

ЗАКОН

О ПОТВРЂИВАЊУ СПОРАЗУМА ИЗМЕЂУ ВЛАДЕ РЕПУБЛИКЕ СРБИЈЕ И ВЛАДЕ СЈЕДИЊЕНИХ АМЕРИЧКИХ ДРЖАВА У ВЕЗИ СА БЕЗБЕДНОСНИМ МЕРАМА ЗА ЗАШТИТУ ТАЈНИХ ВОЈНИХ ПОДАТАКА

Члан 1.

Потврђује се Споразум између Владе Републике Србије и Владе Сједињених Америчких Држава у вези са безбедносним мерама за заштиту тајних војних података, који је потписан у Вашингтону, 27. јануара 2014. године, у оригиналу, на српском и енглеском језику.

Члан 2.

Текст Споразума у оригиналу на српском језику гласи:

СПОРАЗУМ
ИЗМЕЂУ ВЛАДЕ РЕПУБЛИКЕ СРБИЈЕ И ВЛАДЕ СЈЕДИЊЕНИХ
АМЕРИЧКИХ ДРЖАВА У ВЕЗИ СА БЕЗБЕДНОСНИМ МЕРАМА
ЗА ЗАШТИТУ ТАЈНИХ ВОЈНИХ ПОДАТАКА

ПРЕАМБУЛА

Влада Републике Србије и Влада Сједињених Америчких Држава (у даљем тексту: „Стране”, а појединачно: „Страна”);

У циљу унапређења узајамне сарадње ради осигурања заштите тајних војних података;

Споразумеле су се о следећем:

ЧЛАН 1.

Тајни војни подаци које директно или индиректно пружи једна Страна другој Страни, заштићени су у складу са условима дефинисаним у овом споразуму, као и у складу са законима и прописима државе Стране примаоца.

ЧЛАН 2.

Свака Страна одмах обавештава другу Страну о свим изменама својих закона и прописа који би утицали на заштиту тајних војних података, у складу са овим споразумом. У том случају, Стране се консултују, сагласно члану 23. Споразума, како би размотриле могуће измене Споразума. Тајни војни подаци биће и даље заштићени сагласно овом споразуму, осим уколико се Страна давалац, писаним путем, не сагласи другачије.

ЧЛАН 3.

Тајни војни податак, у смислу овог споразума, је податак који је настао у или за потребе Министарства одбране Републике Србије или Министарства одбране Сједињених Америчких Држава, или који је под њиховом јурисдикцијом или контролом и који захтева заштиту у интересу националне безбедности Стране у којој или за коју је податак настао. Податак из члана 1. овог споразума може да буде у усменом, визуелном, електронском, магнетном или документарном облику. Такође, опрема и/или технологија могу да садрже тајне војне податке дефинисане у овом члану.

Стране, у складу са својим националним законима и прописима, користе следеће еквивалентне степене тајности:

РЕПУБЛИКА СРБИЈА	СЈЕДИЊЕНЕ АМЕРИЧКЕ ДРЖАВЕ
ДРЖАВНА ТАЈНА	TOP SECRET
СТРОГО ПОВЕРЉИВО	SECRET
ПОВЕРЉИВО	CONFIDENTIAL
ИНТЕРНО (RESTRICTED)	нема еквивалента

Уколико српска страна током спровођења овог споразума, достави тајне војне податке са ознаком „ИНТЕРНО-RESTRICTED”, америчка страна ће као Страна прималац, поступати са њима у складу са Додатком овог споразума.

ЧЛАН 4.

Надлежни органи Страна задужени за имплементацију овог споразума, могу закључити протоколе, техничке аранжмане и друге уговоре. За Владу Републике Србије, надлежни орган за имплементацију је Министарство одбране. За Владу Сједињених Америчких Држава, надлежни орган за имплементацију је Министарство одбране.

ЧЛАН 5.

Нико нема право приступа тајним војним подацима само на основу чина, функције или безбедносне дозволе. Приступ таквим подацима одобрава се само оним појединцима чије званичне дужности захтевају такав приступ и којима је издата безбедносна дозвола у складу са прописаним стандардима Стране примаоца.

Стране ће се постарати да:

а) Страна прималац не уступа податке влади, лицу, предузећу, институцији, организацији или другом телу треће земље, без претходне писане сагласности Стране даваоца;

б) Страна прималац додељује податку степен заштите еквивалентан оном који је доделила Страна давалац;

в) Страна прималац неће, без претходне писане сагласности Стране даваоца, да користи податке у било коју другу сврху осим оне за коју је податак пружен;

г) Страна прималац поштује лична права као што су патентна, ауторска права, или пословне тајне, које податак садржи и

д) У сваком објекту или установи у којој се рукује тајним војним подацима, води се регистар дозвола појединаца у објекту или установи који имају овлашћење за приступ таквим подацима.

ЧЛАН 6.

Одлучивање о издавању безбедносних дозвола појединцима у складу је са интересима националне безбедности и засновано је на свим доступним подацима у којима се наводи да ли лице поседује неспорну лојалност, интегритет, поузданост и добре особине и да има такве навике и сараднике да се не доводи у сумњу његова/њена дискреција или расуђивање приликом руковања тајним војним подацима.

ЧЛАН 7.

Свака од Страна спроводи одговарајућу, довољно детаљну проверу како би пружила гаранцију да су испуњени критеријуми наведени у овом споразуму и то за сва лица која имају њено држављанство и којима ће бити одобрен приступ тајним војним подацима обухваћеним овим споразумом.

ЧЛАН 8.

Пре него што представник Стране пружи тајне војне податке службенику или представнику друге Стране, Страна прималац пружа гаранцију Страни даваоцу да тај службеник или представник поседује безбедносну дозволу неопходног нивоа и да му је приступ потребан у службене сврхе, као и да ће Страна прималац заштитити тај податак како је предвиђено овим споразумом.

ЧЛАН 9.

Одобрења за посете представника једне Стране објектима и установама друге Стране где је потребан приступ тајним војним подацима, ограничен је на оне које су неопходне за службене потребе. Одобрење за посету објекту или установи издаје само Страна на чијој територији се налази објект или установа, односно државни званичници које одреди та Страна. Страна која прима посету или именовани представник, одговоран је за обавештавање представника објекта или установе о предложеној посети, као и о обиму и највишем степену тајних војних података који се могу дати посетиоцу. Захтеви за посете представника Страна достављају се преко Канцеларије изасланика одбране Републике Србије у Вашингтону, ако се ради о посетиоцима из Републике Србије и преко Канцеларије изасланика одбране Сједињених Америчких Држава у Београду, ако се ради о посетиоцима из Сједињених Америчких Држава.

ЧЛАН 10.

Свака Страна одговорна је за чување свих тајних војних података које прими од друге Стране док су подаци у транзиту или на чувању на територији државе те Стране.

ЧЛАН 11.

Свака Страна одговорна је за безбедност свих државних и приватних објеката и установа где се чувају тајни војни подаци друге Стране и дужна је да се стара да се за сваки такав објект или установу именују квалификовани појединци који су одговорни и овлашћени за контролу и заштиту тајних војних података.

ЧЛАН 12.

Подаци се чувају на начин који дозвољава приступ само оним лицима која имају овлашћење приступа у складу са чл. 5. до 8. овог споразума.

ЧЛАН 13.

Тајни војни подаци преносе се између Страна дипломатским путем (између две владе). Минимални захтеви за безбедност података за време преноса су следећи:

А. Документи

(1) Документи или други медији који садрже тајне војне податке преносе се у дуплим, запечаћеним ковертама, при чему унутрашњи коверат има само ознаку степена тајности докумената или других медија и адресу организације примаоца коме су намењени, док спољни коверат садржи адресу организације примаоца, адресу организације пошиљаоца и, по потреби, број регистра.

(2) На спољном коверту неће бити ознаке степена тајности приложених докумената или других медија. Запечаћени коверат се потом преноси у складу са прописаним правилима и процедурама Стране даваоца.

(3) За пакете који садрже документе или друге медије са степеном тајности који се преносе између Страна, припрема се потврда пријема. Потврду пријема приложених докумената или медија потписује крајњи прималац и враћа је пошиљаоцу.

Б. Опрема са ознаком тајности

(1) Опрема која садржи тајне војне податке транспортује се у запечаћеним, покривеним возилима или се безбедно пакује или штити како би се спречило препознавање њеног садржаја. Таква опрема се чува под сталним надзором како би се спречио приступ неовлашћених лица.

(2) Опрема која садржи тајне војне податке која се мора привремено чувати у складишту док чека на испоруку, смешта се у заштићени складишни простор. Тај простор је заштићен против-провалном опремом или од стране чувара са безбедносним дозволама који континуирано врше надзор складишног простора. Само овлашћено особље са обавезним безбедносним дозволама, има приступ складишном простору.

(3) Потврде пријема се обезбеђују сваки пут када у току транспорта опрема која садржи тајне војне податке пређе у посед другог лица.

(4) Потврду пријема потписује крајњи прималац и враћа је поштом.

В. Електронски пренос

Тајни војни подаци који се пренесу електронским средствима, заштићени су током преноса помоћу шифри адекватних за тај степен тајних војних података. Информациони системи којима се обрађују, чувају или преносе тајни војни подаци, морају се безбедносно акредитовати од стране одговарајућег органа Стране која користи тај систем.

ЧЛАН 14.

Одговорност и контролне процедуре успостављају се ради управљања, односно контроле ширења и приступа тајним војним подацима.

ЧЛАН 15.

Свака Страна ставља печат или означава назив Стране даваоца на свим документима и другим материјалима који садрже тајне војне податке које прими од друге Стране. Такав податак се означава националном ознаком степена тајности Стране примаоца која ће доделити степен заштите еквивалентан оном који је доделила Страна давалац.

ЧЛАН 16.

Документи и други медији који садрже тајне војне податке уништавају се спаљивањем, сечењем, претварањем у папирну кашу или другим средствима којима се спречава реконструкција тајних војних података које ти документи или медији садрже.

ЧЛАН 17.

Опрема која садржи тајне војне податке сматра се уништеном када није више препознатљива или је измењена тако да онемогући реконструкцију тајних војних података, у целини или делимично.

ЧЛАН 18.

Ако се документи или други медији који садрже тајне војне податке репродукују, све оригиналне ознаке тајности података на њима, такође се репродукују или означавају на свакој копији. Такви репродуковани документи или медији стављају се под исту контролу као и оригинални документи или медији. Број копија ограничава се на број који је потребан за службену употребу.

ЧЛАН 19.

Све преводе докумената који садрже тајне војне податке врше појединци који поседују безбедносне дозволе у складу са чл. 6. до 8. овог споразума. Број примерака треба свести на минимум, а њихова дистрибуција се контролише. Такви преводи носе одговарајуће ознаке степена тајности и одговарајућу напомену на језику превода, при чему се назначава да документ или медиј садржи тајне војне податке Стране даваоца.

ЧЛАН 20.

Пре него што Страна давалац уступи уговарачу или потенцијалном уговарачу било какве тајне војне податке, Страна прималац дужна је:

а) да се постара да такав уговарач или потенцијални уговарач и објект тог уговарача, имају капацитете за заштиту података;

б) да додели објекту одговарајућу безбедносну дозволу за објекте;

в) да за све појединце чије дужности захтевају приступ овим подацима, изда одговарајуће личне безбедносне дозволе;

г) да се постара да сва лица која имају приступ овим подацима буду упозната о својој одговорности да штите податке у складу са важећим законима и прописима;

д) да врши периодичне безбедносне инспекције одобрених објеката како би се осигурало да су подаци заштићени како је предвиђено у овом споразуму и

ђ) да се постара да приступ подацима буде ограничен на она лица која због службених потреба имају потребу да са њима буду упозната.

ЧЛАН 21.

Страна давалац се одмах обавештава о сваком губитку или безбедносном угрожавању, као и о могућем губитку или безбедносном угрожавању њених тајних војних података. У том случају, Страна прималац започиње истрагу ради утврђивања релевантних околности. Страна која спроводи истрагу доставља Страни даваоцу резултате истраге, као и податке у вези са предузетим мерама ради спречавања понављања таквог догађаја.

ЧЛАН 22.

Реализација безбедносних захтева може се унапредити узајамним посетама особља Страна које се бави пословима заштите и безбедности. У складу с тим, представницима сваке Стране који се баве пословима заштите и безбедности, после претходних консултација, биће дозвољено да посете другу Страну како би разговарали и непосредно стекли увид у процедуре које друга Страна примењује у интересу постизања прихватљиве упоредивости безбедносних система. Свака Страна пружа помоћ представницима друге Стране који се баве пословима заштите и безбедности, приликом утврђивања да ли се тајни војни подаци које је пружила друга Страна, адекватно штите.

ЧЛАН 23.

Скидање ознаке тајности и објављивања у јавности тајних војних података које је сачинила нека од Страна, разматраће се двадесет пет година након њиховог сачињавања, осим за категорије података обухваћене другим споразумима између Страна или њихових надлежних органа. Уколико приликом разматрања објављивања тих података Страна прималац утврди да подаци Стране даваоца још увек могу да имају ознаку тајности, Страна прималац ће

продужити трајање ознаке тајности преко двадесет пет година, или ће упутити тај документ Страни даваоцу на мишљење о скидању ознаке тајности и објављивању тих података.

ЧЛАН 24.

У случају захтева за подацима упућеним у складу са одредбама које се односе на право приступа за јавност садржаним у законодавству Републике Србије или Сједињених Америчких Држава, тајни војни подаци, упућују се Страни даваоцу ради истовременог објављивања тих података.

ЧЛАН 25.

Овај споразум ступа на снагу даном пријема другог обавештења којим Стране потврђују да су спровеле интерне правне поступке неопходне за ступање Споразума на снагу. Стране су сагласне да се након ступања на снагу овог споразума, успоставе пуноправне обавезе сагласно међународном праву.

Измене и допуне овог споразума врше се уз узајамну сагласност Страна, у писаном облику и ступају на снагу у складу са поступцима предвиђеним у ставу 1. овог члана.

Овај споразум остаје на снази пет година, након чега се сваке године аутоматски продужава, осим уколико једна од Страна писаним путем не обавести другу Страну дипломатским путем, деведесет дана унапред, о својој намери да откаже овај споразум.

Без обзира на отказивања овог споразума, сви тајни војни подаци који се уступају на основу овог споразума, остају и даље заштићени у складу са одредбама које су утврђене у овом споразуму.

Неслагања између Страна која настану на основу или у вези са овим споразумом, решавају се путем консултација између Страна и неће се предавати националном суду, међународном суду или било ком другом лицу или институцији на решавање.

ПОТВРЂУЈУЋИ ОВО, доле потписани, прописно овлашћени од стране својих влада, потписали су овај споразум.

САЧИЊЕНО у Washington DC, дана 27 January 2014 године, у по два оригинална примерка, сваки на српском и енглеском језику, при чему су оба текста подједнако веродостојна.

ЗА ВЛАДУ
РЕПУБЛИКЕ СРБИЈЕ

ЗА ВЛАДУ
СЈЕДИЊЕНИХ АМЕРИЧКИХ ДРЖАВА

Небојша Родић, с.р.

Чарлс Хејгел, с.р.

ДОДАТАК

ПРОЦЕДУРЕ ЗА ПОСТУПАЊЕ СА ПОДАЦИМА СА ОЗНАКОМ „ИНТЕРНО” У СЈЕДИЊЕНИМ АМЕРИЧКИМ ДРЖАВАМА

1. По пријему докумената или материјала из Републике Србије који носе ознаку тајности „ИНТЕРНО”, у Сједињеним Америчким Државама поступа се као да се ради о подацима „БЕЗ ОЗНАКЕ ТАЈНОСТИ” (UNCLASSIFIED), који се изузимају од објављивања у јавности према једном или више закона Сједињених Америчких Држава. Ови закони укључују Закон о слободи информисања (FOIA) и Наслов 10. Законика Сједињених Америчких Држава, одељак 130 (ц) „Неодавање података: Одређени осетљиви подаци страних држава и међународних организација.” Тако означени документи и материјали складиште се у закључаним сандуцима/контејнерима који пружају одговарајућу заштиту или у затвореним просторима или зонама које ће спречити приступ неовлашћеним лицима.

2. Са документима који имају ознаку „ИНТЕРНО” поступа се на начин којим ће се онемогућити отворено објављивање, као и приступ или коришћење за друге сврхе осим за званичне државне потребе Сједињених Америчких Држава или Републике Србије. Подаци који су садржани у овим документима изузимају се од објављивања у јавности према важећим законима Сједињених Америчких Држава о слободи информисања, осим ако Влада Србије не изда претходно писано одобрење.

3. Подаци са ознаком „ИНТЕРНО” преносе се или им се приступа електронским путем употребом акредитованих система. Пре него што се дозволи да се неки комуникационо-информациони систем користи за складиштење, обраду или прослеђивање података са ознаком „ИНТЕРНО”, мора му се дати безбедносно одобрење, познато под називом „акредитација”. Акредитација се дефинише као званична изјава од стране одговарајућег органа за акредитовање којом се потврђује да употреба неког система испуњава одговарајући безбедносни захтев и да не представља неприхватљив ризик. За независне аутоматизоване информационе системе као што су стони или преносиви рачунари (desktop/laptop computers) који се користе у установама Министарства одбране Сједињених Америчких Држава, регистрациони документ за одређени систем заједно са Безбедносним оперативним процедурама врши улогу потребне акредитације. Што се тиче уговарача, упутство за употребу комуникационо-информационих система биће садржано у клаузули о захтевима за услове ограниченог приступа у дотичном уговору.

4. Документи са ознаком „ИНТЕРНО” преносе се поштом прве класе унутар Сједињених Америчких Држава, у једном обезбеђеном коверту. Пренос изван Сједињених Америчких Држава врши се у два обезбеђена коверта, при чему је унутрашњи коверат обележен ознаком „ИНТЕРНО”. Такви преноси се врше средствима која се могу пратити, као што су комерцијални курири или друга средства о којима се постигне писани договор.

5. С друге стране, документи Сједињених Америчких Држава без ознаке тајности који потичу од неког органа Владе Сједињених Америчких Држава, а који садрже податке које је Србија означила ознаком „ИНТЕРНО”, носе на коверти и на првој страни ознаку „ИНТЕРНО – изузето од објављивања у јавности, сагласно Наслову 10. Законика Сједињених Америчких Држава,

одељак 130(ц)". Део документа који садржи податке са ознаком „ИНТЕРНО” такође се мора обележити у тим документима.

6. Телефонски разговори, видео-конференције или преноси путем факсимила који садрже податке са ознаком „ИНТЕРНО” могу бити у форми чистог текста, уколико није на располагању одобрени систем крипто-заштите.

7. Безбедносна дозвола за објект није потребна да би уговарач закључивао уговоре који захтевају пријем или израду тајних војних података на нивоу „ИНТЕРНО”.

8. Приступ подацима са ознаком „ИНТЕРНО” одобрава се само оним појединцима за чије службене дужности је такав приступ потребан и који поседују одобрење „треба да зна”. Одобрење приступа за особље се не захтева за приступ подацима са ознаком „ИНТЕРНО”.

Члан 3.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије - Међународни уговори”.