Република Србија
МИНИСТАРСТВО ТРГОВИНЕ,
ТУРИЗМА И ТЕЛЕКОМУНИКАЦИЈА
Сектор за информационо друштво и
информациону безбедност
Одсек за информациону безбедност и
електронско пословање
Датум: 10. октобар 2019. године

ИЗМЕНА И ДОПУНА ГОДИШЊЕГ ПЛАНА ИНСПЕКЦИЈСКОГ НАДЗОРА ЗА 2019. ГОДИНУ

1. УВОД

Годишњи план инспекцијског надзора за 2019. годину инспекције унутар Одсека за информациону безбедност и електронско пословање у Сектору за информационо друштво и информациону безбедност Министарства трговине, туризма и телекомуникација донет је у складу са чланом 10. Закона о инспекцијском надзору („Службени гласник РС”, број 36/15, 44/2018-др. закон и 95/2018).

Инспекцијски надзор над применом Закона о информационој безбедности ("Службени гласник РС", бр. 6/2016 и 94/2017), Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, бр. 94/2017) и других прописа којима се уређује делатност везана за информациону безбедност и електронско пословање, обавља инспектор за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности, сагласно овлашћењима утврђеним чл. 28. и 29. Закона о информационој безбедности (у даљем тексту: ЗИБ) и чл. 64. и 65. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (у даљем тексту: ЗЕП).

У Одсеку за информациону безбедност и електронско пословање запослен је један инспектор за инспекцијски надзор над применом прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационе безбедности.

Годишњи план инспекцијског надзора доноси инспекција, на основу прикупљених података и праћења и анализирања стања у области надзора из свог делокруга и процењеног ризика, и исти ће бити спроведен кроз оперативне (шестомесечне, тромесечне и месечне) планове инспекцијског надзора.

2. ОБЛИЦИ ИНСПЕКЦИЈСКОГ НАДЗОРА

Теренски и канцеларијски инспекцијски надзор

Теренски инспекцијски надзор се врши изван службених просторија инспекције, непосредним увидом у објекте, просторије, уређаје и друге предмете, акте и

документацију надзираног субјекта, као и узимањем писаних и усмених изјава од одговорних лица и сведока о питањима која су од значаја за утврђивање чињеничног стања.

Канцеларијски инспекцијски надзор се врши у службеним просторијама инспекције, увидом у пословне књиге и другу документацију надзираног субјекта која се односи на обављање послова који су предмет инспекцијског надзора, као и увидом у податке о надзираном субјекту прибављене по службеној дужности.

3. ВРСТЕ ИНСПЕКЦИЈСКОГ НАДЗОРА

Редован, ванредан и контролни инспекцијски надзор

Инспектор за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности ће, према планираним активностима, у 2019. години вршити:

1) редовне инспекцијске надзоре код оператора ИКТ система од посебног значаја;
2) ванредне инспекцијске надзоре - поступања по пријавама физичких и правних лица;
3) ванредне инспекцијске надзоре - поступања на основу сазнања о постојању незаконитости;
4) контролне инспекцијске надзоре – утврђивање извршења мера наложених или предложених у поступку редовног или ванредног инспекцијског надзора.

4. НАДЗИРАНИ СУБЈЕКТИ И УЧЕСТАЛОСТ ВРШЕЊА ИНСПЕКЦИЈСКОГ НАДЗОРА

Надзирани субјекти су ИКТ системи од посебног значаја.

Инспекцијски надзори ће се вршити у ИКТ системима од посебног значаја, како у седишту, тако и у њиховим пословним јединицама.

Редовни инспекцијски надзори ће се вршити код оних ИКТ система од посебног значаја који су на основу делатности које обављају процењени као нарочито важни и у којима је због тога потребно успоставити и одржавати адекватан ниво информационе безбедности.

Ванредни инспекцијски надзори ће се вршити као приоритетни, уколико се оцени да се хитно морају предузимати одређене мере и уколико се дође до сазнања о постојању незаконитости (нпр. обављање делатности без одговарајуће дозволе или уписа у одговарајући регистар).

После сваког поступка редовног или ванредног инспекцијског надзора, који је окончан налагањем или предлагањем одређених мера, врши се контролни инспекцијски надзор, којим се утврђује извршење мера наложених или предложених у поступку редовног или ванредног инспекцијског надзора.

5. ПРЕДМЕТ ИНСПЕКЦИЈСКОГ НАДЗОРА

У складу са датим овлашћењима, инспектор за примену закона у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности ће приликом редовних, односно ванредних надзора, утврђивати и у зависности од врсте инспекције контролисати следеће:

1) да ли је донет Акт о безбедности;

2) да ли је Акт о безбедности донет у складу са постојећим прописима (члан 8. ЗИБ и Уредба о ближем садржају Акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја);
3) да ли су примењене мере заштите;
4) да ли је извршена годишња провера усклађености примењених мера заштите;
5) да ли је у складу са прописима сачињен извештај о годишњој провери ИКТ система од посебног значаја;
6) да ли пружалац квалификоване услуге од поверења (у даљем тексту: пружалац услуге) има запослене који поседују неопходну стручност, искуство и квалификације за примену административних и управљачких процедура које одговарају домаћим и међународним стандардима;
7) да ли је пружалац услуге осигуран од ризика одговорности за штету насталу вршењем услуге квалификоване услуге од поверења, у складу са прописима (ЗЕП и Правилник о износу осигурања од ризика одговорности за штету насталу вршењем квалификоване услуге од поверења);
8) да ли пружалац услуге има сигурне уређаје и производе који су заштићени од неовлашћене промене и гарантују техничку безбедност и поузданост процеса које подржавају;
9) да ли пружалац услуге користи сигурне системе за чување података који су му поверени;
10) да ли пружалац услуге спроводи мере против фалсификовања и крађе података;
11) да ли пружалац услуге чува у одговарајућем временском периоду све релевантне информације које се односе на податке који су креирани или примљени од стране пружаоца;
12) да ли пружалац услуге води ажурну, тачну и безбедним мерама заштићену базу података издатих електронских сертификата;
13) да ли пружалац услуге има ажуран план завршетка рада који осигурава континуитет квалификованих услуга од поверења;
14) да ли пружалац услуге има Опште услове за пружање услуга, у складу са прописима, који су јавно објављени;
15) да ли је, у складу са прописима, пружалац услуге донео Политику пружања услуге, Практична правила за пружање услуга и Политику информационе безбедности;
16) да ли квалификовани електронски сертификати испуњавају услове утврђене прописима (ЗЕП и Правилник о условима које морају да испуњавају квалификовани електронски сертификати);
17) да ли издавалац квалификованих електронских сертификата чува комплетну документацију о издатим и опозваним квалификованим електронским сертификатима, у складу са прописима;
18) да ли је квалификовани електронски временски жиг повезан са координираним универзалним временом (UTC) тако да се спречава свака могућност промене податка која се не може открити и да ли је заснован на прецизном временском оквиру;
19) да ли припрема докумената за поуздано електронско чување испуњава прописане услове (из ЗЕП и Уредбе о условима за припрему документа за поуздано електронско чување и форматима документа који су погодни за дуготрајно чување);
20) да ли поуздано електронско чување испуњава прописане услове (из ЗЕП и Правилника о условима за поступке и технолошка решења који се користе током поузданог електронског чувања документа);

21) да ли пружалац услуге електронске идентификације проверава идентитет корисника ради издавања средстава електронске идентификације у складу са нивоом шеме коју пружа (Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости);
22) да ли пружалац услуге електронске идентификације испоручује средство електронске идентификације на начин који осигурава испоруку само лицу којем је намењено;
23) да ли пружалац услуге електронске идентификације спроводи аутентикациони механизам за шему електронске идентификације у складу са нивоом шеме коју пружа (Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости);
24) да ли пружалац услуге електронске идентификације испуњава техничке, организационе и безбедносне услове за издавање шема електронске идентификације (Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости);
25) да ли средства за електронску идентификацију испуњавају прописане услове (Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости).

6. УЧЕСТАЛОСТ ВРШЕЊА ИНСПЕКЦИЈСКОГ НАДЗОРА ПО ОБЛАСТИМА И НАДЗИРАНИ СУБЈЕКТИ

Годишњим планом инспекцијског надзора за 2019. годину обухваћене су следеће активности инспектора за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности, односно редовни инспекцијски надзори и студијске посете код надзираних субјеката, и то по кварталима:

Р.Б.	Надзирани субјект	Закон	Степен ризика
III квартал			
1.	ЈП „Електропривреда Србије”, Београд;	ЗИБ	Средњи
2.	Регулаторна агенција за електронске комуникације и поштанске услуге, Београд;	ЗИБ	Средњи
IV квартал			
1.	„Banca Intesa” а.д. Београд;	ЗИБ	Средњи
2.	„Телеком Србија“ а.д. Београд;	ЗИБ	Средњи
3.	Централни регистар обавезног социјалног осигурања, Београд;	ЗИБ	Средњи
4.	Контрола летења Србије и Црне Горе SMATSA д.о.о. Београд.	ЗИБ	Средњи
5.	Републички геодетски завод, Београд	ЗИБ	Средњи
6.	Фондација "Регистар националног интернет домена Србије", Београд.	ЗИБ	Средњи

7. МЕРЕ ИНСПЕКЦИЈСКОГ НАДЗОРА

Инспектор за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности ће, у зависности од утврђеног стања у поступку инспекцијског надзора, а сходно овлашћењима утврђеним законом, предузимати следеће мере:

1) наложити отклањање утврђених неправилности, недостатака или пропуста и одредити рок за њихово отклањање;
2) привремено забранити коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност;
3) забранити употребу неадекватних поступака и инфраструктуре, и дати рок пружаоцу услуга у којем је дужан да обезбеди адекватне поступке и инфраструктуру;
4) привремено забранити вршење услуге пружаоца услуга до отклањања неадекватности поступака и инфраструктуре;
5) наредити привремени опозив неког или свих сертификата издатих од стране пружаоца услуге, ако постоји основана сумња да се ради о неадекватном поступку или фалсификату;
6) поднети пријаву надлежном органу за учињено кривично дело или привредни преступ, односно поднети захтев за покретање прекршајног поступка;
7) друге мере и активности.

8. ПРЕВЕНТИВНО ДЕЛОВАЊЕ И ПЛАНИРАНЕ МЕРЕ И АКТИВНОСТИ ЗА СПРЕЧАВАЊЕ ОБАВЉАЊА ДЕЛАТНОСТИ И ВРШЕЊА АКТИВНОСТИ НЕРЕГИСТРОВАНИХ СУБЈЕКАТА

Превентивно деловање инспекције биће остварено објављивањем контролних листа и планова инспекцијског надзора, као и организовањем службених саветодавних посета и других активности усмерених ка подстицању и подржавању законитости и безбедности поступања у области информационе безбедности и електронског пословања.

У циљу делотворнијег сузбијања делатности или активности нерегистрованих субјеката, инспекција ће у обављању послова из свог делокруга сарађивати са другим инспекцијама и органима ради међусобног обавештавања, размене података, пружања помоћи и предузимања заједничких мера и радњи од значаја за инспекцијски надзор.