PREDLOG

Z A K O N

O IZMENAMA I DOPUNAMA ZAKONA O INFORMACIONOJ BEZBEDNOSTI

Član 1.

U Zakonu o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16 i 94/17), u članu 2. stav 1. tačka 1) podtačka (3) reč: „pohranjuje” zamenjuje se rečima: „vode, čuvaju”.

Posle podtačke (4) dodaje se podtačka (5), koja glasi:

„(5) sve tipove sistemskog i aplikativnog softvera i softverske razvojne alate.”.

U tački 2) reči: „organ javne vlasti ili organizaciona jedinica organa javne vlasti” zamenjuju se rečima: „organ vlasti ili organizaciona jedinica organa vlasti”.

Tačka 11) menja se i glasi:

„11) incident je svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema;”

Posle tačke 11) dodaje se tačka 11a), koja glasi:

„11a) jedinstveni sistem za prijem obaveštenja o incidentima je informacioni sistem u koji se unose podaci o incidentima u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti;”.

Tačka 15) menja se i glasi:

„15) organ vlasti je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, organizacija i drugo pravno ili fizičko lice kome je povereno vršenje javnih ovlašćenja;”

Tačka 24) menja se i glasi:

„24) informaciona dobra obuhvataju podatke u datotekama i bazama podataka, programski kôd, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, zapise o korišćenju hardverskih komponenti, podataka iz datoteka i baza podataka i sprovođenju procedura ako se isti vode, unutrašnje opšte akte, procedure i slično;”

Posle tačke 24) dodaju se tač. 25) i 26), koje glase:

„25) usluga informacionog društva je usluga u smislu zakona kojim se uređuje elektronska trgovina;

26) pružalac usluge informacionog društva je pravno lice koje je pružalac usluge u smislu zakona kojim se uređuje elektronska trgovina”.

Član 2.

Posle člana 3. dodaje se član 3a, koji glasi:

„Obrada podataka o ličnosti

Član 3a

U slučaju obrade podataka o ličnosti prilikom vršenja nadležnosti i ispunjenja obaveza iz ovog zakona postupa se u skladu sa propisima koji uređuju zaštitu podataka o ličnosti.”

Član 3.

U članu 5. stav 1. posle reči: „Generalnog sekretarijata Vlade” dodaju se reči: „Narodne banke Srbije”, a reči: „CERT-a republičkih organa i Nacionalnog CERT-a” zamenjuju se rečima: „Centra za bezbednost IKT sistema u organima vlasti i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima.”

U stavu 2. reči: „organa javne vlasti” zamenjuju se rečima: „organa vlasti”.

Član 4.

Član 6. menja se i glasi:

„IKT sistemi od posebnog značaja

Član 6.

IKT sistemi od posebnog značaja su sistemi koji se koriste:

1) u obavljanju poslova u organima vlasti;

2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti;

3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima:

(1) energetika:

- proizvodnja, prenos i distribucija električne energije;
- proizvodnja i prerada uglja;
- istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata;
- istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa.

(2) saobraćaj:

- železnički, poštanski, vodni i vazdušni saobraćaj;

(3) zdravstvo:

- zdravstvena zaštita;

(4) bankarstvo i finansijska tržišta:

- poslovi finansijskih institucija;
- poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;
- poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta;

(5) digitalna infrastruktura:

- razmena internet saobraćaja;
- upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi)

(6) dobra od opšteg interesa:

- korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja);

(7) usluge informacionog društva:

- usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona;

(8) ostale oblasti:

- elektronske komunikacije;
- izdavanje službenog glasila Republike Srbije;
- upravljanje nuklearnim objektima;
- proizvodnja, promet i prevoz naoružanja i vojne opreme;
- upravljanje otpadom;
- komunalne delatnosti;
- proizvodnja i snabdevanje hemikalijama;

4) u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti iz tačke 3) ovog stava.

Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu delatnosti iz stava 1. tačka 3) ovog člana.”

Član 5.

Posle člana 6. dodaju se čl. 6a i 6b, koji glase:

„Obaveze operatora IKT sistema od posebnog značaja

Član 6a

Operator IKT sistema od posebnog značaja u skladu sa ovim zakonom u obavezi je da:

1) upiše IKT sistem od posebnog značaja kojim upravlja u evidenciju operatora IKT sistema od posebnog značaja;

2) preduzme mere zaštite IKT sistema od posebnog značaja;

3) donese akt o bezbednosti IKT sistema;

4) vrši proveru usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje;

5) uredi odnos sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom, ukoliko poverava aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima;

6) dostavlja obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema;

7) dostavi statističke podatke o incidentima u IKT sistemu.

Evidencija operatora IKT sistema od posebnog značaja

Član 6b

Nadležni organ uspostavlja i vodi evidenciju IKT sistema od posebnog značaja (u daljem tekstu: Evidencija) koja sadrži:

1) naziv i sedište operatora IKT sistema od posebnog značaja;

2) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon administratora IKT sistema od posebnog značaja;

3) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon odgovornog lica IKT sistema od posebnog značaja;

4) podatak o vrsti IKT sistema od posebnog značaja, u skladu sa članom 6. ovog zakona.

Pored podataka iz stava 1. ovog člana, evidencija može da sadrži i druge dopunske podatke o IKT sistemu od posebnog značaja koje propisuje Nadležni organ.

Operator IKT sistema od posebnog značaja dužan je da IKT sistem od posebnog značaja kojim upravlja upiše u evidenciju iz stava 1. ovog člana.

Operator IKT sistema od posebnog značaja dužan je da nadležnom organu dostavi podatke iz stava 1. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 2. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja.

Nadležni organ stavlja na raspolaganje Nacionalnom centru za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: nacionalni CERT) ažurnu evidenciju iz stava 1. ovog člana.”

Član 6.

U članu 7. stav 2. reč: „minimizacija” zamenjuje se rečju: „smanjenje”.

U stavu 3. tačka 11) reč: „odnosno” zamenjuje se rečju: „i”.

U tački 23) reči: „pitanja informacione bezbednosti” zamenjuju se rečima: „ispunjenje zahteva za informacionu bezbednost”.

Član 7.

Član 11. menja se i glasi:

„Obaveštavanje o incidentima

Član 11.

Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko veb stranice Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima kojeg održava Nadležni organ.

Ukoliko organi iz stava 1. ovog člana budu obavešteni o incidentu na drugi način, podatke o incidentu unose u sistem iz stava 1. ovog člana.

Izuzetno od stava 1. ovog člana, obaveštenje o incidentima se upućuje:

1) Narodnoj banci Srbije, u slučaju incidenata u IKT sistemima iz člana 6. stav 1. tačka 3) podtačka (4) alineje prva i druga ovog zakona;

2) regulatornom telu za elektronske komunikacije u slučaju incidenata u IKT sistemima iz člana 6. stav 1. tačka 3) podtačka 8) alineja prva ovog zakona.

Narodna banka Srbije i regulatorno telo za elektronske komunikacije obaveštenja iz stava 3. ovog člana dostavljaju u jedinstveni sistem za prijem obaveštenja o incidentima na način iz stava 1. ovog člana.

Nakon prijave incidenta, ukoliko je incident i dalje u toku, operatori IKT sistema od posebnog značaja dostavljaju obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta organu kome su u skladu sa ovim zakonom prijavili incident.

Operatori IKT sistema od posebnog značaja dostavljaju završni izveštaj o incidentu organu koga su u skladu sa ovim zakonom obaveštavali o incidentu u roku od 15 dana od dana prestanka incidenta, a koji obavezno sadrži vrstu i opis incidenta, vreme i trajanje incidenta, posledice koje je incident izazvao, preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge relevantne informacije.

U slučaju incidenata u IKT sistemima za rad sa tajnim podacima operatori tih IKT sistema postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.

Odredbe st. 1. i 7. ovog člana ne odnose se na samostalne operatore IKT sistema.

Vlada, na predlog Nadležnog organa, uređuje postupak obaveštavanja o incidentima, listu, vrste i značaj incidenata prema nivou opasnosti, postupanje i razmenu informacija o incidentima između organa iz člana 5. ovog zakona.

Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 3. ovog člana kome se upućuju obaveštenja o incidentima, može objaviti informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio.

Ako je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, organ kome je upućeno obaveštenje o incidentu, obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove.

Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje odbrane Republike Srbije, organ kome je upućeno obaveštenje o incidentu obaveštava Vojnobezbednosnu agenciju.

Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje nacionalne bezbednosti, organ kome je upućeno obaveštenje o incidentu obaveštava Bezbednosno-informativnu agenciju.

U slučaju nastupanja okolnosti ugrožavanja, ometanja rada ili uništenja IKT sistema od posebnog značaja rukovođenje i koordinaciju sprovođenja mera i zadataka u navedenim okolnostima preduzima Republički štab za vanredne situacije, u skladu sa zakonom.”

Član 8.

Posle člana 11. dodaju se čl. 11a i 11b, koji glase:

„Incidenti u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti

Član 11a

Operator IKT sistema od posebnog značaja dužan je da prijavi sledeće incidente koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti:

1) incidente koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;

2) incidente koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period;

3) incidente koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;

4) incidente koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;

5) incidente koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose;

6) incidente koji su nastali kao posledica incidenta u IKT sistemu iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge IKT sistema iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona.

Operator IKT sistema od posebnog značaja dužan je da prijavi i incidente koji su doveli do značajnog povećanja rizika od nastupanja posledica iz stava 1. ovog člana.

Dostavljanje statističkih podataka o incidentima

Član 11b

Operator IKT sistema od posebnog značaja dužan je da, pored obaveštavanja o incidentima iz člana 11. ovog zakona, dostavi Nacionalnom CERT-u statističke podatke o svim incidentima u IKT sistemu u prethodnoj godini najkasnije do 28. februara tekuće godine.

Nacionalni CERT objedinjene statističke podatke iz stava 1. ovog člana dostavlja Nadležnom organu i objavljuje ih na veb stranici Nacionalnog CERT-a.

Vrstu, formu i način dostavljanja statističkih podataka iz stava 1. ovog člana utvrđuje Nacionalni CERT.”.

Član 9.

U članu 12. stav 1. tačka 1) reči: „visoki rizici” zamenjuju se rečju: „visokorizični”.

Član 10.

Iznad člana 13. dodaje se naziv člana, koji glasi: „Samostalni operatori IKT sistema”.

Član 11.

Posle člana 13. dodaje se član 13a, koji glasi:

„Shodna primena odredaba o samostalnim operatorima IKT sistema

Član 13a

Na Narodnu banku Srbije kao operatora IKT sistema shodno se primenjuju odredbe čl. 13, 15, 15a, 19, 22, 26, 27. i 28. ovog zakona koje se odnose na samostalne operatore IKT sistema.

Na Narodnu banku Srbije kao operatora IKT sistema shodno se primenjuju i odredbe čl. 11. i 11a ovog zakona koje se odnose na operatore IKT sistema od posebnog značaja.”

Član 12.

U nazivu člana 14. i u stavu 1. reči: „Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT)” zamenjuju se rečima: „Nacionalni CERT”.

Član 13.

Član 15. menja se i glasi:

„Delokrug Nacionalnog CERT-a

Član 15.

Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno:

1) prati stanje o incidentima na nacionalnom nivou,

2) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima,

3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i po prijavama fizičkih i pravnih lica, tako što pruža savete i preporuke na osnovu raspoloživih informacija o incidentima i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja,

4) kontinuirano izrađuje analize rizika i incidenata,

5) podiže svest kod građana, privrednih subjekata i organa vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti,

6) vodi evidenciju Posebnih CERT-ova,

7) izveštava Nadležni organ na kvartalnom nivou o preduzetim aktivnostima.

Nacionalni CERT je ovlašćen da vrši obradu podataka o licu koje se obrati Nacionalnom CERT-u u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti i drugim propisima.

Obrada podataka o licu iz stava 1. tačka 3) ovog člana obuhvata ime, prezime i broj telefona i/ili adresu elektronske pošte i vrši se u svrhu evidentiranja podnetih prijava, informisanja podnosioca prijave o statusu predmeta i, u slučaju potrebe, upućivanja prijave nadležnim organima radi daljeg postupanja, u skladu sa zakonom.

Nacionalni CERT obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije.

Prostorije i informacioni sistemi Nacionalnog CERT-a moraju da se nalaze na bezbednim lokacijama.

U cilju obezbeđivanja kontinuiteta rada, Nacionalni CERT treba da:

1) bude opremljen sa odgovarajućim sistemima za obavljanje poslova iz svog delokruga;

2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u svako doba;

3) obezbedi infrastrukturu čiji je kontinuitet osiguran, odnosno da obezbedi redundantne sisteme i rezervni radni prostor.

Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om organa vlasti.

Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih procedura za:

1) upravljanje i saniranje rizika i incidenata;

2) klasifikaciju informacija o rizicima i incidentima, odnosno klasifikaciju prema nivou incidenata i rizika.”

Član 14.

Posle člana 15. dodaje se član 15a, koji glasi:

„Saradnja CERT-ova u Republici Srbiji

Član 15a

Nacionalni CERT, CERT organa vlasti i CERT-ovi samostalnih operatora IKT sistema održavaju kontinuiranu saradnju.

CERT-ovi iz stava 1. ovog člana održavaju međusobne sastanke u organizaciji Nacionalnog CERT-a najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

Sastancima CERT-ova iz stava 1. ovog člana prisustvuju i predstavnici Nadležnog organa.

Sastancima CERT-ova iz stava 1. ovog člana mogu, po pozivu, da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica.”

Član 15.

Iznad člana 16. dodaje se naziv člana koji glasi: „Nadzor nad radom Nacionalnog CERT-a”.

Član 16.

U članu 17. stav 2. posle reči: „pravnog lica” dodaju se reči: „sa sedištem na teritoriji Republike Srbije”.

U stavu 4. posle reči: „pošte” dodaje se zapeta i reči: „a u svrhu angažovanja posebnih CERT-ova u slučaju bezbednosnih rizika i incidenata u IKT sistemima.”.

Stav 5. menja se i glasi:

„Nacionalni CERT propisuje sadržaj, način upisa i vođenja evidencije iz stava 3. ovog člana.”

Član 17.

Član 18. menja se i glasi:

„Centar za bezbednost IKT sistema u organima vlasti (CERT organa vlasti)

„Član 18.

CERT organa vlasti obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti, izuzev IKT sistema samostalnih operatora.

Poslove CERT-a organa vlasti obavlja organ nadležan za projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa.

Poslovi CERT-a organa vlasti obuhvataju:

1) zaštitu Jedinstvene informaciono-komunikacione mreže elektronske uprave;

2) koordinaciju i saradnju sa operatorima IKT sistema koje povezuje jedinstvena mreža iz tačke 1) ovog stava u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;

3) izdavanje stručnih preporuka za zaštitu IKT sistema organa vlasti, osim IKT sistema za rad sa tajnim podacima.”

Član 18.

Iznad člana 19. dodaje se naziv člana koji glasi: „CERT samostalnog operatora IKT sistema”.

U stavu 2. reči: „republičkih organa” zamenjuju se rečima: „organa vlasti”.

Član 19.

Posle člana 19. dodaje se član 19a, koji glasi:

„Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija

Član 19a

Nadležni organ preduzima preventivne mere za bezbednost i zaštitu dece na internetu, kao aktivnosti od javnog interesa, putem edukacije i informisanja dece, roditelja i nastavnika o prednostima, rizicima i načinima bezbednog korišćenja interneta, kao i putem jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, i upućuje prijave nadležnim organima radi daljeg postupanja.

Operator elektronskih komunikacija koji pruža javno dostupne telefonske usluge dužan je da omogući svim pretplatnicima uslugu besplatnog poziva prema jedinstvenom mestu za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu.

U slučaju da navodi iz prijave upućuju na postojanje krivičnog dela, na povredu prava, zdravstvenog statusa, dobrobiti i/ili opšteg integriteta deteta, na rizik stvaranja zavisnosti od korišćenja interneta, prijava se prosleđuje nadležnom organu vlasti radi postupanja u skladu sa utvrđenim nadležnostima.

Nadležni organ je ovlašćen da vrši obradu podataka o licu koje se obrati Nadležnom organu u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti i drugim propisima.

Obrada podataka o licu iz stava 4. ovog člana obuhvata ime, prezime i broj telefona i/ili adresu elektronske pošte i vrši se u svrhu evidentiranja podnetih prijava, informisanja podnosioca prijave o statusu predmeta i, u slučaju potrebe, upućivanja prijave nadležnim organima radi daljeg postupanja, u skladu sa zakonom.

Podaci o ličnosti iz stava 5. ovog člana čuvaju se u rokovima predviđenim propisima koji uređuju kancelarijsko poslovanje.

U cilju obezbeđivanja kontinuiteta rada jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, Nadležni organ treba da:

1) bude opremljen sa odgovarajućim sistemima za prijem prijava;

2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u radu;

3) obezbedi infrastrukturu čiji je kontinuitet osiguran.

Vlada bliže uređuje način sprovođenja mera za bezbednost i zaštitu dece na internetu iz st. 1. i 3. ovog člana.”

Član 20.

Člana 30. menja se i glasi:

„Član 30.

Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako:

1) ne izvrši upis u evidenciju u roku iz člana 6b stav 4. ovog zakona;

2) ne donese Akt o bezbednosti IKT sistema iz člana 8. stav 1. ovog zakona;

3) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 8. stav 2. ovog zakona;

4) ne izvrši proveru usklađenosti primenjenih mera iz člana 8. stav 4. ovog zakona;

5) ne dostavi statističke podatke iz člana 11b stav 1. ovog zakona;

6) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 29. stav 1. tačka 1. ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.”

Član 21.

Član 31. menja se i glasi:

„Član 31.

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako:

1) o incidentima u IKT sistemu ne obavesti organe iz člana 11. st. 1, 3. i 7. ovog zakona;

2) ne dostavlja obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima iz člana 11. stav 5. ovog zakona;

3) ne dostavi završni izveštaj u roku iz člana 11. stav 6. ovog zakona.

Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Izuzetno od st. 1. i 2. ovog člana, ako finansijska institucija ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu od posebnog značaja, Narodna banka Srbije izriče toj finansijskoj instituciji mere i kazne u skladu sa zakonom kojim se uređuje njeno poslovanje.”

Član 22.

Podzakonski akti iz čl. 4, 7. i 19. ovog zakona doneće se u roku od šest meseci od dana stupanja na snagu ovog zakona.

Podzakonski akti iz čl. 5. i 8. ovog zakona doneće se u roku od tri meseca od dana stupanja na snagu ovog zakona.

Član 23.

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

O B R A Z L O Ž E Nj E

I. USTAVNI OSNOV ZA DONOŠENjE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u članu 97. tač. 4, 16. i 17. Ustava Republike Srbije, kojima je, između ostalog, propisano da Republika Srbija uređuje i obezbeđuje bezbednost Republike Srbije, organizaciju, nadležnost i rad republičkih organa, i da obezbeđuje druge odnose od interesa za Republiku Srbiju.

II. RAZLOZI ZA DONOŠENjE ZAKONA

Zakon o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16 i 94/17) donet je u januaru 2016. godine i uredio je mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i nadležne organe za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite. Ovaj zakon donet je u periodu pre usvajanja Direktive EU o merama za visok nivo bezbednosti mrežnih i informacionih sistema u Evropskoj uniji broj 2016/1148 (NIS direktiva), koja je usvojena u julu 2016. godine. Iako je bio donet pre usvajanja ove direktive, Zakon je u velikoj meri usklađen sa ovom direktivom, budući da sadrži rešenja koja odgovaraju odredbama navedene direktive. Izradi izmena i dopuna Zakona o informacionoj bezbednosti pristupilo se prvenstveno iz dva razloga: prvi je preostalo usklađivanje sa odredbama NIS direktive radi postizanja potpune usaglašenosti, a drugi je unapređenje postojećih zakonodavnih rešenja na bazi potreba utvrđenih na osnovu dosadašnje primene zakona.

Radi preostalih usklađivanja sa NIS direktivom, u Predlogu zakona izvršene su sledeće izmene i dopune:

- dopuna oblasti u kojima se koriste IKT sistemi od posebnog značaja, i to oblast digitalne infrastrukture i usluga informacionog društva (član 6.);
- određeno je da se pre javnog objavljivanja obaveštenja o incidentu od strane nadležnog organa izvrše prethodne konsultacije sa operatorom IKT sistema od posebnog značaja koji je dostavio obaveštenje o incidentu (član 11.);
- predviđena je dopuna odredaba o Nacionalnom CERT-u koje se odnose na njegovu nadležnost i potrebne kapacitete (član 15.).

Tokom primene zakona utvrđena je potreba za izmenom i dopunom određenih normi, u cilju efikasnijeg sprovođenja zakona u praksi. Shodno tome, Predlogom zakona predviđeno je sledeće:

- uključivanje Narodne banke Srbije u rad Tela za koordinaciju poslova informacione bezbednosti (član 5.);
- dopuna oblasti u kojima se koriste IKT sistemi od posebnog značaja (proizvodnja i snabdevanje hemikalijama, član 6.);
- taksativno su nabrojane obaveze IKT sistema od posebnog značaja (član 6a);
- uspostavljanje Evidencije operatora IKT sistema od posebnog značaja (član 6b);
- definisan je način obaveštavanja o incidentima koji značajno ugrožavaju informacionu bezbednost preko portala Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima (član 11.);

- obaveza Narodne banke Srbije i RATEL-a da dobijena obaveštenja o incidentu proslede Nadležnom organu (član 11.);
- dostavljanje obaveštenja o incidentu koji je povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje nacionalne bezbednosti, Bezbednosno-informativnoj agenciji (član 11.);
- definisani su incidenti koji treba da se prijave, a koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (član 11a);
- određena je obaveza IKT sistema od posebnog značaja da dostavljaju statističke podatke o incidentima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (član 11b);
- definisana je saradnja CERT-ova u Republici Srbiji (član 15a);
- dodate su odredbe o zaštiti pri korišćenju informaciono-komunikacionih tehnologija (član 19a).

Navedene izmene zakona doprineće boljoj povezanosti svih relevantnih aktera u oblasti informacione bezbednosti, budući da se Predlogom zakona predviđa uspostavljanje evidencije IKT sistema od posebnog značaja. Na taj način Nadležni organ i Nacionalni CERT imaće mogućnost intenzivnije saradnje sa svim operatorima IKT sistema od posebnog značaja, naročito u slučaju kada se dešava incident, ali u smislu pružanja podrške, preporuke i saveta za zaštitu IKT sistema od posebnog značaja.

Značajno unapređenje leži i u činjenici da je Nadležni organ uspostavio Jedinstveni sistem za prijem obaveštenja o incidentima, tako da ih IKT sistemi od posebnog značaja obaveštenja mogu prosleđivati preko portala Nadležnog organa i Nacionalnog CERT-a. Ovo rešenje doprinosi efikasnosti prijavljivanja incidenata, kao i potpunoj informisanosti svih relevantnih učesnika (Nadležni organ, Nacionalni CERT) koji potom mogu da učestvuju u otklanjanju incidenta.

Takođe, Predlog zakona predviđa odredbe o Nacionalnom CERT-u koje se odnose na jačanje kapaciteta Nacionalnog CERT-a, kako bi se uspostavilo blagovremena i efikasna podrška u slučaju incidenta, a za takvu vrstu podrške neophodno je stručno osoblje, odgovarajuća infrastruktura u smislu opreme i prostorija za rad, čije obezbeđivanje je predviđeno Predlogom zakona. Kako Nacionalni CERT ima i ulogu prevencije u oblasti informacione bezbednosti, predviđeno je dostavljanje statističkih podataka od strane IKT sistema od posebnog značaja na bazi kojih će Nacionalni CERT imati mogućnost izrade adekvatnih analiza u oblasti informacione bezbednosti i na osnovu čega će pripremati preporuke i savete za mere zaštite u ovoj oblasti.

S obzirom da je prepoznata potreba za kontinuiranom saradnjom CERT-ova u Republici Srbiji, predviđene su odredbe kojima se definiše ova saradnja kroz organizaciju redovnih zajedničkih sastanaka, a posebno u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

Imajući u vidu važnost pitanja bezbednosti na internetu, Predlogom zakona definisane su odredbe kojima se predviđaju mere za bezbednost i zaštitu na internetu, kao i generalno prilikom korišćenja informaciono-komunikacionih tehnologija.

III. OBJAŠNjENjE OSNOVNIH PRAVNIH INSTITUTA I POJEDINAČNIH REŠENjA

U članu 1. vrše se izmene i dopune pojmova u Zakonu.

Članom 2. dodaje se novi član 3a koji se odnosi na obradu podataka o ličnosti prilikom vršenja nadležnosti i ispunjenja obaveza iz ovog zakona.

Članom 3. dopunjuje se član 5. Zakona tako što se predviđa uključenje Narodne banke Srbije u rad Tela za koordinaciju poslova informacione bezbednosti.

U članu 4. menja se član 6. Zakona koji se odnosi na određivanje IKT sistema od posebnog značaja u Republici Srbiji.

Članom 5. dodaju se novi čl. 6a i 6b koji se odnose na definisanje obaveza IKT sistema od posebnog značaja i na Evidenciju operatora IKT sistema od posebnog značaja.

Članom 6. vrše se preciziranja pojedinih termina koji se odnose na mere zaštite IKT sistema od posebnog značaja.

U članu 7. menja se član 11. Zakona kojim se uređuje obaveštavanje o incidentima koji mogu da imaju značaj na narušavanje informacione bezbednosti.

U članu 8. dodaju se novi čl. 11a i 11b, koji uređuju značajne incidente koje treba prijaviti, kao i dostavljanje statističkih podataka o incidentima Nacionalnom CERT-u.

U članu 9. vrši se jezičko prilagođavanje u članu 12. Zakona.

Članom 10. dodaje se naziv člana 13. koji glasi: „Samostalni operatori IKT sistema".

Članom 11. predviđa se shodna primena odredaba o samostalnim operatorima IKT sistema na Narodnu banku Srbije.

Članom 12. se menja član 14. iz pravnotehničkih razloga, budući da se pun naziv Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima i skraćenje njegovog naziva već pojavljuju u članu 6b Zakona.

Članom 13. menja se član 15. koji uređuje nadležnosti Nacionalnog CERT-a.

Članom 14. dodaje se član 15a kojim se uređuje saradnja CERT-ova u Republici Srbiji.

Članom 15. se dodaje se naziv člana 16. „Nadzor nad radom Nacionalnog CERT-a".

Članom 16. vrši se promena člana 17. tako da određuje da Nacionalni CERT donosi Pravilnik o bližim uslovima za upis u Evidenciju Posebnih centara za prevenciju bezbednosnih rizika u IKT sistemima.

Članom 17. vrši se izmena u članu 18. koji se odnosi na promenu naziva dosadašnjeg CERT-a republičkih organa.

Članom 18. dopunjuje se član 19. Zakona tako što se dodaje naziv koji glasi: „CERT samostalnog operatora IKT sistema".

Članom 19. dodaje se novi član 19a koji reguliše zaštitu pri korišćenju informaciono-komunikacionih tehnologija.

Čl. 20. i 21. menjaju se i dopunjuju prekršajne odredbe Zakona.

Članom 22. utvrđuju se rokovi za donošenje podzakonskih akata.

Članom 23. utvrđuje se stupanje na snagu ovog zakona.

IV. SREDSTVA POTREBNA ZA SPROVOĐENjE ZAKONA

Za sprovođenje ovog zakona nije potrebno obezbediti sredstva u budžetu Republike Srbije.

V. PREGLED ODREDABA KOJE SE MENjAJU, ODNOSNO DOPUNjUJU

Značenje pojedinih termina

Član 2.

Pojedini termini u smislu ovog zakona imaju sledeće značenje:

1) informaciono-komunikacioni sistem (IKT sistem) je tehnološko-organizaciona celina koja obuhvata:

(1) elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;

(2) uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;

(3) podatke koji se ~~pohranjuju~~ VODE, ČUVAJU, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ove tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;

(4) organizacionu strukturu putem koje se upravlja IKT sistemom;

(5) SVE TIPOVE SISTEMSKOG I APLIKATIVNOG SOFTVERA I SOFTVERSKE RAZVOJNE ALATE.

2) operator IKT sistema je pravno lice, ~~organ javne vlasti ili organizaciona jedinica organa javne vlasti~~ ORGAN VLASTI ILI ORGANIZACIONA JEDINICA ORGANA VLASTI koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti;

3) informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

4) tajnost je svojstvo koje znači da podatak nije dostupan neovlašćenim licima;

5) integritet znači očuvanost izvornog sadržaja i kompletnosti podatka;

6) raspoloživost je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;

7) autentičnost je svojstvo koje znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio;

8) neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći;

9) rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;

10) upravljanje rizikom je sistematičan skup mera koji uključuje planiranje, organizovanje i usmeravanje aktivnosti kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;

11) ~~*incident* je unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost~~

11) INCIDENT JE SVAKI DOGAĐAJ KOJI IMA STVARAN NEGATIVAN UTICAJ NA BEZBEDNOST MREŽNIH I INFORMACIONIH SISTEMA;

11a) JEDINSTVENI SISTEM ZA PRIJEM OBAVEŠTENjA O INCIDENTIMA JE INFORMACIONI SISTEM U KOJI SE UNOSE PODACI O INCIDENTIMA U IKT SISTEMIMA OD POSEBNOG ZNAČAJA KOJI MOGU DA IMAJU ZNAČAJAN UTICAJ NA NARUŠAVANjE INFORMACIONE BEZBEDNOSTI;

12) mere zaštite IKT sistema su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema;

13) tajni podatak je podatak koji je, u skladu sa propisima o tajnosti podataka, određen i označen određenim stepenom tajnosti;

14) IKT sistem za rad sa tajnim podacima je IKT sistem koji je u skladu sa zakonom određen za rad sa tajnim podacima;

15) ~~*organ javne vlasti* je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja, pravno lice koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave, kao i pravno lice koje se pretežno, odnosno u celini finansira iz budžeta;~~

15) ORGAN VLASTI JE DRŽAVNI ORGAN, ORGAN AUTONOMNE POKRAJINE, ORGAN JEDINICE LOKALNE SAMOUPRAVE, ORGANIZACIJA I DRUGO PRAVNO ILI FIZIČKO LICE KOME JE POVERENO VRŠENjE JAVNIH OVLAŠĆENjA;

16) služba bezbednosti je služba bezbednosti u smislu zakona kojim se uređuju osnove bezbednosno-obaveštajnog sistema Republike Srbije;

17) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove i službe bezbednosti;

18) kompromitujuće elektromagnetno zračenje (KEMZ) predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka;

19) kriptobezbednost je komponenta informacione bezbednosti koja obuhvata kriptozaštitu, upravljanje kriptomaterijalima i razvoj metoda kriptozaštite;

20) kriptozaštita je primena metoda, mera i postupaka radi transformisanja podataka u oblik koji ih za određeno vreme ili trajno čini nedostupnim neovlašćenim licima;

21) kriptografski proizvod je softver ili uređaj putem koga se vrši kriptozaštita;

22) kriptomaterijali su kriptografski proizvodi, podaci, tehnička dokumentacija kriptografskih proizvoda, kao i odgovarajući kriptografski ključevi;

23) bezbednosna zona je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci;

24) ~~*informaciona dobra* obuhvataju podatke u datotekama i bazama podataka, programski kôd, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje opšte akte, procedure i slično;~~

24) INFORMACIONA DOBRA OBUHVATAJU PODATKE U DATOTEKAMA I BAZAMA PODATAKA, PROGRAMSKI KÔD, KONFIGURACIJU HARDVERSKIH KOMPONENATA, TEHNIČKU I KORISNIČKU DOKUMENTACIJU, ZAPISE O KORIŠĆENjU HARDVERSKIH KOMPONENTI, PODATAKA IZ DATOTEKA I BAZA PODATAKA I SPROVOĐENjU PROCEDURA AKO SE ISTI VODE, UNUTRAŠNjE OPŠTE AKTE, PROCEDURE I SLIČNO;

25) USLUGA INFORMACIONOG DRUŠTVA JE USLUGA U SMISLU ZAKONA KOJIM SE UREĐUJE ELEKTRONSKA TRGOVINA;

26) PRUŽALAC USLUGE INFORMACIONOG DRUŠTVA JE PRAVO LICE KOJE JE PRUŽALAC USLUGE U SMISLU ZAKONA KOJIM SE UREĐUJE ELEKTRONSKA TRGOVINA.

OBRADA PODATAKA O LIČNOSTI

ČLAN 3A

U SLUČAJU OBRADE PODATAKA O LIČNOSTI PRILIKOM VRŠENjA NADLEŽNOSTI I ISPUNjENjA OBAVEZA IZ OVOG ZAKONA POSTUPA SE U SKLADU SA PROPISIMA KOJI UREĐUJU ZAŠTITU PODATAKA O LIČNOSTI.

Telo za koordinaciju poslova informacione bezbednosti

Član 5.

U cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti, kao i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti Vlada osniva Telo za koordinaciju poslova informacione bezbednosti (u daljem tekstu: Telo za koordinaciju), kao koordinaciono telo Vlade, u čiji sastav ulaze predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, NARODNE BANKE SRBIJE, ~~CERT-a republičkih organa i Nacionalnog CERT-~~a, CENTRA ZA BEZBEDNOST IKT SISTEMA U ORGANIMA VLASTI I NACIONALNOG CENTRA ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA.

U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih ~~organa javne vlasti~~ ORGANA VLASTI, privrede, akademske zajednice i nevladinog sektora.

Odlukom kojom osniva Telo za koordinaciju Vlada određuje i njegov sastav, zadatke, rok u kome ono podnosi izveštaje Vladi i druga pitanja koja su vezana za njegov rad.

II. BEZBEDNOST IKT SISTEMA OD POSEBNOG ZNAČAJA

~~IKT sistemi od posebnog značaja~~

~~Član 6~~

~~IKT sistemi od posebnog značaja su sistemi koji se koriste:~~

~~1) u obavljanju poslova u organima javne vlasti;~~

~~2) za obradu podataka koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti;~~

~~3) u obavljanju delatnosti od opšteg interesa i to u oblastima:~~

~~(1) proizvodnja, prenos i distribucija električne energije;~~

~~(2) proizvodnja i prerada uglja;~~

~~(3) istraživanje, proizvodnja, prerada, transport i distribucija nafte i prirodnog i tečnog gasa;~~

~~(4) promet nafte i naftnih derivata; železničkog, poštanskog i vazdušnog saobraćaja;~~

~~(5) elektronska komunikacija;~~

~~(6) izdavanje službenog glasila Republike Srbije;~~

~~(7) upravljanje nuklearnim objektima;~~

~~(8) korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja);~~

~~(9) proizvodnja, promet i prevoz naoružanja i vojne opreme;~~

~~(10) upravljanje otpadom;~~

~~(11) komunalne delatnosti;~~

~~(12) poslovi finansijskih institucija;~~

~~(13) zdravstvena zaštita;~~

~~(14) usluge informacionog društva namenjene drugim pružaocima usluga informacionog društva u cilju omogućavanja pružanja njihovih usluga.~~

~~Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu poslova i delatnosti iz stava 1. tačka 3) ovog člana.~~

IKT SISTEMI OD POSEBNOG ZNAČAJA

ČLAN 6.

IKT SISTEMI OD POSEBNOG ZNAČAJA SU SISTEMI KOJI SE KORISTE:

1) U OBAVLjANjU POSLOVA U ORGANIMA VLASTI;

2) ZA OBRADU POSEBNIH VRSTA PODATAKA O LIČNOSTI, U SMISLU ZAKONA KOJI UREĐUJE ZAŠTITU PODATAKA O LIČNOSTI;

3) U OBAVLjANjU DELATNOSTI OD OPŠTEG INTERESA I DRUGIM DELATNOSTIMA I TO U SLEDEĆIM OBLASTIMA:

(1) ENERGETIKA:

- PROIZVODNjA, PRENOS I DISTRIBUCIJA ELEKTRIČNE ENERGIJE;
- PROIZVODNjA I PRERADA UGLjA;
- ISTRAŽIVANjE, PROIZVODNjA, PRERADA, TRANSPORT I DISTRIBUCIJA NAFTE I PROMET NAFTE I NAFTNIH DERIVATA;
- ISTRAŽIVANjE, PROIZVODNjA, PRERADA, TRANSPORT I DISTRIBUCIJA PRIRODNOG I TEČNOG GASA.

(2) SAOBRAĆAJ:

- ŽELEZNIČKI, POŠTANSKI, VODNI I VAZDUŠNI SAOBRAĆAJ;

(3) ZDRAVSTVO:

- ZDRAVSTVENA ZAŠTITA;

(4) BANKARSTVO I FINANSIJSKA TRŽIŠTA:

- POSLOVI FINANSIJSKIH INSTITUCIJA;
- POSLOVI VOĐENjA REGISTRA PODATAKA O OBAVEZAMA FIZIČKIH I PRAVNIH LICA PREMA FINANSIJSKIM INSTITUCIJAMA;
- POSLOVI UPRAVLjANjA, ODNOSNO OBAVLjANjA DELATNOSTI U VEZI SA FUNKCIONISANjEM REGULISANOG TRŽIŠTA;

(5) DIGITALNA INFRASTRUKTURA:

- RAZMENA INTERNET SAOBRAĆAJA;
- UPRAVLjANjE REGISTROM NACIONALNOG INTERNET DOMENA I SISTEMOM ZA IMENOVANjE NA MREŽI (DNS SISTEMI)

(6) DOBRA OD OPŠTEG INTERESA:

- KORIŠĆENjE, UPRAVLjANjE, ZAŠTITA I UNAPREĐIVANjE DOBARA OD OPŠTEG INTERESA (VODE, PUTEVI, MINERALNE SIROVINE, ŠUME, PLOVNE REKE, JEZERA, OBALE, BANjE, DIVLjAČ, ZAŠTIĆENA PODRUČJA);

(7) USLUGE INFORMACIONOG DRUŠTVA:

- USLUGE INFORMACIONOG DRUŠTVA U SMISLU ČLANA 2. TAČKA 25) OVOG ZAKONA;

(8) OSTALE OBLASTI:

- ELEKTRONSKE KOMUNIKACIJE;
- IZDAVANjE SLUŽBENOG GLASILA REPUBLIKE SRBIJE;
- UPRAVLjANjE NUKLEARNIM OBJEKTIMA;
- PROIZVODNjA, PROMET I PREVOZ NAORUŽANjA I VOJNE OPREME;
- UPRAVLjANjE OTPADOM;
- KOMUNALNE DELATNOSTI;
- PROIZVODNjA I SNABDEVANjE HEMIKALIJAMA;

4) U PRAVNIM LICIMA I USTANOVAMA KOJE OSNIVA REPUBLIKA SRBIJA, AUTONOMNA POKRAJINA ILI JEDINICA LOKALNE SAMOUPRAVE ZA OBAVLjANjE DELATNOSTI IZ TAČKE 3) OVOG STAVA.

VLADA, NA PREDLOG MINISTARSTVA NADLEŽNOG ZA POSLOVE INFORMACIONE BEZBEDNOSTI, UTVRĐUJE LISTU DELATNOSTI IZ STAVA 1. TAČKA 3) OVOG ČLANA.

OBAVEZE OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA

ČLAN 6A

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA U SKLADU SA OVIM ZAKONOM U OBAVEZI JE DA:

1) UPIŠE IKT SISTEM OD POSEBNOG ZNAČAJA KOJIM UPRAVLjA U EVIDENCIJU OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA;

2) PREDUZME MERE ZAŠTITE IKT SISTEMA OD POSEBNOG ZNAČAJA;

3) DONESE AKT O BEZBEDNOSTI IKT SISTEMA;

4) VRŠI PROVERU USKLAĐENOSTI PRIMENjENIH MERA ZAŠTITE IKT SISTEMA SA AKTOM O BEZBEDNOSTI IKT SISTEMA I TO NAJMANjE JEDNOM GODIŠNjE;

5) UREDI ODNOS SA TREĆIM LICIMA NA NAČIN KOJI OBEZBEĐUJE PREDUZIMANjE MERA ZAŠTITE TOG IKT SISTEMA U SKLADU SA ZAKONOM, UKOLIKO POVERAVA AKTIVNOSTI U VEZI SA IKT SISTEMOM OD POSEBNOG ZNAČAJA TREĆIM LICIMA;

6) DOSTAVLjA OBAVEŠTENjA O INCIDENTIMA KOJI ZNAČAJNO UGROŽAVAJU INFORMACIONU BEZBEDNOST IKT SISTEMA;

7) DOSTAVI STATISTIČKE PODATKE O INCIDENTIMA U IKT SISTEMU.

EVIDENCIJA OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA

ČLAN 6B

NADLEŽNI ORGAN USPOSTAVLjA I VODI EVIDENCIJU IKT SISTEMA OD POSEBNOG ZNAČAJA (U DALjEM TEKSTU: EVIDENCIJA) KOJA SADRŽI:

1) NAZIV I SEDIŠTE OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA;

2) IME I PREZIME, SLUŽBENA ADRESA ZA PRIJEM ELEKTRONSKE POŠTE I SLUŽBENI KONTAKT TELEFON ADMINISTRATORA IKT SISTEMA OD POSEBNOG ZNAČAJA;

3) IME I PREZIME, SLUŽBENA ADRESA ZA PRIJEM ELEKTRONSKE POŠTE I SLUŽBENI KONTAKT TELEFON ODGOVORNOG LICA IKT SISTEMA OD POSEBNOG ZNAČAJA;

4) PODATAK O VRSTI IKT SISTEMA OD POSEBNOG ZNAČAJA, U SKLADU SA ČLANOM 6. OVOG ZAKONA.

PORED PODATAKA IZ STAVA 1. OVOG ČLANA, EVIDENCIJA MOŽE DA SADRŽI I DRUGE DOPUNSKE PODATKE O IKT SISTEMU OD POSEBNOG ZNAČAJA KOJE PROPISUJE NADLEŽNI ORGAN.

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA DUŽAN JE DA IKT SISTEM OD POSEBNOG ZNAČAJA KOJIM UPRAVLjA UPIŠE U EVIDENCIJU IZ STAVA 1. OVOG ČLANA.

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA DUŽAN JE DA NADLEŽNOM ORGANU DOSTAVI PODATKE IZ STAVA 1. OVOG ČLANA NAJKASNIJE 90 DANA OD DANA USVAJANjA PROPISA IZ STAVA 2. OVOG ČLANA, ODNOSNO 90 DANA OD DANA USPOSTAVLjANjA IKT SISTEMA OD POSEBNOG ZNAČAJA.

NADLEŽNI ORGAN STAVLjA NA RASPOLAGANjE NACIONALNOM CENTRU ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA (U DALjEM TEKSTU: NACIONALNI CERT) AŽURNU EVIDENCIJU IZ STAVA 1. OVOG ČLANA.

Mere zaštite IKT sistema od posebnog značaja

Član 7.

Operator IKT sistema od posebnog značaja odgovara za bezbednost IKT sistema i preduzimanje mera zaštite IKT sistema.

Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i ~~minimizacija~~ SMANjENjE štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

Mere zaštite IKT sistema se odnose na:

1) uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema;

2) postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja;

3) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost;

4) zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema;

5) identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu;

6) klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. ovog zakona;

7) zaštitu nosača podataka;

8) ograničenje pristupa podacima i sredstvima za obradu podataka;

9) odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža;

10) utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju;

11) predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti ~~odnosno~~ I integriteta podataka;

12) fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu;

13) zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem;

14) obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka;

15) zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera;

16) zaštitu od gubitka podataka;

17) čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema;

18) obezbeđivanje integriteta softvera i operativnih sistema;

19) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;

20) obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema;

21) zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove;

22) bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema;

23) ~~pitanja informacione bezbednosti~~ ISPUNjENjE ZAHTEVA ZA INFORMACIONU BEZBEDNOST u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;

24) zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema;

25) zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga;

26) održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;

27) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama;

28) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima.

Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema, uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.

~~Obaveštavanje Nadležnog organa o incidentima~~

~~Član 11~~

~~Operatori IKT sistema od posebnog značaja obavezni su da obaveste Nadležni organ o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.~~

~~Izuzetno od stava 1. ovog člana, finansijske institucije obaveštenja upućuju Narodnoj banci Srbije, telekomunikacioni operatori regulatornom telu za elektronske komunikacije, a operatori IKT sistema za rad sa tajnim podacima postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.~~

~~Odredbe st. 1 i 2. ovog člana ne odnose se na samostalne operatore IKT sistema.~~

~~Postupak dostavljanja podataka, listu, vrste i značaj incidenata i postupak obaveštavanja iz stava 1. ovog člana uređuje Vlada.~~

~~Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima, može naložiti njegovo objavljivanje.~~

~~Ako je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima, obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove.~~

~~Ako je incident povezan sa narušavanjem prava na zaštitu podataka o ličnosti, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima i samostalni operator IKT sistema, o tome obaveštavaju i Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.~~

OBAVEŠTAVANjE O INCIDENTIMA

ČLAN 11.

OPERATORI IKT SISTEMA OD POSEBNOG ZNAČAJA OBAVEŠTAVANjE O INCIDENTIMA U IKT SISTEMIMA KOJI MOGU DA IMAJU ZNAČAJAN UTICAJ NA NARUŠAVANjE INFORMACIONE BEZBEDNOSTI VRŠE PREKO VEB STRANICE NADLEŽNOG ORGANA ILI NACIONALNOG CERT-A U JEDINSTVENI

SISTEM ZA PRIJEM OBAVEŠTENjA O INCIDENTIMA KOJEG ODRŽAVA NADLEŽNI ORGAN.

UKOLIKO ORGANI IZ STAVA 1. OVOG ČLANA BUDU OBAVEŠTENI O INCIDENTU NA DRUGI NAČIN, PODATKE O INCIDENTU UNOSE U SISTEM IZ STAVA 1. OVOG ČLANA.

IZUZETNO OD STAVA 1. OVOG ČLANA, OBAVEŠTENjE O INCIDENTIMA SE UPUĆUJE:

1) NARODNOJ BANCI SRBIJE, U SLUČAJU INCIDENATA U IKT SISTEMIMA IZ ČLANA 6. STAV 1. TAČKA 3) PODTAČKA (4) ALINEJE PRVA I DRUGA OVOG ZAKONA;

2) REGULATORNOM TELU ZA ELEKTRONSKE KOMUNIKACIJE U SLUČAJU INCIDENATA U IKT SISTEMIMA IZ ČLANA 6. STAV 1. TAČKA 3) PODTAČKA 8) ALINEJA PRVA OVOG ZAKONA.

NARODNA BANKA SRBIJE I REGULATORNO TELO ZA ELEKTRONSKE KOMUNIKACIJE OBAVEŠTENjA IZ STAVA 3. OVOG ČLANA DOSTAVLjAJU U JEDINSTVENI SISTEM ZA PRIJEM OBAVEŠTENjA O INCIDENTIMA NA NAČIN IZ STAVA 1. OVOG ČLANA.

NAKON PRIJAVE INCIDENTA, UKOLIKO JE INCIDENT I DALjE U TOKU, OPERATORI IKT SISTEMA OD POSEBNOG ZNAČAJA DOSTAVLjAJU OBAVEŠTENjA O BITNIM DOGAĐAJIMA U VEZI SA INCIDENTOM I AKTIVNOSTIMA KOJE PREDUZIMAJU DO PRESTANKA INCIDENTA ORGANU KOME SU U SKLADU SA OVIM ZAKONOM PRIJAVILI INCIDENT.

OPERATORI IKT SISTEMA OD POSEBNOG ZNAČAJA DOSTAVLjAJU ZAVRŠNI IZVEŠTAJ O INCIDENTU ORGANU KOGA SU U SKLADU SA OVIM ZAKONOM OBAVEŠTAVALI O INCIDENTU U ROKU OD 15 DANA OD DANA PRESTANKA INCIDENTA, A KOJI OBAVEZNO SADRŽI VRSTU I OPIS INCIDENTA, VREME I TRAJANjE INCIDENTA, POSLEDICE KOJE JE INCIDENT IZAZVAO, PREDUZETE AKTIVNOSTI RADI OTKLANjANjA POSLEDICA INCIDENTA I, PO POTREBI, DRUGE RELEVANTNE INFORMACIJE.

U SLUČAJU INCIDENATA U IKT SISTEMIMA ZA RAD SA TAJNIM PODACIMA OPERATORI TIH IKT SISTEMA POSTUPAJU U SKLADU SA PROPISIMA KOJIMA SE UREĐUJE OBLAST ZAŠTITE TAJNIH PODATAKA.

ODREDBE ST. 1. I 7. OVOG ČLANA NE ODNOSE SE NA SAMOSTALNE OPERATORE IKT SISTEMA.

VLADA, NA PREDLOG NADLEŽNOG ORGANA, UREĐUJE POSTUPAK OBAVEŠTAVANjA O INCIDENTIMA, LISTU, VRSTE I ZNAČAJ INCIDENATA PREMA NIVOU OPASNOSTI, POSTUPANjE I RAZMENU INFORMACIJA O INCIDENTIMA IZMEĐU ORGANA IZ ČLANA 5. OVOG ZAKONA.

AKO JE INCIDENT OD INTERESA ZA JAVNOST, NADLEŽNI ORGAN, ODNOSNO ORGAN IZ STAVA 3. OVOG ČLANA KOME SE UPUĆUJU OBAVEŠTENjA O INCIDENTIMA, MOŽE OBJAVITI INFORMACIJU O INCIDENTU, NAKON SAVETOVANjA SA OPERATOROM IKT SISTEMA OD POSEBNOG ZNAČAJA U KOME SE INCIDENT DOGODIO.

AKO JE INCIDENT VEZAN ZA IZVRŠENjE KRIVIČNIH DELA KOJA SE GONE PO SLUŽBENOJ DUŽNOSTI, ORGAN KOME JE UPUĆENO OBAVEŠTENjE O INCIDENTU, OBAVEŠTAVA NADLEŽNO JAVNO TUŽILAŠTVO, ODNOSNO MINISTARSTVO NADLEŽNO ZA UNUTRAŠNjE POSLOVE.

AKO JE INCIDENT POVEZAN SA ZNAČAJNIM NARUŠAVANjEM INFORMACIONE BEZBEDNOSTI, KOJE IMA ILI MOŽE IMATI ZA POSLEDICU UGROŽAVANjE ODBRANE REPUBLIKE SRBIJE, ORGAN KOME JE UPUĆENO OBAVEŠTENjE O INCIDENTU OBAVEŠTAVA VOJNOBEZBEDNOSNU AGENCIJU.

AKO JE INCIDENT POVEZAN SA ZNAČAJNIM NARUŠAVANjEM INFORMACIONE BEZBEDNOSTI, KOJE IMA ILI MOŽE IMATI ZA POSLEDICU UGROŽAVANjE NACIONALNE BEZBEDNOSTI, ORGAN KOME JE UPUĆENO OBAVEŠTENjE O INCIDENTU OBAVEŠTAVA BEZBEDNOSNO-INFORMATIVNU AGENCIJU.

U SLUČAJU NASTUPANjA OKOLNOSTI UGROŽAVANjA, OMETANjA RADA ILI UNIŠTENjA IKT SISTEMA OD POSEBNOG ZNAČAJA RUKOVOĐENjE I KOORDINACIJU SPROVOĐENjA MERA I ZADATAKA U NAVEDENIM OKOLNOSTIMA PREDUZIMA REPUBLIČKI ŠTAB ZA VANREDNE SITUACIJE, U SKLADU SA ZAKONOM.

INCIDENTI U IKT SISTEMIMA OD POSEBNOG ZNAČAJA KOJI MOGU DA IMAJU ZNAČAJAN UTICAJ NA NARUŠAVANjE INFORMACIONE BEZBEDNOSTI

ČLAN 11A

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA DUŽAN JE DA PRIJAVI SLEDEĆE INCIDENTE KOJI MOGU DA IMAJU ZNAČAJAN UTICAJ NA NARUŠAVANjE INFORMACIONE BEZBEDNOSTI:

1) INCIDENTE KOJI DOVODE DO PREKIDA KONTINUITETA VRŠENjA POSLOVA I PRUŽANjA USLUGA, ODNOSNO ZNATNIH TEŠKOĆA U VRŠENjU POSLOVA I PRUŽANjU USLUGA;

2) INCIDENTE KOJI UTIČU NA VELIKI BROJ KORISNIKA USLUGA, ILI TRAJU DUŽI VREMENSKI PERIOD;

3) INCIDENTE KOJI DOVODE DO PREKIDA KONTINUITETA, ODNOSNO TEŠKOĆA U VRŠENjU POSLOVA I PRUŽANjA USLUGA, KOJI UTIČU NA OBAVLjANjE POSLOVA I VRŠENjE USLUGA DRUGIH OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA ILI UTIČU NA JAVNU BEZBEDNOST;

4) INCIDENTE KOJI DOVODE DO PREKIDA KONTINUITETA, ODNOSNO TEŠKOĆE U VRŠENjU POSLOVA I PRUŽANjU USLUGA I IMAJU UTICAJ NA VEĆI DEO TERITORIJE REPUBLIKE SRBIJE;

5) INCIDENTE KOJI DOVODE DO NEOVLAŠĆENOG PRISTUPA ZAŠTIĆENIM PODACIMA ČIJE OTKRIVANjE MOŽE UGROZITI PRAVA I INTERESE ONIH NA KOJE SE PODACI ODNOSE;

6) INCIDENTE KOJI SU NASTALI KAO POSLEDICA INCIDENTA U IKT SISTEMU IZ ČLANA 6. STAV 1. TAČKA 3) PODTAČKA (7) OVOG ZAKONA, KADA

IKT SISTEM OD POSEBNOG ZNAČAJA U SVOM POSLOVANjU KORISTI INFORMACIONE USLUGE IKT SISTEMA IZ ČLANA 6. STAV 1. TAČKA 3) PODTAČKA (7) OVOG ZAKONA.

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA DUŽAN JE DA PRIJAVI I INCIDENTE KOJI SU DOVELI DO ZNAČAJNOG POVEĆANjA RIZIKA OD NASTUPANjA POSLEDICA IZ STAVA 1. OVOG ČLANA.

DOSTAVLjANjE STATISTIČKIH PODATAKA O INCIDENTIMA

ČLAN 11B

OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA DUŽAN JE DA, PORED OBAVEŠTAVANjA O INCIDENTIMA IZ ČLANA 11. OVOG ZAKONA, DOSTAVI NACIONALNOM CERT-U STATISTIČKE PODATKE O SVIM INCIDENTIMA U IKT SISTEMU U PRETHODNOJ GODINI NAJKASNIJE DO 28. FEBRUARA TEKUĆE GODINE.

NACIONALNI CERT OBJEDINjENE STATISTIČKE PODATKE IZ STAVA 1. OVOG ČLANA DOSTAVLjA NADLEŽNOM ORGANU I OBJAVLjUJE IH NA VEB STRANICI NACIONALNOG CERT-A.

VRSTU, FORMU I NAČIN DOSTAVLjANjA STATISTIČKIH PODATAKA IZ STAVA 1. OVOG ČLANA UTVRĐUJE NACIONALNI CERT.

Međunarodna saradnja i rana upozorenja o rizicima i incidentima

Član 12.

Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova:

1) brzo rastu ili imaju tendenciju da postanu ~~visoki rizici~~ VISOKORIZIČNI;

2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete;

3) mogu da imaju negativan uticaj na više od jedne države.

Ukoliko je incident u vezi sa izvršenjem krivičnog dela, po dobijanju obaveštenja od Nadležnog organa, ministarstvo nadležno za unutrašnje poslove će u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima.

SAMOSTALNI OPERATORI IKT SISTEMA

Član 13.

Samostalni operatori IKT sistema odrediće posebna lica, odnosno organizacione jedinice za internu kontrolu sopstvenih IKT sistema.

Lica za internu kontrolu samostalnih operatora IKT sistema izveštaj o izvršenoj internoj kontroli podnose rukovodiocu samostalnog operatora IKT sistema.

SHODNA PRIMENA ODREDABA O SAMOSTALNIM OPERATORIMA IKT SISTEMA

ČLAN 13A

NA NARODNU BANKU SRBIJE KAO OPERATORA IKT SISTEMA SHODNO SE PRIMENjUJU ODREDBE ČL. 13, 15, 15A, 19, 22, 26, 27. I 28. OVOG ZAKONA KOJE SE ODNOSE NA SAMOSTALNE OPERATORE IKT SISTEMA.

NA NARODNU BANKU SRBIJE KAO OPERATORA IKT SISTEMA SHODNO SE PRIMENjUJU I ODREDBE ČL. 11. I 11A OVOG ZAKONA KOJE SE ODNOSE NA OPERATORE IKT SISTEMA OD POSEBNOG ZNAČAJA.

III. PREVENCIJA I ZAŠTITA OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA U REPUBLICI SRBIJI

~~NACIONALNI CENTAR ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA (Nacionalni CERT)~~ NACIONALI CERT

Član 14.

~~NACIONALNI CENTAR ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA (U DALjEM TEKSTU: Nacionalni CERT)~~ NACIONALNI CERT obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou.

Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge.

~~Član 15~~

~~Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno:~~

~~1) prati stanje o incidentima na nacionalnom nivou,~~

~~2) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima,~~

~~3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja,~~

~~4) kontinuirano izrađuje analize rizika i incidenata,~~

~~5) podiže svest kod građana, privrednih subjekata i organa javne vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti,~~

~~6) vodi evidenciju Posebnih CERT-ova.~~

~~Evidencija iz stava 1. tačka 6) ovog člana od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkciju i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte.~~

~~Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om republičkih organa.~~

~~Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih pravila za:~~

~~1) upravljanje i saniranje rizika i incidenata;~~

~~2) klasifikaciju informacija o rizicima i incidentima;~~

~~3) klasifikaciju ozbiljnosti incidenata i rizika;~~

~~4) definiciju formata i modela podataka za razmenu informacija o rizicima i incidentima i definiciju pravila po kojima će se imenovati značajni sistemi.~~

DELOKRUG NACIONALNOG CERT-A

ČLAN 15.

NACIONALNI CERT PRIKUPLjA I RAZMENjUJE INFORMACIJE O RIZICIMA ZA BEZBEDNOST IKT SISTEMA, KAO I DOGAĐAJIMA KOJI UGROŽAVAJU BEZBEDNOST IKT SISTEMA I U VEZI TOGA OBAVEŠTAVA, PRUŽA PODRŠKU, UPOZORAVA I SAVETUJE LICA KOJA UPRAVLjAJU IKT SISTEMIMA U REPUBLICI SRBIJI, KAO I JAVNOST, A POSEBNO:

1) PRATI STANjE O INCIDENTIMA NA NACIONALNOM NIVOU,

2) PRUŽA RANA UPOZORENjA, UZBUNE I NAJAVE I INFORMIŠE RELEVANTNA LICA O RIZICIMA I INCIDENTIMA,

3) REAGUJE PO PRIJAVLjENIM ILI NA DRUGI NAČIN OTKRIVENIM INCIDENTIMA U IKT SISTEMIMA OD POSEBNOG ZNAČAJA, KAO I PO PRIJAVAMA FIZIČKIH I PRAVNIH LICA, TAKO ŠTO PRUŽA SAVETE I PREPORUKE NA OSNOVU RASPOLOŽIVIH INFORMACIJA O INCIDENTIMA I PREDUZIMA DRUGE POTREBNE MERE IZ SVOJE NADLEŽNOSTI NA OSNOVU DOBIJENIH SAZNANjA,

4) KONTINUIRANO IZRAĐUJE ANALIZE RIZIKA I INCIDENATA,

5) PODIŽE SVEST KOD GRAĐANA, PRIVREDNIH SUBJEKATA I ORGANA VLASTI O ZNAČAJU INFORMACIONE BEZBEDNOSTI, O RIZICIMA I MERAMA ZAŠTITE, UKLjUČUJUĆI SPROVOĐENjE KAMPANjA U CILjU PODIZANjA TE SVESTI,

6) VODI EVIDENCIJU POSEBNIH CERT-OVA,

7) IZVEŠTAVA NADLEŽNI ORGAN NA KVARTALNOM NIVOU O PREDUZETIM AKTIVNOSTIMA.

NACIONALNI CERT JE OVLAŠĆEN DA VRŠI OBRADU PODATAKA O LICU KOJE SE OBRATI NACIONALNOM CERT-U U SKLADU SA ZAKONOM KOJI UREĐUJE ZAŠTITU PODATAKA O LIČNOSTI I DRUGIM PROPISIMA.

OBRADA PODATAKA O LICU IZ STAVA 1. TAČKA 3) OVOG ČLANA OBUHVATA IME, PREZIME I BROJ TELEFONA I/ILI ADRESU ELEKTRONSKE POŠTE I VRŠI SE U SVRHU EVIDENTIRANjA PODNETIH PRIJAVA, INFORMISANjA PODNOSIOCA PRIJAVE O STATUSU PREDMETA I, U SLUČAJU POTREBE, UPUĆIVANjA PRIJAVE NADLEŽNIM ORGANIMA RADI DALjEG POSTUPANjA, U SKLADU SA ZAKONOM.

NACIONALNI CERT OBEZBEĐUJE NEPREKIDNU DOSTUPNOST SVOJIH USLUGA PUTEM RAZLIČITIH SREDSTAVA KOMUNIKACIJE.

PROSTORIJE I INFORMACIONI SISTEMI NACIONALNOG CERT-A MORAJU DA SE NALAZE NA BEZBEDNIM LOKACIJAMA.

U CILjU OBEZBEĐIVANjA KONTINUITETA RADA, NACIONALNI CERT TREBA DA:

1) BUDE OPREMLjEN SA ODGOVARAJUĆIM SISTEMIMA ZA OBAVLjANjE POSLOVA IZ SVOG DELOKRUGA;

2) IMA DOVOLjNO ZAPOSLENIH KAKO BI SE OSIGURALA DOSTUPNOST U SVAKO DOBA;

3) OBEZBEDI INFRASTRUKTURU ČIJI JE KONTINUITET OSIGURAN, ODNOSNO DA OBEZBEDI REDUNDANTNE SISTEME I REZERVNI RADNI PROSTOR.

NACIONALNI CERT NEPOSREDNO SARAĐUJE SA NADLEŽNIM ORGANOM, POSEBNIM CERT-OVIMA U REPUBLICI SRBIJI, SLIČNIM ORGANIZACIJAMA U DRUGIM ZEMLjAMA, SA JAVNIM I PRIVREDNIM SUBJEKTIMA, CERT-OVIMA SAMOSTALNIH OPERATORA IKT SISTEMA, KAO I SA CERT-OM ORGANA VLASTI.

NACIONALNI CERT PROMOVIŠE USVAJANjE I KORIŠĆENjE PROPISANIH I STANDARDIZOVANIH PROCEDURA ZA:

1) UPRAVLjANjE I SANIRANjE RIZIKA I INCIDENATA;

2) KLASIFIKACIJU INFORMACIJA O RIZICIMA I INCIDENTIMA, ODNOSNO KLASIFIKACIJU PREMA NIVOU INCIDENATA I RIZIKA.

SARADNjA CERT-OVA U REPUBLICI SRBIJI

ČLAN 15A

NACIONALNI CERT, CERT ORGANA VLASTI I CERT-OVI SAMOSTALNIH OPERATORA IKT SISTEMA ODRŽAVAJU KONTINUIRANU SARADNjU.

CERT-OVI IZ STAVA 1. OVOG ČLANA ODRŽAVAJU MEĐUSOBNE SASTANKE U ORGANIZACIJI NACIONALNOG CERT-A NAJMANjE TRI PUTA GODIŠNjE, KAO I PO POTREBI U SLUČAJU INCIDENATA KOJI ZNAČAJNO UGROŽAVAJU INFORMACIONU BEZBEDNOST U REPUBLICI SRBIJI.

SASTANCIMA CERT-OVA IZ STAVA 1. OVOG ČLANA PRISUSTVUJU I PREDSTAVNICI NADLEŽNOG ORGANA.

SASTANCIMA CERT-OVA IZ STAVA 1. OVOG ČLANA MOGU, PO POZIVU, DA PRISUSTVUJU I PREDSTAVNICI POSEBNIH CERT-OVA, KAO I DRUGA LICA.

NADZOR NAD RADOM NACIONALNOG CERT-A

Član 16.

Nadzor nad radom Nacionalnog CERT-a u vršenju poslova poverenih ovim zakonom vrši Nadležni organ, koji periodično, a najmanje jednom godišnje, proverava da li Nacionalni CERT raspolaže odgovarajućim resursima, vrši poslove u skladu sa članom 15. ovog zakona i kontroliše učinak uspostavljenih procesa za upravljanje sigurnosnim incidentima.

Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima

Član 17.

Poseban centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Poseban CERT) obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica SA SEDIŠTEM NA TERITORIJI REPUBLIKE SRBIJE, koje je upisano u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT.

Upis u evidenciju posebnih CERT-ova vrši se na osnovu prijave pravnog lica u okviru koga se nalazi poseban CERT.

Evidencija posebnih CERT-ova od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkciju i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte, A U SVRHU ANGAŽOVANjA POSEBNIH CERT-OVA U SLUČAJU BEZBEDNOSNIH RIZIKA I INCIDENATA U IKT SISTEMIMA.

~~Bliže uslove za upis u evidenciju iz stava 3. ovog člana donosi nadležni organ.~~

NACIONALNI CERT PROPISUJE SADRŽAJ, NAČIN UPISA I VOĐENjA EVIDENCIJE IZ STAVA 3. OVOG ČLANA.

~~Član 18~~

~~Centar za bezbednost IKT sistema u republičkim organima (u daljem tekstu: CERT republičkih organa) obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima republičkih organa, izuzev IKT sistema samostalnih operatora.~~

~~Poslove CERT-a republičkih organa obavlja organ nadležan za projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa.~~

~~Poslovi CERT-a republičkih organa obuhvataju:~~

~~1) zaštitu IKT sistema Računarske mreže republičkih organa (u daljem tekstu: RMRO);~~

~~2) koordinaciju i saradnju sa operatorima IKT sistema koje povezuje RMRO u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;~~

~~3) izdavanje stručnih preporuka za zaštitu IKT sistema republičkih organa, osim IKT sistema za rad sa tajnim podacima.~~

CENTAR ZA BEZBEDNOST IKT SISTEMA U ORGANIMA VLASTI (CERT ORGANA VLASTI)

„ČLAN 18.

CERT ORGANA VLASTI OBAVLjA POSLOVE KOJI SE ODNOSE NA ZAŠTITU OD INCIDENATA U IKT SISTEMIMA ORGANA VLASTI, IZUZEV IKT SISTEMA SAMOSTALNIH OPERATORA.

POSLOVE CERT-A ORGANA VLASTI OBAVLjA ORGAN NADLEŽAN ZA PROJEKTOVANjE, RAZVOJ, IZGRADNjU, ODRŽAVANjE I UNAPREĐENjE RAČUNARSKE MREŽE REPUBLIČKIH ORGANA.

POSLOVI CERT-A ORGANA VLASTI OBUHVATAJU:

1) ZAŠTITU JEDINSTVENE INFORMACIONO-KOMUNIKACIONE MREŽE ELEKTRONSKE UPRAVE;

2) KOORDINACIJU I SARADNjU SA OPERATORIMA IKT SISTEMA KOJE POVEZUJE JEDINSTVENA MREŽA IZ TAČKE 1) OVOG STAVA U PREVENCIJI INCIDENATA, OTKRIVANjU INCIDENATA, PRIKUPLjANjU INFORMACIJA O INCIDENTIMA I OTKLANjANjU POSLEDICA INCIDENATA;

3) IZDAVANjE STRUČNIH PREPORUKA ZA ZAŠTITU IKT SISTEMA ORGANA VLASTI, OSIM IKT SISTEMA ZA RAD SA TAJNIM PODACIMA.

CERT SAMOSTALNOG OPERATORA IKT SISTEMA

Član 19.

Samostalni operatori IKT sistema su u obavezi da formiraju sopstvene centre za bezbednost IKT sistema radi upravljanja incidentima u svojim sistemima.

Centri iz stava 1. ovog člana međusobno razmenjuju informacije o incidentima, kao i sa nacionalnim CERT-om i sa CERT-om ~~republičkih organa~~ ORGANA VLASTI, a po potrebi i sa drugim organizacijama.

Delokrug centra za bezbednost IKT sistema, kao organizacione jedinice samostalnog operatora IKT sistema, pored poslova iz st. 1. i 2. ovog člana, može obuhvatati:

1) izradu internih akata u oblasti informacione bezbednosti;

2) izbor, testiranje i implementaciju tehničkih, fizičkih i organizacionih mera zaštite, opreme i programa;

3) izbor, testiranje i implementaciju mera zaštite od KEMZ;

4) nadzor implementacije i primene bezbednosnih procedura;

5) upravljanje i korišćenje kriptografskih proizvoda;

6) analizu bezbednosti IKT sistema u cilju procene rizika;

7) obuku zaposlenih u oblasti informacione bezbednosti.

ZAŠTITA DECE PRI KORIŠĆENjU INFORMACIONO-KOMUNIKACIONIH TEHNOLOGIJA

ČLAN 19A

NADLEŽNI ORGAN PREDUZIMA PREVENTIVNE MERE ZA BEZBEDNOST I ZAŠTITU DECE NA INTERNETU, KAO AKTIVNOSTI OD JAVNOG INTERESA, PUTEM EDUKACIJE I INFORMISANjA DECE, RODITELjA I NASTAVNIKA O PREDNOSTIMA, RIZICIMA I NAČINIMA BEZBEDNOG KORIŠĆENjA INTERNETA, KAO I PUTEM JEDINSTVENOG MESTA ZA PRUŽANjE SAVETA I PRIJEM PRIJAVA U VEZI BEZBEDNOSTI DECE NA INTERNETU, I UPUĆUJE PRIJAVE NADLEŽNIM ORGANIMA RADI DALjEG POSTUPANjA.

OPERATOR ELEKTRONSKIH KOMUNIKACIJA KOJI PRUŽA JAVNO DOSTUPNE TELEFONSKE USLUGE DUŽAN JE DA OMOGUĆI SVIM PRETPLATNICIMA USLUGU BESPLATNOG POZIVA PREMA JEDINSTVENOM MESTU ZA PRUŽANjE SAVETA I PRIJEM PRIJAVA U VEZI BEZBEDNOSTI DECE NA INTERNETU.

U SLUČAJU DA NAVODI IZ PRIJAVE UPUĆUJU NA POSTOJANjE KRIVIČNOG DELA, NA POVREDU PRAVA, ZDRAVSTVENOG STATUSA, DOBROBITI I/ILI OPŠTEG INTEGRITETA DETETA, NA RIZIK STVARANjA ZAVISNOSTI OD KORIŠĆENjA INTERNETA, PRIJAVA SE PROSLEĐUJE NADLEŽNOM ORGANU VLASTI RADI POSTUPANjA U SKLADU SA UTVRĐENIM NADLEŽNOSTIMA.

NADLEŽNI ORGAN JE OVLAŠĆEN DA VRŠI OBRADU PODATAKA O LICU KOJE SE OBRATI NADLEŽNOM ORGANU U SKLADU SA ZAKONOM KOJI UREĐUJE ZAŠTITU PODATAKA O LIČNOSTI I DRUGIM PROPISIMA.

OBRADA PODATAKA O LICU IZ STAVA 4. OVOG ČLANA OBUHVATA IME, PREZIME I BROJ TELEFONA I/ILI ADRESU ELEKTRONSKE POŠTE I VRŠI SE U SVRHU EVIDENTIRANjA PODNETIH PRIJAVA, INFORMISANjA PODNOSIOCA PRIJAVE O STATUSU PREDMETA I, U SLUČAJU POTREBE, UPUĆIVANjA PRIJAVE NADLEŽNIM ORGANIMA RADI DALjEG POSTUPANjA, U SKLADU SA ZAKONOM.

PODACI O LIČNOSTI IZ STAVA 5. OVOG ČLANA ČUVAJU SE U ROKOVIMA PREDVIĐENIM PROPISIMA KOJI UREĐUJU KANCELARIJSKO POSLOVANjE.

U CILjU OBEZBEĐIVANjA KONTINUITETA RADA JEDINSTVENOG MESTA ZA PRUŽANjE SAVETA I PRIJEM PRIJAVA U VEZI BEZBEDNOSTI DECE NA INTERNETU, NADLEŽNI ORGAN TREBA DA:

1) BUDE OPREMLjEN SA ODGOVARAJUĆIM SISTEMIMA ZA PRIJEM PRIJAVA;

2) IMA DOVOLjNO ZAPOSLENIH KAKO BI SE OSIGURALA DOSTUPNOST U RADU;

3) OBEZBEDI INFRASTRUKTURU ČIJI JE KONTINUITET OSIGURAN.

VLADA BLIŽE UREĐUJE NAČIN SPROVOĐENjA MERA ZA BEZBEDNOST I ZAŠTITU DECE NA INTERNETU IZ ST. 1. I 3. OVOG ČLANA.

VI. KAZNENE ODREDBE

~~Član 30~~

~~Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice ako:~~

~~1) ne donese Akt o bezbednosti IKT sistema iz člana 8. stav 1. ovog zakona;~~

~~2) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 8. stav 2. ovog zakona;~~

~~3) ne izvrši proveru usklađenosti primenjenih mera iz člana 8. stav 4. ovog zakona;~~

~~4) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 29. stav 1. tačka 1. ovog zakona.~~

~~Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.~~

ČLAN 30.

NOVČANOM KAZNOM U IZNOSU OD 50.000,00 DO 2.000.000,00 DINARA KAZNIĆE SE ZA PREKRŠAJ OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA AKO:

1) NE IZVRŠI UPIS U EVIDENCIJU U ROKU IZ ČLANA 6B STAV 4. OVOG ZAKONA;

2) NE DONESE AKT O BEZBEDNOSTI IKT SISTEMA IZ ČLANA 8. STAV 1. OVOG ZAKONA;

3) NE PRIMENI MERE ZAŠTITE ODREĐENE AKTOM O BEZBEDNOSTI IKT SISTEMA IZ ČLANA 8. STAV 2. OVOG ZAKONA;

4) NE IZVRŠI PROVERU USKLAĐENOSTI PRIMENjENIH MERA IZ ČLANA 8. STAV 4. OVOG ZAKONA;

5) NE DOSTAVI STATISTIČKE PODATKE IZ ČLANA 11B STAV 1. OVOG ZAKONA;

6) NE POSTUPI PO NALOGU INSPEKTORA ZA INFORMACIONU BEZBEDNOST U OSTAVLjENOM ROKU IZ ČLANA 29. STAV 1. TAČKA 1. OVOG ZAKONA.

ZA PREKRŠAJ IZ STAVA 1. OVOG ČLANA KAZNIĆE SE I ODGOVORNO LICE U OPERATORU IKT SISTEMA OD POSEBNOG ZNAČAJA NOVČANOM KAZNOM U IZNOSU OD 5.000,00 DO 50.000,00 DINARA.

~~Član 31~~

~~Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice ako o incidentima u IKT sistemu ne obavesti Nadležni organ, odnosno organ nadležan za obezbeđenje primene standarda u oblasti zaštite tajnih podataka, Narodnu banku Srbije ili regulatorno telo za elektronske komunikacije (član 11. st. 1. i 2.).~~

~~Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.~~

ČLAN 31.

NOVČANOM KAZNOM U IZNOSU OD 50.000,00 DO 500.000,00 DINARA KAZNIĆE SE ZA PREKRŠAJ OPERATOR IKT SISTEMA OD POSEBNOG ZNAČAJA AKO:

1) O INCIDENTIMA U IKT SISTEMU NE OBAVESTI ORGANE IZ ČLANA 11. ST. 1, 3. I 7. OVOG ZAKONA;

2) NE DOSTAVLjA OBAVEŠTENjA O BITNIM DOGAĐAJIMA U VEZI SA INCIDENTOM I AKTIVNOSTIMA IZ ČLANA 11. STAV 5. OVOG ZAKONA;

3) NE DOSTAVI ZAVRŠNI IZVEŠTAJ U ROKU IZ ČLANA 11. STAV 6. OVOG ZAKONA.

ZA PREKRŠAJE IZ STAVA 1. OVOG ČLANA KAZNIĆE SE I ODGOVORNO LICE U OPERATORU IKT SISTEMA OD POSEBNOG ZNAČAJA NOVČANOM KAZNOM U IZNOSU OD 5.000,00 DO 50.000,00 DINARA.

IZUZETNO OD ST. 1. I 2. OVOG ČLANA, AKO FINANSIJSKA INSTITUCIJA NE OBAVESTI NARODNU BANKU SRBIJE O INCIDENTIMA U IKT SISTEMU OD POSEBNOG ZNAČAJA, NARODNA BANKA SRBIJE IZRIČE TOJ FINANSIJSKOJ INSTITUCIJI MERE I KAZNE U SKLADU SA ZAKONOM KOJIM SE UREĐUJE NjENO POSLOVANjE.

VI. ANALIZA EFEKATA ZAKONA O IZMENAMA I DOPUNAMA ZAKONA O INFORMACIONOJ BEZBEDNOSTI

1) Koji pokazatelji se prate u oblasti, koji su razlozi zbog kojih se ovi pokazatelji prate i koje su njihove vrednosti?

U oblasti informacione bezbednosti pokazatelji koji se prate odnose se na:

- primenu mera od bezbednosnih rizika u informaciono-komunikacionim sistemima i
- incidente koji značajno ugrožavaju informacionu bezbednost, a kojima su izloženi IKT sisteme pod posebnog značaja.

Naime, Zakonom i informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16 i 94/17) (u daljem tekstu: Zakon) definisani su operatori IKT sistema od posebnog značaja, kao i mere zaštite, odnosno tehničke i organizacione mere koje su operatori IKT sistemi od posebnog značaja u obavezi da primenjuju, a u cilju održavanja adekvatnog nivoa bezbednosti sistema.

Shodno tome, operatori IKT sistema od posebnog značaja dužni su da donesu akt o bezbednosti IKT sistema i definišu mere zaštite, a naročito principe, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja.

Inspekcijskim nadzorom nad radom operatora IKT sistema od posebnog značaja utvrđuje se da li su operatori doneli akt o bezbednosti i primenili mere zaštite, odnosno da li je uspostavljen adekvatan nivo bezbednosti sistema. Inspekcijski nadzor do sada nije vršen, budući da je prvi inspektor u novoformiranoj inspekciji za informacionu bezbednost zaposlen u drugoj polovini 2018. godine i, shodno tome, inspekcijski nadzor se sprovodi od 2019. godine.

Operatori IKT sistema od posebnog značaja u skladu sa Zakonom obavezni su da obaveste Nadležni organ, odnosno Ministarstvo trgovine, turizma i telekomunikacija o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

Na osnovu prijavljenih incidenata Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT) reaguje po prijavljenim ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja. Nacionalni CERT na osnovu prijavljenih incidenata prati trendove u ovoj oblasti i kontinuirano izrađuje analize rizika i incidenata. Prema izveštajima Nacionalnog CERT-a u 2017. godini prijavljeno je 17 incidenata koji značajno ugrožavaju informacionu bezbednost, a u 2018. godini ukupno 31 incident.

2) Da li se u predmetnoj oblasti sprovodi ili se sprovodio dokument javne politike ili propis? Predstaviti rezultate sprovođenja tog dokumenta javne politike ili propisa i obrazložiti zbog čega dobijeni rezultati nisu u skladu sa planiranim vrednostima.

U predmetnoj oblasti na snazi je Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine („Službeni glasnik RS”, broj 53/17), kao i akcioni plan za 2018. i 2019. godinu kojim se bliže definišu aktivnosti predviđene ovom strategijom. U skladu sa navedenim dokumentima, u prethodnom periodu sprovedene su sledeće aktivnosti u okviru strateških prioriteta:

1) Bezbednost informaciono-komunikacionih sistema, što se odnosi na rizike narušavanja funkcionisanja organa vlasti, privrede i organizacija kao posledica incidenata u informaciono-komunikacionim sistemima:

- uspostavljeno je Vladino Telo za koordinaciju poslova informacione bezbednosti u Republici Srbiji, koje čine predstavnici organa čiji su poslovi od značaja za informacionu bezbednost;
- uspostavljen je Nacionalni CERT u okviru RATEL-a;
- uspostavljen je CERT republičkih organa, kao i CERT-ovi samostalnih operatora IKT sistema;
- registrovano je 6 posebnih CERT-ova;
- uspostavljen je jedinstveni sistem za prijem obaveštenja o incidentima u IKT sistemima od posebnog značaja;
- formirana je inspekcija za informacionu bezbednost u Ministarstvu trgovine, turizma i telekomunikacija;
- Nacionalni CERT i CERT MUP akreditovani su na „Trusted Introducer" listi.

2) informaciona bezbednost građana, što se odnosi na rizike narušavanja bezbednosti građana zloupotrebom informaciono-komunikacionih tehnologija:

- U februaru 2017. godine Ministarstvo trgovine, turizma i telekomunikacija je osnovalo Nacionalni kontakt centar za bezbednost dece na internetu. Putem Nacionalnog kontakt centra za bezbednost dece na internetu, pored savetovanja, omogućava se i prijem prijava štetnog, neprimerenog i nelegalnog sadržaja i ponašanja na internetu, odnosno ugroženosti interesa i prava dece, telefonskim putem i putem elektronskog obrasca na veb sajtu. Počev od osnivanja, ukupna komunikacija registrovana u Nacionalnom kontakt centru za bezbednost dece na internetu ostvarena putem telefonskih poziva, mejlova, prijava putem sajta i društvenih mreža od osnivanja iznosi 7.965.
- Radi unapređenja saradnje i razmene ideja, operateri/edukatori Nacionalnog kontakt centra za bezbednost dece na internetu održali su do danas prezentacije na temu bezbednosti dece na internetu i to:
    - Za 150 zaposlenih u domovima zdravlja (direktorima, pedijatrima školskih dispanzera i psiholozima) i
    - Za 12.405 dece i 4.335 roditelja u 112 osnovnih škola
- Od 2016. godine Ministarstvo trgovine, turizma i telekomunikacija svake godine sprovodi „IT karavan", edukativnu kampanju za promociju korisne, kreativne i bezbedne upotrebe informacionih tehnologija. i uključuje edukaciju o bezbednosti dece na internetu (predstave za decu, interaktivni razgovori sa decom kroz ilustrativne primere, takmičarski kviz i sl.). IT karavan, održana je četvrtu godinu za redom u 2019. godini. Do sada je ovom kampanjom obuhvaćeno ukupno 58 osnovnih škola, više od 11.000 đaka, a direktan prenos prezentacije, koji je prethodne godine organizovan iz Niša i Novog Pazara, pratilo je putem interneta još oko 800 škola.

3) borba protiv visokotehnološkog kriminala, što se odnosi na prevenciju i sankcionisanje krivičnih dela koja se zasnivaju na zloupotrebi informaciono-komunikacionih tehnologija;

- Republika Srbija je potpisnica Konvencije o visokotehnološkom kriminalu, Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, kao i Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja.
- Republika Srbija je učestvovala u projektu „Saradnja u borbi protiv kriminala u sajber prostoru: ciljanje imovine stečene kriminalom na internetu u Jugoistočnoj Evropi i Turskoj"; naučno-istraživačkom projektu „Advanced Tools for fighting online illegal trafficking – ANITA (787061)" u sklopu Horizon 2020; projektu Evropske unije i Saveta Evrope iPROCEEDS@IPA koji ima za cilj osposobljavanje i jačanje kapaciteta državnih organa nadležnih za borbu protiv visokotehnološkog kriminala u Republici Srbiji i zemljama u regionu u postupcima oduzimanja imovine u predmetima visokotehnološkog kriminala.
- Prema podacima Posebnog odeljenja za borbu protiv visokotehnološkog kriminala u proteklih pet godina na teritoriji Republike Srbije (period 2013–2017. godina) stopa kriminala je u porastu.

4) informaciona bezbednost Republike Srbije, što se odnosi na rizike narušavanja nacionalne bezbednosti putem informaciono-komunikacionih sistema;

- Od 2016. godine u Republici Srbiji organizuju se na godišnjem nivou sajber vežbe „Sajber Tesla" u saradnji Vojske Srbije i Nacionalne garde Ohaja.
- U cilju podizanja kapaciteta zaposlenih u CERT-ovima u Republici Srbiji, uključujući i CERT-ove samostalnih operatora, u okviru projekta „Unapređenje informacione bezbednosti" na Zapadnom Balkanu organizovane su treninzi i obuke.

5) međunarodna saradnja, što podrazumeva saradnju sa stranim državnim organima, međunarodnim organizacijama i drugim partnerima u oblasti informacione bezbednosti.

- Republika Srbija postala član Globalnog foruma za sajber ekspertizu u 2018. godini;
- Republika Srbija aktivno učestvuje u radu neformalne radne grupe OEBS za definisanje mera poverenja u sajber prostoru;
- Republika Srbija učestvovala u radu Grupe UN za informacionu bezbednost u 2017. godini.

3) Da li su uočeni problemi u oblasti i na koga se oni odnose? Predstaviti uzroke i posledice problema.

Članom 6. Zakona definisani su IKT sistemi od posebnog značaja i podeljeni su u tri grupe i to:

1) IKT sistemi koji se koriste u obavljanju poslova u organima javne vlasti;

2) IKT sistemi koji se koriste za obradu podataka koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti;

3) IKT sistemi koji se koriste u obavljanju delatnosti od opšteg interesa.

Međutim, tokom implementacije Zakona utvrđeno je da navedenom definicijom obuhvaćen veliki broj organa javne vlasti, čiji sistemi po svom značaju ne spadaju u IKT sisteme od posebnog značaja. Budući da primena mera zaštite podrazumeva primenu tehničkih i organizacionih mera, za čiju primenu su potrebna finansijska ulaganja, ovi sistemi su bili u obavezi da svoje sisteme unaprede, odnosno primene mere zaštite, međutim, predloženom izmenom Zakona, predviđeno je smanjenje broja IKT sisteme koji se koriste u organima javne vlasti, jer je utvrđeno da ti sistemi nisu od posebnog značaja za informacionu bezbednost u Republici Srbiji.

Tokom implementacije Zakona utvrđeno je da IKT sistemi od posebnog značaja ne dostavljaju informacije o incidentima koji značajno ugrožavaju informacionu bezbednost, iako su obavezni da to čine. Usled toga Nacionalni CERT nije u mogućnosti da prati trendove u ovoj oblasti, niti da izrađuje analize rizika i incidenata na osnovu kojih bi se pružali saveti i predlagale mere za otklanjanja potencijalnih incidenata.

U skladu sa Zakonom predviđeno je osnivanje Nacionalnog CERT, međutim, iako je Nacionalni CERT osnovan, potrebno je i dalje ulagati u njegove kapacitete u smislu tehničkih, organizacionih i ljudskih kapaciteta. Naime, kako bi Nacionalni CERT bio u mogućnosti da pruža adekvatnu podršku IKT sistemima od posebnog značaja u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost postojeći resursi nisu dovoljni, jer pored opreme, neophodno je da se Nacionalni CERT osnaži i zaposli stručnjake u ovoj oblasti. U suprotnom, može se nastaviti trend neprijavljivanja incidenata u IKT sistemima od posebnog značaja, usled čega nije moguće pratiti kretanja u ovoj oblasti, niti predlagati mere za njeno unapređenje.

Kako je u skladu sa Zakonom predviđen rad kako Nacionalnog CERT, tako i CERTa republičkih organa i CERTova samostalnih operatora IKT sistema, u prethodnom periodu je konstatovano da ne postoji zakonski osnov za njihovu sistemsku saradnju koja bi omogućavala razmenu informacija i međusobno pružanje podrške u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost.

4) Koja promena se predlaže i da li je promena zaista neophodna i u kom obimu?

Izmene Zakona su inicirane iz razloga što je Zakon stupio na snagu pre usvajanja Direktive EU o merama za visok nivo bezbednosti mrežnih i informacionih sistema u Evropskoj uniji broj 2016/1148 (u daljem tekstu: NIS direktiva), koja je usvojena u julu 2016. godine. Iako je bio donet pre usvajanja NIS direktive, Zakon je u velikoj meri usklađen sa ovom direktivom, budući da sadrži rešenja koja odgovaraju odredbama navedene direktive.

Međutim, izradi Predloga zakona o izmenama i dopunama Zakona o informacionoj bezbednosti (u daljem tekstu: Predlog zakona) pristupilo se prvenstveno iz dva razloga: prvi je preostalo usklađivanje sa odredbama NIS direktive radi postizanja potpune usaglašenosti Zakona, a drugi je unapređenje postojećih zakonodavnih rešenja na bazi potreba utvrđenih na osnovu dosadašnje primene.

Radi preostalih usklađivanja sa NIS direktivom, u Predlogu zakona izvršene su sledeće izmene i dopune:

- dopuna oblasti u kojima se koriste IKT sistemi od posebnog značaja, i to oblast digitalne infrastrukture i usluga informacionog društva (član 6.);
- određeno je da se pre javnog objavljivanja obaveštenja o incidentu od strane nadležnog organa izvrše prethodne konsultacije sa operatorom IKT sistema od posebnog značaja koji je dostavio obaveštenje o incidentu (član 11.);
- predviđena je dopuna odredaba o Nacionalnom CERT-u koje se odnose na njegovu nadležnost i potrebne kapacitete (član 15.).

Tokom primene zakona utvrđena je potreba za izmenom i dopunom određenih normi, u cilju efikasnijeg sprovođenja zakona u praksi. Shodno tome, Predlogom zakona predviđeno je sledeće:

- uključivanje Narodne banke Srbije u rad Tela za koordinaciju poslova informacione bezbednosti (član 5.);
- dopuna oblasti u kojima se koriste IKT sistemi od posebnog značaja (proizvodnja i snabdevanje hemikalijama, član 6.);
- taksativno su nabrojane obaveze IKT sistema od posebnog značaja (član 6a);
- uspostavljanje Evidencije operatora IKT sistema od posebnog značaja (član 6b);
- definisan je način obaveštavanja o incidentima koji značajno ugrožavaju informacionu bezbednost preko portala Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima (član 11.);
- obaveza Narodne banke Srbije i RATEL-a da dobijena obaveštenja o incidentu proslede Nadležnom organu (član 11.);
- dostavljanje obaveštenja o incidentu koji je povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje nacionalne bezbednosti, Bezbednosno-informativnoj agenciji (član 11.);
- definisani su incidenti koji treba da se prijave, a koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (član 11a);
- određena je obaveza IKT sistema od posebnog značaja da dostavljaju statističke podatke o incidentima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (član 11b);
- definisana je saradnja CERT-ova u Republici Srbiji (član 15a);
- dodate su odredbe o zaštiti pri korišćenju informaciono-komunikacionih tehnologija (član 19a).

Navedene izmene zakona doprineće boljoj povezanosti svih relevantnih aktera u oblasti informacione bezbednosti, budući da se Predlogom zakona predviđa uspostavljanje evidencije IKT sistema od posebnog značaja. Na taj način Nadležni organ i Nacionalni CERT imaće mogućnost intenzivnije saradnje sa svim operatorima IKT sistema od posebnog značaja, naročito u slučaju kada se dešava incident, ali u

smislu pružanja podrške, preporuke i saveta za zaštitu IKT sistema od posebnog značaja.

Značajno unapređenje leži i u činjenici da je Nadležni organ uspostavio Jedinstveni sistem za prijem obaveštenja o incidentima, tako da ih IKT sistemi od posebnog značaja obaveštenja mogu prosleđivati preko portala Nadležnog organa i Nacionalnog CERT-a. Ovo rešenje doprinosi efikasnosti prijavljivanja incidenata, kao i potpunoj informisanosti svih relevantnih učesnika (Nadležni organ, Nacionalni CERT) koji potom mogu da učestvuju u otklanjanju incidenta.

Takođe, Predlog zakona predviđa odredbe o Nacionalnom CERT-u koje se odnose na jačanje kapaciteta Nacionalnog CERT-a, kako bi se uspostavilo blagovremena i efikasna podrška u slučaju incidenta, a za takvu vrstu podrške neophodno je stručno osoblje, odgovarajuća infrastruktura u smislu opreme i prostorija za rad, čije obezbeđivanje je predviđeno Predlogom zakona. Kako Nacionalni CERT ima i ulogu prevencije u oblasti informacione bezbednosti, predviđeno je dostavljanje statističkih podataka od strane IKT sistema od posebnog značaja na bazi kojih će Nacionalni CERT imati mogućnost izrade adekvatnih analiza u oblasti informacione bezbednosti i na osnovu čega će pripremati preporuke i savete za mere zaštite u ovoj oblasti.

S obzirom da je prepoznata potreba za kontinuiranom saradnjom CERT-ova u Republici Srbiji, predviđene su odredbe kojima se definiše ova saradnja kroz organizaciju redovnih zajedničkih sastanaka, a posebno u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

Imajući u vidu važnost pitanja bezbednosti na internetu, Predlogom zakona definisane su odredbe kojima se predviđaju mere za bezbednost i zaštitu na internetu, kao i generalno prilikom korišćenja informaciono-komunikacionih tehnologija.

5) Na koje ciljne grupe će uticati predložena promena? Utvrditi i predstaviti ciljne grupe na koje će promena imati neposredan odnosno posredan uticaj.

Izmene i dopune Zakona imaće neposredan uticaj na:

- IKT sisteme od posebnog značaja;
- Nacionalni CERT;
- nove IKT sisteme od posebnog značaja u oblast digitalne infrastrukture i usluga informacionog društva
- CERTove samostalnih operatora IKT sistema.

6) Zbog čega je neophodno postići željenu promenu na nivou društva? (odgovorom na ovo pitanje definiše se opšti cilj).

Izmene i dopune Zakona su neophodne prvenstveno radi potpunog usklađivanja sa NIS direktivom, a potom radi bolje povezanosti svih relevantnih aktera u oblasti informacione bezbednosti, čime se doprinosi adekvatnijem nivou bezbednosti informacionih sistema od posebnog značaja u Republici Srbiji.

7) Šta se predmetnom promenom želi postići? (odgovorom na ovo pitanje definišu se posebni ciljevi, čije postizanje treba da dovode do ostvarenja opšteg cilja. U odnosu na posebne ciljeve, formulišu se mere za njihovo postizanje).

Izmenama i dopunama Zakona postiže se uspostavljanje evidencije o IKT sistemima od posebnog značaja, što će doprineti boljoj komunikaciji između

Ministarstva i Nacionalnog CERTa sa jedne strane i IKT sistema od posebnog značaja sa druge strane.

Navedena evidencija biće uspostavljena u Ministarstvu kao nadležnom organu za informacionu bezbednost koje poseduje kapacitete za vođenje ove evidencije, budući da Ministarstvo već vodi različite vrste registara iz oblasti elektronskog poslovanja.

Takođe se predviđa jačanje kapaciteta Nacionalnog CERTa i to tehnoloških, ljudskih i organizacionih kapaciteta, što će Nacionalnom CERTu omogućiti prelazak sa informativne i savetodavne uloge na operativniju ulogu. Pružajući adekvatniju pomoć IKT sistemima od posebnog značaja u slučaju prijavljenih incidenata, pospešiće se međusobna saradnja i stvoriti poverenje što će posledično dovesti do toga da IKT sistemi od posebnog značaja prijavljuju incidente u skladu sa Zakonom.

Obavezivanjem IKT sistema od posebnog značaja da dostavljaju statističke podatke o svim incidentima koji se dešavaju u njihovim sistemima, Nacionalni CERT će biti u mogućnosti da prati trendove u ovoj oblasti i priprema analize rizika i incidenata na osnovu kojih bi se pružali saveti i predlagale mere za otklanjanje potencijalnih incidenata.

Predviđena saradnja između CERTova u Republici Srbiji omogućiće razmenu informacija i međusobno pružanje podrške u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost.

8) Da li su opšti i posebni ciljevi usklađeni sa važećim dokumentima javnih politika i postojećim pravnim okvirom, a pre svega sa prioritetnim ciljevima Vlade?

Strategijom razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine neki od predviđenih prioritetnih oblasti informacione bezbednosti u skladu su sa opštim i posebnim ciljevima koji se postižu izmenama i dopunama Zakona, i to:

- bezbednost informaciono-komunikacionih sistema, što se odnosi na rizike narušavanja funkcionisanja organa vlasti, privrede i organizacija kao posledica incidenata u informaciono-komunikacionim sistemima i
- informaciona bezbednost Republike Srbije, što se odnosi na rizike narušavanja nacionalne bezbednosti putem informaciono-komunikacionih sistema.

9) Na osnovu kojih pokazatelja učinka će biti moguće utvrditi da li je došlo do ostvarivanja opštih odnosno posebnih ciljeva?

Osnovni pokazatelji učinka izmena i dopuna Zakona ogledaju se u sledećem:

- uspostavljena evidencija IKT sistema od posebnog značaja
- uspostavljen sistem dostave statističkih podataka od strane IKT sistema od posebnog značaja
- uspostavljena saradnja između CERTova u Republici Srbiji.

Na osnovu gore navedenih pokazatelja, uspostaviće se Evidencija IKT sistema od posebnog značaja, što će omogućiti koordinaciju sa IKT sistemima od posebnog značaja i dati mogućnost za preispitivanje obuhvata IKT sistema od posebnog značaja i na bazi toga formiranje dodatnih kriterijuma za njihovo utvrđivanje.

Na osnovu dostavljenih statističkih podataka, biće omogućeno ispunjavanje zakonskih odredbi koji se tiču praćenja stanja u oblasti informacione

bezbednosti i izrada neophodnih analiza u ovoj oblasti, a cilju unapređenja stanja u IKT sistemima od posebnog značaja.

Uvođenjem mehanizma saradnje između CERT-ova u Republici Srbiji doprinosi se većem stepenu zaštite IKT sistema u svim oblastima u Republici Srbiji i boljoj koordinaciji u slučaju incidenata koji mogu da ugroze informacionu bezbednost, ali i nacionalnu bezbednost Republike Srbije.

10) Da li je finansijske resurse za sprovođenje izabrane opcije potrebno obezbediti u budžetu, ili iz drugih izvora finansiranja i kojih?

Sredstva potrebna za realizaciju obaveza iz Predloga zakona nije potrebno obezbediti u budžetu, budući da će ista biti obezbeđena iz sredstava RATELa, za potrebe podizanja kapaciteta Nacionalnog CERTa.

11) Koliki su procenjeni troškovi uvođenja promena koji proističu iz sprovođenja izabrane opcije (osnivanje novih institucija, restrukturiranje postojećih institucija i obuka državnih službenika) iskazani u kategorijama kapitalnih troškova, tekućih troškova i zarada i da li je moguće finansirati rashode izabrane opcije kroz redistribuciju postojećih sredstava?

Budući da je NIS direktivom predviđeno povećavanje kapaciteta Nacionalnog CERTa u narednom periodu predviđa se povećavanje broja zaposlenih kao i kupovina neophodne opreme. U tom smislu troškovi povećanja kapaciteta Nacionalnog CERTa bi bili sledeći:

- 150.000 evra za nabavku platforme za uvežbavanje sajber napada radi promovisanja informacione bezbednosti;
- 10.000 evra u periodu od tri godine za nabavku forenzičke laboratorije;
- 20.000 evra u periodu od tri godine za nabavku softver za sajber bezbednost i prateće licence;
- 15.000 evra u periodu od tri godine za nabavku hardvera;
- 144.000 evra u periodu od tri godine dana iznos zarade za 5 novozaposlenih (5 x zaposlenih x 800 evra x 3 godine);
- 90.000 evra u periodu od tri godine za obuke za zaposlene (10 zaposlenih x 3.000 evra x 3 godine)

12) Koje troškove i koristi (materijalne i nematerijalne) će izabrana opcija prouzrokovati privredi, pojedinoj grani, odnosno određenoj kategoriji privrednih subjekata?

Novi IKT sistemi od posebnog značaja u oblasti digitalne infrastrukture i usluga informacionog društva koji su predviđeni izmenama i dopunama Zakona su u obavezi da primene mere zaštite, odnosno tehničke i organizacione mere u cilju uspostavljanja adekvatnog nivoa bezbednosti sistema.

Ukoliko su ti privredni subjekti već uspostavili sistem upravljanja informacionom bezbednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primena zakona izazove značajne troškove. Međutim, privredni subjekti koji predstavljaju operatore IKT sistema od posebnog značaja u skladu sa izmenama Zakona, a koji do sada nisu uspostavili odgovarajući sistem upravljanja informacionom bezbednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično. Precizni iznosi dodatnih troškova za navedene subjekte variraju u velikom rasponu, budući da isti zavise od više faktora koji mogu da budu veoma različiti u različitim

privrednim subjektima. Naime, koliko će finansijskih sredstava za primenu zakona izdvojiti ovi privredni subjekti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbednosti, i drugih faktora od kojih funkcionisanje informacione bezbednosti zavisi u jednom privrednom subjektu. Shodno navedenom, nije moguće dati ni tačne, ni okvirne iznose po privrednom subjektu.

13) Da li je za sprovođenje izabrane opcije obezbeđena podrška svih ključnih zainteresovanih strana i ciljnih grupa? Da li je sprovođenje izabrane opcije prioritet za donosioce odluka u narednom periodu (Narodnu skupštinu, Vladu, državne organe i slično)?

Ministarstvo trgovine, turizma i telekomunikacija je u 2018. godini formiralo radnu grupu za izradu Nacrta zakona o izmenama i dopunama Zakona o informacionoj bezbednosti koga su činili predstavnici relevantnih ministarstava i institucija.

Ministarstvo trgovine, turizma i telekomunikacija sprovelo je javnu raspravu o Nacrtu zakona o izmenama i dopunama Zakona o informacionoj bezbednosti u periodu od 04. do 25. februara 2019. godine, na osnovu zaključka Odbora za privredu i finansije Vlade 05 Broj: 011-882/2019 od 31. januara 2019. godine. Nacrt zakona je objavljen na sajtu Ministarstva trgovine, turizma i telekomunikacija www.mtt.gov.rs i portalu eUprava www.euprava.gov.rs. U okviru javne rasprave, održan je okrugli sto u Privrednoj komori Srbije 20. februara 2019. godine, koji je bio veoma uspešan i posećen. U javnoj raspravi učestvovali su predstavnici državnih organa, privrednog sektora, akademske zajednice, nevladinih organizacija i eminentni stručnjaci u ovoj oblasti. Ministarstvo je po okončanju javne rasprave putem Ministarstva za evropske integracije uputilo Nacrt zakona Evropskoj komisiji, radi davanja mišljenja.

Donošenje ovog zakona je prioritet imajući u vidu činjenicu da se istim vrši usklađivanje sa evropskom regulativom, odnosno NIS direktivom.

14) Koje dodatne mere treba sprovesti i koliko vremena će biti potrebno da se sprovede izabrana opcija i obezbedi njeno kasnije dosledno sprovođenje, odnosno njena održivost?

Radi realizacije Predloga zakona, predviđeno je donošenje sledećih podzakonskih akata:

- Uredba o utvrđivanju Liste delatnosti u kojima se koriste IKT sistemi od posebnog značaja;
- Uredba o postupku obaveštavanja o incidentima, listi, vrstama i značaju incidenata prema nivou opasnosti, postupanje i razmeni informacija o incidentima
- Pravilnik o evidenciji IKT sistema od posebnog značaja;
- Pravilnik o statističkim podacima o incidentima u IKT sistemima od posebnog značaja
- Uredba o načinu sprovođenja mera za bezbednost i zaštitu dece na internetu.

15) Da li su obezbeđena finansijska sredstva za sprovođenje izabrane opcije? Da li je za sprovođenje izabrane opcije obezbeđeno dovoljno vremena za sprovođenje postupka javne nabavke ukoliko je ona potrebna?

Sredstva za realizaciju zakonskih obaveza obezbeđuje RATEL, kao organizacija u čijem se sastavu nalazi Nacionalni CERT. Očekuje se da će u budžetu navedene institucije počev od 2020. godine biti obezbeđena sredstva potrebna za dodatno zapošljavanje kao i za kupovinu neophodne opreme.

OBRAZAC IZJAVE O USKLAĐENOSTI PROPISA SA PROPISIMA EVROPSKE UNIJE

1. Organ državne uprave, odnosno drugi ovlašćeni predlagač propisa: Vlada
   Obrađivač: Ministarstvo trgovine, turizma i telekomunikacija

2. Naziv propisa

Predlog zakona o izmenama i dopunama Zakona o informacionoj bezbednosti
Draft Law on Amendments to the Law on Information Security

3. Usklađenost propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane, i Republike Srbije sa druge strane („Službeni glasnik RS”, broj 83/08) (u daljem tekstu: Sporazum):

a) Odredba Sporazuma koja se odnose na normativnu sadržinu propisa

Član 105. Informaciono društvo - Sporazum o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane, i Republike Srbije sa druge strane.

b) Prelazni rok za usklađivanje zakonodavstva prema odredbama Sporazuma

Tri godine.

v) Ocena ispunjenosti obaveze koje proizlaze iz navedene odredbe Sporazuma

Ispunjava u potpunosti.

g) Razlozi za delimično ispunjavanje, odnosno neispunjavanje obaveza koje proizlaze iz navedene odredbe Sporazuma
/
d) Veza sa Nacionalnim programom za usvajanje pravnih tekovina Evropske unije

Nacionalni program za usvajanje pravnih tekovina Evropske unije, Prilog A – Plan usklađivanja zakonodavstva Republike Srbije sa pravnim tekovinama Evropske unije, 3.10. Informaciono društvo i mediji, 3.10.2. Informaciono društvo, Redni broj 1, Šifra plan. propisa: 2017-510

4. Usklađenost propisa sa propisima Evropske unije:

a) Navođenje odredbi primarnih izvora prava Evropske unije i ocene usklađenosti sa njima
/
b) Navođenje sekundarnih izvora prava Evropske unije i ocene usklađenosti sa njima

Direktiva EU o merama za visok nivo bezbednosti mrežnih i informacionih sistema u Evropskoj uniji broj 2016/1148 (NIS direktiva) koja je usvojena u julu 2016. godine.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

v) Navođenje ostalih izvora prava Evropske unije i usklađenost sa njima
/

g) Razlozi za delimičnu usklađenost, odnosno neusklađenost
/
d) Rok u kojem je predviđeno postizanje potpune usklađenosti propisa sa propisima Evropske unije
/
5. Ukoliko ne postoje odgovarajuće nadležnosti Evropske unije u materiji koju reguliše propis, i/ili ne postoje odgovarajući sekundarni izvori prava Evropske unije sa kojima je potrebno obezbediti usklađenost, potrebno je obrazložiti tu činjenicu. U ovom slučaju, nije potrebno popunjavati Tabelu usklađenosti propisa. Tabelu usklađenosti nije potrebno popunjavati i ukoliko se domaćim propisom ne vrši prenos odredbi sekundarnog izvora prava Evropske unije već se isključivo vrši primena ili sprovođenje nekog zahteva koji proizilazi iz odredbe sekundarnog izvora prava (npr. Predlogom odluke o izradi strateške procene uticaja biće sprovedena obaveza iz člana 4. Direktive 2001/42/EZ, ali se ne vrši i prenos te odredbe direktive).
/

6. Da li su prethodno navedeni izvori prava Evropske unije prevedeni na srpski jezik?
/
7. Da li je propis preveden na neki službeni jezik Evropske unije?

Predlog zakona o izmenama i dopunama Zakona o informacionoj bezbednosti preveden je na engleski jezik.

8. Saradnja sa Evropskom unijom i učešće konsultanata u izradi propisa i njihovo mišljenje o usklađenosti

Predlog zakona o izmenama i dopunama Zakona o informacionoj bezbednosti poslat je na mišljenje Evropskoj komisiji.

1. Naziv propisa Evropske unije : Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	2. „CELEX" oznaka EU propisa 32016L1148
3. Organ državne uprave, odnosno drugi ovlašćeni predlagač propisa: Vlada	4. Datum izrade tabele:
Obrađivač: Ministarstvo trgovine, turizma i telekomunikacija	25.3.2019.
5. Naziv (nacrta, predloga) propisa čije odredbe su predmet analize usklađenosti sa propisom Evropske unije: Predlog zakona o izmenama i dopunama Zakona o informacionoj bezbednosti	6. Brojčane oznake (šifre) planiranih propisa iz baze NPAA: 2017-510
7. Usklađenost odredbi propisa sa odredbama propisa EU:	

a)	a1)	b)	b1)	v)	g)	d)
Odredba propisa EU	Sadržina odredbe	Odredbe propisa R. Srbije	Sadržina odredbe	Usklađenost[1]	Razlozi za delimičnu usklađenost, neusklađenost ili neprenosivost	Napomena o usklađenosti
1.1.	This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.			NP	Odredba je neprenosiva, s obzirom da se njome određuje predmet EU direktive.	
1.2.	To that end, this Directive: (a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;			NP	Odredba je neprenosiva, s obzirom da se njome određuje predmet EU direktive.	

[1] Potpuno usklađeno - PU, delimično usklađeno - DU, neusklađeno - NU, neprenosivo – NP

a)	a1)	b)	b1)	v)	g)	d)
	(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; (c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; (d) establishes security and notification requirements for operators of essential services and for digital service providers; (e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.					
1.3.	The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.			NP	Odredba je neprenosiva, s obzirom da se njom određuje primena EU direktive.	
1.4.	This Directive applies without prejudice to Council Directive 2008/114/EC (14) and Directives 2011/93/EU (15) and 2013/40/EU (16) of the European Parliament and of the Council.			NP	Odredba je neprenosiva, s obzirom da se njom određuje primena EU direktive.	
1.5.	Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union			NP	Odredba je neprenosiva, s obzirom da reguliše razmenu poverljivih	

a)	a1)	b)	b1)	v)	g)	d)
	and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.				informacija država članica EU sa Evropskom komisijom i drugim telima EU.	
1.6.	This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.			NP	Odredba je neprenosiva, s obzirom da reguliše razmenu poverljivih informacija država članica EU sa Evropskom komisijom i drugim telima EU.	
1.7.	Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.			NP	Odredba je neprenosiva, jer se njome određuje da drugi akti EU koji propisuju mere zaštite IKT sistema i obaveštavanje o incidentima u IKT sistemima za pojedine oblasti treba da propišu odredbe koje zahtevaju najmanje jednak nivo obaveza kao NIS direktiva.	
2.1.	Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.	3a	U slučaju obrade podataka o ličnosti prilikom vršenja nadležnosti i ispunjenja obaveza iz ovog zakona postupa se u skladu sa	PU		

a)	a1)	b)	b1)	v)	g)	d)
			propisima koji uređuju zaštitu podataka o ličnosti.			
2.2.	Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.			NP	Odredba propisuje obradu ličnih podatke od strane institucija i tela EU.	
3.	Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.			NP	Odredba se odnosi na davanje mogućnosti državama članicama EU da svojim propisima odrede viši nivo bezbednosti IKT sistema.	
4.1.	'For the purposes of this Directive, the following definitions apply: network and information system' means:	2.1.1.	Pojedini termini u smislu ovog zakona imaju sledeće značenje: informaciono -komunikacioni sistem (IKT sistem) je tehnološko -organizaciona celina koja obuhvata:	PU		
4.1.a)	an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;	2.1.1.1.	elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije	PU		
4.1.b)	any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or	2.1.1.2.	uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem	PU		

a)	a1)	b)	b1)	v)	g)	d)
			računarskog programa;			
4.1.c)	digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	2.1.1.3.	podatke koji se vode, čuvaju, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ove tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja.	PU		
4.2.	'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;	2.1.3.	informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;	PU		
4.3.	'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level;			NP	Odredba nije prenosiva u Zakon o informacionoj bezbednosti, budući da su drugim propisima RS utvrđeni pojam i predmet strategija Vlade.	
4.4.	'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);	2.1.2.	operator IKT sistema je pravno lice, organ vlasti ili organizaciona jedinica organa vlasti koji koristi IKT sistem	PU		

a)	a1)	b)	b1)	v)	g)	d)
			u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti			
4.5.	‘digital service’ means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (17) which is of a type listed in Annex III;	2.1.25.	25) usluga informacionog društva je usluga u smislu zakona kojim se uređuje elektronska trgovina	PU		
4.6.	‘digital service provider’ means any legal person that provides a digital service;	2.1.26.	26) pružalac usluge informacionog društva je pravno lice koje je pružalac usluge u smislu zakona kojim se uređuje elektronska trgovina	PU		
4.7.	‘incident’ means any event having an actual adverse effect on the security of network and information systems;	2.1.11.	incident je unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;	PU		
4.8.	‘incident handling’ means all procedures supporting the detection, analysis and containment of an incident and the response thereto;	7.3.27.	Mere zaštite IKT sistema se odnose na: 27) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama	PU		
4.9.	‘risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information	2.1.9.	rizik znači mogućnost narušavanja informacione bezbednosti, odnosno	PU		

a)	a1)	b)	b1)	v)	g)	d)
	systems;		mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;			
4.10.	‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;			NP	Odredba je neprenosiva, s obzirom da se odnosi na pojam predstavnika (zastupnika) sa prebivalištem ili sedištem u Evropskoj uniji. Zakon o informacionoj bezbednosti se odnosi na IKT sisteme u Republici Srbiji.	
4.11.	‘standard’ means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;	7.4.	Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.	PU		
4.12.	‘specification’ means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;	7.4.	Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se	PU		

a)	a1)	b)	b1)	v)	g)	d)
			primenjuju u odgovarajućim oblastima rada.			
4.13.	‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	6.1.3.5.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (5) digitalna infrastruktura: - razmena internet saobraćaja;	PU		
4.14.	‘domain name system (DNS)’ means a hierarchical distributed naming system in a network which refers queries for domain names;	6.1.3.5.2.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (5) digitalna infrastruktura: - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi)	PU		
4.15.	‘DNS service provider’ means an entity which provides DNS services on the internet;	6.1.3.5.2.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (5) digitalna infrastruktura: - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi)	PU		

a)	a1)	b)	b1)	v)	g)	d)
4.16.	top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);	6.1.3.5.2.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 5) digitalna infrastruktura: - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi)	PU		
4.17.	'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;	6.1.3.7.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (7)usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona	DU	Ova vrsta IKT sistema od posebnog značaja biće definisana podzakonskim aktom.	
4.18.	'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;	6.1.3.7.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (7)usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona	DU	Ova vrsta IKT sistema od posebnog značaja biće definisana podzakonskim aktom.	
4.19.	'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.	6.1.3.7.	IKT sistemi od posebnog značaja su sistemi koji se koriste: (7)usluge informacionog društva: - usluge informacionog društva	DU	Ova vrsta IKT sistema od posebnog značaja biće definisana podzakonskim aktom.	

a)	a1)	b)	b1)	v)	g)	d)
			u smislu člana 2. tačka 25) ovog zakona			
5.1.	By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.			NP	Odredba je neprenosiva u Zakon o izmenama i dopunama Zakona o informacionoj bezbednosti, s obzirom da propisuje obavezu država članica da u datom roku utvrde listu operatora ključnih usluga na svojoj teritoriji.	
5.2.	The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:	6.1.				
5.2.a)	an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;	6.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 1) u obavljanju poslova u organima vlasti; 2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti; 3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima: (1) energetika: - proizvodnja, prenos i distribucija električne energije; - proizvodnja i prerada uglja; - istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata; - istraživanje,	PU		

a)	a1)	b)	b1)	v)	g)	d)
			proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa. (2) saobraćaj: - železnički, poštanski, vodeni i vazdušni saobraćaj; (3) zdravstvo: - zdravstvena zaštita; (4) bankarstvo i finansijska tržišta: - poslovi finansijskih institucija; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; (5) digitalna infrastruktura: - razmena internet saobraćaja; - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi) (6) dobra od opšteg interesa: - korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa			

a)	a1)	b)	b1)	v)	g)	d)
			(vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja); (7) usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona; (8) ostale oblasti: - elektronske komunikacije; - izdavanje službenog glasila Republike Srbije; - upravljanje nuklearnim objektima; - proizvodnja, promet i prevoz naoružanja i vojne opreme; - upravljanje otpadom; - komunalne delatnosti; - proizvodnja i snabdevanje hemikalijama. 4) u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti iz tačke 3) ovog stava.			
5.2b)	the provision of that service depends on network and information systems; and	6.1.	IKT sistemi od posebnog značaja su	PU		

a)	a1)	b)	b1)	v)	g)	d)
			sistemi koji se koriste: 1) u obavljanju poslova u organima vlasti; 2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti; 3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima: (1) energetika: - proizvodnja, prenos i distribucija električne energije; - proizvodnja i prerada uglja; - istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata; - istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa. (2) saobraćaj: - železnički, poštanski, vodeni i vazdušni saobraćaj; (3) zdravstvo: - zdravstvena zaštita; (4) bankarstvo i finansijska tržišta: - poslovi finansijskih institucija; - poslovi			

a)	a1)	b)	b1)	v)	g)	d)
			vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; (5) digitalna infrastruktura: - razmena internet saobraćaja; - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi) (6) dobra od opšteg interesa: - korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja); (7) usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona; (8) ostale oblasti: - elektronske komunikacije; - izdavanje			

a)	a1)	b)	b1)	v)	g)	d)
			službenog glasila Republike Srbije; - upravljanje nuklearnim objektima; - proizvodnja, promet i prevoz naoružanja i vojne opreme; - upravljanje otpadom; - komunalne delatnosti; - proizvodnja i snabdevanje hemikalijama. 4) u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti iz tačke 3) ovog stava.			
5.2.c)	an incident would have significant disruptive effects on the provision of that service.	6.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 1) u obavljanju poslova u organima vlasti; 2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti; 3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima: (1) energetika:	PU		

a)	a1)	b)	b1)	v)	g)	d)
			- proizvodnja, prenos i distribucija električne energije; - proizvodnja i prerada uglja; - istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata; - istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa. (2) saobraćaj: - železnički, poštanski, vodeni i vazdušni saobraćaj; (3) zdravstvo: - zdravstvena zaštita; (4) bankarstvo i finansijska tržišta: - poslovi finansijskih institucija; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; (5) digitalna infrastruktura: - razmena internet saobraćaja; - upravljanje			

a)	a1)	b)	b1)	v)	g)	d)
			registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi) (6) dobra od opšteg interesa: - korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja); (7) usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona; (8) ostale oblasti: - elektronske komunikacije; - izdavanje službenog glasila Republike Srbije; - upravljanje nuklearnim objektima; - proizvodnja, promet i prevoz naoružanja i vojne opreme; - upravljanje otpadom; - komunalne delatnosti; - proizvodnja i snabdevanje hemikalijama.			

a)	a1)	b)	b1)	v)	g)	d)
			4) u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti iz tačke 3) ovog stava. Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu delatnosti iz stava 1. tačka 3) ovog člana.”			
5.3.	For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.	6.2.	Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu delatnosti iz stava 1. tačka 3) ovog člana.”	PU		
5.4.	For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.			NP	Odredba se odnosi na saradnju dve ili više država članica EU u slučaju da operator IKT sistema pruža usluge u dve ili više država članica.	
5.5.	Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.			NP	Odredba se odnosi na obavezu država članica EU da na svake dve godine razmotre liste operatora ključnih usluga i po potrebi ih menjaju.	
5.6.	The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of			NP	Norma se odnosi na zadataak Grupe za saradnju koju, na osnovu člana 11. predmetne direktive obrazuju predstavnici država članica EU,	

a)	a1)	b)	b1)	v)	g)	d)
	operators of essential services.				Evropske komisije i ENISA.	
5.7.	For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least: a) national measures allowing for the identification of operators of essential services; b) the list of services referred to in paragraph 3; c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector; d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).			NP	Odredbe su neprenosive, s obzirom da se odnosi na obavezu država članica EU da podnose Evropskoj komisiji izveštaje o primeni direktive, kao i da se odnosi na sadržaj izveštaja.	
5.8.	In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.					

a)	a1)	b)	b1)	v)	g)	d)
6.1.	When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors: a)the number of users relying on the service provided by the entity concerned; b)the dependency of other sectors referred to in Annex II on the service provided by that entity; c)he impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; d)the market share of that entity; e)the geographic spread with regard to the area that could be affected by an incident; f)the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.			NP	Odredba je neprenosiva, s obzirom da su njome predviđene smernice za određivanje operatora ključnih usluga prilikom izrade odgovarajućih propisa.	
6.2.	In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.			NP	Odredba je neprenosiva, s obzirom da je njome predviđena smernica za određivanje operatora ključnih usluga prilikom izrade odgovarajućih propisa.	
7.1.	Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at			PU	Republika Srbija je usvojila Strategiju razvoja informacione bezbednosti u Republici Srbnji za period od 2017.do 2020. godine («Službeni glasnik RS» 53/17), u skladu sa obavezom iz NIS direktive.	

a)	a1)	b)	b1)	v)	g)	d)
	least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues: a)the objectives and priorities of the national strategy on the security of network and information systems; b)a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors; c)the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors; d)an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems; e)an indication of the research and development plans relating to the national strategy on the security of network and information systems; f)a risk assessment plan to identify risks; g)a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.					
7.2.	Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.			NP	Odredba je neprenosiva, jer se odnosi na mogućnost država članica EU da prilikom izrade nacionalnih strategija zamole za pomoć ENISA.	

a)	a1)	b)	b1)	v)	g)	d)
7.3.	Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.			NP	Odredba je neprenosiva, jer se odnosi na obavezu država članica EU da dostave Evropskoj komisiji svoje nacionalne strategije u roku od tri meseca od dana usvajanja.	
8.1.	Each Member State shall designate one or more national competent authorities on the security of network and information systems (‘competent authority’), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.	4.	Organ državne uprave nadležan za bezbednost IKT sistema je ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Nadležni organ).	PU		
8.2.	The competent authorities shall monitor the application of this Directive at national level.	16. 28.	Nadzor nad radom Nacionalnog CERT-a u vršenju poslova poverenih ovim zakonom vrši Nadležni organ, koji periodično, a najmanje jednom godišnje, proverava da li Nacionalni CERT raspolaže odgovarajućim resursima, vrši poslove u skladu sa članom 15. ovog zakona i kontroliše učinak uspostavljenih procesa za upravljanje sigurnosnim incidentima. Inspekcija za informacionu bezbednost vrši inspekcijski nadzor nad	PU		

a)	a1)	b)	b1)	v)	g)	d)
			primenom ovog zakona i radom operatora IKT sistema od posebnog značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslove inspekcije za informacionu bezbednost obavlja ministarstvo nadležno za poslove informacione bezbednosti preko inspektora za informacionu bezbednost. U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim na osnovu ovog zakona.			
8.3.	Each Member State shall designate a national single point of contact on the security of network and information systems (‘single point of contact’). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority	12.1.	Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju	PU		

a)	a1)	b)	b1)	v)	g)	d)
	shall also be the single point of contact.		najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postanu visokorizični; 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države.			
8.4.	The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.	12.1.	Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postanu visokorizični; 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države.	PU		
8.5.	Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.			NP	Odredba je neprenosiva, s obzirom da se odnosi na obavezu država članica EU da obezbede adekvatne resurse za primenu ove direktive.	

a)	a1)	b)	b1)	v)	g)	d)
8.6.	The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.			NP	Prema zakonodavstvu Republike Srbije, državni organi su u obavezi da međusobno sarađuju, te smatramo da nije neophodno da se ova odredba prenese u ovaj zakon.	
8.7.	Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.			NP	Odredba je neprenosiva, s obzirom da se odnosi na obavezu država članica EU da obaveste Evropsku komisiju o nadležnim organima i tačkama za kontakt.	
9.1.	Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.	14.	Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou. Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge.	PU		
9.2.	Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I. Member States shall ensure the effective, efficient			NP	Odredba je neprenosiva, s obzirom da se odnosi na obavezu članica EU da obezbede adekvatne resurse za funkcionisanje CERT-ova, kao i na obavezu saradnje sa nacionalnim	

a)	a1)	b)	b1)	v)	g)	d)
	and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.				CERT-ovima država članica EU.	
9.3.	Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.	15.4.	U cilju obezbeđivanja kontinuiteta rada, Nacionalni CERT treba da: 1) bude opremljen sa odgovarajućim sistemima za upravljanje incidentima; 2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u svako doba; 3) obezbedi infrastrukturu čiji je kontinuitet osiguran, odnosno da obezbedi redundantne sisteme i rezervni radni prostor.	PU		
9.4.	Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.		.	NP	Odredba je neprenosiva, jer se odnosi na obavezu obaveštavanja Evropske komisije od strane država članica o radu Nacionalnog CERT-a.	
9.5.	Member States may request the assistance of ENISA in developing national CSIRTs.			NP	Odredba je neprenosiva, s obzirom da se odnosi na pravo članica EU da zatraže pomoć ENISA u razvoju nacionalnih CERT-ova.	
10.1.	Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.	15.6.	Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa	PU		

a)	a1)	b)	b1)	v)	g)	d)
			javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om organa vlasti.			
10.2.	Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).	11.1.	Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko portala Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja koji održava Nadležni organ.	PU		
10.3.	Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive. By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).			NP	Odredba je neprenosiva, s obzirom da se odnosi na obavezu podnošenja izveštaja EU Grupi za koordinaciju o incidentima.	
11.1.	1. In order to support and facilitate strategic cooperation and the exchange of information among			NP	Odredbe su neprenosive, s obzirom da se odnosi na uspostavljanje, sastav,	

a)	a1)	b)	b1)	v)	g)	d)
	Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established. 2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3. 11.2. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA. Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work. The Commission shall provide the secretariat. 3. The Cooperation Group shall have the following tasks: a) providing strategic guidance for the activities of the CSIRTs network established under Article 12; b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6); c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems; d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the				poslove i obaveze tela Evropske unije (Grupe za koordinaciju).	

a)	a1)	b)	b1)	v)	g)	d)
	effectiveness of CSIRTs, and identifying best practice; e) exchanging information and best practice on awareness-raising and training; f) exchanging information and best practice on research and development relating to the security of network and information systems; g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies; h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations; i) collecting best practice information on risks and incidents; j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3); k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA; l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents; m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16. By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to					

a)	a1)	b)	b1)	v)	g)	d)
	implement its objectives and tasks, which shall be consistent with the objectives of this Directive. 4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article. 5. The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2). For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017.					
12.	In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established. 2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the			NP	Odredbe su neprenosive, s obzirom da se odnosi na uspostavljanje, sastav, poslove i obaveze tela Evropske unije (mreže CERT-ova EU).	

a)	a1)	b)	b1)	v)	g)	d)
	cooperation among the CSIRTs. 3.The CSIRTs network shall have the following tasks: a) exchanging information on CSIRTs' services, operations and cooperation capabilities; b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident; c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents; d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State; e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance; f) discussing, exploring and identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Member States respond to cross-border risks					

a)	a1)	b)	b1)	v)	g)	d)
	and incidents; g)informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard; h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA; i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; .j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation. 4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group. 5. The CSIRTs network shall lay down its own rules of procedure.					
13.	The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.			NP	Odredba je neprenosiva, jer se odnosi na zaključenje međunarodnih ugovora Evropske unije sa trećim državama o pridruživanju pojedinim aktivnostima Grupe za koordinaciju.	

a)	a1)	b)	b1)	v)	g)	d)
14.1.	Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.	7.2.	Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.	PU		
14.2	Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.	7.2.	Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.	PU		
14.3.	Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.	11.1.	Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko portala Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima koji	PU		

a)	a1)	b)	b1)	v)	g)	d)
			održava Nadležni organ.			
14.4.a)	In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: the number of users affected by the disruption of the essential service;	11a.1.2.	Operator IKT sistema od posebnog značaja dužan je da prijavi sledeće incidente: 2) incidenti koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period.	PU		
14.4.b)	the duration of the incident;	11a.1.1. 11a.1.2.	1) incidenti koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga; 2) incidenti koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period.	PU		
14.4.c)	the geographical spread with regard to the area affected by the incident.	11a.1.4.	4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;	PU		
14.5.1.	On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the	12.1.1.	Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT	PU		

a)	a1)	b)	b1)	v)	g)	d)
	other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.		sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postanu visoki rizici; 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države.			
14.5.2.	Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.	15.1.3.	Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno: 3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i drugim IKT sistemima u Republici Srbiji, tako što pruža savete i	PU		

a)	a1)	b)	b1)	v)	g)	d)
			preporuke na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja			
14.5.3.	At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.	12.1.	Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postanu visokorizični; 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države.	PU		
14.6.	After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.	11.10..	Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 3. ovog člana kome se upućuju obaveštenja o incidentima, može objaviti informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident	PU		

a)	a1)	b)	b1)	v)	g)	d)
			dogodio..			
14.7.	Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.			NP	Odredba je neprenosiva, s obzirom da se odnosi na rad tela EU (Grupe za koordinaciju).	
15.1.	Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.	28.	Inspekcija za informacionu bezbednost vrši inspekcijski nadzor nad primenom ovog zakona i radom operatora IKT sistema od posebnog značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslove inspekcije za informacionu bezbednost obavlja ministarstvo nadležno za poslove informacione bezbednosti preko inspektora za informacionu bezbednost. U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi	PU		

a)	a1)	b)	b1)	v)	g)	d)
			propisani ovim zakonom i propisima donetim na osnovu ovog zakona.			
15.2.a)	Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide: the information necessary to assess the security of their network and information systems, including documented security policies;	29.1.	Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok.	PU		
15.2.b)	evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority. When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.	29.1.	Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok;	PU		

a)	a1)	b)	b1)	v)	g)	d)
			2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok.			
15.3.	Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.	29.1.	Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok.	PU		
15.4.	The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.			NP		Obaveza prijavljivanja narušavanja prava na zaštitu podataka o ličnosti, kao i saradnje rukovaoca podataka o ličnosti sa Poverenikom već je utvrđena Zakonom o zaštiti podataka o

a)	a1)	b)	b1)	v)	g)	d)
						ličnosti.
16.1.a)	Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: the security of systems and facilities;	6.1.3.7. 7.2.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (7) usluge informacionog društva. Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i smanjenje štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.	PU		
16.1.b)	incident handling;	7.3.27.	Mere zaštite IKT sistema se odnose na: 27) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama;	PU		
16.1.c)	business continuity management;	7.3.28.	28) mere koje obezbeđuju kontinuitet	PU		

a)	a1)	b)	b1)	v)	g)	d)
			obavljanja posla u vanrednim okolnostima.			
16.1.d)	monitoring, auditing and testing;	8.4.	Operator IKT sistema od posebnog značaja je dužan da samostalno ili uz angažovanje spoljnih eksperata vrši proveru usklađenosti primenjenih mera IKT sistema sa aktom iz stava 1. ovog člana i to najmanje jednom godišnje i da o tome sačini izveštaj.	PU		
16.1.e)	compliance with international standards.	7.4.	Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.	PU		
16.2.	Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.	7.3.28.	28) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima.	PU		
16.3.	Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as	11.1.	Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da	PU		

a)	a1)	b)	b1)	v)	g)	d)
	referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.		imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko portala Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima koji održava Nadležni organ.			
16.4.a)	In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: the number of users affected by the incident, in particular users relying on the service for the provision of their own services;	11a.1.2.	Operator IKT sistema od posebnog značaja dužan je da prijavi sledeće incidente: 2) incidente koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period;	PU		
16.4.b)	the duration of the incident;	11a.1.1. 11a.1.2.	1) incidenti koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga; 2) incidenti koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period.	PU		
16.4.c)	the geographical spread with regard to the area affected by the incident;	11a.1.4.	4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i	PU		

a)	a1)	b)	b1)	v)	g)	d)
			pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;			
16.4.d)	the extent of the disruption of the functioning of the service;	11a.1.1.	1) incidenti koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;	PU		
16.4.e)	the extent of the impact on economic and societal activities. The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.	11a.1.3.	3) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;	PU		
16.5	Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.	11a.1.6.	6) incidente koji su nastali kao posledica incidenta u IKT sistemu iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge IKT sistema iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona.	PU		

a)	a1)	b)	b1)	v)	g)	d)
16.6.	Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.	12.1. 11.10.	Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postanu visokorizični; 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države. Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 3. ovog člana kome se upućuju obaveštenja o incidentima, može objaviti informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio..	PU		
16.7.	After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where	11.10.	Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 3. ovog člana kome se upućuju obaveštenja o incidentima, može	PU		

a)	a1)	b)	b1)	v)	g)	d)
	public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.		objaviti informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio..			
16.8.	The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.			NP	Odredba je neprenosiva, jer se njome određuje ovlašćenje Evropskoj komisiji da bliže uredi odredbe ove direktive.	
16.9.	The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).			NP	Odredba je neprenosiva, jer se njome određuje ovlašćenje Evropskoj komisiji da bliže uredi odredbe ove direktive.	
16.10.	Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.			NP	Odredba je neprenosiva, jer se odnosi na obavezu država članica EU da u svom zakonodavstvu ne predvide dodatne zahteve za pružaoce digitalnih usluga.	
16.11.	Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (19).			NU	Odredba nije usklađena, jer i ovakva preduzeća mogu da obavljaju delatnosti koje su od posebnog značaja.	
17.1.	Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such	28.1.	Inspekcija za informacionu bezbednost vrši inspekcijski nadzor nad primenom ovog zakona i radom operatora IKT sistema od posebnog	PU		

a)	a1)	b)	b1)	v)	g)	d)
	evidence may be submitted by a competent authority of another Member State where the service is provided.		značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor.			
17.2.a)	For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to: provide the information necessary to assess the security of their network and information systems, including documented security policies;	28.3.	U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim na osnovu ovog zakona.	PU		
17.2.b)	remedy any failure to meet the requirements laid down in Article 16.	29.1.1.	Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok;	PU		
17.3.	If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the			NP	Odredba je neprenosiva, jer se odnosi na saradnju država članica EU u slučaju da pružalac digitalnih usluga ima svoje IKT sisteme u jednoj ili više država.	

a)	a1)	b)	b1)	v)	g)	d)
	Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.					
18.1.	For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.			NP	Odredba je neprenosiva, jer se odnosi na određivanje jurisdikcije država članica EU.	
18.2.	A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.			NP	Odredba je neprenosiva, jer se odnosi na određivanje jurisdikcije država članica EU.	
18.3.	The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.			NP	Odredba je neprenosiva, jer se odnosi na određivanje jurisdikcije država članica EU.	
19.1.	In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European	7.3.	Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona,	PU		

a)	a1)	b)	b1)	v)	g)	d)
	or internationally accepted standards and specifications relevant to the security of network and information systems.		nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.			
19.2.	ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.			NP	Odredba je neprenosiva, jer se odnosi na davanje ovlašćenja ENISA da izradi smernice koji se odnose na standarde zaštite IKT sistema.	
20.1.	Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.	15.1.3.	Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno: 3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i drugim IKT sistemima u Republici Srbiji, tako što pruža savete na osnovu raspoloživih	PU		

a)	a1)	b)	b1)	v)	g)	d)
			informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja,			
20.2.	When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned. Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.			NP	Odredba je neprenosiva, s obzirom da se njome daje mogućnost (ne i obaveza) država članica da predvide mogućnost dobrovoljnog obaveštavanja o incidentu u IKT sistemu. Napominjemo da se obaveze koje proističu iz Predloga zakona odnose samo na one IKT sisteme od posebnog značaja koji imaju obavezu prijavljivanja incidenata.	
21.	Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.	30.	Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako: 1) ne izvrši upis u evidenciju u roku iz člana 6b ovog zakona; 2) ne donese Akt o bezbednosti IKT sistema iz člana 8. stav 1. ovog zakona; 3) ne primeni mere zaštite određene Aktom	PU		

a)	a1)	b)	b1)	v)	g)	d)
		31.	o bezbednosti IKT sistema iz člana 8. stav 2. ovog zakona; 4) ne izvrši proveru usklađenosti primenjenih mera iz člana 8. stav 4. ovog zakona; 5) ne dostavi statističke podatke iz člana 11b ovog zakona; 6) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 29. stav 1. tačka 1. ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu ne obavesti organe iz člana 11. st. 1, 3. i 7. ovog zakona; 2) ne dostavlja obaveštenja o bitnim događajima u vezi sa incidentom i			

a)	a1)	b)	b1)	v)	g)	d)
			aktivnostima iz člana 11 stav 5. ovog zakona; 3) ne dostavi završni izveštaj iz člana 11. stav 6. ovog zakona. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st.1. i 2. ovog člana, ako finansijska institucija ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu od posebnog značaja, Narodna banka Srbije izriče toj finansijskoj instituciji mere i kazne u skladu sa zakonom kojim se uređuje poslovanje finansijskih institucija.			
22.1.	The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.			NP	Odredba je neprenosiva, jer se odnosi na uspostavljanje komiteta Evropske komisije.	
22.2.	Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.			NP	Odredba je neprenosiva, jer se odnosi na uspostavljanje komiteta Evropske komisije.	
23.1.	By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by			NP	Odredba je neprenosiva, s obzirom da se odnosi na podnošenje izveštaja od strane Evropske komisije.	

a)	a1)	b)	b1)	v)	g)	d)
	Member States in the identification of the operators of essential services.					
23.2.	The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021.			NP	Odredba je neprenosiva, jer se odnosi na razmatranje primene ove direktive od strane Evropske komisije.	
24.1.	Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017.			NP	Odredba je neprenosiva, jer se odnosi na početak rada tela EU (Grupe za koordinaciju i mreže CERT-ova EU).	
24.2.	For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also			NP	Odredba je neprenosiva, jer se odnosi na rad tela EU (Grupe za koordinaciju).	

a)	a1)	b)	b1)	v)	g)	d)
	discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.					
24.3.	By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.			NP	Odredba je neprenosiva, jer se odnosi na rad tela EU (Grupe za koordinaciju).	
25.1.	Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 10 May 2018. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.			NP	Odredba je neprenosiva, s obzirom da se odnosi na rok u kome države članice EU moraju da implementiraju ovu direktivu.	
25.2.	Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.			NP	Odredba je neprenosiva, jer se odnosi na obavezu izveštavanja Evropske komisije od strana država članica EU.	
26.	This Directive shall enter into force on the twentieth			NP	Odredba je neprenosiva, jer se odnosi	

a)	a1)	b)	b1)	v)	g)	d)
	day following that of its publication in the Official Journal of the European Union.				na stupanje na snagu ove direktive.	
27.	This Directive is addressed to the Member States.			NP	Odredba je neprenosiva, jer propisuje da se ova direktiva odnosi na države članice EU.	
A.I.1.a)	REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following: CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.	15.2.	Nacionalni CERT obezbeđuje dostupnost svojih usluga putem različitih sredstava komunikacije, koja su neprekidno dostupna.	PU	Prvi paragraf A 1.1.a) tačke predstavlja instruktivnu odredbu NIS direktive koja je realizovana određivanjem zahteva za CERT i njegovih nadležnosti u skladu sa datom instrukcijom. Drugi paragraf A 1.1. a) prenet je odredbom člana 15. stav 2) zakona tako što je predviđeno da CERT obezbeđuje dostupnost svojih usluga putem različitih sredstava komunikacije (čime se izbegava da postoji samo jedno sredstvo u slučaju čije nedostupnosti bi bila onemogućena komunikacija sa CERT-om, odnosno obezbeđuje se da CERT ima više sredstava komunikacije).	
A.I.1.b)	CSIRTs' premises and the supporting information systems shall be located in secure sites.	15.3.	Prostorije i informacioni sistemi Nacionalnog CERT-a moraju da se nalaze na bezbednim lokacijama.	PU		
A.I.1.c)	Business continuity: CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.	15.4.	U cilju obezbeđivanja kontinuiteta rada, Nacionalni CERT treba da: 1) bude opremljen sa odgovarajućim sistemima za	PU		

a)	a1)	b)	b1)	v)	g)	d)
	CSIRTs shall be adequately staffed to ensure availability at all times. CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.		upravljanje incidentima; 2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u svako doba; 3) obezbedi infrastrukturu čiji je kontinuitet osiguran, odnosno da obezbedi redundantne sisteme i rezervni radni prostor.			
A.I.1.d)	CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.	15.5.	Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om organa javne vlasti.	PU		
A.I.2.a)	CSIRTs' tasks: CSIRTs' tasks shall include at least the following: (i) monitoring incidents at a national level; (ii) providing early warning, alerts, announcement and dissemination of information to relevar stakeholders about risks and incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis ar situational awareness; (v) participating in the CSIRTs network.	15.1.	Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a	PU		

a)	a1)	b)	b1)	v)	g)	d)
			posebno: 1) prati stanje o incidentima na nacionalnom nivou, 2) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima, 3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i drugim IKT sistemima u Republici Srbiji, tako što pruža savete i preporuke na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja, 4) kontinuirano izrađuje analize rizika i incidenata, 5) podiže svest kod građana, privrednih subjekata i organa vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti, 6) vodi evidenciju Posebnih CERT-ova; 7) izveštava Nadležni			

a)	a1)	b)	b1)	v)	g)	d)
			organ na kvartalnom nivou o preduzetim aktivnostima.			
A.I.2.b)	CSIRTs shall establish cooperation relationships with the private sector.	15.5.	Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om organa vlasti.	PU		
A.I.2.c)	To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for: (i) incident and risk-handling procedures; (ii)incident, risk and information classification schemes.	15.7.	Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih pravila za: 1) upravljanje i saniranje rizika i incidenata; 2) klasifikaciju informacija o rizicima i incidentima.	PU		
A.II.						
A.II.1.						
A.II.1.a)	TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4 Energy	6.1.3.1.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima:	PU		

a)	a1)	b)	b1)	v)	g)	d)
	Electricity –Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council (1), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive –Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC –Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC		(1) energetika: - proizvodnja, prenos i distribucija električne energije;			
A.II.1.b)	Oil — Operators of oil transmission pipelines –Operators of oil production, refining and treatment facilities, storage and transmission	6.1.3.1.3.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (1) energetika: -istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata;	PU		
A.II.1.c)	Gas –Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council (2) –Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC –Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC –Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC	6.1.3.1.4.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (1) energetika: -istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa;	PU		

a)	a1)	b)	b1)	v)	g)	d)
	–LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC –Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC —Operators of natural gas refining and treatment facilities					
A.II.2.a)	Air transport –Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council (3) –Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council (4), airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council (5), and entities operating ancillary installations contained within airports –Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council (6)	6.1.3.2.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (2) saobraćaj: -železnički, poštanski, vodeni i vazdušni saobraćaj;	PU		
A.II.2.b)	Rail transport –Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council (7) –Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point	6.1.3.2.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (2) saobraćaj: -železnički, poštanski,	PU		

a)	a1)	b)	b1)	v)	g)	d)
	(12) of Article 3 of Directive 2012/34/EU		vodeni i vazdušni saobraćaj;			
A.II.2.c)	Water transport –Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council (8), not including the individual vessels operated by those companies –Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council (9), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports –Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council (10)	6.1.3.2.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (2) saobraćaj: -železnički, poštanski, vodeni i vazdušni saobraćaj;	PU		
A.II.2.d)	Road transport –Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 (11) responsible for traffic management control –Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council (12)	6.1.2.6.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (6) dobra od opšteg interesa: - korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale,	PU		

a)	a1)	b)	b1)	v)	g)	d)
			banje, divljač, zaštićena područja);			
A.II.3.	Banking Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council (13)A	6.1.3.4.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (4) bankarstvo i finansijska tržišta: - poslovi finansijskih institucija;	PU		
A.II.4.	Financial market infrastructures –Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council (14) –Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council (15)	6.1.3.4.3.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (4) bankarstvo i finansijska tržišta: - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta;	PU		
A.II.5.	Health sector Health care settings (including hospitals and private clinics) Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council (16)	6.1.3.3.1.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (3) zdravstvo: -zdravstvena zaštita.	PU		

a)	a1)	b)	b1)	v)	g)	d)
A.II.6.	Drinking water supply and distribution Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC (17) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services	6.1.3.8.5.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (8) ostale oblasti: - komunalne delatnosti;	PU		Napomena: Snabdevanje vodom za piće je komunalna delatnost u skladu sa Zakonom o komunalnim delatnostima.
A.II.7.	Digital Infrastructure — IXPs — DNS service providers — TLD name registries	6.1.3.5.	IKT sistemi od posebnog značaja su sistemi koji se koriste: 3) u obavljanju delatnosti od opšteg interesa i to u oblastima: (5)digitalna infrastruktura -razmena internet saobraćaja; -upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi)	PU		

a)	a1)	b)	b1)	v)	g)	d)
A.III.	TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF POINT (5) OF ARTICLE 4 Online marketplace. Online search engine Cloud computing service.	6.1.3.7. .	IKT sistemi od posebnog značaja su sistemi koji se koriste: (7)usluge informacionog društva: - usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona	DU		IKT sistemi u kojima se vrše ove usluge biće definisani kao IKT sistemi od posebnog značaja podzakonskim aktom.