

ZAKON O ELEKTRONSKOM POTPISU

I OSNOVNE ODREDBE

Član 1

Ovim zakonom uređuje se upotreba elektronskog potpisa u pravnim poslovima i drugim pravnim radnjama, poslovanju, kao i prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima, ako posebnim zakonima nije drugačije određeno.

Odredbe ovog zakona primenjuju se na opštenje organa, opštenje organa i stranaka, dostavljanje i izradu odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom - ako je zakonom kojim se uređuje taj postupak propisana upotreba elektronskog potpisa.

Član 2

Pojedini izrazi koji se koriste u ovom zakonu imaju sledeće značenje:

1. "Elektronski dokument" - dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom;
2. "Elektronski potpis" - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
3. "Kvalifikovani elektronski potpis" - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene ovim zakonom;
4. "Potpisnik" - lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica;
5. "Podaci za formiranje elektronskog potpisa" - jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa;
6. "Sredstva za formiranje elektronskog potpisa" - odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektronskog potpisa;
7. "Sredstva za formiranje kvalifikovanog elektronskog potpisa" - sredstva za formiranje elektronskog potpisa koja ispunjavaju uslove utvrđene ovim zakonom;
8. "Podaci za proveru elektronskog potpisa" - podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste za proveru i overu elektronskog potpisa;

9. "Sredstva za proveru elektronskog potpisa" - odgovarajuća tehnička sredstva (softver i hardver) koja služe za proveru elektronskog potpisa, uz korišćenje podataka za proveru elektronskog potpisa;
10. "Sredstva za proveru kvalifikovanog elektronskog potpisa" - sredstva za proveru elektronskog potpisa koja ispunjavaju uslove utvrđene ovim zakonom;
11. "Elektronski sertifikat" - elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;
12. "Kvalifikovani elektronski sertifikat" - elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene ovim zakonom;
13. "Korisnik" - pravno lice, preduzetnik, državni organ, organ teritorijalne autonomije, organ lokalne samouprave ili fizičko lice kome se izdaje elektronski sertifikat;
14. "Sertifikaciono telo" - pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama ovog zakona.

Član 3

Elektronskom dokumentu se ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku.

Stav 1 ovog člana se ne primenjuje na:

1. pravne poslove kojima se vrši prenos prava svojine na nepokretnosti ili kojima se ustanovljavaju druga stvarna prava na nepokretnostima;
2. izjave stranaka i drugih učesnika u postupku za raspravljanje zaostavštine, formu zaveštanja, ugovore o ustupanju i raspodeli imovine za života, ugovore o doživotnom izdržavanju i sporazume u vezi sa nasleđivanjem, kao i druge ugovore iz oblasti naslednog prava;
3. ugovore o utvrđivanju imovinskih odnosa između bračnih drugova;
4. ugovore o raspolaganju imovinom lica kojima je oduzeta poslovna sposobnost;
5. ugovore o poklonu;
6. druge pravne poslove ili radnje, za koje je posebnim zakonom ili na osnovu zakona donetih propisa, izričito određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.

Član 4

Ako je zakonom ili drugim propisom predviđeno da određeni dokument treba čuvati, to se može učiniti i u elektronskom obliku, pod uslovom da je elektronski dokument:

1. dostupan i da je na raspolaganju za kasniju upotrebu;
2. sačuvan u obliku u kome je formiran ili primljen;
3. sačuvan na način koji omogućava identifikaciju vremena i mesta nastanka ili prijema, i lica koje ga je formiralo;
4. formiran primenom tehnologije i postupaka koji omogućavaju da se na pouzdan način može utvrditi bilo kakva izmena u elektronskom dokumentu.

Obaveza čuvanja dokumenta iz stava 1 ovog člana, ne odnosi se na podatke čiji je jedini cilj da omoguće prijem ili slanje elektronskog dokumenta (komunikacioni podaci).

Član 5

Lica koja čuvaju elektronske dokumente koji su elektronski potpisani, dužna su da čuvaju podatke i sredstva za proveru elektronskog potpisa onoliko vremena koliko se čuvaju sami dokumenti.

II ELEKTRONSKI POTPIS I KVALIFIKOVANI ELEKTRONSKI POTPIS

Član 6

Elektronski potpis može imati pravno dejstvo i može se koristiti kao dokazno sredstvo u zakonom uređenom postupku, osim kada se, u skladu sa posebnim zakonom, zahteva da samo svojeručni potpis ima pravno dejstvo i dokaznu snagu.

Član 7

Kvalifikovani elektronski potpis, mora da zadovolji sledeće uslove:

1. isključivo je povezan sa potpisnikom;
2. nedvosmisleno identifikuje potpisnika;
3. nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika;
4. direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka;
5. formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa;
6. proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Član 8

Sredstva za formiranje kvalifikovanog elektronskog potpisa su sredstva koja moraju da obezbede:

1. da se podaci za formiranje kvalifikovanog elektronskog potpisa mogu pojaviti samo jednom i da je obezbeđena njihova poverljivost;
2. da se iz podataka za proveru kvalifikovanog elektronskog potpisa, ne mogu u razumno vreme i trenutno dostupnim sredstvima, dobiti podaci za formiranje kvalifikovanog elektronskog potpisa;
3. da kvalifikovani elektronski potpis bude zaštićen od falsifikovanja upotrebom trenutno dostupne tehnologije;
4. da podaci za formiranje kvalifikovanog elektronskog potpisa budu pouzdano zaštićeni od neovlašćenog korišćenja.

Sredstva za formiranje kvalifikovanog elektronskog potpisa, prilikom formiranja potpisa, ne smeju promeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke pre procesa formiranja kvalifikovanog elektronskog potpisa.

Član 9

Sredstva za proveru kvalifikovanog elektronskog potpisa su sredstva koja obezbeđuju:

1. pouzdano utvrđivanje da podaci korišćeni za proveru elektronskog potpisa odgovaraju podacima prikazanim licu koje vrši proveru;
2. pouzdano verifikovanje potpisa i korektno prikazivanje rezultata provere;
3. omogućavanje pouzdanog uvida u sadržaj potpisanih podataka;
4. pouzdano verifikovanje autentičnosti i validnosti elektronskog sertifikata potpisnika u trenutku provere elektronskog potpisa;
5. korektno prikazivanje identiteta potpisnika;
6. da se bilo koje izmene u potpisanim podacima pouzdano otkriju.

Član 10

Kvalifikovani elektronski potpis u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

Član 11

Ministarstvo nadležno za informaciono društvo (u daljem tekstu: nadležni organ) propisuje tehničko-tehnološke postupke za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

III ELEKTRONSKI SERTIFIKATI I SERTIFIKACIONA TELA

Član 12

Elektronski sertifikat, u smislu ovog zakona, je elektronska potvrda kojom se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

Elektronske sertifikate izdaje sertifikaciono telo.

Sertifikaciono telo u smislu ovog zakona jeste pravno lice koje drugim pravnim i fizičkim licima pruža usluge izdavanja elektronskih sertifikata, kao i druge usluge povezane sa ovom delatnošću.

Član 13

Sertifikacionim telima nije potrebna posebna dozvola za izdavanje elektronskih sertifikata.

Član 14

Nadležni organ vodi evidenciju sertifikacionih tela.

Član 15

Sertifikaciono telo je dužno da nadležnom organu prijavi početak obavljanja usluga izdavanja elektronskih sertifikata, najmanje 15 dana pre početka rada.

Član 16

Nadležni organ evidentira sertifikaciono telo odmah nakon podnošenja prijave kojom se nadležni organ obaveštava o početku obavljanja usluga.

Nadležni organ propisuje sadržaj i način vođenja evidencije, obrasce prijave za upis u evidenciju, prijave za upis promena kao i vrstu, sadržaj i način dostavljanja dokumentacije neophodne za uvođenje u evidenciju.

Član 17

Kvalifikovani elektronski sertifikat, u smislu ovog zakona, je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata i koji mora da sadrži:

1. oznaku o tome da se radi o kvalifikovanom elektronskom sertifikatu;
2. skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat;
3. skup podataka koji jedinstveno identifikuje potpisnika;
4. podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa a koji su pod kontrolom potpisnika;
5. podatke o početku i kraju važenja elektronskog sertifikata;
6. identifikacionu oznaku izdatog elektronskog sertifikata;
7. kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat;
8. ograničenja vezana za upotrebu sertifikata, ako ih ima.

Član 18

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata mora ispunjavati sledeće uslove:

1. sposobnost za pouzdano obavljanje usluga izdavanja elektronskih sertifikata;
2. bezbedno i ažurno vođenje registra korisnika kao i sprovođenje bezbednog i trenutnog opoziva elektronskog sertifikata;
3. obezbeđivanje tačnog utvrđivanja datuma i vremena izdavanja ili opoziva elektronskog sertifikata;
4. da izvršava proveru identiteta i, ako je potrebno, drugih dodatnih obeležja licu kojem se izdaje sertifikat, na pouzdan način i u skladu sa propisima;
5. da ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za vršenje usluge izdavanja elektronskih sertifikata, a naročito u odnosu na:

- upravljačke sposobnosti, stručnost u primeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura i bezbednu primenu odgovarajućih administrativnih i upravljačkih postupaka koji su usaglašeni sa priznatim standardima;
6. da koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmena i koji obezbeđuju tehničku i kriptografsku sigurnost procesa;
 7. da preduzima mere protiv falsifikovanja elektronskih sertifikata, a u slučajevima u kojima generiše podatke za formiranje, elektronskog potpisa da garantuje tajnost procesa formiranja tih podataka;
 8. da obezbedi finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata;
 9. da obezbedi čuvanje svih relevantnih informacija koje se odnose na elektronske sertifikate u propisanom vremenskom periodu i to u izvornom obliku;
 10. da ne čuva i ne kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu;
 11. da obezbedi sisteme za fizičku zaštitu uređaja, opreme i podataka, i sigurnosna rešenja za zaštitu od neovlašćenog pristupa;
 12. da informiše lica koja traže izdavanje kvalifikovanog elektronskog sertifikata o tačnim uslovima izdavanja i korišćenja tog sertifikata, uključujući bilo koja ograničenja u korišćenju, kao i o postupcima za rešavanje sporova. Takve informacije, koje mogu biti dostavljene elektronski, moraju biti napisane i pripremljene u razumljivom obliku na srpskom jeziku. Odgovarajući delovi tih informacija moraju biti raspoloživi na zahtev trećim licima koja koriste elektronski sertifikat;
 13. da koristi pouzdan sistem upravljanja elektronskim sertifikatima u obliku koji omogućava njihovu proveru kako bi:
 - a. unos i promene radila samo ovlašćena lica;
 - b. mogla biti proverena autentičnost informacija iz sertifikata;
 - c. elektronski sertifikati bili javno raspoloživi za pretraživanje samo u onim slučajevima za koje je vlasnik sertifikata dao saglasnost;
 - d. bilo koja tehnička promena koja bi mogla da naruši bezbednosne zahteve bila poznata sertifikacionom telu.

Nadležni organ propisuje bliže uslove i način provere ispunjenosti uslova iz stava 1 ovog člana.

Član 19

Nadležni organ vodi Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji (u daljem tekstu: Registar).

Nadležni organ propisuje sadržaj i način vođenja Registra, način podnošenja zahteva za upis u Registar, potrebnu dokumentaciju uz zahtev, obrazac zahteva, kao i način objavljivanja podataka iz Registra.

Član 20

Ako sertifikaciono telo ispunjava uslove iz člana 18 ovog zakona, nadležni organ donosi rešenje o upisu u Registar.

Rešenje se donosi na zahtev sertifikacionog tela, u roku od 30 dana od dana podnošenja urednog zahteva.

Rešenje mora da sadrži registarski broj pod kojim je sertifikaciono telo upisano u Registar i datum upisa u Registar.

Sertifikaciono telo može početi da pruža usluge izdavanja kvalifikovanih elektronskih sertifikata danom upisa u Registar.

Sertifikaciona tela koja su upisana u Registar mogu tu činjenicu da naznače u izdatim kvalifikovanim sertifikatima.

Član 21

Izdavanje kvalifikovanih elektronskih sertifikata može obavljati i organ državne uprave, u skladu sa posebnim propisima.

Član 22

Registar i evidencija sertifikacionih tela dostupni su javnosti.

IV PRAVA, OBAVEZE I ODGOVORNOSTI KORISNIKA

I SERTIFIKACIONIH TELA

Član 23

Elektronski sertifikat se može izdati korisniku na njegov zahtev, o čemu se zaključuje poseban ugovor.

Korisnik je slobodan u izboru sertifikacionog tela, osim u slučajevima predviđenim posebnim propisima.

Korisnik može koristiti usluge sertifikacije jednog ili više sertifikacionih tela.

Član 24

Kvalifikovani elektronski sertifikat može se izdati svakom licu na njegov zahtev, na osnovu nesumnjivo utvrđenog identiteta i ostalih podataka o licu koje je podnelo zahtev.

Član 25

Korisnik je dužan da čuva sredstva i podatke za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe, i iste koristi u skladu sa odredbama ovog zakona.

Član 26

Korisnik je dužan da dostavi sertifikacionom telu sve potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost utvrđivanja identiteta potpisnika odmah, a najkasnije u roku od sedam dana od dana nastanka promene.

Korisnik je dužan da odmah zatraži opoziv svog sertifikata u svim slučajevima gubitka ili oštećenja sredstava ili podataka za formiranje elektronskog potpisa.

Član 27

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obaveza utvrđenih odredbama čl. 25 i 26 ovog zakona.

Korisnik može biti oslobođen odgovornosti u slučajevima kada se može dokazati da oštećeno lice nije preduzelo ili je pogrešno preduzelo radnje za proveru elektronskog potpisa i elektronskog sertifikata.

Član 28

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata dužno je da:

1. obezbedi da svaki izdati kvalifikovani elektronski sertifikat sadrži sve potrebne podatke u skladu sa članom 17 ovog zakona;
2. izvrši potpunu proveru identiteta korisnika za koga vrši usluge sertifikacije;
3. obezbedi tačnost i celovitost podataka koje unosi u evidenciju izdatih sertifikata;
4. unese u svaki sertifikat osnovne podatke o svom identitetu;
5. omogući svakom zainteresovanom licu uvid u identifikacione podatke sertifikacionog tela i uvid u rešenje za izdavanje kvalifikovanih elektronskih sertifikata;
6. vodi ažurnu, tačnu i bezbednim merama zaštićenu evidenciju izdatih elektronskih sertifikata koja mora da bude javno dostupna, osim u slučajevima kada vlasnik sertifikata izričito zahteva da njegovi podaci ne budu javno dostupni;
7. vodi tačnu i bezbednim merama zaštićenu evidenciju nevažećih elektronskih sertifikata;
8. obezbedi vidljiv podatak o tačnom datumu i vremenu (sat i minut) izdavanja odnosno opoziva elektronskih sertifikata u evidenciji izdatih elektronskih sertifikata;
9. postupa po odredbama zakona i drugih propisa kojima je uređena zaštita ličnih podataka.

Član 29

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata je dužno da, pre zaključivanja ugovora iz člana 23 stav 1 ovog zakona, obavesti lice koje je podnelo zahtev za izdavanje kvalifikovanog elektronskog sertifikata o svim važnim okolnostima njegove upotrebe.

Obaveštenje iz stava 1 ovog člana sadrži:

1. izvod iz sadržaja važećih propisa, internih pravila i drugih uslova koji se odnose na upotrebu elektronskog sertifikata;
2. podatke o eventualnim ograničenjima upotrebe elektronskog sertifikata;
3. podatke o odgovarajućim pravnim lekovima u slučaju spora;
4. podatke o merama koje treba da realizuju korisnici sertifikata i o potrebnoj tehnologiji za bezbedno elektronsko potpisivanje i proveravanje elektronskih potpisa.

Član 30

Sertifikaciono telo je dužno da prekine uslugu sertifikacije, odnosno izvrši opoziv izdatih kvalifikovanih elektronskih sertifikata, u slučajevima kad:

1. opoziv sertifikata zahteva vlasnik sertifikata ili njegov punomoćnik;
2. vlasnik sertifikata izgubi poslovnu sposobnost, ili je prestao da postoji ili su se promenile okolnosti koje bitno utiču na važenje sertifikata;
3. utvrdi da je podatak u sertifikatu pogrešan ili je sertifikat izdat na osnovu pogrešnih podataka;
4. utvrdi da su podaci za proveru elektronskog potpisa ili informacioni sistem sertifikacionog tela ugroženi na način koji utiče na bezbednost i pouzdanost sertifikata;
5. utvrdi da su podaci za elektronsko potpisivanje ili informacioni sistem vlasnika sertifikata ugroženi na način koji utiče na pouzdanost i bezbednost izrade elektronskog potpisa;
6. prestaje sa radom ili mu je rad zabranjen, a izdati sertifikati su važeći.

Sertifikaciono telo je dužno da ažurno vodi evidenciju svih opozvanih elektronskih sertifikata.

Sertifikaciono telo je dužno da obavesti korisnika o opozivu elektronskog sertifikata u roku od 24 časa od primljenog obaveštenja odnosno nastanka okolnosti zbog kojih se elektronski sertifikat opoziva.

Član 31

Sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate je dužno da čuva kompletnu dokumentaciju o izdatim i opozvanim elektronskim sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja kvalifikovanih elektronskih sertifikata.

Podaci iz stava 1 ovog člana mogu se čuvati u elektronskom obliku.

Član 32

Sertifikaciono telo je dužno da o raskidu ugovora zbog potrebe odnosno namere prestanka obavljanja delatnosti, obavesti svakog korisnika i nadležni organ najmanje tri meseca pre nastanka ovih okolnosti.

Sertifikaciono telo je dužno da obezbedi kod drugog sertifikacionog tela nastavak obavljanja usluge sertifikacije za korisnike kojima je izdalo sertifikate, a ukoliko za to nema mogućnosti, dužno je da opozove sve izdate sertifikate i o tome odmah obavesti nadležni organ.

Sertifikaciono telo koje prekida sa obavljanjem poslova sertifikacije dužno je da dostavi svu dokumentaciju u vezi sa obavljanjem usluge sertifikacije drugom sertifikacionom telu na koga prenosi obaveze obavljanja usluge sertifikacije, odnosno nadležnom organu ako nema drugog sertifikacionog tela.

Nadležni organ mora odmah, na trošak sertifikacionog tela, izvršiti opoziv svih sertifikata koje je izdalo sertifikaciono telo koje je iz bilo kojih razloga prekinulo obavljanje sertifikacije, a nije obezbedilo nastavljanje obavljanja sertifikacije kod drugog sertifikacionog tela i nije opozvalo izdate sertifikate.

Član 33

Nadležni organ propisuje najniži iznos osiguranja od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata.

Član 34

Sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate ili garantuje za kvalifikovane elektronske sertifikate drugog sertifikacionog tela, odgovorno je za štetu pričinjenu licu koje se pouzdalo u taj sertifikat, ako:

1. informacija koju sadrži kvalifikovani elektronski sertifikat nije tačna u trenutku njegovog izdavanja;
2. sertifikat ne sadrži sve elemente propisane za kvalifikovani elektronski sertifikat;
3. nije proverilo da potpisnik u trenutku izdavanja sertifikata poseduje podatke za izradu elektronskog potpisa koji odgovaraju podacima za proveru elektronskog potpisa koji su dati, odnosno identifikovani u sertifikatu;
4. ne obezbedi da se podaci za izradu i podaci za proveru elektronskog potpisa mogu koristiti komplementarno, u slučaju kada te podatke generiše sertifikaciono telo;
5. propusti da opozove sertifikat u skladu sa odredbama člana 30 ovog zakona;
6. sertifikat ne sadrži informacije o ograničenjima koja se odnose na upotrebu sertifikata, a koja su sadržana u ugovoru sa korisnikom.

Sertifikaciono telo nije odgovorno za štetu iz stava 1 ovog člana, ako dokaže da je postupalo u skladu sa zakonom i svojim opštim i internim pravilima rada.

Sertifikaciono telo nije odgovorno za štetu koja je nastala zbog korišćenja sertifikata izvan ograničenja, ukoliko su ta ograničenja jasno naznačena u sertifikatu.

Član 35

Elektronski sertifikati koje izdaje strano sertifikaciono telo ravnopravni su sa domaćim elektronskim sertifikatima.

Kvalifikovani elektronski sertifikati izdati od strane inostranih sertifikacionih tela ravnopravni su sa domaćim:

1. ako je inostrano sertifikaciono telo dobilo rešenje od nadležnog organa, u skladu sa odredbama čl. 18 i 20 ovog zakona; ili
2. ako potiču iz zemlje sa kojom postoji bilateralni sporazum o međusobnom priznavanju kvalifikovanih elektronskih sertifikata.

V NADZOR

Član 36

Nadležni organ vrši inspekcijski nadzor nad primenom ovog zakona i radom sertifikacionih tela.

Nadzor nad radom sertifikacionih tela na poslovima prikupljanja, upotrebe i zaštite ličnih podataka korisnika vrše organi određeni zakonom i drugim propisima kojima se uređuje zaštita ličnih podataka.

Član 37

U okviru inspekcijskog nadzora registrovanih i evidentiranih sertifikacionih tela nadležni organ:

1. utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim za sprovođenje ovog zakona;
2. kontroliše pravilnost primene propisanih postupaka i organizaciono-tehničkih mera, primenu internih pravila koja su u vezi sa uslovima propisanim ovim zakonom i propisima donetim za sprovođenje ovog zakona;
3. vrši kontrolu postupka izdavanja, čuvanja i opoziva elektronskih sertifikata;
4. vrši kontrolu zakonitosti obavljanja drugih usluga sertifikacionih tela.

Član 38

U vršenju inspekcijskog nadzora nad radom sertifikacionih tela ovlašćena lica nadležnog organa imaju pravo i dužnost da:

1. pregledaju akte i svu dokumentaciju koja je povezana sa tom delatnošću;
2. provere njegove poslovne prostorije, informacioni sistem, računarsku mrežu, ostalu opremu, tehničku dokumentaciju, kao i sigurnosne mere koje se preduzimaju;
3. izvrše uvid u celokupnu dokumentaciju, radi obezbeđivanja dokaza ili tačnog utvrđivanja eventualne neregularnosti.

Ovlašćeno lice nadležnog organa je dužno da čuva kao službenu tajnu sve podatke o sertifikatima i lične podatke o korisniku sertifikata.

Član 39

Ovlašćeno lice nadležnog organa rešenjem:

1. zabranjuje upotrebu neadekvatnih postupaka i infrastrukture, i daje rok sertifikacionom telu u kojem je ono dužno da obezbedi adekvatne postupke i infrastrukturu;
2. privremeno zabranjuje poslovanje sertifikacionog tela do otklanjanja neadekvatnosti postupaka i infrastrukture;
3. naređuje privremeni opoziv nekog ili svih sertifikata izdatih od strane sertifikacionog tela, ako postoji osnovana sumnja da se radi o neadekvatnom postupku ili falsifikatu.

U slučaju privremene zabrane poslovanja, sertifikati izdati do dana nastanka uzroka zbog kojih je izrečena mera zabrane, ostaju u važnosti.

Član 40

Ako sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata prestane da ispunjava uslove propisane ovim zakonom nadležni organ donosi rešenje o njegovom brisanju iz registra sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata.

Rešenje iz stava 1 ovog člana konačno je i protiv njega se može voditi upravni spor.

Član 41

Sertifikaciono telo je dužno da u cilju sprovođenja nadzora omogući ovlašćenim licima nadležnog organa pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika i primenjenoj računarskoj opremi i uređajima.

VI KAZNENE ODREDBE

Član 42

Novčanom kaznom od 100.000 do 400.000 dinara kazniće se za prekršaj korisnik - pravno lice:

1. koje ne čuva sredstva i podatke za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe i ako iste ne koristi u skladu sa odredbama ovog zakona (član 25);
2. koje u propisanom roku ne dostavi sertifikacionom telu potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost utvrđivanja identiteta potpisnika (član 26 stav 1);
3. koje odmah ne dostavi sertifikacionom telu zahtev za opoziv elektronskog sertifikata (član 26 stav 2).

Korisnik - preduzetnik kazniće se za prekršaje iz stava 1 ovog člana novčanom kaznom od 100.000 do 200.000 dinara.

Odgovorno lice u pravnom licu, državnom organu, organu teritorijalne autonomije i organu lokalne samouprave kazniće se za prekršaje iz stava 1 ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

Korisnik - fizičko lice kazniće se za prekršaje iz stava 1 ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

Član 43

Novčanom kaznom od 200.000 do 400.000 dinara kazniće se za prekršaj sertifikaciono telo ako:

1. ne prijavi nadležnom organu početak obavljanja usluga izdavanja elektronskih sertifikata (član 15);
2. izda kvalifikovani elektronski sertifikat koji ne sadrži sve potrebne podatke (član 17);
3. čuva i kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu (član 18 stav 1 tačka 10);
4. ne obavesti korisnika kome izdaje elektronski sertifikat o svim tačnim uslovima izdavanja i korišćenja elektronskog sertifikata (član 18 stav 1 tačka 12);
5. ne ispunjava obaveze propisane članom 28 ovog zakona;
6. ne prekine usluge sertifikacije odnosno ne izvrši opoziv izdatih kvalifikovanih elektronskih sertifikata u propisanim slučajevima (član 30 stav 1);
7. ne vodi ažurno evidenciju svih opozvanih elektronskih sertifikata (član 30 stav 2);
8. ne obavesti korisnika o opozivu elektronskog sertifikata u propisanom roku (član 30 stav 3);
9. ne čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima u predviđenom roku (član 31 stav 1);
10. blagovremeno ne obavesti korisnike kojima je izdalo elektronske sertifikate i nadležni organ o okolnostima koje mogu dovesti do prestanka obavljanja usluga sertifikacije (član 32 stav 1);
11. ne omogući ovlašćenim licima nadležnog organa pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika, računarskoj opremi i uređajima (član 38).

Odgovorno lice u sertifikacionom telu kazniće se za prekršaj iz stava 1 ovog člana novčanom kaznom od 15.000 do 20.000 dinara.

Član 44

Novčanom kaznom od 200.000 do 400.000 dinara kazniće se za prekršaj - pravno lice u slučaju da ne čuva podatke i sredstva za proveru elektronskog potpisa onoliko vremena koliko se čuvaju sama elektronska dokumenta (član 5).

Preduzetnik kazniće se za prekršaj iz stava 1 ovog člana novčanom kaznom od 100.000 do 200.000 dinara.

Odgovorno lice u pravnom licu, državnom organu, organu teritorijalne autonomije i organu lokalne samouprave kazniće se za prekršaj iz stava 1 ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

VII PRELAZNE I ZAVRŠNE ODREDBE

Član 45

Nadležni organ donosi podzakonska akta za sprovođenje ovog zakona u roku od tri meseca od dana stupanja na snagu ovog zakona.

Član 46

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije".