З А К О Н

О ЕЛЕКТРОНСКОМ ПОТПИСУ

I. ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим законом уређује се употреба електронског потписа у правним пословима и другим правним радњама, пословању, као и права, обавезе и одговорности у вези са електронским сертификатима, ако посебним законима није другачије одређено.

Одредбе овог закона примењују се на општење органа, општење органа и странака, достављање и израду одлуке органа у електронском облику у управном, судском и другом поступку пред државним органом – ако је законом којим се уређује тај поступак прописана употреба електронског потписа.

Члан 2.

Поједини изрази који се користе у овом закону имају следеће значење:

1) "Електронски документ" – документ у електронском облику који се користи у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом;

2) "Електронски потпис" – скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника;

3) "Квалификовани електронски потпис" – електронски потпис којим се поуздано гарантује идентитет потписника, интегритет електронских докумената, и онемогућава накнадно порицање одговорности за њихов садржај, и који испуњава услове утврђене овим законом;

4) "Потписник" – лице које поседује средства за електронско потписивање и врши електронско потписивање у своје име или у име правног или физичког лица;

5) "Подаци за формирање електронског потписа" – јединствени подаци, као што су кодови или приватни криптографски кључеви, које потписник користи за израду електронског потписа;

6) "Средства за формирање електронског потписа" – одговарајућа техничка средства (софтвер и хардвер) која се користе за формирање електронског потписа, уз коришћење података за формирање електронског потписа;

7) "Средства за формирање квалификованог електронског потписа" – средства за формирање електронског потписа која испуњавају услове утврђене овим законом;

8) "Подаци за проверу електронског потписа" – подаци, као што су кодови или јавни криптографски кључеви, који се користе за проверу и оверу електронског потписа;

9) "Средства за проверу електронског потписа" – одговарајућа техничка средства (софтвер и хардвер) која служе за проверу електронског потписа, уз коришћење података за проверу електронског потписа;

10) "Средства за проверу квалификованог електронског потписа" – средства за проверу електронског потписа која испуњавају услове утврђене овим законом;

11) "Електронски сертификат" – електронски документ којим се потврђује веза између података за проверу електронског потписа и идентитета потписника;

12) "Квалификовани електронски сертификат" – електронски сертификат који је издат од стране сертификационог тела за издавање квалификованих електронских сертификата и садржи податке предвиђене овим законом;

13) "Корисник" – правно лице, предузетник, државни орган, орган територијалне аутономије, орган локалне самоуправе или физичко лице коме се издаје електронски сертификат;

14) "Сертификационо тело" – правно лице које издаје електронске сертификате у складу са одредбама овог закона.

Члан 3.

Електронском документу се не може оспорити пуноважност или доказна снага само због тога што је у електронском облику.

Став 1. овог члана се не примењује на:

1) правне послове којима се врши пренос права својине на непокретности или којима се установљавају друга стварна права на непокретностима;

2) изјаве странака и других учесника у поступку за расправљање заоставштине, форму завештања, уговоре о уступању и расподели имовине за живота, уговоре о доживотном издржавању и споразуме у вези са наслеђивањем, као и друге уговоре из области наследног права;

3) уговоре о уређивању имовинских односа између брачних другова;

4) уговоре о располагању имовином лица којима је одузета пословна способност;

5) уговоре о поклону;

6) друге правне послове или радње, за које је посебним законом или на основу закона донетих прописа, изричито одређена употреба својеручног потписа у документима на папиру или овера својеручног потписа.

Члан 4.

Ако је законом или другим прописом предвиђено да одређени документ треба чувати, то се може учинити и у електронском облику, под условом да је електронски документ:

1) доступан и да је на располагању за каснију употребу;

2) сачуван у облику у коме је формиран или примљен;

3) сачуван на начин који омогућава идентификацију времена и места настанка или пријема, и лица које га је формирало;

4) формиран применом технологије и поступака који омогућавају да се на поуздан начин може утврдити било каква измена у електронском документу.

Обавеза чувања документа из става 1. овог члана, не односи се на податке чији је једини циљ да омогуће пријем или слање електронског документа (комуникациони подаци).

Члан 5.

Лица која чувају електронске документе који су електронски потписани, дужна су да чувају податке и средства за проверу електронског потписа онолико времена колико се чувају сами документи.

II. ЕЛЕКТРОНСКИ ПОТПИС И КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ПОТПИС

Члан 6.

Електронски потпис може имати правно дејство и може се користити као доказно средство у законом уређеном поступку, осим када се, у складу са посебним законом, захтева да само својеручни потпис има правно дејство и доказну снагу.

Члан 7.

Квалификовани електронски потпис, мора да задовољи следеће услове:

1) искључиво је повезан са потписником;

2) недвосмислено идентификује потписника;

3) настаје коришћењем средстава којима потписник може самостално да управља и која су искључиво под надзором потписника;

4) директно је повезан са подацима на које се односи, и то на начин који недвосмислено омогућава увид у било коју измену изворних података;

5) формиран је средствима за формирање квалификованог електронског потписа;

6) проверава се на основу квалификованог електронског сертификата потписника.

Члан 8.

Средства за формирање квалификованог електронског потписа су средства која морају да обезбеде:

1) да се подаци за формирање квалификованог електронског потписа могу појавити само једном и да је обезбеђена њихова поверљивост;

2) да се из података за проверу квалификованог електронског потписа, не могу у разумно време и тренутно доступним средствима, добити подаци за формирање квалификованог електронског потписа;

3) да квалификовани електронски потпис буде заштићен од фалсификовања, употребом тренутно доступне технологије;

4) да подаци за формирање квалификованог електронског потписа буду поуздано заштићени од неовлашћеног коришћења.

Средства за формирање квалификованог електронског потписа, приликом формирања потписа, не смеју променити податке који се потписују или онемогућити потписнику увид у те податке пре процеса формирања квалификованог електронског потписа.

Члан 9.

Средства за проверу квалификованог електронског потписа су средства која обезбеђују:

1) поуздано утврђивање да подаци коришћени за проверу електронског потписа одговарају подацима приказаним лицу које врши проверу;

2) поуздано верификовање потписа и коректно приказивање резултата провере;

3) омогућавање поузданог увида у садржај потписаних података;

4) поуздано верификовање аутентичности и валидности електронског сертификата потписника у тренутку провере електронског потписа;

5) коректно приказивање идентитета потписника;

6) да се било које измене у потписаним подацима поуздано открију.

Члан 10.

Квалификовани електронски потпис у односу на податке у електронском облику има исто правно дејство и доказну снагу као и својеручни потпис, односно својеручни потпис и печат, у односу на податке у папирном облику.

Члан 11.

Министарство надлежно за информационо друштво (у даљем тексту: надлежни орган) прописује техничко–технолошке поступке за формирање квалификованог електронског потписа и критеријуме које треба да испуне средства за формирање квалификованог електронског потписа.

III. ЕЛЕКТРОНСКИ СЕРТИФИКАТИ И СЕРТИФИКАЦИОНА ТЕЛА

Члан 12.

Електронски сертификат, у смислу овог закона, је електронска потврда којом се потврђује веза између података за проверу електронског потписа и идентитета потписника.

Електронске сертификате издаје сертификационо тело.

Сертификационо тело у смислу овог закона јесте правно лице које другим правним и физичким лицима пружа услуге издавања електронских сертификата, као и друге услуге повезане са овом делатношћу.

Члан 13.

Сертификационим телима није потребна посебна дозвола за издавање електронских сертификата.

Члан 14.

Надлежни орган води евиденцију сертификационих тела.

Члан 15.

Сертификационо тело је дужно да надлежном органу пријави почетак обављања услуга издавања електронских сертификата, најмање 15 дана пре почетка рада.

Члан 16.

Надлежни орган евидентира сертификационо тело одмах након подношења пријаве којом се надлежни орган обавештава о почетку обављања услуга.

Надлежни орган прописује садржај и начин вођења евиденције, обрасце пријаве за упис у евиденцију, пријаве за упис промена као и врсту, садржај и начин достављања документације неопходне за увођење у евиденцију.

Члан 17.

Квалификовани електронски сертификат, у смислу овог закона, је електронски сертификат који издаје сертификационо тело за издавање квалификованих електронских сертификата и који мора да садржи:

1) ознаку о томе да се ради о квалификованом електронском сертификату;

2) скуп података који јединствено идентификује правно лице које издаје сертификат;

3) скуп података који јединствено идентификује потписника;

4) податке за проверу електронског потписа, који одговарају подацима за израду квалификованог електронског потписа а који су под контролом потписника;

5) податке о почетку и крају важења електронског сертификата;

6) идентификациону ознаку издатог електронског сертификата;

7) квалификовани електронски потпис сертификационог тела које је издало квалификовани електронски сертификат;

8) ограничења везана за употребу сертификата, ако их има.

Члан 18.

Сертификационо тело за издавање квалификованих електронских сертификата мора испуњавати следеће услове:

1) способност за поуздано обављање услуга издавања електронских сертификата;

2) безбедно и ажурно вођење регистра корисника као и спровођење безбедног и тренутног опозива електронског сертификата;

3) обезбеђивање тачног утврђивања датума и времена издавања или опозива електронског сертификата;

4) да извршава проверу идентитета и, ако је потребно, других додатних обележја лицу којем се издаје сертификат, на поуздан начин и у складу са прописима;

5) да има запослена лица са специјалистичким знањима, искуством и стручним квалификацијама потребним за вршење услуге издавања електронских сертификата, а нарочито у односу на: управљачке способности, стручност у примени технологија електронског потписа и одговарајућих сигурносних процедура и безбедну примену одговарајућих административних и управљачких поступака који су усаглашени са признатим стандардима;

6) да користи поуздане системе и производе који су заштићени од неовлашћених измена и који обезбеђују техничку и криптографску сигурност процеса;

7) да предузима мере против фалсификовања електронских сертификата, а у случајевима у којима генерише податке за

формирање електронског потписа да гарантује тајност процеса формирања тих података;

8) да обезбеди финансијске ресурсе за осигурање од ризика и одговорности за могућу штету насталу вршењем услуге издавања електронских сертификата;

9) да обезбеди чување свих релевантних информација које се односе на електронске сертификате у прописаном временском периоду и то у изворном облику;

10) да не чува и не копира податке за формирање електронског потписа за лица у чије име пружа ту услугу;

11) да обезбеди системе за физичку заштиту уређаја, опреме и података, и сигурносна решења за заштиту од неовлашћеног приступа;

12) да информише лица која траже издавање квалификованог електронског сертификата о тачним условима издавања и коришћења тог сертификата, укључујући било која ограничења у коришћењу, као и о поступцима за решавање спорова. Такве информације, које могу бити достављене електронски, морају бити написане и припремљене у разумљивом облику на српском језику. Одговарајући делови тих информација морају бити расположиви на захтев трећим лицима која користе електронски сертификат;

13) да користи поуздан систем управљања електронским сертификатима у облику који омогућава њихову проверу како би:

(а) унос и промене радила само овлашћена лица;

(б) могла бити проверена аутентичност информација из сертификата;

(в) електронски сертификати били јавно расположиви за претраживање само у оним случајевима за које је власник сертификата дао сагласност;

(г) било која техничка промена која би могла да наруши безбедносне захтеве била позната сертификационом телу.

Надлежни орган прописује ближе услове и начин провере испуњености услова из става 1. овог члана.

Члан 19.

Надлежни орган води Регистар сертификационих тела за издавање квалификованих електронских сертификата у Републици Србији (у даљем тексту: Регистар).

Надлежни орган прописује садржај и начин вођења Регистра, начин подношења захтева за упис у Регистар, потребну документацију уз захтев, образац захтева, као и начин објављивања података из Регистра.

Члан 20.

Ако сертификационо тело испуњава услове из члана 18. овог закона, надлежни орган доноси решење о упису у Регистар.

Решење се доноси на захтев сертификационог тела, у року од 30 дана од дана подношења уредног захтева.

Решење мора да садржи регистарски број под којим је сертификационо тело уписано у Регистар и датум уписа у Регистар.

Сертификационо тело може почети да пружа услуге издавања квалификованих електронских сертификата даном уписа у Регистар.

Сертификациона тела која су уписана у Регистар могу ту чињеницу да назначе у издатим квалификованим сертификатима.

Члан 21.

Издавање квалификованих електронских сертификата може обављати и орган државне управе, у складу са посебним прописима.

Члан 22.

Регистар и евиденција сертификационих тела доступни су јавности.

IV. ПРАВА, ОБАВЕЗЕ И ОДГОВОРНОСТИ КОРИСНИКА И СЕРТИФИКАЦИОНИХ ТЕЛА

Члан 23.

Електронски сертификат се може издати кориснику на његов захтев, о чему се закључује посебан уговор.

Корисник је слободан у избору сертификационог тела, осим у случајевима предвиђеним посебним прописима.

Корисник може користити услуге сертификације једног или више сертификационих тела.

Члан 24.

Квалификовани електронски сертификат може се издати сваком лицу на његов захтев, на основу несумњиво утврђеног идентитета и осталих података о лицу које је поднело захтев.

Члан 25.

Корисник је дужан да чува средства и податке за формирање електронског потписа од неовлашћеног приступа и употребе, и исте користи у складу са одредбама овог закона.

Члан 26.

Корисник је дужан да достави сертификационом телу све потребне податке и информације о променама које утичу или могу утицати на тачност утврђивања идентитета потписника одмах, а најкасније у року од седам дана од дана настанка промене.

Корисник је дужан да одмах затражи опозив свог сертификата у свим случајевима губитка или оштећења средстава или података за формирање електронског потписа.

Члан 27.

Корисник одговара за неправилности које су настале због неиспуњавања обавеза утврђених одредбама чл. 25. и 26. овог закона.

Корисник може бити ослобођен одговорности у случајевима када се може доказати да оштећено лице није предузело или је погрешно предузело радње за проверу електронског потписа и електронског сертификата.

Члан 28.

Сертификационо тело за издавање квалификованих електронских сертификата дужно је да:

1) обезбеди да сваки издати квалификовани електронски сертификат садржи све потребне податке у складу са чланом 17. овог закона;

2) изврши потпуну проверу идентитета корисника за кога врши услуге сертификације;

3) обезбеди тачност и целовитост података које уноси у евиденцију издатих сертификата;

4) унесе у сваки сертификат основне податке о свом идентитету;

5) омогући сваком заинтересованом лицу увид у идентификационе податке сертификационог тела и увид у решење за издавање квалификованих електронских сертификата;

6) води ажурну, тачну и безбедним мерама заштићену евиденцију издатих електронских сертификата која мора да буде јавно доступна, осим у случајевима када власник сертификата изричито захтева да његови подаци не буду јавно доступни;

7) води тачну и безбедним мерама заштићену евиденцију неважећих електронских сертификата;

8) обезбеди видљив податак о тачном датуму и времену (сат и минут) издавања односно опозива електронских сертификата у евиденцији издатих електронских сертификата;

9) поступа по одредбама закона и других прописа којима је уређена заштита личних података.

Члан 29.

Сертификационо тело за издавање квалификованих електронских сертификата је дужно да, пре закључивања уговора из члана 23. став 1. овог закона, обавести лице које је поднело захтев за издавање квалификованог електронског сертификата о свим важним околностима његове употребе.

Обавештење из става 1. овог члана садржи:

1) извод из садржаја важећих прописа, интерних правила и других услова који се односе на употребу електронског сертификата;

2) податке о евентуалним ограничењима употребе електронског сертификата;

3) податке о одговарајућим правним лековима у случају спора;

4) податке о мерама које треба да реализују корисници сертификата и о потребној технологији за безбедно електронско потписивање и проверавање електронских потписа.

Члан 30.

Сертификационо тело је дужно да прекине услугу сертификације, односно изврши опозив издатих квалификованих електронских сертификата, у случајевима кад:

1) опозив сертификата захтева власник сертификата или његов пуномоћник;

2) власник сертификата изгуби пословну способност, или је престао да постоји или су се промениле околности које битно утичу на важење сертификата;

3) утврди да је податак у сертификату погрешан или је сертификат издат на основу погрешних података;

4) утврди да су подаци за проверу електронског потписа или информациони систем сертификационог тела угрожени на начин који утиче на безбедност и поузданост сертификата;

5) утврди да су подаци за електронско потписивање или информациони систем власника сертификата угрожени на начин који утиче на поузданост и безбедност израде електронског потписа;

6) престаје са радом или му је рад забрањен, а издати сертификати су важећи.

Сертификационо тело је дужно да ажурно води евиденцију свих опозваних електронских сертификата.

Сертификационо тело је дужно да обавести корисника о опозиву електронског сертификата у року од 24 часа од примљеног обавештења односно настанка околности због којих се електронски сертификат опозива.

Члан 31.

Сертификационо тело које издаје квалификоване електронске сертификате је дужно да чува комплетну документацију о издатим и опозваним електронским сертификатима као средство за доказивање и верификацију у управним, судским и другим поступцима најмање десет година по престанку важења квалификованих електронских сертификата.

Подаци из става 1. овог члана могу се чувати у електронском облику.

Члан 32.

Сертификационо тело је дужно да о раскиду уговора због потребе односно намере престанка обављања делатности, обавести сваког корисника и надлежни орган најмање три месеца пре настанка ових околности.

Сертификационо тело је дужно да обезбеди код другог сертификационог тела наставак обављања услуге сертификације за кориснике којима је издало сертификате, а уколико за то нема могућности, дужно је да опозове све издате сертификате и о томе одмах обавести надлежни орган.

Сертификационо тело које прекида са обављањем послова сертификације дужно је да достави сву документацију у вези са обављањем услуге сертификације другом сертификационом телу на кога преноси обавезе обављања услуге сертификације, односно надлежном органу ако нема другог сертификационог тела.

Надлежни орган мора одмах, на трошак сертификационог тела, извршити опозив свих сертификата које је издало сертификационо тело које је из било којих разлога прекинуло обављање сертификације, а није обезбедило настављање обављања сертификације код другог сертификационог тела и није опозвало издате сертификате.

Члан 33.

Надлежни орган прописује најнижи износ осигурања од ризика и одговорности за могућу штету насталу вршењем услуге издавања електронских сертификата.

Члан 34.

Сертификационо тело које издаје квалификоване електронске сертификате или гарантује за квалификоване електронске сертификате другог сертификационог тела, одговорно је за штету причињену лицу које се поуздало у тај сертификат, ако:

1) информација коју садржи квалификовани електронски сертификат није тачна у тренутку његовог издавања;

2) сертификат не садржи све елементе прописане за квалификовани електронски сертификат;

3) није проверило да потписник у тренутку издавања сертификата поседује податке за израду електронског потписа који одговарају подацима за проверу електронског потписа који су дати, односно идентификовани у сертификату;

4) не обезбеди да се подаци за израду и подаци за проверу електронског потписа могу користити комплементарно, у случају када те податке генерише сертификационо тело;

5) пропусти да опозове сертификат у складу са одредбама члана 30. овог закона;

6) сертификат не садржи информације о ограничењима која се односе на употребу сертификата, а која су садржана у уговору са корисником.

Сертификационо тело није одговорно за штету из става 1. овог члана, ако докаже да је поступало у складу са законом и својим општим и интерним правилима рада.

Сертификационо тело није одговорно за штету која је настала због коришћења сертификата изван ограничења, уколико су та ограничења јасно назначена у сертификату.

Члан 35.

Електронски сертификати које издаје страно сертификационо тело равноправни су са домаћим електронским сертификатима.

Квалификовани електронски сертификати издати од стране иностраних сертификационих тела равноправни су са домаћим:

1) ако је инострано сертификационо тело добило решење од надлежног органа, у складу са одредбама чл. 18. и 20. овог закона; или

2) ако потичу из земље са којом постоји билатерални споразум о међусобном признавању квалификованих електронских сертификата.

V. НАДЗОР

Члан 36.

Надлежни орган врши инспекцијски надзор над применом овог закона и радом сертификационих тела.

Надзор над радом сертификационих тела на пословима прикупљања, употребе и заштите личних података корисника врше органи одређени законом и другим прописима којима се уређује заштита личних података.

Члан 37.

У оквиру инспекцијског надзора регистрованих и евидентираних сертификационих тела надлежни орган:

1) утврђује да ли су испуњени услови прописани овим законом и прописима донетим за спровођење овог закона;

2) контролише правилност примене прописаних поступака и организационо–техничких мера, примену интерних правила која су у вези са условима прописаним овим законом и прописима донетим за спровођење овог закона;

3) врши контролу поступка издавања, чувања и опозива електронских сертификата;

4) врши контролу законитости обављања других услуга сертификационих тела.

Члан 38.

У вршењу инспекцијског надзора над радом сертификационих тела овлашћена лица надлежног органа имају право и дужност да:

1) прегледају акте и сву документацију која је повезана са том делатношћу;

2) провере његове пословне просторије, информациони систем, рачунарску мрежу, осталу опрему, техничку документацију, као и сигурносне мере које се предузимају;

3) изврше увид у целокупну документацију, ради обезбеђивања доказа или тачног утврђивања евентуалне нерегуларности.

Овлашћено лице надлежног органа је дужно да чува као службену тајну све податке о сертификатима и личне податке о кориснику сертификата.

Члан 39.

Овлашћено лице надлежног органа решењем:

1) забрањује употребу неадекватних поступака и инфраструктуре, и даје рок сертификационом телу у којем је оно дужно да обезбеди адекватне поступке и инфраструктуру;

2) привремено забрањује пословање сертификационог тела до отклањања неадекватности поступака и инфраструктуре;

3) наређује привремени опозив неког или свих сертификата издатих од стране сертификационог тела, ако постоји основана сумња да се ради о неадекватном поступку или фалсификату.

У случају привремене забране пословања, сертификати издати до дана настанка узрока због којих је изречена мера забране, остају у важности.

Члан 40.

Ако сертификационо тело за издавање квалификованих електронских сертификата престане да испуњава услове прописане овим законом надлежни орган доноси решење о његовом брисању из регистра сертификационих тела за издавање квалификованих електронских сертификата.

Решење из става 1. овог члана коначно је и против њега се може водити управни спор.

Члан 41.

Сертификационо тело је дужно да у циљу спровођења надзора омогући овлашћеним лицима надлежног органа приступ у своје пословне просторије и увид у податке о пословању, увид у пословну документацију, приступ регистру корисника и примењеној рачунарској опреми и уређајима.

VI. КАЗНЕНЕ ОДРЕДБЕ

Члан 42.

Новчаном казном од 100.000 до 400.000 динара казниће се за прекршај корисник – правно лице:

1) које не чува средства и податке за формирање електронског потписа од неовлашћеног приступа и употребе и ако исте не користи у складу са одредбама овог закона (члан 25);
2) које у прописаном року не достави сертификационом телу потребне податке и информације о променама које утичу или могу утицати на тачност утврђивања идентитета потписника (члан 26. став 1);
3) које одмах не достави сертификационом телу захтев за опозив електронског сертификата (члан 26. став 2).

Корисник – предузетник казниће се за прекршаје из става 1. овог члана новчаном казном од 100.000 до 200.000 динара.

Одговорно лице у правном лицу, државном органу, органу територијалне аутономије и органу локалне самоуправе казниће се за прекршаје из става 1. овог члана новчаном казном од 12.000 до 20.000 динара.

Корисник – физичко лице казниће се за прекршаје из става 1. овог члана новчаном казном од 12.000 до 20.000 динара.

Члан 43.

Новчаном казном од 200.000 до 400.000 динара казниће се за прекршај сертификационо тело ако:

1) не пријави надлежном органу почетак обављања услуга издавања електронских сертификата (члан 15);

2) изда квалификовани електронски сертификат који не садржи све потребне податке (члан 17);

3) чува и копира податке за формирање електронског потписа за лица у чије име пружа ту услугу (члан 18. став 1. тачка 10);

4) не обавести корисника коме издаје електронски сертификат о свим тачним условима издавања и коришћења електронског сертификата (члан 18. став 1. тачка 12);

5) не испуњава обавезе прописане чланом 28. овог закона;

6) не прекине услуге сертификације односно не изврши опозив издатих квалификованих електронских сертификата у прописаним случајевима (члан 30. став 1);

7) не води ажурно евиденцију свих опозваних електронских сертификата (члан 30. став 2);

8) не обавести корисника о опозиву електронског сертификата у прописаном року (члан 30. став 3);

9) не чува комплетну документацију о издатим и опозваним квалификованим електронским сертификатима у предвиђеном року (члан 31. став 1);

10) благовремено не обавести кориснике којима је издало електронске сертификате и надлежни орган о околностима које могу довести до престанка обављања услуга сертификације (члан 32. став 1);

11) не омогући овлашћеним лицима надлежног органа приступ у своје пословне просторије и увид у податке о пословању, увид у пословну документацију, приступ регистру корисника, рачунарској опреми и уређајима (члан 38).

Одговорно лице у сертификационом телу казниће се за прекршаје из става 1. овог члана новчаном казном од 15.000 до 20.000 динара.

Члан 44.

Новчаном казном од 200.000 до 400.000 динара казниће се за прекршај – правно лице у случају да не чува податке и средства за проверу електронског потписа онолико времена колико се чувају сама електронска документа (члан 5).

Предузетник казниће се за прекршај из става 1. овог члана новчаном казном од 100.000 до 200.000 динара.

Одговорно лице у правном лицу, државном органу, органу територијалне аутономије и органу локалне самоуправе казниће се за прекршај из става 1. овог члана новчаном казном од 12.000 до 20.000 динара.

VII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 45.

Надлежни орган доноси подзаконска акта за спровођење овог закона у року од три месеца од дана ступања на снагу овог закона.

Члан 46.

Овај закон ступа на снагу осмог дана од дана објављивања у ″Службеном гласнику Републике Србије″.