ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

У складу са чланом 87. став 1. тачка 9. Закона о тајности података („Службени гласник РС“), Канцеларија Савета за националну безбедност и заштиту тајних података надлежна је за припрему, координацију и праћење спровођења Плана за поступање у ванредним и хитним ситуацијама у систему заштите тајних података. Ова надлежност остварује се успостављањем јединственог методолошког и нормативног оквира, заснованог на принципу поделе надлежности и пропорционалне примене мера, који обезбеђује континуитет заштите тајних података – како у физичком, тако и у дигиталном облику – у условима ванредног стања, кризе, природних катастрофа, техничко-технолошких инцидената, сајбер-претњи или других околности које могу угрозити безбедност тајних података.

Циљ овог система није само формално доношење документа, већ изградња динамичног и функционалног механизма који, у складу са Законом о тајности података и Законом о информационој безбедности, обезбеђује да заштита тајних података остане ефикасна, правно утемељена и оперативно изводљива и у условима ванредних и хитних ситуација, чиме се доприноси очувању националне безбедности, институционалне стабилности и поверења грађана у систем безбедности Републике Србије.

Шта представља План?

План за поступање у ванредним и хитним ситуацијама представља системски и динамички механизам заснован на принципу поделе надлежности и пропорционалне примене мера, чија је сврха обезбеђивање континуитета заштите тајних података и функционалне стабилности система и у условима повећаног ризика. План обухвата:

• Дефинисање принципа и стандарда поступања у условима повећаног ризика, усклађених са Законом о тајности података, Законом о информационој безбедности и секторским прописима (заштита и спасавање, противпожарна заштита, одбрана);
• Утврђивање мера заштите, измештања, евакуације, алтернативног чувања или уништавања тајних података – како у физичком, тако и у дигиталном облику – у случају непосредне опасности, уз примену техничких стандарда који обезбеђују њихову неповратну неупотребљивост у случају уништавања;
• Јасно одређивање одговорности, хијерархије одлучивања и правила сукцесије, укључујући ланац командовања и овлашћења за активацију Плана у случају недоступности руководиоца или других кључних лица;
• Механизме координације између органа државне управе, других обвезника Закона, имаоца дозволе, субјеката приватног обезбеђења (уколико су ангажовани) и надлежних националних тела (ЦЕРТ, јединице за ванредне ситуације), у складу са утврђеним нивоом угрожености;

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

• Поступке извештавања, документовања и надзора над применом прописаних мера, укључујући обавезу састављања записника, вођења релевантних евиденција и накнадног извештавања Канцеларије Савета и Министарства правде;
• Мере обезбеђења континуитета информационо-комуникационих система, укључујући заштићене резервне копије, примену криптозаштите приликом преноса података, протоколе за поступање у случају сајбер-инцидената и прелазак на алтернативне режиме рада;
• Обавезу периодичног тестирања, спровођења вежби и редовног ажурирања Плана (најмање једном годишње), као и посткризне ревизије засноване на анализи искустава и извучених поука (Lessons Learned).
План није статичан документ, већ оперативни и развојни оквир који се континуирано унапређује на основу резултата вежби, реалних инцидената, процене ризика и измена важећих прописа, како би остао функционалан, правно усклађен и оперативно применљив у свим нивоима угрожености.

Нивои ванредних ситуација

Ради пропорционалне примене мера, у складу са прописима о заштити и спасавању, противпожарној заштити, приватном обезбеђењу и одбрани, План разликује следеће нивое:

Ниво 1 – Локални инцидент: Инцидент ограниченог обима који се може контролисати ресурсима једног органа или једног објекта (нпр. пожар, поплава, технички квар, краткотрајни прекид напајања). Примењују се мере предвиђене интерним плановима заштите и плановима заштите тајних података тог органа, уз координацију са надлежним јединицама за ванредне ситуације и противпожарну заштиту, у складу са Законом о заштити и спасавању у ванредним ситуацијама и Законом о заштити од пожара. Одговорност за поступање носи руководилац органа, односно овлашћено лице за заштиту тајних података, у оквиру утврђених интерних надлежности.

Ниво 2 – Регионална или системска криза: Догађај ширег обима који угрожава функционисање више органа, критичне инфраструктуре или ширег подручја (нпр. елементарна непогода већег обима, масовни сајбер-напад, дуготрајни прекид комуникација или енергетског снабдевања). Примењују се мере координисаног одговора на нивоу више органа, уз укључивање надлежних државних органа, субјеката приватног обезбеђења (уколико су ангажовани), као и надлежних ЦЕРТ структура, у складу са Законом о заштити и спасавању, Законом о приватном обезбеђењу и Законом о информационој безбедности. У овом нивоу посебно се обезбеђује међуинституционална координација, размена релевантних информација и усклађено спровођење мера заштите тајних података.

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

Ниво 3 – Ратно стање или непосредна претња по безбедност и опстанак државе: Ситуације које подразумевају оружану агресију, окупацију, масовну саботажу или друге облике егзистенцијалне претње по државу и њене институције.
Примењују се мере предвиђене плановима одбране и мобилизације, уз приоритет заштите живота, очувања кључних функција државе и спречавања компромитације тајних података, у складу са Законом о одбрани, Законом о тајности података и другим прописима из области националне безбедности. Поступање се спроводи у складу са хијерархијом командовања и одлучивања утврђеном у систему одбране и безбедности. Мере заштите и поступања ескалирају сразмерно степену угрожености, уз обавезу координације са надлежним органима и стриктно поштовање хијерархије одлучивања утврђене овим Планом, како би се обезбедио континуитет заштите тајних података и функционална стабилност система у свим нивоима кризе.

Дигитални аспект – континуитет ИТ система

У складу са Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима, континуитет ИТ система заснива се на примени техничких и организационих мера заштите, усклађених са проценом ризика безбедности система. То подразумева:

• спровођење периодичне процене ризика и управљања безбедношћу система;
• одређивање овлашћеног лица за управљање безбедношћу и дефинисање безбедносних режима рада;
• успостављање заштићених резервних архива (backup) и вођење безбедносних записа (логова);
• обавезну примену криптозаштите приликом преноса података изван безбедносних зона;
• забрану коришћења приватних информационих средстава за обраду тајних података;
• протокол поступања у случају сајбер-инцидената, неовлашћеног упада, нестанка електричне енергије или отказа инфраструктуре;
• прелазак на алтернативне режиме рада у условима делимичне компромитације система.

У складу са Законом о информационој безбедности („Сл. гласник РС“, бр. 91/2025), субјекти који управљају ИКТ системима за обраду тајних података дужни су да спроводе мере управљања ризиком, обезбеде механизме за благовремено пријављивање инцидената и сарађују са надлежним националним телима. Ове обавезе примењују се супсидијарно, без нарушавања специфичних мера заштите прописаних Законом о тајности података. Систем мора обезбедити поверљивост, интегритет и доступност података чак и у условима ванредних околности.

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

Разграничење надлежности

Систем заштите тајних података у ванредним и хитним ситуацијама функционише на принципу јасно дефинисане поделе надлежности између стратешког, оперативно-координационог, надзорног и оперативно-извршног нивоа. Оваква структура омогућава раздвајање функција доношења нормативног оквира, координације у условима кризе, инспекцијског надзора и непосредне примене мера, чиме се спречава преклапање овлашћења и обезбеђује пуни капацитет одговорности сваког нивоа. Разграничење надлежности усклађено је са одредбама Закона о тајности података и има за циљ обезбеђивање јединства концепта, правне сигурности у поступању и функционалне кохерентности свих учесника у систему заштите.

Улога Владе Републике Србије:

• усваја општи нормативни и методолошки оквир;
• утврђује минималне стандарде и обавезне елементе планова;
• обезбеђује јединство и усклађеност система.

Влада не усваја појединачне оперативне планове органа, већ успоставља обавезујући оквир.

Улога Канцеларије Савета за националну безбедност и заштиту тајних података:
• припрема предлог методолошког и нормативног оквира;
• даје стручне смернице органима јавне власти и имаоцима сертификата или дозволе;
• координира активности у условима кризе;
• прати усклађеност појединачних планова;
• извештава надлежне органе о степену спремности система.

Улога органа јавне власти и правних лица у примени Закона о тајности података

Сваки орган јавне власти и правно лице које поседује одговарајући сертификат или дозволу:

• доноси сопствени оперативни план;
• прилагођава га својој организационој структури и врсти података;
• утврђује прецизан ланац руковођења/командовања и правило сукцесије (одређује лице које активира План у случају спречености руководиоца);
• спроводи и редовно ажурира мере;
• спроводи редовне симулације и вежбе примене Плана (најмање једном годишње) и о томе извештава Канцеларију Савета;
• обезбеђује заштиту лица која рукују тајним подацима, уз приоритет заштите живота и спречавања компромитације овлашћених лица;
• обезбеђује непосредну примену Плана у случају настанка ванредне или хитне ситуације.

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

Улога Министарства правде (надзорни орган)

Министарство правде, у складу са чланом 97. Закона о тајности података, врши инспекцијски надзор над спровођењем Закона и Плана:

• прати стање у области заштите тајних података и идентификује системске пропусте;
• налаже мере за унапређивање заштите уколико утврди недостатке у плановима или у њиховој примени;
• контролише примену критеријума за одређивање степена тајности, као и спровођење мера обезбеђења, коришћења и размене података;
• врши надзор без претходног обавештавања (инспекцију на лицу места), путем овлашћених лица која поседују одговарајућу безбедносну проверу;
• подноси кривичне пријаве и захтеве за покретање прекршајног поступка због повреде одредаба Закона, укључујући и повреде настале услед неадекватног поступања у ванредним ситуацијама;
• подноси годишњи извештај одбору Народне скупштине надлежном за надзор и контролу у области одбране и безбедности.

Упутство/Протокол уништавања тајних података

Уништавање тајних података представља крајњу меру заштите и спроводи се искључиво:

• по наредби овлашћеног лица, у складу са утврђеним нивоом угрожености;
• уз примену техничких средстава и метода који обезбеђују неповратну неупотребљивост података (нпр. уситњавање до димензија ≤ 2 mm $\times$ 15 mm за папирне носиоце, degaussing (магнетна демагнетизација магнетних носилаца података) или физичко уништавање електронских медија);
• уз састављање записника о уништавању, ако околности то дозвољавају, који садржи податке о врсти, обиму, степену тајности, времену, месту и начину уништавања;
• уз присуство најмање три овлашћена лица, од којих најмање једно поседује безбедносну проверу за одговарајући степен тајности.

У ситуацијама непосредне опасности по живот или ризика од заплене података, овлашћено лице може наредити хитно уништавање и без претходног састављања записника, уз обавезу накнадног подношења детаљног извештаја Канцеларији Савета у року од 24 часа од стабилизације ситуације. Овим упутством/протоколом спречава се злоупотреба ванредних околности ради незаконитог уништавања тајних података, уз истовремено обезбеђивање ефикасне заштите у екстремним условима.

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ВАНРЕДНИМ И ХИТНИМ СИТУАЦИЈАМА

Суштина система

План није формални акт, већ динамичан механизам обезбеђивања континуитета заштите тајних података, инструмент превенције компромитације у условима кризе и сегмент ширег система континуитета државних функција.

Он представља нормативно-оперативни оквир заснован на принципу поделе надлежности (стратешки, оперативно-координациони, надзорни и извршни ниво) и пропорционалне примене мера, сразмерно степену угрожености. План интегрише мере физичке и дигиталне заштите, уз обавезу периодичног тестирања, ажурирања и усклађивања са важећим прописима, укључујући Закон о тајности података и Закон о информационој безбедности.

Оваквим приступом обезбеђује се да заштита тајних података остане функционална, правно утемељена и оперативно изводљива и у условима ванредног или ратног стања, чиме се чувају интегритет, поверљивост и доступност информација од значаја за националну безбедност и институционалну стабилност Републике Србије.