне јавности, као што су финансијски извештаји, пословни планови и интерни процеси.

Заштићене су како законом, тако и уговорним обавезама, а откривање може довести до озбиљних правних и пословних последица.

Облици одговорности и санкције у случају кршења:

Кривична одговорност:

Намерно откривање или злоупотреба информација може бити кажњиво у складу са кривичним законом.

Прекршајна одговорност:

Мањи пропусти, као што је занемаривање мера заштите, могу резултирати новчаним казнама.

Грађанско-правна одговорност:

Оштећена страна може тражити накнаду штете у случају кршења поверљивости.

Дисциплинска одговорност:

У случају запослених, интерне мере могу укључивати опомене, деградацију или отпуштање.

Санкције:

Новчане казне: Казне за кршење пословне и професионалне тајне могу бити знатне, у зависности од тежине пропуста.

Административне мере: Регулаторни органи могу изрећи привремене или трајне санкције.

Судске мере: Судови могу наложити прекид обраде података или надокнаду штете.

Репутацијска штета: Компаније које крше тајне ризикују губитак клијената и конкурентске позиције.

Примери из праксе:

Банке: Штите податке клијената од неовлашћеног приступа, у складу са прописима о банкарској тајни.

Компаније: Успостављају интерне протоколе за заштиту пословних и професионалних података, као што су ограничен приступ и NDA уговори.

Штићени подаци о финансијским трансакцијама, иако нису формално означени степеном тајности, подлежу строгим прописима који имају за циљ заштиту од неовлашћеног приступа и злоупотребе. Законски оквири као што су Закон о заштити података о личности, Закон о Народној банци Србије и Закон о платном промету обезбеђују да се ова врста података чува поверљиво и у складу са правним нормама. Кршење ових обавеза може довести до значајних правних и пословних последица, укључујући кривичну, прекршајну и грађанску одговорност, као и репутацијске штете. Стога је неопходно да све укључене стране, било да су у питању банке, компаније или други субјекти, успоставе адекватне механизме за заштиту ових података, како би избегли правне последице и очували поверење својих клијената.

19. Штићени подаци у безбедносним и обавештајним службама Републике Србије

Законски оквир и оснивање служби безбедности Службе безбедности Републике Србије – Безбедносно-информативна агенција (БИА), Војнобезбедносна агенција (ВБА) и Војнообавештајна агенција (ВОА) – основане су на основу *Закона о основама уређења служби безбедности Републике Србије*. Овај закон пружа основну правну структуру за рад и функционисање свих безбедносних служби у земљи. Поред тога, специфични аспекти рада ВБА и ВОА регулисани су *Законом о Војнобезбедносној агенцији и Војнообавештајној агенцији*, док се рад БИА уређује засебним *Законом о Безбедносно-информативној агенцији*.

Штићени подаци и њихова правна регулатива Поред тајних података, постоје и подаци који се дефинишу као штићени, а који су подвргнути посебном режиму заштите. Штићени подаци представљају информације које могу угрозити националну безбедност, сигурност институција или интересе државе, али нису формално означени као тајни. Они обухватају:

Поверљиве податке: Информације које се односе на безбедносне активности, али нису од највеће осетљивости (нпр. подаци о терористичким претњама или организованом криминалу).

Стратешке податке: Подаци који су од значаја за националне интересе, као што су процене безбедносних ризика или анализа одбрамбених способности.

Професионалне тајне: Информације повезане са стручним знањем, методама рада или интерним протоколима служби, које је потребно чувати ради заштите њихове оперативне ефикасности.

Пословне тајне: Податке од комерцијалног или економског значаја, као што су уговори или техничке спецификације, чије би откривање могло нанети штету државним институцијама или партнерским предузећима.

Правна регулатива за професионалне и пословне тајне Заштита професионалних и пословних тајни регулисана је *Законом о заштити пословне тајне* (Службени гласник РС, бр. 72/2019). Овај закон пружа смернице за идентификовање и заштиту информација које имају комерцијалну вредност, као и за спречавање њиховог неовлашћеног откривања.

У оквиру служби безбедности, ови прописи допуњују постојеће законе како би се обезбедило да критичне информације остану заштићене од индустријске шпијунаже или злоупотребе.

Примена у пракси и заштита података У раду БИА, поверљиви подаци могу се односити на особе повезане са организованим криминалом или тероризмом. Ови подаци обухватају информације коришћене за процену потенцијалних претњи, али не садрже осетљиве детаље као што су тајни извори. ВБА и ВОА користе штићене податке у анализама стратешких процена, као што су извештаји о безбедности на граници. Поред тога, професионалне и пословне тајне могу укључивати:

Методолошке приступе анализи претњи.

Техничке податке који су од виталног значаја за рад информационих система служби.

Комерцијалне уговоре са партнерима или добављачима чије би откривање могло штетити стратешким интересима.

Разлика између поверљивих и тајних података

Поверљиви подаци подразумевају информације које су осетљиве, али не укључују најкритичније елементе, попут тајних извора или оперативних планова. Иако су под посебном заштитом, ови подаци нису формално класификовани као "тајни".

Тајни подаци, с друге стране, представљају најосетљивије и најкритичније информације од суштинског значаја за националну безбедност, као што су одбрамбене стратегије и идентитети тајних агената. Ове информације су увек формално класификоване и обележене ознакама попут "строго поверљиво" или "државна тајна".

Санкције и дисциплинска одговорност У случају непоштовања прописа о заштити штићених података, примењују се релевантне одредбе *Кривичног законика Републике Србије* и прописи о дисциплинској одговорности припадника служби безбедности.

Кривични законик регулише кривична дела као што су неовлашћено откривање тајних података и злоупотреба службеног положаја.

Дисциплинска одговорност укључује мере попут опомена, смањења плата или губитка радног односа у случају тежих прекршаја.

Међународна пракса и стандарди У складу са процесом евроинтеграција, Србија примењује међународне стандарде за заштиту података, што доприноси сарадњи са глобалним безбедносним партнерима.

Етичка одговорност служби Етичка одговорност подразумева строго придржавање закона, транспарентност у обради података и заштиту права грађана, чиме се гради поверење јавности у рад безбедносних институција.

Штићени подаци су од суштинског значаја за функционисање безбедносних служби у Србији. Уз очување поверљивих, стратешких, професионалних и пословних тајни, систем заштите обезбеђује националну безбедност, интегритет институција и сарадњу са међународним партнерима. Строга примена закона и етички приступ раду јачају транспарентност и поверење јавности.

20. Категорије штићених података о безбедности животне средине (без тајних података)

Подаци о животној средини у Републици Србији могу бити штићени у складу са различитим правним основима, али без доделе степена тајности. То су углавном подаци који се штите ради очувања јавног интереса, заштите личних података и пословних интереса.

1. Подаци заштићени као пословна тајна

Правни основ:

Закон о заштити пословне тајне („Службени гласник РС”, бр. 53/2021)

Закон о привредним друштвима („Службени гласник РС”, бр. 36/2011, 99/2011, 83/2014, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021 и 123/2021)

Примери из праксе:

Хемијски састав индустријског отпада ако би откривање угрозило конкурентску позицију предузећа.

Технолошки процеси у фабрикама који могу утицати на загађење, али су истовремено предмет интелектуалне својине.

Податак о планираним инвестицијама у системе за пречишћавање воде и ваздуха пре њихове реализације.

2. Лични подаци у вези са утицајем животне средине на здравље

Правни основ:

Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018)

Закон о заштити животне средине („Службени гласник РС”, бр. 135/2004 и изм.)

Примери из праксе:

Медицинске студије о болестима узрокованим загађењем (под условом да садрже личне податке пацијената).

Податак о индивидуалним здравственим последицама изложености опасним материјама.

Личне информације о учесницима у истраживањима утицаја животне средине.

Напомена: Агрегирани и анонимизовани подаци могу бити доступни јавности.

3. Подаци о природним ресурсима који се штите због пословних или истраживачких интереса

Правни основ:

Закон о рударству и геолошким истраживањима („Службени гласник РС”, бр. 101/2015, 95/2018 и 40/2021)

Закон о заштити природе („Службени гласник РС”, бр. 36/2009, 88/2010, 91/2010, 14/2016, 95/2018 и 71/2021)

Примери из праксе:

Геолошки подаци о залихама минералних сировина ако би њихово откривање утицало на економски интерес Србије.

Локације ретких биљних и животињских врста ако би њихово откривање довело до угрожавања екосистема (нпр. прекомерно сакупљање лековитих биљака).

Подаци о истражним бушотинама за нафту и гас.

4. Подаци о управљању опасним материјама у привредним објектима

Правни основ:

Закон о управљању отпадом („Службени гласник РС”, бр. 36/2009, 88/2010, 14/2016, 95/2018 и 95/2018 – др. закон)

Закон о заштити од пожара („Службени гласник РС”, бр. 111/2009 и 20/2015)

Примери из праксе:

Подаци о количини и врсти опасног отпада који настаје у индустријским постројењима (осим у случајевима када постоји законска обавеза објављивања).

Интерне процене ризика од еколошких инцидената које компаније израђују у складу са законским прописима.

Локације одређених депонија опасног отпада које су у процесу санације.

5. Подаци из стратешких планова и студија о животној средини

Правни основ:

Закон о стратешкој процени утицаја на животну средину („Службени гласник РС”, бр. 135/2004, 88/2010 и 95/2018)

Закон о процени утицаја на животну средину („Службени гласник РС”, бр. 135/2004, 36/2009, 88/2010, 91/2010 и 14/2016)

Примери из праксе:

Делови стратешких планова који се односе на будуће индустријске зоне пре завршетка званичних процедура.

Прелиминарне студије утицаја на животну средину које су у поступку ревизије.

Интерни документи који садрже анализе економске оправданости еколошких пројеката.

Подаци о животној средини у Србији могу бити штићени без доделе степена тајности ако су у питању:

✓ **Пословне тајне** (индустријски процеси, комерцијални планови),
✓ **Лични подаци** (утицај загађења на појединце),
✓ **Научни и геолошки подаци** (истраживања природних ресурса),
✓ **Подаци о опасним материјама** (интерни безбедносни извештаји компанија),
✓ **Стратешки документи у припреми**.

Проблем преклапања прописа

У Србији постоји значајна разлика у приступу штићењу података из различитих области, где се подаци који су важни за одбрану третирају као **тајни подаци** у складу са **Законом о тајности података**, док су подаци који се односе на рударство и геолошка истраживања заштићени, али не спадају у категорију **тајних података** у складу са **Законом о рударству и геолошким истраживањима**.

Закон о одбрани и Закон о тајности података - Према **Закону о одбрани** и **Закону о тајности података**, подаци који су од значаја за националну безбедност или одбрану могу бити **означени као тајни подаци**. Ови подаци могу обухватати информације о стратешким резервама природних ресурса, инфраструктури која има војну важност, као и податке који се односе на сигурност рударских и геолошких истраживања која се користе у контексту одбрамбених капацитета.

Закон о рударству и геолошким истраживањима - С друге стране, **Закон о рударству и геолошким истраживањима** прописује да одређени подаци из ове области, као што су информације о налазиштима минералних сировина или геолошким истраживањима, могу бити **штићени** због заштите економских интереса, али не носе ознаку тајности. Ови подаци се могу категорисати као **поверљиви** или **заштићени подаци**, али не припадају категорији **тајних података**.

Изазови у пракси

Различита дефиниција и третман штићених података: У пракси се јавља дилема када исти подаци, који могу бити корисни за националну безбедност (нпр. резерве минералних сировина) или имају војну вредност, не носе ознаку тајности, али су

истовремено заштићени према другим прописима. Ово доводи до конфузије и могућих правних неусаглашености.

Контроле и приступ: У случају података који су означени као **тајни подаци** према Закону о одбрани, контроле приступа и механизми заштите су много строжи, док су код података из рударства и геолошких истраживања мање рестриктивни, али такође постоји обавеза заштите тих података од неовлашћеног приступа. У пракси, ово може довести до различитог третмана истих података у зависности од правног оквира.

Ризик од злоупотребе или пропуста: Када подаци који су од важности за одбрану нису обележени као тајни подаци, постоји ризик да они буду објављени или злоупотребљени, што може довести до нарушавања националне безбедности. Са друге стране, ако подаци који су само привремено значајни за економију, али не и за одбрану, носе ознаку тајности, то може довести до непотребног ограничења приступа јавним ресурсима.

Предлог за решење - Један од могућих приступа за решавање овог дуализма могао би бити:

Дефинисање прецизнијих смерница и процедура у правним актима који ће разјаснити који подаци у једној области (нпр. рударству) могу бити сматрани као тајни подаци у контексту одбране. То би укључивало тачну класификацију података који имају потенцијалну војну вредност.

Размеравање нивоа тајности: Податке који имају двоструку вредност (економску и војну) требало би класификовати са већом прецизношћу, уз издавање посебних упутстава и процедура које ће обезбедити да се подаци из области рударства и геолошких истраживања који се користе за одбрамбене сврхе третирају као тајни подаци, али уз специфичан механизам заштите који је прилагођен овом двоструком контексту.

Управо оваква разматрања могу помоћи у стварању правног оквира који ће смањити правну неусаглашеност и омогућити бољу заштиту података од значаја за безбедност земље.

21. Штићени подаци о персоналу јавних служби и државних органа који нису означени степеном тајности

Ако подаци о запосленима у јавним службама и државним органима **нису означени као тајни подаци**, они и даље могу бити **штићени подаци** јер њихово откривање може угрозити безбедност, функционалност државних органа или права појединаца.

Категорије штићених података о персоналу

Подаци о радном ангажовању и унутрашњој организацији

Интерне кадровске евиденције које садрже информације о **распоређивању службеника** у одређеним секторима или организационим јединицама (посебно у безбедносним структурама, судству, тужилаштву, инспекцијским органима).

Податоци о **специјализованим функцијама** службеника (нпр. који полицајци или тужиоци су задужени за одређене истраге).

Распоред смена и дежурстава у органима који обављају критичне послове (нпр. у полицији, војсци, судству, центрима за управљање кризама).

Информације о стручним оспособљавањима и безбедносним проверама

Податке о томе **ко је прошао безбедносне провере**, који запослени имају приступ одређеним подацима, које нивое овлашћења поседују.

Листе државних службеника који су прошли **специјализоване обуке у области безбедности, сајбер-заштите, противтерористичких мера**.

Податке о учешћу запослених у тајним или осетљивим операцијама, иако сами подаци нису класификовани као тајни.

Финансијски и материјални подаци о персоналу

Детаљни подаци о платама и додатцима **за одређене категорије државних службеника**, ако би њихово откривање могло угрозити оперативну способност службе или изазвати злоупотребу.

Податке о коришћењу службених возила, станова, накнадама за рад на поверљивим пословима.

Евиденције о службеним путовањима које би могле открити информације о оперативним активностима (нпр. честа путовања инспектора у одређене регионе).

Информације о дисциплинским поступцима и интерним истрагама

Подаци о дисциплинским поступцима против државних службеника, посебно ако се односе на области безбедности, полиције, војске, правосуђа.

Интерне евиденције о пријавама корупције или кршења службене дужности, ако нису предмет судских поступака, али су битне за унутрашње функционисање органа.

Извештаји о резултатима интерних истрага, ако нису формално означени као тајни, али могу утицати на безбедност институција.

Информације о запосленима у специјалним и осетљивим службама

Листе запослених у **службама безбедности**, ако нису класификоване као тајне, али могу угрозити интегритет тих особа (нпр. тачна радна места, функције).

Подаци о агентима под прикрићем или припадницима специјалних јединица, ако нису формално означени као тајни, али их идентификују у јавним регистрима.

Информације о службеницима који раде на заштити сведока или у посебним истражним тимовима.

Примери из праксе

✓ **Пример 1:** Интерна листа службеника који имају овлашћење за руковање поверљивим подацима у полицији – иако није означена као тајна, откривање тих података би могло довести до злоупотреба.

✓ **Пример 2:** Распоред смена судија и тужилаца у предметима организованог криминала – није класификован, али може угрозити безбедност тих особа.

✓ **Пример 3:** Детаљни финансијски извештаји о накнадама за ангажовање службеника у безбедносним операцијама – нису тајни, али могу открити структуру и организацију одређених јединица.

✓ **Пример 4:** Интерна документа о запосленима који су прошли безбедносне провере за рад у одређеним критичним секторима (енергетика, сајбер-безбедност, национална одбрана).

✓ **Пример 5:** Извештаји о унутрашњим контролама рада полицијских службеника – нису формално означени као тајни, али могу садржати осетљиве информације о оперативним процедурама.

Правни оквир заштите ових података

Закон о заштити података о личности – Штити личне податке службеника, чак и ако ти подаци нису означени степеном тајности. Односи се на запослене у државним органима, јавним службама и јавним предузећима.

Закон о слободном приступу информацијама од јавног значаја – Омогућава ограничавање приступа подацима о запосленима у државним органима, јавним службама и јавним предузећима ако би њихово објављивање угрозило **националну безбедност, критичну инфраструктуру или функционисање тих органа и установа**.

Закон о државним службеницима – Прописује да се одређене кадровске евиденције (подаци о радним местима, интерним премештајима, систематизацији) могу третирати као **штићени подаци**, уколико би њихово откривање угрозило рад државних органа.

Закон о јавним предузећима – Дефинише правни статус јавних предузећа и омогућава ограничење приступа одређеним кадровским и оперативним подацима ако су од значаја за **безбедност или критичну инфраструктуру**.

Закон о спољним пословима – Уређује податке о дипломатско-конзуларном особљу и кадровским питањима у Министарству спољних послова, што може укључивати **штићене податке**, у зависности од функције и природе посла.

Закон о критичној инфраструктури – Омогућава заштиту података о запосленима у секторима који управљају виталним ресурсима (енергетика, транспорт, телекомуникације), чиме се спречава потенцијална угроженост тих система.

Закон о раду – Прописује општа правила за заштиту личних података запослених, укључујући податке који могу бити осетљиви или **штићени у контексту радних односа у државним органима и јавним предузећима**.

Закон о полицији – Уређује руковање кадровским и оперативним подацима о полицијским службеницима, при чему одређени подаци могу бити **штићени**, чак и ако нису означени као тајни, ради заштите службеника и ефикасног обављања полицијских послова.

Јавна предузећа нису класични државни органи, али уколико обављају послове **од значаја за националну безбедност, критичну инфраструктуру или међународну сарадњу**, подаци о њиховом персоналу могу се сматрати штићеним.

Који подаци о запосленима у јавним предузећима могу бити штићени (иако нису означени као тајни)?

Подаци о запосленима који раде на пословима критичне инфраструктуре

ЕПС, Србијагас, Телеком Србија, Железнице Србије, НИС (државно власништво у НИС-у), Аеродроми Србије и слична предузећа која управљају стратешки важним ресурсима.

Подаци о руководиоцима и техничком особљу у енергетском сектору, телекомуникацијама, железници, аеродромима, саобраћају, јер њихово откривање може угрозити оперативну безбедност ових система.

Подаци о овлашћеним инжењерима, сервисерима и техничарима који одржавају виталне системе.

Подаци о запосленима који раде на осетљивим међународним пројектима

Информације о особама које раде на пројектима сарадње са **иностраном безбедносном инфраструктуром (нпр. нуклеарна енергија, гасоводи, ИТ-безбедност)**.

Имена и контакт подаци стручњака ангажованих у **регионалним или међународним иницијативама** где Србија има улогу у заштити инфраструктуре (нпр. гранична контрола, заједнички енергетски пројекти).

Подаци о особљу јавних предузећа која учествују у кризном управљању и заштити грађана

Запослени у јавним водоводним, електродистрибутивним, комуналним службама ако су задужени за управљање у кризним ситуацијама (нпр. епидемије, природне катастрофе).

Листе запослених у секторима **Цивилне заштите и служби хитних интервенција** у јавним предузећима (нпр. Србијаводе током поплава).

Подаци о корпоративној безбедности и сличним структурама у јавним предузећима

Имена и дужности **лица задужених за физичку и информациону безбедност** у стратешким јавним предузећима.

Распоред смена, безбедносни протоколи и лични подаци запослених у секторима који раде на заштити објеката.

Који правни оквири уређују заштиту ових података?

Закон о раду – Општи прописи о заштити података о запосленима.

Закон о заштити података о личности – Лични подаци запослених, укључујући контакт информације, морају се штитити.

Закон о слободном приступу информацијама од јавног значаја – Државни органи могу одбити приступ подацима ако би њихово откривање угрозило функционисање јавног предузећа или безбедност.

Закон о безбедности и здрављу на раду – Прописује заштиту одређених података о радним местима у ризичним секторима.

Закон о јавним предузећима – Дефинише обавезе јавних предузећа у погледу извештавања и заштите података.

Закон о критичној инфраструктури – Подаци о особљу ангажованом у критичним секторима могу бити заштићени због ризика по безбедност.

Јавна предузећа у Србији могу имати штићене податке о свом особљу, али се морају разликовати од строго тајних података. Ако се подаци односе на раднике који управљају критичном инфраструктуром, учествују у међународној сарадњи или имају безбедносне функције, њихово откривање може бити ограничено из безбедносних разлога.

22. Штићени подаци у вези с националном безбедношћу који нису означени као тајни

Ако искључимо **тајне податке** (означене степеном тајности: „Поверљиво“, „Строго поверљиво“ или „Државна тајна“), и **личне податке** (који су заштићени Законом о заштити података о личности), остају **штићени подаци** који су **релевантни за националну безбедност**, али нису формално класификовани као тајни.

Категорије штићених података у вези са националном безбедношћу

Оперативни и аналитички подаци који нису означени као тајни, али имају стратешки значај

Податци о **кризнима плановима и процедурама** за одговор на ванредне ситуације (терористички напади, сајбер-напади, природне катастрофе) ако нису формално означени степеном тајности.

Интерне **анализе безбедносних ризика**, које се користе за планирање мера заштите критичне инфраструктуре.

Технички описи **безбедносних система на границама**, у енергетском сектору и транспорту, ако нису сврстани у тајне податке.

Информације о критичној инфраструктури и системима од значаја за безбедност

Податоци о капацитетима и функционисању **болница, водовода, електроенергетских објеката** и других виталних система.

Детаљи о безбедносним протоколима **у јавним установама** (нпр. мере евакуације у случају напада или хаварије).

Локације и карактеристике **објеката у државном власништву** који нису формално означени као објекти посебне намене, али имају безбедносни значај.

Информације о сарадњи са међународним безбедносним организацијама

Подаци о заједничким војним и полицијским вежбама са НАТО, ОДКБ или ЕУ, ако нису класификовани.

Интерна документација о **размени података у области борбе против тероризма и организованог криминала** (документи који нису формално означени као тајни, али су осетљиви).

Извештаји о учешћу Србије у мировним мисијама, ако садрже интерне операционе податке.

Јавне набавке и финансирање у области безбедности

Финансијски и технички подаци о набавци **опреме за полицију и војску**, ако нису тајни, али би могли открити осетљиве детаље о оперативним способностима.

Уговори са приватним безбедносним компанијама који обављају послове за државу (нпр. ИТ заштита, надзор).

Подаци о **безбедносним процедурама у јавним набавкама** (који нису тајни, али могу открити потенцијалне рањивости у систему).

Информације о сајбер-безбедности

Подаци о **инцидентима у националним ИТ системима** који нису формално означени степеном тајности, али откривају слабости.

Детаљи о **технолошкој инфраструктури државних органа** (извештаји о безбедносним проверама, капацитетима државних сервера).

Унутрашње анализе сајбер-напада који нису тајни подаци, али могу послужити за даљу заштиту система.

Правни оквир за заштиту ових података

Закон о слободном приступу информацијама од јавног значаја (члан 9) – дозвољава ускраћивање информација ако би њихово откривање угрозило националну безбедност.

Закон о заштити тајности података – одређује критеријуме за означавање тајних података, али се може применити и на штићене податке који нису формално класификовани.

Закон о одбрани и Закон о безбедносним службама – регулишу руковање информацијама од значаја за одбрану и безбедност, чак и ако нису формално означене као тајне.

Закони о критичној инфраструктури – предвиђају мере заштите одређених категорија информација, чак и ако нису формално класификоване.

Примери из праксе

✓ **Пример 1:** Извештај о вежби за реаговање на терористички напад који садржи детаље о слабостима у безбедносном систему (али није формално означен као тајан).

✓ **Пример 2:** Финансијска анализа потрошње у сектору безбедности, која може открити како држава финансира безбедносне операције и системе.

✓ **Пример 3:** Извештај о безбедносним ризицима на јавним скуповима, који садржи интерне процене могућих инцидената и планиране мере реаговања.

✓ **Пример 4:** Листа технолошке опреме која се користи у државним безбедносним институцијама, која није означена као тајна, али би могла открити осетљиве податке о капацитетима и рањивостима.

✓ **Пример 5:** Документација о преговорима са страним партнерима у области безбедности (нпр. о куповини опреме или заједничким акцијама), која није означена као тајна, али би могла нашкодити интересима Србије ако постане јавна.

23. Подаци о међународној сарадњи Републике Србије

Подаци о међународној сарадњи Републике Србије, уколико нису означени као тајни подаци, представљају информације које се односе на активности државних органа, институција и организација у оквиру међународних односа. Ови подаци могу укључивати:

билатералне и мултилатералне споразуме,

дипломатске и економске односе,

сарадњу у области безбедности, одбране, правосуђа, науке, културе и образовања,

учешће у међународним организацијама,

споразуме о слободној трговини,

међународне програме и пројекте финансиране из страних извора,

званичне комуникације са међународним партнерима, осим ако су заштићене степеном тајности.

Правни оквир - Овакви подаци регулисани су различитим законима и подзаконским актима, укључујући:

Закон о Влади Републике Србије – дефинише надлежности Владе у међународним односима.

Закон о спољним пословима – уређује рад Министарства спољних послова и дипломатско-конзуларних представништава.

Закон о тајности података – одређује услове под којима се подаци могу означити као тајни и прописује поступке заштите.

Закон о слободном приступу информацијама од јавног значаја – омогућава приступ подацима о међународној сарадњи који нису означени као тајни.

Закон о међународним уговорима – прописује процедуре за закључивање, ратификацију и спровођење међународних споразума.

Закон о безбедности и сарадњи у области одбране – регулише сарадњу у безбедносним и одбрамбеним питањима.

Закони који регулишу привредну сарадњу – нпр. Закон о спољнотрговинском пословању.

Ако изузмемо **тајне податке** (означене степеном тајности) и **личне податке** (који су заштићени Законом о заштити података о личности), преостала категорија **штићених података** у контексту међународне сарадње Републике Србије може обухватати **пословно осетљиве и поверљиве податке**, као и **осетљиве податке који нису класификовани као тајни, али захтевају посебан ниво заштите**.

Категорије штићених података

Пословно осетљиви подаци

Финансијски и комерцијални подаци о међународним уговорима и пројектима пре њихове финализације.

Преговарачке позиције Србије у трговинским и инвестиционим споразумима.

Податоци о стратешким пројектима са страним партнерима пре њиховог јавног објављивања.

Поверљиви подаци институција и органа управе

Интерна комуникација државних органа у вези са припремом међународних уговора и иницијатива.

Неразматрани предлози за билатералну и мултилатералну сарадњу.

Извештаји и анализе намењене унутрашњем коришћењу у институцијама.

Оперативни подаци о међународној сарадњи

Детаљи о текућим дипломатским преговорима који још нису званично објављени.

Интерна документација о имплементацији споразума и међународних програма.

Логистички подаци о сарадњи у области безбедности, одбране, правосуђа, енергетике и других критичних сектора.

Информације заштићене уговорним обавезама

Подаци који су обухваћени клаузулама о поверљивости у међународним споразумима.

Уговори са страним партнерима који садрже клаузуле о ограниченом приступу информацијама.

Информације из размене у оквиру међународних пројеката које нису предвиђене за широку јавност.

Правни оквир за заштиту ових података

Закон о слободном приступу информацијама од јавног значаја (члан 9) – ограничава доступност информација ако би њихово објављивање нанело штету међународним односима, безбедности, одбрани или економским интересима Србије.

Закон о привредним друштвима – штити пословно осетљиве информације у међународним пословним односима.

Закони о заштити интелектуалне својине и пословне тајне – штите одређене аспекте сарадње који укључују патенте, технологију и стратешке податке.

Уговори и меморандуми о сарадњи – могу садржати клаузуле о заштити информација које нису тајне, али се не смеју слободно објављивати.

Ова врста података није означена као **тајни податак**, али њихово неприкладно откривање може имати **правне, финансијске или безбедносне последице**.

Примери из праксе за штићене податке у међународној сарадњи

1. Преговори о споразуму о слободној трговини (нпр. са Кином или ЕАЕУ) - Када Србија преговара о споразуму о слободној трговини са другом државом или економским блоком (нпр. Кином или Евроазијском економском унијом - ЕАЕУ), подаци као што су:

Предложене тарифе и квоте за робу,

Стратегија Србије у преговорима,

Анализе утицаја споразума на домаћу привреду,

Интерни извештаји министарстава о потенцијалним ризицима и добитима – сматрају се **штићеним подацима**, јер би њихово рано објављивање могло угрозити преговарачку позицију Србије.

2. Споразуми у области енергетике (нпр. сарадња са Русијом око гаса или са ЕУ око обновљивих извора) - Када Србија склапа дугорочне уговоре о испоруци гаса, електричне енергије или инвестицијама у енергетску инфраструктуру, неки подаци могу бити заштићени јер:

Уговори често садрже поверљиве комерцијалне клаузуле (цене, услове испоруке, могућности измена уговора),

Објављивање детаља пре ратификације може изазвати шпекулације на тржишту,

Конкурентске фирме би могле добити предност ако би приступиле анализама и стратегијама државе.

Ови подаци нису **тајни** у смислу Закона о тајности података, али су **штићени** уговорним клаузулама и одредбама о поверљивости.

3. Преговори о страним инвестицијама (нпр. долазак великог инвеститора у Србију) - Када Србија преговара о доласку великог инвеститора (нпр. неке светске компаније која жели да отвори фабрику у Србији), држава често разматра:

Пореске олакшице и субвенције које ће понудити,

Локације које долазе у обзир за изградњу погона,

Утицај инвестиције на домаћу привреду и радну снагу.

Ако би се ови подаци открили пре закључења споразума, конкуренција би могла искористити информације, а јавност би могла вршити непотребан притисак на доносиоце одлука.

4. Дипломатски меморандуми и интерна комуникација - Министарство спољних послова и дипломатска представништва воде интензивну преписку у припреми међународних договора. Интерни извештаји, анализе и дипломатске депеше нису **тајни подаци**, али се често третирају као **поверљиви или штићени**, јер откривају ставове, процене и тактике које Србија користи у односима са другим државама.

Штићени подаци у међународној сарадњи Србије су они који нису **званично означени степеном тајности**, али чије би објављивање могло нанети штету државним интересима, економији или дипломатским односима. Они су обухваћени уговорним клаузулама, законима о пословној тајни, комерцијалним споразумима и интерним процедурама државних органа.

24. Поверљивост података у истраживачким пројектима

Поверљивост података у истраживачким пројектима представља један од најважнијих аспеката научног рада, јер осигурава заштиту права учесника, интегритет истраживања и поштовање етичких и правних стандарда. У Републици Србији, ова област је регулисана низом закона и етичких кодекса који дефинишу обавезе истраживача и институција. С обзиром на брз развој технологија и све већу дигитализацију истраживања, потребно је стално осавремењивати приступи у заштити података како би се осигурала њихова безбедност.

Правне основе

У Републици Србији, правни оквир за заштиту података у истраживачким пројектима обухвата следеће законе и прописе:

Закон о заштити података о личности („Службени гласник РС“, бр. 87/2018), који регулише обраду података о личности, укључујући научна истраживања, и у складу са Општом уредбом о заштити података (GDPR) која важи у Европској унији, што подразумева обавезе истраживача у погледу прикупљања, обраде и складиштења личних података.

Закон о научноистраживачкој делатности („Службени гласник РС“, бр. 110/2005, 50/2006, 18/2010, 112/2015), који дефинише услове за спровођење истраживања и обавезу заштите података, али и захтева да сви истраживачи у Србији поштују одредбе које се односе на поштовање етичких стандарда у научном раду.

Закон о здравственој документацији и евиденцијама у области здравства („Службени гласник РС“, бр. 123/2014), који се односи на заштиту здравствених података у истраживањима, нарочито у клиничким испитивањима и другим медицинским истраживањима где је потребно осигурати анонимност и безбедност података пацијената.

Категорије података

Подаци који се обрађују у истраживачким пројектима могу се поделити на различите категорије, сваку од којих треба пажљиво заштитити:

Подаци о личности: Име, презиме, адреса, контакт информације и други подаци који идентификују учеснике истраживања. Ови подаци морају бити заштићени од неовлашћеног приступа и у складу са законом.

Осетљиви подаци: Здравствени, генетички и биометријски подаци који су посебно осетљиви и захтевају највишу меру заштите. У овом контексту, анонимизација и енкрипција података су кључне.

Анонимизовани подаци: Подаци који су обрађени тако да се не могу повезати са конкретним лицем. Ова категорија је важна у истраживањима која захтевају велико узорковање и примену статистичких метода.

Подаци о малолетницима: Захтевају посебну заштиту и сагласност родитеља или старатеља. У овом контексту, треба бити посебно пажљив на начин прикупљања и чувања ових података како би се осигурала сигурност и приватност деце.

Етички кодекси научних институција

Етички кодекси играју кључну улогу у дефинисању стандарда за поверљивост и интегритет података. Примери укључују:

Етички кодекс Универзитета у Београду: Прописује обавезе истраживача у погледу заштите података, информисаног пристанка учесника у истраживању и етичког поступања са осетљивим информацијама. Кодекс захтева да се подаци прикупљени у истраживањима чувају у складу са највишим безбедносним стандардима.

Етички кодекс Института за јавно здравље „Др Милан Јовановић Батут“: Дефинише смернице за заштиту здравствених података и анонимност пацијената у научним студијама. Кодекс прописује обавезу добијања сагласности учесника и обезбеђује да се сви здравствени подаци користе само у научне сврхе.

Етички кодекс Природно-математичког факултета у Новом Саду: Обухвата мере за заштиту података у истраживањима која укључују људске субјекте, као и правила за обраду и чување научних података. Строга правила о чувању података и заштити личних података су један од основних принципа овог кодекса.

Улоге и одговорности истраживача и институција

Истраживачи и институције имају одговорност да:

Осигурају **информисани пристанак** учесника у истраживању и да учесници буду обавештени о начину обраде података.

Примењују **анонимизацију** података како би заштитили идентитет учесника и обезбедили да подаци не могу бити повезани са конкретним особама.

Обрађују податке искључиво за **сврхе истраживања** и у складу са релевантним законима и етичким смерницама, као и обезбеде да подаци буду употребљени само у оквиру одређених истраживачких пројеката.

Омогуће **сигурно складиштење података**, са ограниченим приступом, како би се спречила неовлашћена употреба или злоупотреба података.

Примери из праксе у Србији

Примери успешне примене заштите података у истраживањима укључују:

Програм „ПРОМИС“: Фонд за науку Републике Србије финансирао је пројекте младих истраживача који укључују заштиту података у складу са законом, са посебним акцентом на анонимизацију података и сигурност њиховог складиштења.

Програм „ИДЕЈЕ“: Истраживања у областима здравства и друштвених наука, са нагласком на поверљивост података и примени GDPR стандарда у Србији. Овај програм је значајно побољшао разумевање и примену највиших стандардима заштите података.

Сарадња са ЕУ: Истраживачи који учествују у програмима попут **„Хоризонт 2020“** морају да поштују **GDPR стандарде**, што подразумева усаглашавање са правилима заштите података и као услов за добијање истраживачких средстава.

Будући изазови

Развој нових технологија, као што су **вештачка интелигенција** и **машинско учење**, доноси нове изазове у заштити података. Потребно је развијати додатне мере које ће омогућити да научна истраживања остану безбедна и у будућности. У овом контексту, **криптографија** и нове методе заштите као што су **блокчејн** технологије могу помоћи у осигурању интегритета података и спречавању њихове злоупотребе.

Поверљивост података у истраживачким пројектима није само законска обавеза, већ и етичка дужност која осигурава интегритет истраживања и заштиту права учесника. Успостављање јасних процедура, усклађеност са важећим законима и поштовање етичких кодекса кључни су за одржавање поверења у научну заједницу и друштво у целини. Стално усавршавање приступа заштити података, у складу са новим технологијама и правним регулативама, остаје изазов за истраживаче и институције.

25. Архивска грађа у Републици Србији

Архивска грађа у Републици Србији чини значајан део културног наслеђа и регулисана је кроз низ закона и прописа. Њен значај огледа се у очувању историјске, културне и друштвене баштине, али и у осигурању приступа информацијама од јавног интереса.

Кључни закони

Закон о архивској грађи и архивској делатности ("Службени гласник РС", бр. 6/2020): Уређује систем заштите архивске грађе и документарног материјала, њихово чување, сређивање и обраду, као и услове коришћења.

Закон о културном наслеђу ("Службени гласник РС", бр. 129/2021): Регулише заштиту материјалног и нематеријалног културног наслеђа.

Закон о културним добрима („Службени гласник РС”, бр. 71/1994 и измене): Прописује евиденцију и заштиту културних добара.

Отворена и затворена архивска грађа

1. Отворена архивска грађа Отворена архивска грађа подразумева документа и материјале који су доступни за истраживање и коришћење у складу са законом.

Примери:

Материјали старији од 70 година.

Подаци о личности (матичне књиге, пописи становништва) након истека рока од 100 година од рођења лица.

Грађа која се односи на историјске догађаје, културне и научне делатности.

Посебни услови приступа:

Неке врсте грађе дигитализоване су како би се омогућила бржа и једноставнија претрага.

Отвореност може бити ограничена у случају оштећених материјала који захтевају конзервацију.

2. Затворена архивска грађа Затворена архивска грађа обухвата податке и документа са ограниченим приступом због њихове осетљивости или правних ограничења.

Примери:

Подаци који су настали у раду служби безбедности.

Досијеа или документи који садрже поверљиве информације (подлежу ограничењима из Закона о архивској грађи).

Посебни услови приступа:

За ову грађу је потребна сагласност надлежних органа.

Приступ се може одобрити за истраживачке сврхе уз поштовање строгих процедура.

Закон предвиђа заштиту поверљивости у периоду од 70 или више година, у зависности од природе информација.

Државни архив Србије

Улога и надлежност: Државни архив Србије је главна институција задужена за чување и заштиту архивске грађе од значаја за државу, укључујући:

Историјску архивску грађу насталу до краја 1918. године.

Материјале из Другог светског рата и послератног периода.

Личне и породичне фондове, као и јавну архивску грађу.

Јавна доступност: Јавна архивска грађа доступна је за истраживаче и грађане уз поштовање законских ограничења.

Војни архив

Главни задатак: Војни архив има кључну улогу у чувању и заштити војне документације од 1847. године до данас.

Надлежности:

Обрађује и чува грађу српских и југословенских војних институција.

Грађа обухвата документа Краљевске војске Србије, Југословенске народне армије, Војске Србије и других војних формација.

Дигитализација: Стари и оштећени материјали пролазе кроз процес дигитализације, чиме се омогућава приступ дигиталним копијама, док се оригинали чувају под строгим условима.

Архивска мрежа Републике Србије

Организација: Архивску мрежу чине јавни и специјализовани архиви који обављају евиденцију, обраду и заштиту архивске грађе на територији Републике Србије.

Архивска грађа, била она отворена или затворена, представља важан сегмент културног, историјског и националног наслеђа Србије. Њена заштита и правилно управљање од суштинског су значаја за осигурање доступности информација за будуће генерације и очување националне меморије. Континуирани рад на дигитализацији и унапређењу приступа архивској грађи омогућава модернизацију архивског система у Србији.

26. Ознаке штићених података које недостају у Републици Србији

Одређене ознаке за документе и податке, иако коришћене у међународној пракси, нису формализоване у Републици Србији. Оне представљају додатне нивое класификације и управљања осетљивим информацијама. Ево кратког прегледа значајних ознака које би могле допринети бољем управљању информацијама:

1. Unclassified (Некласификовано)

Карактеристике:

Ова ознака се не сматра техничким степеном тајности.

Користи се за означавање докумената који не испуњавају критеријуме за доделу степена тајности или за документе са којих је скинут степен тајности.

За заштиту ових података користе се процедуре „ограничене дистрибуције“.

2. OFFICIAL (Службени)

Карактеристике:

Користи се за означавање докумената који се односе на свакодневне послове јавног сектора.

Ова ознака се примењује у државним органима и јавним службама за управљање редовним активностима.

3. PROTECT (Заштићени)

Карактеристике:

Ознака PROTECT означава информације чије би откривање могло:

Нанети финансијски губитак или омогућити неправедну предност.

Довести у питање истрагу или олакшати извршење кривичног дела.

Угрозити позицију владе у трговинским или политичким преговорима.

Обично укључује дескрипторе као што су:

Commercial (Трговински)

Management (Управљање)

Personal (Лични)

4. For Official Use Only (FOUO) – Само за службену употребу

Карактеристике:

Ова ознака подразумева употребу података искључиво од стране запослених, представника или уговарача владе у оквиру службених активности.

Примењује се на документе и податке који су намењени интерној употреби.

5. Осетљиви подаци (Sensitive Information)

Карактеристике:

Ови подаци се односе на информације чије би откривање могло:

Узроковати губитак безбедности или предности.

Нанети штету приватности лица, пословним субјектима или државним интересима.

Примери укључују поверљиве пословне информације, безбедносне пропусте, или податке у оквиру унутрашњих и спољних послова.

6. Law Enforcement Sensitive (LES) – Осетљиво за полицијске службе

Карактеристике:

Примењује се на информације које могу нанети штету активностима полицијских органа ако буду откривене.

Ова ознака укључује податке попут:

Информација које могу угрозити истраге, компромитовати оперативне активности или довести у опасност животе сведока, агената или поверљивих извора.

Ова ознака се не примењује на информације административне природе или на податке из јавних извора.

У међународној пракси и у различитим државним системима, поред претходно наведених постоје још и друге ознаке за административне и осетљиве податке које нису нужно формализоване у Републици Србији, али би могле допринети прецизнијем управљању информацијама. Ево неколико додатних ознака:

Controlled Unclassified Information (CUI)

Ова ознака се користи у системима попут америчког за означавање некласификованих информација које и даље подлежу ограничењима заштите.

Примери укључују финансијске, правне или податке везане за инфраструктуру.

Restricted (Ограничено)

Често коришћена у међународним организацијама, ова ознака обухвата податке који нису класификовани као тајни, али њихово откривање може довести до штете за одређени сектор или организацију.

Confidential but Not Classified (CBNC)

Користи се за информације које имају повремено ограничен приступ, али не испуњавају критеријуме за формалну класификацију.

Sensitive but Unclassified (SBU)

Слично ознаци "Осетљиви подаци", ова категорија обухвата информације које, уколико би се откриле, могу угрозити безбедност, приватност или пословне интересе, али нису довољно осетљиве да се класификују као поверљиве.

Business Use Only (BUO)

Употребљава се у корпорацијама и владама за податке намењене само интерној пословној употреби.

Need to Know (NTK)

Ова ознака се користи за информације које су доступне само лицима која имају директну потребу за приступом у вези са специфичним задацима.

Internal Use Only (IUO)

Уобичајена ознака у корпоративним и државним структурама за податке намењене само интерној циркулацији.

Eyes Only

Ова ознака подразумева веома ограничен приступ, обично за појединце одређених функција или нивоа унутар организације.

Ове ознаке могу бити драгоцене у побољшању управљања административним и осетљивим подацима, посебно у секторима као што су здравство, правосуђе, јавна управа и индустрија. Иако многе од ових ознака нису званично усвојене у Републици Србији, њихова примена би могла побољшати управљање и заштиту информација.

Примена ознака попут Unclassified, PROTECT, или For Official Use Only омогућила би прецизнију дистрибуцију и унапређење система информационе безбедности. Поред тога, увођење ознака које осетљиве податке јасно раздвајају од тајних података допринело би већој ефикасности институција.

26. Дигитализација штићених података у Републици Србији: детаљна анализа

Дигитализација штићених података у Републици Србији представља комплексну али неопходну иницијативу за побољшање ефикасности, транспарентности и безбедности у раду институција. Овај процес није само техничко унапређење, већ подразумева и системски приступ који обједињује политички, правни и технолошки аспект.

Политички аспект

Политички аспект дигитализације се односи на вољу и иницијативу државног врха да постави дигитализацију као приоритет. За њен успех неопходно је:

Стратегијско планирање: Креирање националне стратегије дигитализације која јасно дефинише визију, циљеве и кораке.

Интензивирање сарадње са међународним партнерима: Посебно у контексту европских интеграција, дигитализација података мора бити усаглашена са стандардима и добрим праксама Европске уније.

Оснаживање јавне свести: Организовање кампања за подизање свести о значају дигитализације и заштите података како међу грађанима тако и међу запосленима у јавном сектору.

Правни аспект

Правни оквир чини темељ сигурне и одрживе дигитализације. Република Србија мора унапредити своје законодавство у следећим областима:

Допуна недостајућих прописа:

Дефинисање различитих категорија штићених података (пословна тајна, здравствени подаци, подаци малолетника, итд.) и њиховог управљања.

Прецизирање улога и одговорности институција у обради и заштити података.

Хармонизација са међународним стандардима:

Усклађивање националних прописа са Општом уредбом о заштити података (GDPR) и другим међународним регулативама.

Механизми надзора и контроле:

Успостављање одговарајући тела и јачање надлежмности постојећих која ће вршити мониторинг безбедности дигитализованих система.

Примена мера заштите:

Енкрипција свих осетљивих података ради спречавања злоупотреба.

Увођење вишефакторске аутентификације и ограничења приступа.

Континуиране провере и ажурирање безбедносних протокола.

Технолошки аспект

Савремене технологије омогућавају дигитализацију, али захтевају значајна улагања и компетенције. Главне области фокуса укључују:

Успостављање информационо-комуникационих система од посебног значаја:

Изградња акредитованих система који задовољавају највише стандарде безбедности.

Централизоване платформе за управљање подацима ради једноставног руковања и праћења.

Развој инфраструктуре:

Јачање серверских капацитета, рачунарских мрежа и база података.

Примена технологија као што су блокчејн за повећање транспарентности и интегритета података.

Континуирана обука запослених:

Инвестирање у развој технолошких вештина особља у јавном и приватном сектору.

Институционални капацитети и побољшање државних структура

Успешна дигитализација штићених података захтева јаке институционалне капацитете, који би обезбедили безбедност, контролу и интегритет података. Уместо оснивања независних тела која могу довести до дуплирања надлежности и неефикасности, фокус би требало ставити на јачање постојећих државних структура и институција Републике Србије. Ове институције већ имају мандат и инфраструктуру која може бити унапређена у складу са савременим технолошким и безбедносним изазовима.

Кључне институције и њихове надлежности

Канцеларија за ИТ и еУправу

Главни актер у развоју и увођењу дигиталних решења у јавном сектору.

Надлежна за креирање јединствених платформи и стандарда за руковање дигитализованим подацима.

Треба да игра водећу улогу у усклађивању активности других институција.

Министарство одбране

Одговорно за заштиту података који се односе на националну безбедност и одбрану.

Потребно је ојачати сајбер капацитете у оквиру војних структура, са посебним фокусом на превенцију сајбер напада.

Канцеларија Савета за националну безбедност и заштиту тајних података

Кључни регулатор који дефинише и спроводи политике заштите тајних података.

Потребно је унапредити капацитете за мониторинг и евалуацију безбедности дигиталних система.

Повереник за слободан приступ информацијама од јавног значаја и заштиту података о личности

Специјализован за надзор над заштитом података о личности.

Потребно је јачати технолошке капацитете и радну снагу како би ефикасно обављао своју функцију у дигиталној ери.

Комерцијална акредитациона тела

Примењују стандарде акредитације за системе и институције које управљају штићеним подацима.

Потребно је обезбедити ближу координацију са државним институцијама ради ефикасније примене стандарда.

Заштитник грађана

Одговоран за заштиту грађанских права, укључујући права везана за безбедност и доступност података.

Могућност активније улоге у спречавању злоупотреба у дигиталном контексту.

Јачање постојећих капацитета

Боља координација међу институцијама

Потребно је креирати јединствени механизам сарадње између горенаведених институција како би се избегле недоследности.

Увођење националног тела за координацију сајбер безбедности које ће усклађивати напоре свих актера.

Технолошко унапређење

Улагање у савремену инфраструктуру и софтверска решења која могу задовољити потребе за дигитализацијом.

Примена напредних технологија, попут блокчејна, ради повећања транспарентности и безбедности.

Континуирана едукација и обука

Запослени у државним структурама морају бити упознати са најновијим технолошким и правним решењима.

Организација редовних тренинга и обука у области сајбер безбедности.

Подизање капацитета за сајбер безбедност

Развијање специјализованих тимова за сајбер безбедност у оквиру постојећих институција.

Увођење раних система за упозоравање на претње и потенцијалне рањивости.

Сајбер безбедност као кровна прича:

Успостављање Националног центра за сајбер безбедност, који би обједињавао активности везане за сајбер претње и рањивости.

Коришћење најсавременијих алата за мониторинг и реаговање, као што су системи за рано упозорење на претње.

Подизање свести институција и грађана о значају сајбер безбедности кроз едукацију и кампање.

Кључни разлози и користи дигитализације

Ефикасније управљање подацима:

Уштеда времена и средстава у приступу и обради података.

Већа сигурност:

Смањење ризика од злоупотребе, неовлашћеног приступа и губитка података.

Транспарентност у раду институција:

Боља доступност информација јавности и већа одговорност институција.

Усклађеност са прописима:

Обезбеђење законитог и етичког руковања подацима.

Заштита животне средине:

Значајно смањење коришћења папира и физичког складиштења.

Јачање капацитета постојећих државних институција у Републици Србији је основа за успешну дигитализацију штићених података. Ове институције, уз координацију и одговарајућу модернизацију, могу ефикасно управљати безбедношћу и интегритетом података, чиме се смањује потреба за стварањем нових структура. Државне институције треба да буду главни актери у овом процесу, уз обезбеђивање транспарентности, одговорности и ефикасности у раду. Успех дигитализације зависи од њихове спремности да одговоре на савремене изазове и потребе.

Дигитализација штићених података представља приоритет за Републику Србију у циљу модернизације и унапређења рада институција. Успешна имплементација зависи од сарадње између свих укључених страна, укључујући државне органе, привреду и грађане. Са снажним правним оквиром, напредном технологијом и политичком подршком, Србија има могућност да створи сигуран и функционалан систем управљања подацима који ће одговорити захтевима савременог доба. Улагање у ову област није само корак ка технолошком напретку, већ и дугорочно улагање у бољу будућност за све грађане.

27. Слободан приступ информацијама од јавног значаја у контексту штићених података: прописи, пракса и проблеми

Правни оквир

Закон о слободном приступу информацијама од јавног значаја у Републици Србији установљен је како би се грађанима, организацијама и медијима омогућио приступ информацијама које поседују органи јавне власти. Међутим, закон истовремено предвиђа ограничења у приступу када су у питању штићени подаци, попут:

Националне безбедности (тајни подаци).

Приватности грађана (подаци о личности).

Пословних и професионалних тајни, као што су адвокатска, банкарска и лекарска тајна.

Поверљивих података у јавним набавкама.

Информација везаних за међународну сарадњу и одбрану.

Повереник за информације од јавног значаја и заштиту података о личности игра кључну улогу у обезбеђивању примене закона, али његова улога није довољна без активног ангажмана органа јавне власти.

Пракса

Одговорност органа јавне власти Иако су органи јавне власти дужни да обезбеде слободан приступ информацијама, често се сусрећу са изазовима у доследној примени закона. Неки од уобичајених проблема су:

Одуговлачење у достављању информација: Институције често пробијају законске рокове за одговор на захтеве.

Недоследна примена критеријума за ускраћивање: Уместо јасног образложења, органи се неретко позивају на "тајност" или "заштиту података," иако за то не постоје законски основи.

Непотпуни одговори: Чести су случајеви да органи јавне власти достављају само делимичне информације.

Рад Повереника Повереник је институција која надгледа примену закона и деловање органа јавне власти. Иако је његова улога важна, у пракси се често суочава са следећим изазовима:

Пропуст у спровођењу решења: Чак и када Повереник донесе решење у корист подносиоца захтева, органи јавне власти понекад не поступе у складу са тим.

Недовољни ресурси и велика оптерећеност: Ограничени капацитети Повереника отежавају ефикасно решавање великог броја притужби.

Усклађеност са штићеним подацима

Конфликт између транспарентности и заштите података: У пракси, органи јавне власти неретко погрешно класификују податке као "тајне" ради избегавања одговорности.

Недостатак стандардизованих критеријума: Многи органи немају јасно дефинисане процедуре за идентификацију података који заиста морају бити заштићени.

Један од значајних проблема у примени Закона о слободном приступу информацијама од јавног значаја у Републици Србији је злоупотреба овог механизма од стране одређених адвокатских канцеларија. Ова злоупотреба се манифестује кроз масовно подношење захтева за приступ информацијама, што затрпава органе јавне власти и утиче на ефикасност процеса, а често се чини у циљу стицања зараде, уместо остварења јавног интереса.

Како се манифестује проблем?

Велики број захтева:

Поједини адвокати подносе десетине или стотине захтева за приступ информацијама, чиме оптерећују ресурсе органа јавне власти.

Комерцијализација поступка:

Захтеви често циљају на ситуације где ће се по основу непоштовања рокова или одлука Повереника остварити основ за покретање судских поступака ради наплате трошкова.

Неповезаност са јавним интересом:

Уместо да захтеви служе за унапређење транспарентности и информисаности јавности, они се неретко подносе у сврхе које немају везе са јавним интересом.

Последице за органе јавне власти

Оптерећење ресурса:

Ограничени кадровски капацитети и технички ресурси отежавају обраду великог броја захтева, што утиче на ефикасност и квалитет рада органа јавне власти.

Одлагање поступања по оправданим захтевима:

Масовно подношење захтева од стране неких адвокатских канцеларија отежава поступање по захтевима који имају стварни јавни значај.

Губитак поверења у систем:

Грађани који користе право на приступ информацијама у доброј намери могу изгубити поверење у институције ако осете да се процедура злоупотребљава.

Могућа решења

Законске измене:

Увести механизме који ће спречити злоупотребе, као што је ограничење броја захтева који могу бити поднети у одређеном временском периоду од стране једног субјекта.

Дефинисање комерцијалних злоупотреба:

Прецизирати у закону ситуације у којима се право на приступ информацијама злоупотребљава ради остваривања финансијске добити, и омогућити санкционисање таквих поступака.

Јачање капацитета органа јавне власти:

Повећати број запослених у институцијама који су задужени за обраду захтева и унапредити техничку подршку за обраду података.

Проактивна транспарентност:

Органи јавне власти би могли проактивно објављивати информације које се најчешће траже, чиме би се смањио број формалних захтева.

Боља сарадња са Повереником:

Унапредити размену информација између органа јавне власти и Повереника како би се брже и ефикасније поступало по случајевима који указују на злоупотребу.

Проблеми и изазови

Недовољно прецизни законски критеријуми за штићене податке:

Неретко се јављају ситуације у којима су границе између штићених и јавних података недовољно дефинисане.

Злоупотреба ограничења приступа:

Органи јавне власти понекад користе "тајност података" као изговор за недостављање информација које би могле указати на потенцијалне злоупотребе или неправилности.

Недостатак усклађивања са међународним стандардима:

Иако је правни оквир делимично усклађен са европским прописима, постоји простор за унапређење, посебно у домену заштите података и транспарентности.

Ниска свест грађана и службеника:

Грађани ретко користе своје право на приступ информацијама, док службеници у органима јавне власти нису довољно упознати са процедуром и законом.

Препоруке

Побољшање законског оквира:

Ревидирати закон о слободном приступу информацијама како би се јасније дефинисала ограничења у складу са европским стандардима.

Обавезна едукација запослених:

Организовати обуке за службенике у јавним институцијама како би разумели како да правилно поступају по захтевима за информације.

Јасни критеријуми за штићене податке:

Увести стандардизоване процедуре за класификацију и де-класификацију података, како би се спречиле злоупотребе.

Јачање капацитета Повереника:

Повећати ресурсе и број запослених у канцеларији Повереника како би се ефикасније поступало по притужбама и решењима.

Проактивна транспарентност органа јавне власти:

Обавезати органе јавне власти да редовно објављују податке од јавног интереса, чиме би се смањила потреба за формалним захтевима.

Злоупотреба права на приступ информацијама од јавног значаја од стране одређених адвокатских канцеларија представља значајан проблем који оптерећује органе јавне власти и нарушава основну сврху закона – транспарентност и одговорност у раду институција. Ревидирање правног оквира, јачање институционалних капацитета и унапређење транспарентности кроз проактивно објављивање информација могу допринети ефикаснијем коришћењу овог механизма, у интересу свих грађана Републике Србије.

Слободан приступ информацијама од јавног значаја и заштита штићених података у Републици Србији захтевају добро уравнотежену примену прописа. Проблеми у пракси указују на неопходност едукације, боље координације и јаснијих критеријума за утврђивање ограничења. Са ревидираним законом, јачим капацитетима институција и транспарентним праксама, могуће је значајно побољшати приступ информацијама, чиме ће се грађанима омогућити боља контрола над радом институција уз истовремену заштиту штићених података.

О АУТОРУ

Проф. др Горан Матић

Директор Канцеларије Савета за националну безбедност и заштиту тајних података Републике Србије, ванредни професор за област безбедност Универзитета УНИОН – „НИКОЛА ТЕСЛА'' и стални судски вештак за безбедност информација.

Учествовао је у процесу израде предлога више закона, Стратегије за супротстављање и борбу против тероризма, Стратегије националне безбедности и Стратегије одбране и у раду Радних група Владе Републике Србије за имплементацију акционих планова за поглавља 10, 24 и 31 за приступање Републике Србије ЕУ.

Од 2015. до 2019. године руководио је Сталном мешовитом радном групом за борбу против тероризма (СМРГ) – формиране одлуком Бироа за координацију рада служби безбедности, од 2019/2021. године обављао и дужност заменика националног координатора Националног координационог тела (НКТ) за спречавање и борбу против тероризма Републике Србије.

У оквиру међународне сарадње Републике Србије на плану заштите тајности података учествовао је као шеф делегације у преговорима за потписивање 14 међународних споразума и био потписник више споразума које је Р. Србија потписала са међународним телима и страним државама у области заштите тајних података. Такође, са Мисијом ОЕБС-а у Београду учествовао је у више пројеката око заштите тајних података, сајбер безбедности и обраде и заштите личних података у сектору безбедности и одбране.

Од 2012. године учествује у раду Форума директора националних безбедносних органа за заштиту тајних података земаља Југоисточне Европе (СЕЕНСА), као и у оквиру Иницијативе „6С'' која окупља директоре националних безбедносних органа земаља региона.

Аутор је више објављених научних и стручних радова и учесник више научних конференција, као и научне монографије „Политички деликти – атентат и побуна'' и коаутор књиге „Тактика и методика деловања обавештајно-безбедносних служби'' у издању Медија центра Одбрана у Београду, и „Основи безбедности'' у издању Факултета за пословне студије и право у Београд

Предавач је на основним академским студијама Војне академије Универзитета одбране и на Факултету за пословне студије и право Универзитета Никола Тесла Унион у Београду.

Гостујући је предавач на Факултету безбедности и Факултету организационих наука Универзитета у Београду, као и на Криминалистичко-полицијском универзитету, Академији за националну безбедност и на Високим студијама безбедности и одбране при Универзитету одбране у Београду. Поред тога предавач је на кратким струковним студијама на Факултету безбедности: "Заштита тајних података и пословне тајне" и "Заштита личних података" од 2022. године. Био је гостујући предавач на мастер

студијама Универзитета у Београду – Тероризам, организовани криминал и безбедност до 2024. године

Акредитовани је предавач Националне академије за јавну управу. Учествује је у раду посебних стручних тела те институције, и то као члан Сталне програмске комисије за електронску управу и дигитализацију (2022-2023) и Сталне програмске комисије за јавну управу (2023-2024).

Члан је Испитне комисије за државни испит (високо образовање) државних службеника и за комуналне милиционере у оквиру министарства државне управе и локалне самоуправе.

Председник је Савета „САМКБ – Српске асоцијације менаџера корпоративне безбедности'' у Београду; члан удружења „ИТ вештак'' у Београду и „Удружења за међународно кривично право'' у Београду. У Привредној комори Србије и Привредној комори Београда више година изводи едукације на тему корпоративне безбедности и обраде и заштите података.