PREDLOG

Z A K O N
O INFORMACIONOJ BEZBEDNOSTI

I. OSNOVNE ODREDBE

Predmet uređivanja

Član 1.

Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite, praćenje pravilne primene propisanih mera zaštite, kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.

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 i usluge* 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 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 fizičko lice u svojstvu registrovanog subjekta, pravno lice, organ ili organizaciona jedinica organa koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti;

3) *informaciona bezbednost* predstavlja sposobnost informaciono-komunikacionih sistema i mreža da se odupru i/ili ublaže, uz određeni stepen pouzdanosti, svaki događaj koji bi mogao da ugrozi raspoloživost, integritet, autentičnost, neporecivost i poverljivost podataka koji se obrađuju, odnosno usluga koje se pružaju ili su dostupne putem tog IKT sistema;

4) *integritet* je svojstvo koje osigurava da podaci ili informacije nisu promenjeni ili uništeni na neovlašćeni način od kada su kreirani, preneti ili uskladišteni;

5) *raspoloživost* je svojstvo kojim se osigurava dostupnost i upotrebljivost IKT sistema na zahtev ovlašćenog subjekta ili procesa onda kada im je potreban;

6) *autentičnost* je svojstvo kojim se osigurava mogućnost da se proveri i potvrdi da je informaciju stvorio ili poslao onaj za koga se tvrdi da je tu radnju izvršio;

7) *poverljivost* je svojstvo kojim se osigurava da su informacije i funkcije IKT sistema dostupne samo ovlašćenim licima;

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* predstavlja mogućnost nastanka događaja ili uslova koji mogu ugroziti nivo informacione bezbednosti ili ispravno funkcionisanje IKT sistema, što se utvrđuje na osnovu procene verovatnoće događaja i veličine njegovog potencijalnog uticaja na nivo informacione bezbednosti;

10) *ranjivost* predstavlja slabost ili nedostatak u IKT proizvodima ili uslugama koji se mogu iskoristiti za realizaciju jedne ili više pretnji;

11) *upravljanje rizikom* je skup sistematičnih aktivnosti identifikacije, procene i uspostavljanje sistema kontrole rizika koji omogućava planiranje, organizovanje i usmeravanje mera zaštite kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;

12) *izbegnuti incident* predstavlja identifikovani događaj u IKT sistemu koji je mogao dovesti do značajnog ugrožavanja raspoloživosti, autentičnosti, integriteta ili poverljivosti podataka, usluga ili sistema, ali je pravovremenom intervencijom ili zaštitnim merama sprečeno ostvarivanje štetnih posledica;

13) *pretnja* predstavlja svaku okolnost, događaj ili radnju koja može da ugrozi, poremeti ili na drugi način štetno utiče na IKT sistem, korisnike sistema i druga lica sa jasnom verovatnoćom nastajanja štete u slučaju da izostane reakcija;

14) *ozbiljna pretnja* predstavlja pretnju po informacionu bezbednost za koju se, s obzirom na njena tehnička svojstva, može pretpostaviti da ima potencijal da izazove značajne negativne posledice po IKT sistem, njegovog operatora ili korisnike usluga tog operatora uzrokujući značajnu materijalnu ili nematerijalnu štetu;

15) *incident* je svaki događaj koji ugrožava raspoloživost, autentičnost, integritet, neporecivost ili poverljivost podataka koji se čuvaju, prenose ili obrađuju ili usluge koje se pružaju, odnosno koje su dostupne putem IKT sistema;

16) *zlonamerni softver* je softver namerno kreiran sa ciljem da ošteti, poremeti, onemogući ili neovlašćeno pristupi informaciono-komunikacionim sistemima i obuhvata različite tipove štetnih programa, uključujući viruse, trojanske konje, crve, ransomver i špijunski softver;

17) *jedinstveni sistem za prijem obaveštenja o incidentima* je informacioni sistem u koji se unose podaci o incidentima i izbegnutim incidentima u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti;

18) *upravljanje incidentom* podrazumeva preduzimanje svih radnji i postupaka čiji je cilj sprečavanje, otkrivanje, analiza i prekid incidenta, kao i preduzimanje drugih mera radi odgovora na incident i otklanjanja njegovih posledica;

19) *kriza informacione bezbednosti* je događaj ili stanje koje ugrožava, ometa rad ili onemogućuje rad IKT sistema od posebnog značaja i pri tom izaziva rizike, pretnje ili posledice po stanovništvo, materijalna dobra ili životnu sredinu izuzetno velikog obima i intenziteta koje nije moguće sprečiti ili otkloniti redovnim delovanjem nadležnih organa i službi, a odgovor na takav događaj ili stanje zahteva učešće više nadležnih organa, kao i primenu odgovarajućih mera*;*

20) *mere zaštite IKT sistema* su tehničke, organizacione, administrativne i fizičke mere za upravljanje bezbednosnim rizicima IKT sistema;

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

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

23) *organ* je državni organ, organ autonomne pokrajine, jedinica lokalne samouprave, organizacija i drugo pravno ili fizičko lice kome je povereno vršenje javnih ovlašćenja;

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

25) *samostalni operatori IKT sistema* su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije;

26) Centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: CERT*)* je funkcionalna celina u okviru organa ili pravnog lica koja obuhvata skup poslova koji se odnose na prevenciju i zaštitu od incidenata;

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

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

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

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

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

32) *bezbednosna zona* je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci, kao i prostor ili prostorija koja je od ključnog značaja za očuvanje informacione bezbednosti IKT sistema;

33) *informaciona dobra* obuhvataju informacije koje se obrađuju u skladu sa funkcijom i namenom IKT sistema; elektronske zapise o konfiguraciji uređaja i elektronske komunikacione mreže; elektronske zapise o interakcijama u IKT sistemima, pristupu i upotrebi IKT sistema (tzv. log zapise); programski kôd; tehničku i korisničku dokumentaciju; elektronske zapise o interakcijama u elektronskoj komunikacionoj mreži (tzv. mrežni saobraćaj); informacije kojima se regulišu namena i korišćenje IKT sistema, procesi, mere zaštite i sl;

34) *usluga informacionog društva* je usluga u smislu zakona kojim se uređuje elektronska trgovina;

35) *pružalac usluge informacionog društva* je pravno lice koje je pružalac usluge u smislu zakona kojim se uređuje elektronska trgovina;

36) *mreža za isporuku sadržaja (Content Delivery Network – CDN)* označava mrežu geografski raspoređenih servera koja je osmišljena da obezbedi visoku dostupnost, pristupačnost i brzu isporuku digitalnog sadržaja i usluga korisnicima interneta, u ime pružalaca sadržaja i usluga;

37) *tačka za razmenu internet saobraćaja (engl. internet exchange point)* je mrežna struktura koja pruža mogućnost povezivanja dve ili više nezavisnih mreža

(autonomnih sistema) prvenstveno u svrhu olakšavanja razmene internet saobraćaja, i koja omogućuje međupovezivanje autonomnih sistema, u kom slučaju nije potrebno da internet saobraćaj između autonomnih sistema prođe kroz treći autonomni sistem, te koja takav saobraćaj ne menja i ne utiče na njega na drugi način;

38) *sistem naziva domena (DNS)* je distribuirani, hijerarhijski organizovan sistem koji povezuje nazive domena sa odgovarajućim IP adresama koje se koriste za usmeravanje i povezivanje korisničkih uređaja sa uslugama i resursima na internetu;

39) *pružalac usluge DNS-a* je subjekat koji pruža usluge razrešavanja DNS upita korisnicima interneta ili pruža uslugu autoritativnih servera imena za nazive domena koje koriste treća lica, sa izuzetkom korenskih (engl. root) servera imena;

40) *usluga od poverenja* je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

41) *pružalac usluge od poverenja* je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

42) *kvalifikovana usluga od poverenja* je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

43) *pružalac kvalifikovane usluge od poverenja* je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

44*) usluge računarstva u klaudu (engl. „cloud computing service”)* su digitalne usluge koje omogućavaju upravljanje na zahtev i široki daljinski pristup nadogradivom i elastičnom skupu deljivih računarskih resursa, uključujući i situacije kada su takvi resursi raspoređeni na nekoliko lokacija;

45) *usluga centra za upravljanje i čuvanje podataka* je usluga koja se pruža u okviru infrastrukture namenjene za centralizovano smeštanje, međupovezivanje i funkcionisanje računarske i mrežne opreme radi čuvanja, obrade i prenosa podataka (data centar), uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu uticaja na životnu sredinu;

46) *naučnoistraživačka organizacija* je organizacija u smislu zakona kojim se uređuju nauka i istraživanje;

47) *javna elektronska komunikaciona mreža* je elektronska komunikaciona mreža u smislu zakona kojim se uređuju elektronske komunikacije;

48) *elektronska komunikaciona usluga* je usluga u smislu zakona kojim se uređuju elektronske komunikacije;

49) *pružalac upravljanih usluga* je subjekt koji pruža usluge u vezi sa postavljanjem, upravljanjem, radom i održavanjem IKT proizvoda, mreža, infrastrukture, aplikacija ili druge mreže i informacionog sistema putem pružanja pomoći ili aktivnog upravljanja koje se sprovodi u prostorijama korisnika usluge ili na daljinu;

50) *pružalac upravljanih bezbednosnih usluga* je pružalac upravljanih usluga koji sprovodi ili pruža pomoć u sprovođenju aktivnosti u vezi sa upravljanjem rizikom u oblasti bezbednosti;

51) *registar naziva domena najvišeg nivoa (engl. TLD name registry)* je subjekt koji je odgovoran za upravljanje nazivom domena najvišeg nivoa (TLD) koji

mu je dodeljen i koji donosi politike i pravila za domen, upravlja bazom registra, generiše datoteku zone i održava tehničku infrastrukturu servera imena za dodeljeni domen najvišeg nivoa;

52) *pružalac usluge registracije naziva domena* je registrator naziva domena ili drugi subjekt koji deluje u ime registratora;

53) *IKT proizvod* je element ili grupa elemenata u okviru informaciono-komunikacionog sistema;

54) *IKT usluga* je usluga koja se u potpunosti ili u većoj meri sastoji iz prenosa, čuvanja, preuzimanja ili obrade podataka korišćenjem IKT sistema;

55) *IKT proces* je skup aktivnosti koji se obavlja u cilju izrade, razvoja, korišćenja i održavanja IKT proizvoda ili IKT usluge;

56) *TLP (Traffic Light Protocol)* predstavlja standard za deljenje informacija u oblasti informacione bezbednosti, koji je uspostavljen u cilju obezbeđivanja efektivne saradnje i deljenja informacija od izvora informacije do jednog ili više primalaca. Protokol pruža jednostavnu i intuitivnu šemu od četiri oznake za upućivanje na to sa kim se potencijalno osetljive informacije mogu podeliti;

57) *podatak o ličnosti* je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta;

58) *administrator* je lice koje je ovlašćeno i odgovorno za održavanje, upravljanje i obezbeđivanje funkcionalnosti i bezbednosti IKT sistema od posebnog značaja, u skladu sa odredbama ovog zakona i drugim važećim propisima.

Termini koji se koriste u ovom zakonu i propisima koji se donose na osnovu njega, a koji imaju rodno značenje, izraženi u gramatičkom muškom rodu, podrazumevaju prirodni ženski i muški pol lica na koja se odnose.

Načela informacione bezbednosti

Član 3.

Prilikom planiranja i primene mera zaštite IKT sistema treba se rukovoditi načelima:

1) načelo upravljanja rizikom – izbor i nivo primene mera se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanja posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti;

2) načelo sveobuhvatne zaštite – mere se primenjuju na svim organizacionim, fizičkim i tehničko-tehnološkim nivoima, kao i tokom celokupnog životnog ciklusa IKT sistema;

3) načelo stručnosti i dobre prakse – mere se primenjuju u skladu sa stručnim i naučnim saznanjima i iskustvima u oblasti informacione bezbednosti;

4) načelo svesti i osposobljenosti – sva lica koja svojim postupcima efektivno ili potencijalno utiču na informacionu bezbednost treba da budu svesna rizika i poseduju odgovarajuća znanja i veštine;

5) načelo kontinuiranog poboljšanja – mere zaštite i upravljanja informacionom bezbednošću treba redovno procenjivati i unapređivati kako bi se osigurala njihova efikasnost i prilagodljivost novim pretnjama i tehnološkim promenama;

6) načelo ravnopravnosti i nediskriminacije – mere zaštite IKT sistema moraju se sprovoditi na način koji osigurava jednak tretman svih korisnika, bez diskriminacije po bilo kom osnovu, u skladu sa zakonom.

Obrada podataka o ličnosti

Član 4.

Na obradu podataka o ličnosti koja je neophodna za vršenje nadležnosti i ispunjenje obaveza iz ovog zakona primenjuju se odredbe ovog zakona, odredbe posebnih zakona kojima se uređuju određene oblasti, kao i odredbe zakona kojim se uređuje zaštita podataka o ličnosti.

II. BEZBEDNOST IKT SISTEMA OD POSEBNOG ZNAČAJA

IKT sistemi od posebnog značaja

Član 5.

IKT sistemi od posebnog značaja su IKT sistemi koji su od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao ili mogao da ima značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio odnosno mogao da stvori značajan sistemski rizik.

IKT sistemi od posebnog značaja su:

1) prioritetni IKT sistemi;
2) važni IKT sistemi.

Operatori prioritetnih IKT sistema su:

1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:

(1) Energetika i rudarstvo

- proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika;
- kombinovana proizvodnja električne i toplotne energije;
- snabdevanje električnom energijom;
- prenos električne energije i upravljanje prenosnim sistemom;
- distribucija električne energije i upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom;
- skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika;
- upravljanje organizovanim tržištem električne energije;
- proizvodnja, distribucija i snabdevanje toplotnom energijom;
- transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta;
- istraživanje i proizvodnja nafte i prirodnog gasa;
- proizvodnja derivata nafte;
- skladištenje nafte i derivata nafte;

- transport i upravljanje transportnim sistemom za prirodni gas;
- skladištenje i upravljanje skladištem prirodnog gasa;
- distribucija i upravljanje distributivnim sistemom za prirodni gas;
- snabdevanje i javno snabdevanje prirodnim gasom;
- proizvodnja i prerada uglja;
- proizvodnja i prerada bakra, zlata, olova, cinka, litijuma i bora;
- proizvodnja, skladištenje i prenos vodonika;

(2) Saobraćaj

- obavljanje javnog avio-prevoza uz važeću operativnu dozvolu;
- upravljanje aerodromom;
- usluge kontrole letenja;
- upravljanje javnom železničkom infrastrukturom;
- poslovi železničkih preduzeća;
- obavljanje prevoza putnika i tereta unutrašnjim vodama;
- upravljanje lukama;
- servis za upravljanje brodskim saobraćajem (VTS);
- rečni informacioni servisi (RIS);
- upravljanje putnom infrastrukturom;
- upravljanje inteligentnim transportnim sistemima (ITS);

(3) Bankarstvo i finansijska tržišta

- poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti;
- poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;
- poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta;
- poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala;
- poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina;

(4) Zdravstvo

- pružanje zdravstvene zaštite;
- rad nacionalnih referentnih laboratorija;
- istraživanje i razvoj lekova;
- proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu;

  proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja;

(5) Voda za piće

- snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima navedeni poslovi nisu pretežni deo njihove delatnosti;

(6) Otpadne vode

- sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti;

(7) Digitalna infrastruktura

- pružanje usluga računarstva u klaudu;
- pružanje usluge centra za čuvanje i skladištenje podataka;

(8) Upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema

- pružanje upravljanih usluga;
- pružanje upravljanih bezbednosnih usluga;

(9) Ostale oblasti

- upravljanje nuklearnim objektima;
- pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena;
- pružanje usluga mreže za isporuku sadržaja;
- obavljanje delatnosti elektronskih komunikacija;
- tačka za razmenu internet saobraćaja;
- izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije;
- oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti;

2) organi;

3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura.

Operatori važnih IKT sistema

Član 6.

Operatori važnih IKT sistema su:

1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:

- poštanske usluge u smislu zakona kojim se uređuje oblast poštanskih usluga;
- upravljanje otpadom, u smislu zakona kojim se uređuje upravljanje otpadom, izuzev privrednih subjekata kojima navedeni posao nije pretežni deo njihove delatnosti;
- upravljanje ambalažnim otpadom, u smislu zakona kojim se uređuje upravljanje ambalažnim otpadom;

- proizvodnja i snabdevanje hemikalijama, u skladu sa zakonom kojim se uređuju hemikalije;
- proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade;
- proizvodnja računara, elektronskih i optičkih proizvoda;
- proizvodnja električne opreme;
- proizvodnja mašina i uređaja;
- proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz;
- proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava;
- usluge informacionog društva u smislu zakona o elektronskoj trgovini;
- proizvodnja, promet i prevoz naoružanja i vojne opreme;

2) naučnoistraživačke institucije;

3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne spadaju u operatore prioritetnih IKT sistema prema kriterijumima za određivanje operatora.

Podzakonski akt kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti.

Ministarstva u čijim nadležnostima su oblasti u kojima operatori prioritetnih i važnih IKT sistema obavljaju delatnosti, dužni su da u postupku izrade podzakonskog akta iz stava 2. ovog člana, dostave ministarstvu nadležnom za poslove informacione bezbednosti predloge sektorskih kriterijuma radi određivanja operatora IKT sistema od posebnog značaja.

Obaveze operatora IKT sistema od posebnog značaja

Član 7.

Operator IKT sistema od posebnog značaja, shodno ovom zakonu, u obavezi je da:

1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja;

2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata;

3) izvrši procenu rizika i donese akt o proceni rizika;

4) donese akt o bezbednosti IKT sistema od posebnog značaja;

5) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje;

6) 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;

7) dostavlja obaveštenja, bez odlaganja, o svakom incidentu koji značajno narušava bezbednost IKT sistem od posebnog značaja;

8) dostavlja obaveštenja o ozbiljnim pretnjama za IKT sistem od posebnog značaja;

9) dostavlja statističke podatke o incidentima i izbegnutim incidentima u IKT sistemima.

Obaveze samostalnih operatora

Član 8.

Samostalni operator dužan je da:

1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja;

2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata;

3) donese akt o bezbednosti IKT sistema;

4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima;

6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima.

Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama.

Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost, odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja.

Samostalni operatori, u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave.

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.

Evidencija operatora IKT sistema od posebnog značaja

Član 9.

Ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Ministarstvo) uspostavlja i vodi evidenciju prioritetnih i važnih IKT sistema (u daljem tekstu: Evidencija) koja sadrži:

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

2) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon administratora zaduženog za održavanje i upravljanje IKT sistemom 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, odnosno da li IKT sistem od posebnog značaja potpada pod prioritetan ili važan;

5) podatak o delatnosti operatora IKT sistema od posebnog značaja;

6) adresni opseg internet protokola (engl. „IP address range“) koji pripadaju IKT sistemu od posebnog značaja, a koji obuhvata podatke o javnim statičkim IP adresama;

7) veb stranice operatora IKT sistema od posebnog značaja;

8) broj lokacija na kojima se IKT sistem od posebnog značaja nalazi.

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

Samostalni operatori IKT sistema izuzeti su od obaveze dostavljanja podataka iz stava 1. tač. 4), 5), 6) i 8) ovog člana.

Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji donosi Ministarstvo.

Operator IKT sistema od posebnog značaja dužan je da Ministarstvu dostavi podatke iz st. 1. i 2. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 4. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja.

Operator IKT sistema od posebnog značaja dužan je da u slučaju promene podataka iz stava 1. ovog člana o tome obavesti Ministarstvo u roku od 15 dana od dana nastanka promene.

Podaci iz stava 1. tač. 2) i 3) ovog člana obrađuju se u svrhu izvršenja odredbi ovog zakona u pogledu dostavljanja obaveštenja i upozorenja značajnih za bezbednost IKT sistema od posebnog značaja, kao i radi uspostavljanja komunikacije i ostvarivanja saradnje u cilju otklanjanja štetnih posledica incidenata i preventivnog delovanja.

Podaci iz stava 1. tač. 2) i 3) ovog člana obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i čuvaju se do trenutka prestanka svrhe obrade ili do izvršene promene podataka u skladu sa stavom 6. ovog člana.

Ministarstvo stavlja na raspolaganje ažurnu Evidenciju Kancelariji za informacionu bezbednost radi izvršenja odredbi ovog zakona u pogledu prikupljanja i razmene informacija o pretnjama, ranjivostima i incidentima i pružanja podrške, upozoravanja i savetovanja lica koja upravljaju IKT sistemima.

Evidencija predstavlja tajni podatak u smislu zakona kojim se uređuje tajnost podataka.

Mere zaštite IKT sistema od posebnog značaja

Član 10.

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 smanjenje štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

Mere zaštite primenjuju se u svim IKT sistemima operatora iz stava 1. ovog člana.

Mere zaštite IKT sistema se odnose na:

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

2) prikupljanje podataka o pretnjama po informacionu bezbednost IKT sistema;

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

4) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne obuke za zaposlene odgovorne za upravljanje informacionom bezbednošću, radi obezbeđivanja kontinuirane edukacije;

5) obezbeđivanje dovoljno resursa za adekvatno upravljanje informacionom bezbednošću;

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

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

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

9) zaštitu nosača podataka;

10) ograničenje pristupa podacima i sredstvima za obradu podataka;

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

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

13) predviđanje upotrebe kriptografskih kontrola i drugih tehnika za sakrivanje podataka radi zaštite poverljivosti, autentičnosti i integriteta podataka;

14) primena mera zaštite radi sprečavanja oticanja podataka;

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

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

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

18) primenu odgovarajućih procedura i mera zaštite prilikom korišćenja usluge računarstva u klaudu;

19) praćenje IKT sistema u cilju otkrivanja ranjivosti i pretnji;

20) ograničenje pristupa internet stranicama koje mogu potencijalno da naruše bezbednost IKT sistema;

21) zaštitu podataka i sredstava za obradu podataka od zlonamernog softvera;

22) zaštitu od gubitka podataka redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za razmenu podataka;

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

24) obezbeđivanje integriteta softvera i operativnih sistema;

25) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;

26) obezbeđivanje zaštite IKT sistema prilikom sprovođenja revizorskog testiranja;

27) zaštitu podataka u komunikacionim mrežama, uključujući uređaje i vodove;

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

29) ispunjenje zahteva za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;

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

31) procedure za čuvanje i brisanje informacija u IKT sistemima, u skladu sa propisima;

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

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

34) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, kao i primenu mera sanacije posledica incidenta;

35) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje se definišu Planom kontinuiteta obavljanja posla;

36) usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite;

37) upotrebu multifaktorske autentikacije ili rešenja kontinuirane provere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije, te bezbednih komunikacionih sistema u hitnim slučajevima unutar operatora IKT sistema

Podzakonski akt kojim se bliže uređuju mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada donosi Vlada, na predlog Ministarstva.

Akt o proceni rizika IKT sistema od posebnog značaja

Član 11.

Operator IKT sistema od posebnog značaja dužan je da donese akt o proceni rizika za IKT sisteme (u daljem tekstu: akt o proceni rizika) kojima upravlja.

Aktom o proceni rizika vrši se procena rizika za IKT sistem od posebnog značaja s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj.

Akt o proceni rizika revidira se najmanje jednom godišnje.

Akt o proceni rizika izrađuje se u skladu sa opštom metodologijom za procenu rizika u IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a.

Operator IKT sistema od posebnog značaja nije u obavezi da donese akt iz stava 1. ovog člana u slučaju kada ima definisanu procenu rizika u drugim postojećim internim aktima, koja obuhvata zahteve iz opšte metodologije iz stava 4. ovog člana.

Akt o bezbednosti IKT sistema od posebnog značaja

Član 12.

Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema (u daljem tekstu: akt o bezbednosti).

Aktom o bezbednosti određuju se mere zaštite, a naročito principi, 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.

Akt o bezbednosti IKT sistema od posebnog značaja zasniva se na Aktu o proceni rizika iz člana 11. ovog zakona. Primena mera zaštite IKT sistema mora biti u skladu sa procenjenim rizicima, kako bi se obezbedila adekvatna zaštita sistema i minimizirao uticaj potencijalnih incidenata.

Akt o bezbednosti mora da bude usklađen s promenama u okruženju i u samom IKT sistemu.

Operator IKT sistema od posebnog značaja dužan je da, samostalno ili uz angažovanje spoljnih eksperata, vrši proveru iz prethodnog stava najmanje jednom godišnje i da o tome sačini izveštaj.

Podzakonski akt kojim se bliže uređuje sadržaj akta o bezbednosti, način provere IKT sistema od posebnog značaja i sadržaj izveštaja o proveri, kao i dostavljanje izveštaja nadležnom organu, donosi Vlada na predlog Ministarstva.

Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost

Član 13.

Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident.

Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su:

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;

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;

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

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

6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 3. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture;

7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima.

Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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.

Dostavljanje obaveštenja o incidentima

Član 14.

Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost.

Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 3. tačka 1) podtačka (3) ovog zakona dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti.

Operatori prioritetnih IKT sistema koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 3. tačka 1) podtačka (9) alineja četvrta ovog zakona i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva ovog zakona, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge.

Narodna banka Srbije, Regulatorno telo za elektronske komunikacije i poštanske usluge i Komisija za hartije od vrednosti dužni su da dobijena obaveštenja iz st. 2. i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima.

Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz st. 2. i 3. ovog člana, dužni su da putem odgovarajućih kanala komunikacije obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta.

Operatori IKT sistema od posebnog značaja iz st. 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima.

Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična

infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture.

Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka.

Sadržaj obaveštenja o incidentu

Član 15.

Obaveštenje o incidentu mora da sadrži sledeće podatke:

1) podatke o podnosiocu prijave;

2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela;

3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta;

4) posledice koje je incident izazvao;

5) preduzete aktivnosti radi ublažavanja posledica incidenta;

6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije;

7) informaciju o eventualnom prekograničnom dejstvu incidenta;

8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete;

9) druge relevantne informacije, po potrebi.

Značaj incidenata prema nivou opasnosti

Član 16.

Incidenti u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti svrstavaju se prema nivou opasnosti, imajući u vidu posledice incidenta, u sledeće nivoe opasnosti:

1) nizak;

2) srednji;

3) visok;

4) veoma visok.

Podzakonski akt kojim se uređuje postupak obaveštavanja o incidentima, obrasci za obaveštavanje, lista incidenata prema vrstama i klasifikacija incidenata prema nivou opasnosti donosi Vlada, na predlog Ministarstva.

Operativni tim za reagovanje na incidente

Član 17.

U cilju koordinisane reakcije na incidente visokog i veoma visokog nivoa Kancelarija za informacionu bezbednost obrazuje stalni operativni tim.

Kancelarija za informacionu bezbednost utvrđuje kriterijume za imenovanje članova operativnog tima.

Kancelarija za informacionu bezbednost može da, zavisno od prirode i posledica incidenta, zatraži uključivanje drugih organa u rad operativnog tima u okviru njihovih nadležnosti.

Po potrebi, sastancima operativnog tima mogu prisustvovati i predstavnici posebnih CERT-ova, kao i druga lica.

Lica koja učestvuju u radu stalnog operativnog tima dužna su da se sertifikuju za rad sa tajnim podacima.

Plan za reagovanje u slučaju incidenta visokog nivoa i kriza informacione bezbednosti

Član 18.

Vlada donosi Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, na predlog Kancelarije za informacionu bezbednost.

Plan iz stava 1. ovog člana obuhvata:

1) ciljeve mera i aktivnosti za reagovanje u slučaju incidenata visokog nivoa i kriza informacione bezbednosti;

2) delovanje nadležnih organa u cilju sprovođenja plana;

3) opis procedura u slučaju incidenata visokog nivoa i kriza informacione bezbednosti;

4) aktivnosti za unapređenje sposobnosti reagovanja na incidente, a pre svega planove odgovarajućih vežbi i obuka;

5) modele saradnje sa privatnim, nevladinim i akademskim sektorom;

6) međusobnu saradnju nadležnih organa.

Prilikom izrade plana iz stava 1. ovog člana uspostavlja se saradnja sa organima i pravnim licima čije su nadležnosti, odnosno poslovi i delatnosti povezani sa planiranim aktivnostima.

Plan iz stava 1. ovog člana se periodično menja i dopunjuje u skladu sa potrebama i novim okolnostima, a u celini se ponovo izrađuje i donosi svake treće godine, a ukoliko su se okolnosti u značajnoj meri promenile i ranije.

Postupanje po prijemu obaveštenja o incidentu

Član 19.

Po prijemu obaveštenja o incidentu u IKT sistemu od posebnog značaja, Kancelarija za informacionu bezbednost postupa u skladu sa nadležnostima utvrđenim zakonom, odnosno prikuplja, analizira i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i incidentu, i u vezi sa tim obaveštava, pruža podršku, upozorava i savetuje operatora IKT sistema od posebnog značaja i vrši druge poslove iz svoje nadležnosti.

Kancelarija za informacionu bezbednost, nakon izvršene analize, utvrđuje nivo opasnosti incidenta.

Kada je neophodno da javnost bude upoznata sa incidentom ili kada je incident takav da je od interesa za javnost, Kancelarija za informacionu bezbednost objavljuje informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio.

Izuzetno od stava 3. ovog člana, Kancelarija za informacionu bezbednost može objaviti informaciju o incidentu koji se dogodio u operatoru prioritetnog IKT sistema od posebnog značaja koji obavlja delatnost u oblasti bankarstva i finansijskih

tržišta iz člana 5. stav 3. tačka 1) podtačka (3) ovog zakona, uz prethodno pribavljenu saglasnost Narodne banke Srbije odnosno Komisije za hartije od vrednosti.

Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da obaveštenja o incidentima proslede:

1) nadležnom javnom tužilaštvu, odnosno ministarstvu nadležnom za unutrašnje poslove, u slučaju da je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti,

2) organu nadležnom za bezbednosne i kontraobaveštajne poslove od značaja za odbranu Republike Srbije ili organu nadležnom za poslove nacionalne bezbednosti, u slučaju da je incident povezan sa značajnim narušavanjem informacione bezbednosti koje ima ili može imati za posledicu ugrožavanje odbrane Republike Srbije ili nacionalne bezbednosti.

Prilikom upravljanja incidentom Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge označavaju obaveštenje o incidentu, odnosno informacije o incidentu u skladu sa propisima i TLP (eng.„traffic light protocol”) protokolom.

Postupanje u slučaju incidenta nivoa opasnosti „nizak”

Član 20.

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „nizak” Kancelarija za informacionu bezbednost po potrebi daje preporuke za postupanje operatoru IKT sistema od posebnog značaja.

Postupanje u slučaju incidenta nivoa opasnosti „srednji”

Član 21.

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „srednji” Kancelarija za informacionu bezbednost daje preporuke za postupanje operatoru IKT sistema od posebnog značaja.

Postupanje u slučaju incidenta nivoa opasnosti „visok”

Član 22.

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „visok” Kancelarija za informacionu bezbednost je dužna da o tome obavesti Ministarstvo.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, priprema preporuke i mere za rešavanje incidenta.

Ministarstvo nakon prijema obaveštenja iz stava 1. ovog člana saziva sednicu Tela za koordinaciju poslova informacione bezbednosti.

Nakon završetka incidenta Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, sačinjava završni izveštaj koji dostavlja Ministarstvu u roku od 30 dana nakon završenog incidenta.

Postupanje u slučaju incidenta nivoa opasnosti „veoma visok”

Član 23.

U slučaju incidenta kojem je u skladu sa klasifikacijom utvrđen nivo opasnosti „veoma visok“ i koji predstavlja krizu informacione bezbednosti, rukovođenje i koordinaciju sprovođenja mera i zadataka preduzima Vlada.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, izrađuje predlog za proglašavanje krize informacione bezbednosti, u skladu sa Planom za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, koji sadrži:

1) podatke o incidentu;

2) informacije o preduzetim merama;

3) razloge za proglašenje krize informacione bezbednosti;

4) zaduženje organa za postupanje u skladu sa svojim nadležnostima;

5) mere za rešavanje krize.

Predlog za proglašenje krize informacione bezbednosti upućuje se Ministarstvu, koje po prijemu predloga bez odlaganja saziva sednicu Tela za koordinaciju poslova informacione bezbednosti.

Vlada na predlog Ministarstva donosi odluku o proglašenju krize informacione bezbednosti i zadužuje organe da postupaju prema predloženim merama u skladu sa svojim nadležnostima.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, koordinira rešavanjem krize informacione bezbednosti i najmanje jednom nedeljno izveštava Ministarstvo i Vladu o svim aktivnostima.

Predlog za proglašenje završetka krize informacione bezbednosti upućuje se Ministarstvu.

Odluku o proglašenju završetka krize informacione bezbednosti donosi Vlada na predlog Ministarstva.

Nakon završetka krize informacione bezbednosti Kancelarija za informacionu bezbednost sačinjava završni izveštaj koji dostavlja Ministarstvu i Vladi u roku od 30 dana nakon završetka krize.

Izveštavanje tokom i nakon incidenta

Član 24.

Operatori IKT sistema od posebnog značaja dužni su da:

1) dostavljaju izveštaj o incidentu, tokom trajanja incidenta, sa opisom mera koje su preduzete za rešavanje incidenta, u jedinstveni sistem za prijem obaveštenja o incidentima i to:

(1) na svaka tri dana u slučaju incidenta srednjeg nivoa;

(2) na svaka 24 sata u slučaju incidenata visokog i veoma visokog nivoa;

2) dostavljaju obaveštenja i dodatne izveštaje o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju, na zahtev Kancelarije;

3) dostavljaju završni izveštaj o incidentu u roku od 15 dana od dana prestanka incidenta, koji sadrži sledeće podatke:

(1) vrstu i detaljan opis incidenta;

(2) vrstu pretnje i uzrok koji je doveo do incidenta;

(3) vreme i trajanje incidenta;

(4) ozbiljnost i uticaj incidenta, odnosno posledice koje je incident izazvao;

(5) informaciju o eventualnom prekograničnom dejstvu incidenta;

(6) preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge informacije od značaja za evidentiranje incidenta i statističku obradu.

Nakon završenog incidenta Kancelarija za informacionu bezbednost priprema preporuke i savete za zaštitu od potencijalnih rizika, na osnovu analize izvršenog incidenta.

Dostavljanje statističkih podataka o incidentima

Član 25.

Operator IKT sistema od posebnog značaja dužan je da, pored obaveštavanja o incidentima iz člana 13. ovog zakona, dostavi organu, odnosno organizaciji nadležnoj za poslove Nacionalnog CERT-a statističke podatke o svim incidentima u IKT sistemu, uključujući i izbegnute incidente, u prethodnoj godini najkasnije do 28. februara tekuće godine.

Organ, odnosno organizacija iz stava 1. ovog člana izveštaje o statističkim podacima dostavlja Ministarstvu i objavljuje na svojoj internet stranici.

Vrstu, formu i način dostavljanja statističkih podataka iz stava 1. ovog člana utvrđuje organ, odnosno organizacija iz stava 1. ovog člana.

III. ORGANI NADLEŽNI ZA PREVENCIJU I ZAŠTITU OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA U REPUBLICI SRBIJI

Nadležni organ

Član 26.

Organ državne uprave nadležan za informacionu bezbednost je ministarstvo nadležno za poslove informacione bezbednosti.

U okviru svojih nadležnosti Ministarstvo:

1) priprema i predlaže propise i planska dokumenta iz oblasti informacione bezbednosti u skladu sa ovim zakonom;

2) vodi evidenciju operatora IKT sistema od posebnog značaja;

3) vrši nadzor nad radom Kancelarije za informacionu bezbednost u vršenju poslova za koje je nadležna u skladu sa ovim zakonom;

4) 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;

5) ostvaruje međunarodnu saradnju u okviru svojih nadležnosti.

Telo za koordinaciju poslova informacione bezbednosti

Član 27.

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, poslove pravosuđa, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih

podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge.

U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa, 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.

Kancelarija za informacionu bezbednost

Član 28.

Radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika i incidenata u IKT sistemima u Republici Srbiji osniva se Kancelarija za informacionu bezbednost (u daljem tekstu: Kancelarija), kao posebna organizacija u smislu zakona kojim se uređuje položaj državne uprave.

Kancelarija ima svojstvo pravnog lica.

Radom Kancelarije rukovodi direktor koji mora da bude lice odgovarajuće stručnosti sa najmanje pet godina radnog iskustva u oblasti informacione bezbednosti i koga imenuje Vlada, u skladu sa zakonom kojim se uređuje položaj državnih službenika.

Kancelarija ima zamenika direktora, koji mora biti lice odgovarajuće stručnosti sa najmanje pet godina radnog iskustva u oblasti informacione bezbednosti, koji se postavlja u skladu sa propisima kojim se uređuje položaj državnih službenika i ima ovlašćenja u skladu sa propisima o državnoj upravi.

Nadzor nad radom Kancelarije

Član 29.

Nadzor nad radom Kancelarije u vršenju poslova sprovodi Ministarstvo, u skladu sa zakonom kojim se uređuje državna uprava.

Nadležnosti Kancelarije

Član 30.

Kancelarija u okviru svoje nadležnosti obavlja sledeće poslove i to:

1) vrši prevenciju i zaštitu od bezbednosnih rizika na nacionalnom nivou u skladu sa ovim zakonom (poslovi Nacionalnog CERT-a);

2) preduzima preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave u skladu sa ovim zakonom (poslovi CERT-a organa vlasti);

3) obavlja saradnju na nacionalnom nivou u oblasti informacione bezbednosti;

4) vrši poslove jedinstvene tačke kontakta;

5) vrši poslove sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga, izuzev sistema, proizvoda, procesa i usluga za potrebe odbrane i bezbednosti i IKT sistema za rad sa tajnim podacima;

6) propisuje minimalne mere zaštite IKT sistema organa, uvažavajući načela iz člana 3. ovog zakona, mere zaštite iz člana 10. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada;

7) u saradnji sa nadležnim organima i drugim subjektima iz javnog, akademskog, privrednog i nevladinog sektora učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti;

8) obavlja saradnju i razmenu informacija na međunarodnom nivou u oblasti informacione bezbednosti u cilju praćenja i usaglašavanja sa međunarodnim propisima i standardima;

9) vrši stručni nadzor nad radom operatora IKT sistema od posebnog značaja;

10) vodi bazu ranjivosti IKT proizvoda i IKT usluga;

11) izveštava Ministarstvo na kvartalnom nivou o preduzetim aktivnostima;

12) obavlja druge poslove u skladu sa ovim zakonom.

Podzakonski akt kojim se bliže uređuje način vršenja sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga iz stava 1. tačka 5) ovog člana donosi Vlada, na predlog Ministarstva.

Poslovi prevencije i zaštite od bezbednosnih rizika na nacionalnom nivou (Nacionalni CERT)

Član 31.

U okviru poslova prevencije i zaštite od bezbednosnih rizika i incidenata Kancelarija vrši poslove Nacionalnog CERT-a i to:

1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost;

2) prati stanje o incidentima u Republici Srbiji;

3) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o pretnjama, ranjivostima i incidentima;

4) reaguje bez odlaganja 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;

5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu;

6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora;

7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom;

8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje;

9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija;

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

11) vodi Evidenciju posebnih CERT-ova;

12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima;

13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima

Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za:

1) upravljanje incidentima;

2) klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata;

3) upravljanje kriznim situacijama;

4) koordinirano otkrivanje ranjivosti.

Kancelarija je ovlašćena da vrši obradu podataka o licu koje prijavi incident, pri čemu obrada podataka o licu 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.

Kancelarija obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije.

U okviru obavljanja poslova Nacionalnog CERT-a potrebno je obezbediti sledeće zahteve:

1) visok nivo dostupnosti komunikacionih kanala izbegavanjem jedinstvenih tačaka prekida i korišćenje više sredstava za dvosmerno kontaktiranje;

2) prostorije Nacionalnog CERT-a i informacioni sistemi za podršku treba da budu smešteni na sigurnim lokacijama;

3) upotrebu odgovarajućeg sistema za upravljanje zahtevima i njihovo usmeravanje, posebno kako bi se olakšala efikasna i efektivna razmena informacija;

4) obezbeđivanje poverljivosti i pouzdanosti svojih aktivnosti;

5) postojanje adekvatnih kadrovskih kapaciteta;

6) opremljenost redundantnim sistemima i rezervnim radnim prostorom kako bi se osigurao kontinuitet usluga.

Podzakonski akt kojim se bliže uređuje postupak proaktivnog skeniranja IKT sistema iz stava 1. tačka 6) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši skeniranje, kao i procedura kojom se utvrđuju uslovi u cilju zaštite bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave (CERT organa vlasti)

Član 32.

U okviru preduzimanja preventivnih i reaktivnih mera u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave (u daljem tekstu: mreža eUprave) Kancelarija obavlja sledeće poslove:

1) vrši zaštitu mreže eUprave;

2) obavlja koordinaciju i saradnju sa operatorima IKT sistema koje povezuje mreža eUprave u prevenciji incidenata;

3) aktivno učestvuje u otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;

4) vrši proaktivno skeniranje mreže operatora IKT sistema od posebnog značaja koji su korisnici mreže, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora;

5) u slučaju otkrivene ranjivosti:

(1) obaveštava operatore IKT sistema koji su korisnici mreže eUprave o tome;

(2) nalaže operatorima IKT sistema od posebnog značaja koji su korisnici mreže da preduzmu adekvatne mere zaštite u cilju sprečavanja, smanjenja i otklanjanja posledica incidenta;

6) izdaje stručne preporuke za zaštitu IKT sistema organa, osim IKT sistema za rad sa tajnim podacima;

7) donosi akt kojim se uređuje postupanje operatora IKT sistema od posebnog značaja koji koriste mreže u slučaju incidenta;

8) u saradnji sa nadležnim organima vrši procenu potrebe za stručnim usavršavanjem zaposlenih u operatorima IKT sistema od posebnog značaja koji koriste mrežu;

9) planira i organizuje proceduralne i praktične vežbe u oblasti informacione bezbednosti za zaposlene u operatorima IKT sistema od posebnog značaja koji koriste mrežu;

10) izrađuje predloge za unapređenje bezbednosnih karakteristika mreže eUprave;

11) izrađuje analize rizika i incidenata u okviru mreže eUprave;

12) obavlja druge poslove u skladu sa zakonom u cilju unapređenja informacione bezbednosti mreže eUprave.

Podzakonski akt kojim se bliže uređuje postupak proaktivnog skeniranja IKT sistema iz stava 1. tačka 4) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši skeniranje, kao i procedura kojom se utvrđuju uslovi u cilju zaštite bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Saradnja na nacionalnom nivou

Član 33.

Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema.

Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica.

Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti.

Međunarodna saradnja i poslovi jedinstvene tačke kontakta

Član 34.

Kancelarija 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.

Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema.

Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije.

Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima.

Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.

Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima

Član 35.

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 organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-a i objavljuje je javno.

Upis u evidenciju posebnih CERT-ova, koju vodi Kancelarija, 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.

Organ, odnosno organizacija iz stava 2. ovog člana propisuje sadržaj, način upisa i vođenja evidencije iz stava 3. ovog člana.

Baza ranjivosti

Član 36.

Organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-a uspostavlja i održava bazu ranjivosti IKT proizvoda i IKT usluga u Republici Srbiji i omogućava fizičkim i pravnim licima, kao i proizvođačima, dobavljačima i pružaocima usluge u IKT sistemu, da na dobrovoljnoj bazi prijave ranjivosti u IKT proizvodima ili IKT uslugama, a koje se mogu prijaviti anonimno.

Baza ranjivosti IKT proizvoda i IKT usluga sadrži:

1) podatke o ranjivosti;

2) podatke o ranjivostima IKT proizvoda ili IKT usluga.

Organ, odnosno organizacija iz stava 1. ovog člana propisuje sadržaj, procedure verifikacije ranjivosti, procedure za upravljanje tehničkim ranjivostima IKT proizvoda i IKT usluga, način upisa i vođenja registra.

Baza podataka o registraciji domena

Član 37.

Organizacije koje su ovlašćene za upravljanje registrom domena najvišeg nivoa i pružanje usluga DNS-a obavezne su da prikupljaju, čuvaju i održavaju tačne i potpune podatke o registraciji domena u posebnoj bazi podataka, uz dužnu pažnju i u skladu sa propisima o zaštiti podataka o ličnosti.

Baza podataka iz stava 1 ovog člana mora da sadrži najmanje sledeće podatke:

1) naziv domena;
2) datum registracije domena;
3) ime, kontakt adresu elektronske pošte i broj telefona registranta;
4) kontakt adresu elektronske pošte i broj telefona lica zaduženog za administraciju domena, ukoliko se razlikuju od podataka registranta.

Organizacije iz stava 1. ovog člana dužne su da usvoje i primene akte i procedure za verifikaciju tačnosti i potpunosti podataka u bazi podataka. Ove procedure moraju biti javno dostupne.

Organizacije iz stava 1. ovog člana dužne su da obezbede javnu dostupnost podataka koji nisu lični odmah po registraciji domena, a u skladu sa pravilima i uslovima registracije naziva nacionalnih internet domena.

Organizacije iz stava 1. ovog člana obavezne su da omoguće pristup specifičnim podacima o registraciji domena na osnovu zakonitih i obrazloženih zahteva ovlašćenih lica ili organa, u skladu sa ovlašćenjima dodeljenim propisima koji uređuju delokrug njihovog rada.

Odgovor na zahtev iz stava 5. ovog člana mora biti dostavljen bez odlaganja, a najkasnije u roku od 72 sata od prijema zahteva.

Akti i procedure za otkrivanje podataka na osnovu ovih zahteva moraju biti javno dostupni.

U skladu sa ovim članom, prikupljanje podataka o registraciji domena ne sme dovesti do dupliranja podataka. Organizacije iz stava 1. ovog člana dužne su da sarađuju radi izbegavanja dupliranja i osiguranja usklađenosti sa zakonom.

Ministar nadležan za informacionu bezbednost propisuje bliže uslove za prikupljanje, čuvanje, verifikaciju i objavljivanje podataka iz ovog člana, a u skladu sa najboljom praksom registara nacionalnih internet domena iz Evropske Unije, kao i Internet korporacije za dodeljene nazive i brojeve (ICANN).

Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija

Član 38.

Ministarstvo 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 radi postupanja u skladu sa utvrđenim nadležnostima.

Ministarstvo je ovlašćeno da vrši obradu podataka o licu koje se obrati Ministarstvu 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.

Podzakonski akt kojim se bliže uređuje način sprovođenja mera za bezbednost i zaštitu dece na internetu iz st. 1. i 3. ovog člana donosi Vlada na predlog Ministarstva.

IV. KRIPTOBEZBEDNOST I ZAŠTITA OD KOMPROMITUJUĆEG ELEKTROMAGNETNOG ZRAČENJA

Nadležnost

Član 39.

Ministarstvo nadležno za poslove odbrane je nadležno za poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih proizvoda koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja i poslove i zadatke u skladu sa zakonom i propisima donetim na osnovu zakona.

Poslovi i zadaci

Član 40.

U skladu sa ovim zakonom, ministarstvo nadležno za poslove odbrane:

1) organizuje i realizuje naučnoistraživački rad u oblasti kriptografske bezbednosti i zaštite od KEMZ;

2) razvija, implementira, verifikuje i klasifikuje kriptografske algoritme;

3) istražuje, razvija, verifikuje i klasifikuje sopstvene kriptografske proizvode i rešenja zaštite od KEMZ;

4) verifikuje i klasifikuje domaće i strane kriptografske proizvode i rešenja zaštite od KEMZ;

5) definiše procedure i kriterijume za evaluaciju kriptografskih bezbednosnih rešenja;

6) vrši funkciju nacionalnog organa za odobrenja kriptografskih proizvoda i obezbeđuje da ti proizvodi budu odobreni u skladu sa odgovarajućim propisima;

7) vrši funkciju nacionalnog organa za zaštitu od KEMZ;

8) vrši proveru IKT sistema sa aspekta kriptobezbednosti i zaštite od KEMZ;

9) vrši funkciju nacionalnog organa za distribuciju kriptomaterijala i definiše upravljanje, rukovanje, čuvanje, distribuciju i evidenciju kriptomaterijala u skladu sa propisima;

10) planira i koordinira izradu kriptoparametara (parametara kriptografskog algoritma), distribuciju kriptomaterijala i zaštite od kompromitujućeg elektromagnetnog zračenja u saradnji sa samostalnim operatorima IKT sistema;

11) formira i vodi centralni registar verifikovanog i distribuiranog kriptomaterijala;

12) formira i vodi registar izdatih odobrenja za kriptografske proizvode;

13) izrađuje elektronske sertifikate za kriptografske sisteme zasnovane na infrastrukturi javnih ključeva (Public Key Infrastructure – PKI);

14) predlaže donošenje propisa iz oblasti kriptobezbednosti i zaštite od KEMZ na osnovu ovog zakona;

15) vrši poslove stručnog nadzora u vezi kriptobezbednosti i zaštite od KEMZ;

16) pruža stručnu pomoć nosiocu inspekcijskog nadzora informacione bezbednosti u oblasti kriptobezbednosti i zaštite od KEMZ;

17) pruža usluge uz naknadu pravnim i fizičkim licima, izvan sistema javne vlasti, u oblasti kriptobezbednosti i zaštite od KEMZ prema propisu Vlade na predlog ministra odbrane;

18) sarađuje sa domaćim i međunarodnim organima i organizacijama u okviru nadležnosti uređenih ovim zakonom.

Sredstva ostvarena od naknade za pružanje usluga iz stava 1. tačka 17) ovog člana su prihod budžeta Republike Srbije.

Kompromitujuće elektromagnetno zračenje

Član 41.

Mere zaštite od KEMZ u IKT sistemima za rukovanje sa tajnim podacima primenjuju se u skladu sa propisima kojima se uređuje zaštita tajnih podataka.

Mere zaštite od KEMZ mogu primenjivati na sopstvenu inicijativu i operatori IKT sistema kojima to nije zakonska obaveza.

Za sve tehničke komponente sistema (uređaje, komunikacione kanale i prostore) kod kojih postoji rizik od KEMZ, a što bi moglo dovesti do narušavanja informacione bezbednosti iz stava 1. ovog člana, vrši se provera zaštićenosti od KEMZ i procena rizika od neovlašćenog pristupa tajnim podacima putem KEMZ.

Proveru zaštićenosti od KEMZ vrši ministarstvo nadležno za poslove odbrane.

Samostalni operatori IKT sistema mogu vršiti proveru KEMZ za sopstvene potrebe.

Podzakonski akt kojim se bliže uređuju uslovi za proveru KEMZ i način procene rizika od oticanja podataka putem KEMZ donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Mere kriptozaštite

Član 42.

Mere kriptozaštite za rukovanje sa tajnim podacima u IKT sistemima primenjuju se u skladu sa propisima kojima se uređuje zaštita tajnih podataka.

Mere kriptozaštite se mogu primeniti i prilikom prenosa i čuvanja podataka koji nisu označeni kao tajni u skladu sa zakonom koji uređuje tajnost podataka, kada je na osnovu zakona ili drugog pravnog akta potrebno primeniti tehničke mere ograničenja pristupa podacima i radi zaštite integriteta, autentičnosti i neporecivosti podataka.

Podzakonski akt kojim se uređuju tehnički uslovi za kriptografske algoritme, parametre, protokole i informaciona dobra u oblasti kriptozaštite koji se u Republici Srbiji koriste u kriptografskim proizvodima radi zaštite tajnosti, integriteta, autentičnosti, odnosno neporecivosti podataka donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Odobrenje za kriptografski proizvod

Član 43.

Kriptografski proizvodi koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, u skladu sa zakonom, moraju biti verifikovani i odobreni za korišćenje.

Podzakonski akt kojim se bliže uređuju uslovi koje moraju da ispunjavaju kriptografski proizvodi iz stava 1. ovog člana donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Izdavanje odobrenja za kriptografski proizvod

Član 44.

Odobrenje za kriptografski proizvod izdaje ministarstvo nadležno za poslove odbrane, na zahtev operatora IKT sistema, proizvođača kriptografskog proizvoda ili drugog zainteresovanog lica.

Odobrenje za kriptografski proizvod se može odnositi na pojedinačni primerak kriptografskog proizvoda ili na određeni model kriptografskog proizvoda koji se serijski proizvodi.

Odobrenje za kriptografski proizvod može imati rok važenja.

Ministarstvo nadležno za poslove odbrane rešava po zahtevu za izdavanje odobrenja za kriptografski proizvod u roku od 45 dana od dana podnošenja urednog zahteva, koji se može produžiti u slučaju posebne složenosti provere najviše za još 60 dana.

Protiv rešenja iz stava 4. ovog člana žalba nije dopuštena, ali može da se pokrene upravni spor.

Ministarstvo nadležno za poslove odbrane vodi registar izdatih odobrenja za kriptografski proizvod.

Registar iz stava 6. ovog člana od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkcija i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte. Ministarstvo nadležno za poslove odbrane objavljuje javnu listu odobrenih modela kriptografskih proizvoda za sve modele kriptografskih proizvoda za koje je u zahtevu za izdavanje odobrenja naglašeno da model kriptografskog proizvoda treba da bude na javnoj listi i ako je zahtev podneo proizvođač ili lice ovlašćeno od strane proizvođača predmetnog kriptografskog proizvoda.

Ministarstvo nadležno za poslove odbrane prethodno izdato odobrenje za kriptografski proizvod može povući ili promeniti uslove iz st. 2. i 3. ovog člana iz razloga novih saznanja vezanih za tehnička rešenja primenjena u proizvodu, a koja utiču na ocenu stepena zaštite koji pruža proizvod.

Podzakonski akt kojim se bliže uređuje sadržaj zahteva za izdavanje odobrenja za kriptografski proizvod, uslove za izdavanje odobrenja za kriptografski proizvod, način izdavanja odobrenja i vođenja registra izdatih odobrenja za kriptografski proizvod donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Opšte odobrenje za korišćenje kriptografskih proizvoda

Član 45.

Samostalni operatori IKT sistema imaju opšte odobrenje za korišćenje kriptografskih proizvoda.

Operator IKT sistema iz stava 1. ovog člana samostalno ocenjuje stepen zaštite koji pruža svaki pojedinačni kriptografski proizvod koji koristi, a u skladu sa propisanim uslovima.

Registri u kriptozaštiti

Član 46.

Samostalni operatori IKT sistema koji imaju opšte odobrenje za korišćenje kriptografskih proizvoda ustrojavaju i vode registre kriptografskih proizvoda, kriptomaterijala, pravila i propisa i lica koja obavljaju poslove kriptozaštite.

Registar lica koja obavljaju poslove kriptozaštite od podataka o ličnosti sadrži sledeće podatke o licima koja obavljaju poslove kriptozaštite: prezime, ime oca i ime, datum i mesto rođenja, matični broj, telefon, adresu elektronske pošte, školsku spremu, podatke o završenom stručnom osposobljavanju za poslove kriptozaštite, naziv radnog mesta, datum početka i završetka rada na poslovima kriptozaštite.

Registar kriptomaterijala za rukovanje sa stranim tajnim podacima vodi Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, u skladu sa ratifikovanim međunarodnim sporazumima.

Podzakonski akt kojim se bliže uređuje vođenje registara iz stava 1. ovog člana donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

V. NADLEŽNOSTI I ODGOVORNOSTI SUBJEKATA ZA NADZOR NAD SPROVOĐENJEM OVOG ZAKONA

Inspekcija za informacionu bezbednost

Član 47.

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 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.

Ovlašćenja inspektora za informacionu bezbednost

Član 48.

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 utvrdi razuman rok;

2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok;

3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika;

4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način;

5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama.

Podzakonski akt kojim se bliže uređuje postupak skeniranja, konfiguracija i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti iz stava 1. tačka 3) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši aktivnosti iz stava 1. tačka 3) ovog člana, kao i procedura kojom se utvrđuju uslovi u cilju zaštite bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Stručni nadzor

Član 49.

Stručni 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, vrši Kancelarija, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor.

Poslove stručnog nadzora obavlja ovlašćeno lice zaposleno u Kancelariji (u daljem tekstu: ovlašćeno lice).

U postupku stručnog nadzora ovlašćeno lice ima pravo i obavezu da kontroliše:

1) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj;

2) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite;

3) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema sa aktom o bezbednosti;

4) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost.

Ako u vršenju stručnog nadzora Kancelarija utvrdi nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, o tome obaveštava nadziranog subjekta i određuje mu rok u kome je dužan da ih otkloni.

Rok iz stava 4. ovog člana ne može biti kraći od osam dana od dana prijema obaveštenja, osim u slučajevima koji zahtevaju hitno postupanje.

Ako Kancelarija utvrdi da nadzirani subjekat nije, u ostavljenom roku, otklonio utvrđene nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, podnosi prijavu inspekciji.

Kancelarija je dužna da po zahtevu inspektora za informacionu bezbednost obavi stručni nadzor i dostavi informaciju o utvrđenom činjeničnom stanju.

Obrazac legitimacije i način izdavanja legitimacije ovlašćenog lica utvrđuje Kancelarija.

Legitimacija ovlašćenog lica obavezno sadrži: grb Republike Srbije i naziv Kancelarije, ime i prezime ovlašćenog lica, fotografiju ovlašćenog lica, službeni broj legitimacije, datum izdavanja legitimacije, pečat Kancelarije, potpis direktora Kancelarije, kao i odštampani tekst sledeće sadržine: „Imalac ove legitimacije ima ovlašćenja u skladu sa odredbama člana 49. st. 3. i 4. Zakona o informacionoj bezbednosti.”

VI. KAZNENE ODREDBE

Član 50.

Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema ako:

1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona;

2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona;

3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona;

4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona;

5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona;

6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona;

7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Član 51.

Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema ako:

1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona;

2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona;

3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona;

4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona;

5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona;

6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona;

7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Član 52.

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema ako:

1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona;

2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona;

3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara.

Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Izuzetno od st. 1–3. ovog člana, ako finansijska institucija ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu, Narodna banka Srbije izriče toj finansijskoj instituciji mere i kazne u skladu sa zakonom kojim se uređuje njeno poslovanje.

Član 53.

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema ako:

1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona;

2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona;

3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara.

Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

VII. PRELAZNE I ZAVRŠNE ODREDBE

Rokovi za donošenje podzakonskih akata

Član 54.

Podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona.

Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti iz člana 18. ovog zakona donosi se u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Član 55.

Operatori IKT sistema od posebnog značaja koji su određeni Zakonom o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16, 94/17 i 77/19) nastavljaju da postupaju u skladu sa obavezama utvrđenim čl. 6a-11b tog zakona do 31. decembra 2025. godine.

Na operatore IKT sistema od posebnog značaja koji su određeni Zakonom o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16, 94/17 i 77/19) do datuma iz stava 1. ovog člana primenjuju se kaznene odredbe iz čl. 30. i 31. tog zakona.

Operatori IKT sistema od posebnog značaja dužni su da donesu akt iz člana 11. stav 1. ovog zakona u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a dužna je da, u roku od devet meseci od dana stupanja na snagu ovog zakona, donese opštu metodologiju za procenu rizika u IKT sistemima od posebnog značaja iz člana 11. stav 4. ovog zakona.

Operator IKT sistema od posebnog značaja dužan je da donese akt iz člana 12. ovog zakona u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Član 56.

Kancelarija za informacionu bezbednost uspostavlja se i poslove iz svoje nadležnosti propisane ovim zakonom počinje da obavlja 1. januara 2027. godine.

Poslove Kancelarije za informacionu bezbednost propisane ovim zakonom, izuzev poslova Nacionalnog CERT-a, obavljaće Kancelarija za informacione tehnologije i elektronsku upravu u periodu koji počinje danom nastupanja 12 meseci od dana stupanja na snagu ovog zakona i koji traje do 1. januara 2027. godine.

Regulatorno telo za elektronske komunikacije i poštanske usluge obavlja poslove Nacionalnog CERT-a utvrđene ovim zakonom do uspostavljanja Kancelarije za informacionu bezbednost odnosno do 1. januara 2027. godine.

Kancelarija za informacionu bezbednost preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Regulatornog tela za elektronske komunikacije i poštanske usluge nastalu u obavljanju poslova Nacionalnog CERT-a potrebne za vršenje stručnih poslova utvrđenih ovim zakonom.

Kancelarija za informacionu bezbednost počev od datuma iz stava 1. ovog člana preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Kancelarije za informacione tehnologije i elektronsku upravu nastalu u obavljanju poslova propisanih ovim zakonom iz nadležnosti Kancelarije za informacionu bezbednost.

Prestanak važenja Zakona o informacionoj bezbednosti

Član 57.

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16, 94/17 i 77/19), izuzev odredbi čl. 6a-11b i čl. 30. i 31. koje važe do 31. decembra 2025. godine.

Podzakonski akti doneti na osnovu Zakona o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16, 94/17 i 77/19) primenjivaće se do stupanja na snagu podzakonskih akata koji se donose u skladu sa ovim zakonom.

Stupanje na snagu

Član 58.

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom glasniku Republike Srbije”, izuzev člana 29. ovog zakona koji počinje da se primenjuje 1. januara 2027. godine.

OBRAZLOŽENjE

I. USTAVNI OSNOV

Ustavni osnov za donošenje Zakona o informacionoj bezbednosti sadržan je u članu 97. tačka 12. Ustava Republike Srbije, kojim je predviđeno da Republika Srbija uređuje i obezbeđuje razvoj Republike Srbije, politiku i mere za podsticanje ravnomernog razvoja pojedinih delova Republike Srbije, uključujući i razvoj nedovoljno razvijenih područja; organizaciju i korišćenje prostora; naučno-tehnološki razvoj.

II. RAZLOZI ZA DONOŠENjE ZAKONA

Kako bi se Republika Srbija uspešno uključila u jedinstveno evropsko digitalno tržište neophodno je obezbediti regulatorne i institucionalne uslove za ubrzan razvoj digitalnog tržišta u Republici Srbiji, kao i obezbediti da se taj razvoj odvija u sigurnim uslovima kako za svakog pojedinca, tako i za društvo u celini.

U digitalnom okruženju koje se menja, imperativ je da Vlada, poslovni subjekti i organizacije rade zajedno na razvoju regulatornog okvira koji unapređuje IKT sisteme i mreže na način da je omogućeno bezbedno i neometano čuvanje podataka i pružanje usluga, kao i odvijanje drugih procesa. Sa konstantnim porastom upotrebe IKT u svakodnevnom životu, kao i sa porastom broja usluga koje se nude građanima elektronskim putem, neophodno je blagovremeno odgovoriti na brojne izazove i pratiti dinamičan razvoj sektora uz obavezu stalnog usklađivanja i praćenja propisa Evropske unije iz ove oblasti.

Oblast informacione bezbednosti uređena je Zakonom o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16, 94/17 i 77/19, u daljem tekstu: ZIB) i podzakonskim aktima donetim na osnovu tog zakona.

ZIB se oslanja na Direktivu EU 2016/1148 Evropskog parlamenta i Saveta od 6. jula 2016. godine koja se tiče mera za visoki zajednički nivo bezbednosti mreža i informacionih sistema (u daljem tekstu: NIS1). U procesu ispunjavanja uslova za punopravno članstvo u Evropskoj uniji, Republika Srbija je dužna da svoje zakonodavstvo uskladi sa pravnim tekovinama Evropske unije u oblasti informacione bezbednosti. U međuvremenu, EU je svoj regulatorni okvir upotpunila i revidirala usvajanjem nove Direktive (EU) 2022/2055 Evropskog parlamenta i Saveta od dana 14. decembra 2022. godine o merama za visok zajednički nivo sajber bezbednosti (u daljem tekstu NIS2). U tom smislu, prvi razlog donošenja novog zakona leži u potrebi da se regulatorni okvir usaglasi sa okvirom koji je na snazi u EU kako bi se blagovremeno ispratili razvojni trendovi u ovoj oblasti i omogućilo da se upotreba IKT u Republici Srbiji odvija u skladu sa najsavremenijim regulatornim tendencijama.

Direktiva NIS2 sa sobom donosi redefinisan pristup informacionoj bezbednosti, prevashodno u smislu identifikacije operatora IKT sistema od posebnog značaja i razlikovanja istih na prioritetne i važne, uz propratne obaveze i pojačani inspekcijski nadzor i reviziju, kao i strožu kaznenu politiku. Direktiva jača ulogu Nacionalnog CERT-a u smislu nadležnosti i reagovanja na incident ili pretnju da može doći do incidenta, omogućava bolju koordinaciju nadležnih organa i detaljnije uređuje pitanje međunarodne saradnje i razmene informacija.

Takođe, imajući u vidu opseg ovih propisa i dodatne obaveze na strani državnih organa da omoguće bezbednu upotrebu IKT, stvorila se i potreba za revizijom dosadašnjeg institucionalnog okvira sa ciljem da se nadležni organi pripreme za neophodan razvoj kapaciteta za odgovor na rizike i pretnje prilikom upotrebe IKT sistema i mreža.

Imajući u vidu navedeno, najznačajniji ciljevi koji se donošenjem novog zakona u oblasti informacione bezbednosti imaju postići jesu usklađivanje sa NIS2 Direktivom sa svrhom da se utvrdi regulatorni okvir koji odgovara savremenim razvojnim tendencijama na tlu Evrope i ispuni obaveza iz Sporazuma o stabilizaciji i pridruživanju i postupka pristupanja Republike Evropskoj uniji, kao i da se unapredi institucionalni okvir sa ciljem da se on osposobi da pravilno primenjuje novouspostavljene obaveze i nadležnosti. Pored toga, ovom izmenom zakonskog okvira potrebno je i unaprediti postojeća rešenja na osnovu iskustva iz dosadašnje primene, kao i organizaciono i strukturalno unaprediti zakonski tekst.

Predlogom zakona uređuju se sledeće oblasti:

1) osnovne odredbe, kojima se uređuje predmet zakona kao i značenje pojedinih pojmova koji se koriste u zakonu;
2) bezbednost IKT sistema od posebnog značaja;
3) pravni položaj i nadležnosti organa nadležnih za prevenciju i zaštitu od bezbednosnih rizika u IKT sistemima u Republici Srbiji;
4) kriptobezbednost i zaštita od kompromitujućeg elektromagnetnog zračenja;
5) nadležnosti i odgovornosti subjekata za nadzor nad sprovođenjem zakona;
6) kaznene odredbe;
7) prelazne i završne odredbe.

Osnovni razlozi zbog kojih se predlaže donošenje zakona su:

- unapređenje zakonskih rešenja i otklanjanje nedostataka važećeg zakona koji su uočeni kroz njegovu dosadašnju primenu;
- sprovođenje aktivnosti koje su usmerene na dalje jačanje kapaciteta i razvojnih mogućnosti organa nadležnih za oblast informacione bezbednosti;
- unapređenje bezbedne upotrebe IKT sistema i mreža u Republici Srbiji;
- promovisanje dodatnog jačanja konkurencije na tržištu daljim razvojem načina pružanja usluga elektronskim putem;
- unapređenje zaštite neometanog pružanja usluga elektronskim putem, kao i bezbednosti čuvanja podataka;
- stimulisanje domaćih i stranih investicija;
- uspostavljanje pravnog osnova i nadležnosti za razvoj okvira i šema sertifikacije IKT proizvoda, procesa i usluga;
- stvaranje optimalnih uslova za bezbedno korišćenje IKT od strane pojedinaca, organizacija, privrednih subjekata i državnih organa i organizacija.

Ovom regulatornom izmenom postižu se ciljevi koji se tiču usklađenosti sa važećim regulatornim okvirom EU, ostvaruje se kreiranje regulatornog okvira koji je u stanju da omogući unapređeni i koordinisani zajednički odgovor na informaciono - bezbednosne rizike i pretnje i unapređuju se institucionalni kapaciteti na način koji će omogućiti njihov dalji razvoj i stvaranje sposobnosti da preuzmu proširene nadležnosti i zadatke.

Imajući u vidu da je u postupku pridruživanja Evropskoj uniji Republika Srbija preuzela obavezu da uskladi svoje zakonodavstvo sa propisima Evropske unije, potrebno je izvršiti usklađivanje zakonodavstva donošenjem ovog zakona i time ispuniti preuzete obaveze. Kako je pristup informacionoj bezbednosti novim okvirom fundamentalno izmenjen i uvode se pojedine nove tematske oblasti u vezi sa kojima postoji pravna praznina, kao i da značajnije unapređenje institucionalnog okvira može samo zakonom da se uspostavi, ni jedna druga mogućnost osim zakonodavna izmena nije adekvatna za ostvarenje ovih ciljeva. Zakoni, a posebno sistemski, predstavljaju osnov za razvoj oblasti.

Svi navedeni efekti novog zakona treba da omoguće adekvatan odgovor na rizike i pretnje u vezi sa upotrebom IKT u odvijanju svakodnevnih aktivnosti, pružanju usluga i cirkulisanju podataka.

Takođe, izražena je potreba da i zakonska rešenja budu fleksibilna i otvorena za nova tehnološka dostignuća, da se zasnivaju na rešenjima sadržanim u međunarodnim dokumentima, propisima i standardima Evropske unije, a posebno na rešenjima tehnološki razvijenih zemalja.

Donošenje ovog zakona nije samo najbolji, već je, u postojećem normativnom okviru i jedini način za rešavanje problema i dostizanje ciljeva, ali i za potpuno transponovanje evropskog regulatornog okvira.

Najvažnija zakonska rešenja odnose se na:

- Definisanje prioritetnih i važnih IKT sistema od posebnog značaja;
- Osnivanje Kancelarije za informacionu bezbednost;
- Određivanje aktivnosti koje IKT sistemi od posebnog značaja treba da preduzmu radi zaštite bezbednosti IKT sistema (mere zaštite, procena rizika, akt o bezbednosti);
- Procedure u slučaju incidenta koji značajno ugrožavaju informacionu bezbednost operatora IKT sistema;
- Aktivnu ulogu Nacionalnog CERT-a i CERT-a organa u otklanjanju incidenata u IKT sistemima;
- Proširena inspekcijska ovlašćenja.

Shodno odredbama NIS2 direktive, ovim zakonom se definišu operatori IKT sistema od posebnog značaja koji se dele na prioritetne i važne. Prioritetni IKT sistemi od posebnog značaja od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Reč je o IKT sistemima u oblastima koje su vitalne za funkcionisanje društva (energetika, zdravstvo, bankarstvo i druge oblasti) i koji zbog svog značaja moraju da budu bezbedni kako bi se delatnosti obavljale neometano.

Pored ovih sistema, zakon propisuje i važne IKT sisteme od posebnog značaja, i to iz oblasti čije bi ugrožavanje potencijalno moglo da ima nepovoljan efekat na javni interes, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik.

Usled neophodnosti da funkcionišu nesmetano i sačuvaju integritet podataka i usluga koje pružaju, IKT sistemi od posebnog značaja treba da budu zaštićeni primenom različitih mera (primena mera zaštite u skladu sa zakonom, nacionalnim i međunarodnim standardima, odgovarajuća procena rizika, donošenje akta o bezbednosti, redovne periodične provere IKT sistema).

Posebna novina u odnosu na postojeći zakonski režim je obavezno obavljanje procene rizika IKT sistema i donošenje Akta o proceni rizika IKT sistema, imajući u vidu da organizacije moraju da budu svesne opasnosti koje mogu da ugroze informacionu bezbednost i na osnovu toga preduzmu mere zaštite odgovarajućeg nivoa u odnosu na potencijalni rizik.

Zakon predviđa procedure u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Predložena je klasifikacija incidenata prema nivou opasnosti, kao i postupanje nadležnih organa zavisno od nivoa opasnosti. Definisano je i postupanje u slučaju krize informacione bezbednosti, koja je događaj ili stanje koje ugrožava, ometa rad ili onemogućuje rad IKT sistema od posebnog značaja i pri tom izaziva rizike, pretnje ili posledice po stanovništvo, materijalna dobra ili životnu sredinu izuzetno velikog obima i intenziteta koje nije moguće sprečiti ili otkloniti redovnim delovanjem nadležnih organa i službi, a odgovor na takav događaj ili stanje zahteva učešće više nadležnih organa, kao i primenu odgovarajućih mera.

U skladu sa sve češćom praksom drugih razvijenih zemalja, koje osnivaju organe posebno zadužene za informacionu bezbednost, tako i naša zemlja planira da ovim zakonom osnuje Kancelariju za informacionu bezbednost.

Kancelarija za informacionu bezbednost, koja bi imala status posebne organizacije u smislu zakona kojim se uređuje državna uprava i koja bi počela sa svojim radom 1. januara 2027. godine, treba da udruži postojeće resurse u oblasti informacione bezbednosti i time poboljša odgovor Republike Srbije na izazove u oblasti informacione bezbednosti. Planirano je da Kancelarija za informacionu bezbednost vrši poslove koordinacije i upravljanja odgovorom na incidente u IKT sistemima od posebnog značaja koji značajno ugrožavaju informacionu bezbednost, kako bi se blagovremeno i adekvatno reagovalo na incidente u ovim sistemima. Kancelarija za informacionu bezbednost biće dužna da reaguje hitno i bez odlaganja i da aktivno učestvuje u otklanjanju incidenta koji mogu da naruše bezbednost IKT sistema od posebnog značaja, kao i da ugroze funkcionisanje države, privrede i građana. Takođe, Kancelarija za informacionu bezbednost obavlja poslove Nacionalnog CERT-a, CERT-a Jedinstvene informaciono-komunikacione mreže elektronske uprave, vrši poslove jedinstvene tačke kontakta u međunarodnoj saradnji, propisuje minimalne mere zaštite IKT sistema organa, u saradnji sa nadležnim organima i drugim subjektima iz javnog, akademskog, privrednog i nevladinog i privatnog sektora učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti u organima i druge poslove u skladu sa zakonom. Zakonom je predviđeno da do obrazovanja Kancelarije za informacionu bezbednost, a u periodu koji počinje danom nastupanja 12 meseci od dana stupanja na snagu ovog zakona, ove poslove vrši Kancelarija za informacione tehnologiju i elektronsku upravu.

Zakonom se uređuju i poslovi kriptobezbednosti i zaštite od kompromitujućeg elektromagnetnog zračenja (KEMZ). Ministarstvo odbrane, kao i u dosadašnjem zakonskom režimu, poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih proizvoda koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja i poslove i zadatke u skladu sa zakonom i propisima donetim na osnovu zakona.

Pored ovoga, predložene su i odredbe koje se odnose na nadzor nad primenom ovog zakona i sankcije u slučaju nepoštovanja odredbi.

III. OBJAŠNjENjE POJEDINIH REŠENjA

Član 1. Predloga zakona – Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite, praćenje pravilne primene propisanih mera zaštite, kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.

Član 2. Predloga zakona – ovim članom utvrđuje se značenje pojedinih termina u smislu ovog zakona.

Član 3. Predloga zakona – ovim članom utvrđuju se načela informacione bezbednosti prilikom planiranja i primene mera zaštite IKT sistema.

Član 4. Predloga zakona – propisuje se opšte pravilo u vezi sa obradom podataka o ličnosti.

Član 5. Predloga zakona – ovim članom utvrđuju se prioritetni operatori IKT sistema od posebnog značaja, odnosno oni operatori IKT sistema od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno

zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori su identifikovani prema delatnostima u sledećim oblastima: energetika, saobraćaj, bankarstvo i finansijska tržišta, zdravstvo, voda za piće, otpadne vode, digitalna infrastruktura, pružanje usluga IKT operatorima IKT sistema od posebnog značaja, upravljanje nuklearnim objektima, pružanje kvalifikovanih usluga od poverenja, pružanje usluga mreže za isporuku sadržaja, pružanje usluga DNS, delatnost elektronskih komunikacija, tačka za razmenu internet saobraćaja, izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije i ona delatnost gde postoji samo jedan pružalac usluge. Pored ovih subjekata, prioritetnim operatorima IKT sistema smatraju se organi javne vlasti, svi subjekti koji su prepoznati kao operatori kritične infrastrukture i operatori koji su po postojećem zakonu prepoznati kao operatori IKT sistema u navedenim delatnostima.

Član 6. Predloga zakona – ovim članom uređuju se važni operatori IKT sistema od posebnog značaja čiji bi prekid ili poremećaj u pružanju usluga mogao da ima značajan uticaj na javni interes, funkcionisanje drugih sektora ili bi se stvorio značajan sistemski rizik. Oni su prepoznati kao operatori u sledećim delatnostima: poštanske usluge, upravljanje otpadom, upravljanje ambalažnim otpadom, proizvodnja i snabdevanje hemikalijama, proizvodnja, prerada i distribucija hrane, računara i elektronskih i optičkih proizvoda, proizvodnja električne opreme, mašina i uređaja, motornih vozila, prikolica i poluprikolica, medicinskih uređaja, usluge informacionog društva, naoružanje i vojna oprema, naučnoistraživački rad, kao i operatori u delatnostima iz člana 5. koji ne prođu sektorski prag za prioritetne operatore IKT sistema. Predviđeno je i donošenje podzakonskog akta kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema od posebnog značaja koje donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti.

Član 7. Predloga zakona – ovim članom uređuju se obaveze operatora IKT sistema u smislu ovog zakona.

Član 8. Predloga zakona – ovim članom uređuju se obaveze samostalnih operatora IKT sistema u smislu ovog zakona.

Član 9. Predloga zakona – ovim članom uređuju se pitanja vođenja evidencije operatora IKT sistema od posebnog značaja, izuzeci od obaveze upisa u evidenciju, sadržina i podaci koji se unose u evidenciji, svrha obrade podataka o ličnosti.

Član 10. Predloga zakona – ovim članom propisuju se mere zaštite IKT sistema koje je svaki operator IKT sistema od posebnog značaja dužan da preduzima.

Član 11. Predloga zakona – ovim članom propisuje obaveza donošenja Akta o proceni rizika IKT sistema od posebnog značaja.

Član 12. Predloga zakona – ovim članom propisuje se obaveza donošenja Akta o bezbednosti IKT sistema od posebnog značaja.

Član 13. Predloga zakona – ovim članom uređuje se obaveza obaveštavanja operatora IKT sistema od posebnog značaja o incidentima koji značajno narušavaju informacionu bezbednost.

Član 14. Predloga zakona – ovim članom uređuje se dostavljanje obaveštenja o incidentima, dok se izuzeci odnose na Narodnu banku Srbije, Komisiju za hartije od vrednosti, Regulatorno telo za elektronske komunikacije i poštanske usluge, kao i način postupanja po prijavi o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura, u skladu sa zakonom kojim se uređuje kritična infrastruktura.

Član 15. Predloga zakona – ovim članom uređuje se sadržaj obaveštenja o incidentu, koje sadrži podatke koji se odnose na podnosioca prijave, vrstu i opis incidenta, datum i vreme početka i trajanja incidenta, posledice koje je incident izazvao, preduzete aktivnosti, procenu nivoa opasnosti i uticaja incidenta na IKT sistem i druge relevantne informacije.

Član 16. Predloga zakona – ovim članom vrši se identifikacija incidenata prema njihovom značaju i dometu, kao i nivou opasnosti.

Član 17. Predloga zakona – ovim članom uspostavlja se stalni operativni tim za reagovanje na incidente „visokog” i „veoma visokog” nivoa, koji obrazuje Kancelarija za informacionu bezbednost.

Član 18. Predloga zakona – ovim članom uređuje se plan za reagovanje u slučaju incidenta „visokog” nivoa i krize informacione bezbednosti, koji donosi Vlada na predlog Kancelarije za informacionu bezbednost.

Član 19. Predloga zakona – ovim članom uređuje se postupanje po prijemu obaveštenja o incidentu.

Član 20 - 23. Predloga zakona – ovim članom uređuje se postupanje u slučaju incidenta prema sledećem nivoima opasnosti: „nizak”, „srednji”, „visok” i „veoma visok”.

Član 24. Predloga zakona – ovim članom uređuje se način izveštavanja operatora IKT sistema od posebnog o incidentu, tokom incidenta i nakon incidenta u zavisnosti od nivoa opasnosti.

Član 25. Predloga zakona – ovim članom uređuje se obaveza i način dostavljanja statističkih podataka o incidentima.

Član 26 - 27. Predloga zakona – ovim članovima uređuje se nadležnost Ministarstva informisanja i telekomunikacija i uspostavlja se Telo za koordinaciju poslova informacione bezbednosti.

Član 28. Predloga zakona – ovim članom predviđa se osnivanje Kancelarije za informacionu bezbednost (u daljem tekstu: Kancelarija), kao posebne organizacija u smislu zakona kojim se uređuje položaj državne uprave.

Član 29. Predloga zakona – ovim članom uređuje se nadzor nad radom Kancelarije.

Član 30. Predloga zakona – ovim članom utvrđuju se nadležnosti Kancelarije.

Član 31. Predloga zakona – ovim članom uređuju se poslovi Nacionalnog CERT-a koje Kancelarija obavlja u okviru prevencije i zaštite od bezbednosnih rizika i incidenata.

Član 32. Predloga zakona - utvrđuju se poslovi CERT-a Jedinstvene informaciono - komunikacione mreže elektronske uprave koje Kancelarija obavlja u okviru preduzimanja preventivnih i reaktivnih mera u cilju zaštite CERT-a organa vlasti.

Član 33. - 34. Predloga zakona – ovim članovima uređuje se saradnja nadležnih organa na nacionalnom nivou, kao i međunarodna saradnja i poslovi jedinstvene tačke kontakta za razmenu informacija o incidentima.

Član 35. Predloga zakona - ovim članom uređuju se pitanja posebnih centara za prevenciju bezbednosnih rizika u IKT sistemima.

Član 36. Predloga zakona – ovim uređuje se obaveza uspostavljanja i održavanje baze ranjivosti.

Član 37. Predloga zakona – ovaj član se odnosi na Bazu podataka o registraciji domena.

Član 38. Predloga zakona – ovim članom uređuje se pitanje zaštite dece pri korišćenju IKT tehnologija.

Član 39. - 46. Predloga zakona – ovim članovima uređuje se pitanje odobravanja kriptografskih proizvoda, distribucija kriptomaterijala i zaštita od kompromitujućeg elektromagnetnog zračenja.

Član 47. – 48. Predloga zakona – ovim članovima reguliše se rad inspekcije za informacionu bezbednost i propisuju ovlašćenja inspektora za informacionu bezbednost.

Član 49. Predloga zakona uređuje stručni nadzor.

Član 50. - 53. Predloga zakona – ovim članovima propisuju se iznosi novčane kazne za prekršaj koji učine pravno lice, odgovorno lice u pravnom licu, kao i preduzetnik i one su podeljene u više raspona zavisno od utvrđenog prekršaja.

Član 54. - 58. Predloga zakona – ovim članovima uređuju se prelazne i završne odredbe i to: rokovi za donošenje podzakonskih akata, primena određenih odredbi Zakona o informacionoj bezbednosti koji je na snazi, datum uspostavljanja Kancelarije za informacionu bezbednost, vršenje poslova Nacionalnog CERT-a do uspostavljanja Kancelarije, prestanak važenja Zakona o informacionoj bezbednosti i stupanje na snagu.

IV. PROCENA FINANSIJSKIH SREDSTAVA POTREBNIH ZA SPROVOĐENjE ZAKONA

Za sprovođenje ovog zakona u 2025, 2026. i 2027. godini nisu potrebna finansijska sredstva iz budžeta Republike Srbije sa razdela Ministarstva informisanja i telekomunikacija.

Za sprovođenje ovog zakona u 2026. godini potrebna su dodatna sredstva u Budžetu Republike Srbije na razdelu Kancelarije za informacione tehnologije u ukupnom iznosu od 46.700.000 dinara, i to na sledećim pozicijama:

- izvor finansiranja 01 – Opšti prihodi i primanja budžeta, Funkcija – 140 – Osnovno istraživanje, Program 0614 – Informacione tehnologije i elektronska uprava, Programska aktivnost 0002 - Razvoj IT i informacione bezbednosti, ekonomska klasifikacija 411 – Plate, dodaci i naknade zaposlenih, u iznosu od 40.000.000 dinara;
- izvor finansiranja 01 – Opšti prihodi i primanja budžeta, Funkcija – 140 – Osnovno istraživanje, Program 0614 – Informacione tehnologije i elektronska uprava, Programska aktivnost 0002 - Razvoj IT i informacione bezbednosti, ekonomska klasifikacija 412 - Socijalni doprinosi na teret poslodavca, u iznosu od 6.000.000 dinara;
- izvor finansiranja 01 – Opšti prihodi i primanja budžeta, Funkcija – 140 – Osnovno istraživanje, Program 0614 – Informacione tehnologije i elektronska uprava, Programska aktivnost 0002 - Razvoj IT i informacione bezbednosti, ekonomska klasifikacija 415 – Naknade troškova za zaposlene, u iznosu od 700.000 dinara.

Za sprovođenje zakona u 2025. i 2027. godini nisu potrebna sredstva na razdelu Kancelarije za informacione tehnologije i elektronsku upravu.

Predviđa se da će za rad Kancelarije za informacionu bezbednost čiji je početak rada planiran 1. januara 2027. godine biti potrebno da se u 2027. godini u Budžetu Republike Srbije obezbedi 150.000.000 dinara, od čega na:

- ekonomskoj klasifikaciji 411 – Plate dodaci i naknade zaposlenih iznos od 40.000.000 dinara;
- ekonomskoj klasifikaciji 412 – Socijalni doprinosi na teret poslodavca iznos od 6.000.000 dinara;
- ekonomskoj klasifikaciji 423 – Usluge po ugovoru iznos od 45.000.000 dinara;
- ekonomskoj klasifikaciji 512 – Mašine i oprema iznos od 50.000.000 dinara;
- ekonomskoj klasifikaciji 515 - Nematerijalna imovina iznos od 9.000.000 dinara.

ANALIZA EFEKATA ZAKONA O INFORMACIONOJ BEZBEDNOSTI

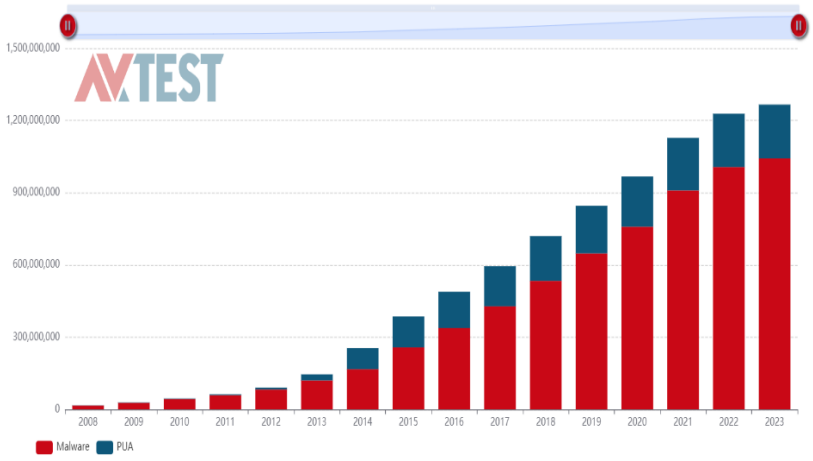
1) Koji pokazatelji se prate u oblasti, koji su razlozi zbog kojih se ovi pokazatelji prate i koje su njihove vrednosti?

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

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

U Strategiji za digitalnu dekadu EU navedeno je da je procena globalne štete od incidenata - sajber napada u 2020. godini bila oko 5.5 triliona evra. Procenjuje se da je oko 12% kompanija u EU bilo na neki način pogođeno sajber napadom, dok je samo 2019. godine zabeleženo 450 incidenata koji su pogodili kritičnu infrastrukturu EU. Evidentan problem je i nedostatak radne snage sa procenom da oko 291.000 ponuda za posao u oblasti informacione bezbednosti nisu realizovane.

Broj malvera i potencijalno neželjenih aplikacija je u stalnom porastu. Prema podacima nezavisnog instituta AV-TEST GmbH iz Magdeburga, svakog dana pojavi se preko 450.000 novih uzoraka.



Dijagram 1 Broj malicioznih softvera

Kako bi se efikasnije borila protiv izazova kojih je svakodnevno sve više u sajber prostoru, Evropska unija je, po pitanju informacione bezbednosti, odredila pet strateških prioriteta:

- Postizanje elastičnosti – sistemi se automatski oporavljaju nakon incidenta;
- Drastično smanjenje sajber kriminala;
- Razvoj politike sajber odbrane i kapaciteta saglasnih Zajedničkoj bezbednosnoj i odbrambenoj politici (CSDP);
- Razvoj industrijskih i tehnoloških resursa za informacionu bezbednost;
- Uspostavljanje povezanih međunarodnih politika informacionu bezbednosti za EU.

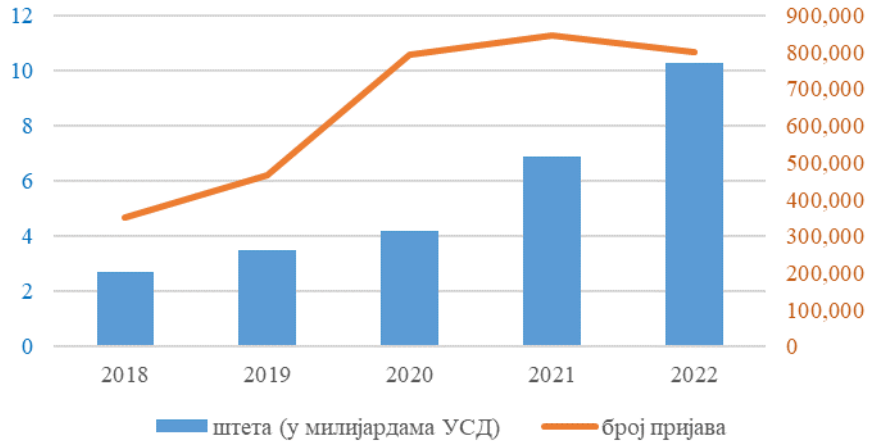
Navedeni prioriteti u prethodnim decenijama realizovali su se kroz sledeće aktivnosti:

- 1992. godine doneta je Odluka Saveta u vezi bezbednosti informacionih sistema
- 2004. godine osniva se Evropska agencija za mrežnu i informacionu bezbednost (ENISA)
- prva Strategija bezbednosti informacionog društva donosi se 2006. godine
- 2008. godine donosi se Direktiva Saveta za identifikaciju i određivanje evropske kritične infrastrukture i procena potrebe za poboljšanjem zaštite
- 2009. godine usvaja se Akcioni plan za zaštitu kritične informacione infrastrukture
- 2012. godine Evropska unija formira CERT_EU

- 2013. godine usvaja se Strategija informacione bezbednosti EU
- 2016. godine donosi se Direktiva o merama za visok zajednički nivo bezbednosti mreža i informacionih sistema širom Unije (NIS Direktiva)
- 2019. godine donosi se Akt o sajber bezbednosti EU kojim su data nova ovlašćenja agenciji ENISA.

Sajber kriminal je svakako najzastupljeniji oblik zlonamernog delovanja u sajber prostoru, uz druge oblike u koje spadaju sajber špijunaža, sajber terorizam, haktivizam i sajber ratovanje. U svom poslednjem izveštaju[1] Evropski centar za sajber kriminal (eng. *European Cybercrime Centre*) navodi da je u okolnostima pandemije sajber kriminal evoluirao i da je to trend koji će se nastaviti. Primeri prilagođavanja su: zloupotrebe nebezbednih RDP protokola (eng. *Remote Desktop Protocol*) i ranjivih VPN konekcija (eng. *virtual private network*), zloupotrebe povećane onlajn kupovine i korišćenje mobilnog bankarstva za implementaciju malvera ili krađu kredencijala i ličnih podataka, ali i sve veća i naprednija upotreba metoda socijalnog inženjeringa.

Centar za žalbe na internet kriminal američkog Federalnog istražnog biroa je u 2022. godini primio 800.944 prijava sa štetom procenjenom na preko 10 milijardi dolara.[2] Zabrinjavajući podatak je da je broj prijava u odnosu na prethodnu godinu manji za oko 5%, ali je ukupna šteta veća za oko 49%, što ukazuje da kriminalci usavršavaju svoje veštine.



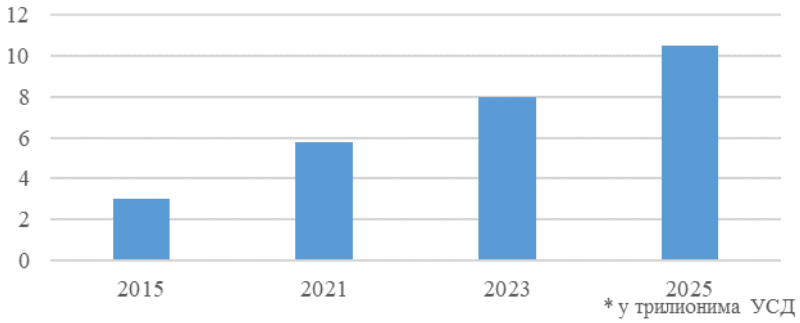
Dijagram 2 Prijave i štete na godišnjem nivou

Kompanija *Cybersecurity Ventures*, koja izrađuje godišnje izveštaje o stanju sajber kriminala[3], procenjuje da će u 2024. godini štete od sajber kriminala dostići osam triliona američkih dolara, što prevazilazi procenjene prihode od trgovine svih narkotika zajedno. Prema dostupnim podacima, štete od sajber kriminala rastu po stopi od 15% godišnje i procenjuje se da će u 2025. godini preći sumu od 10 triliona dolara.

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[3] https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

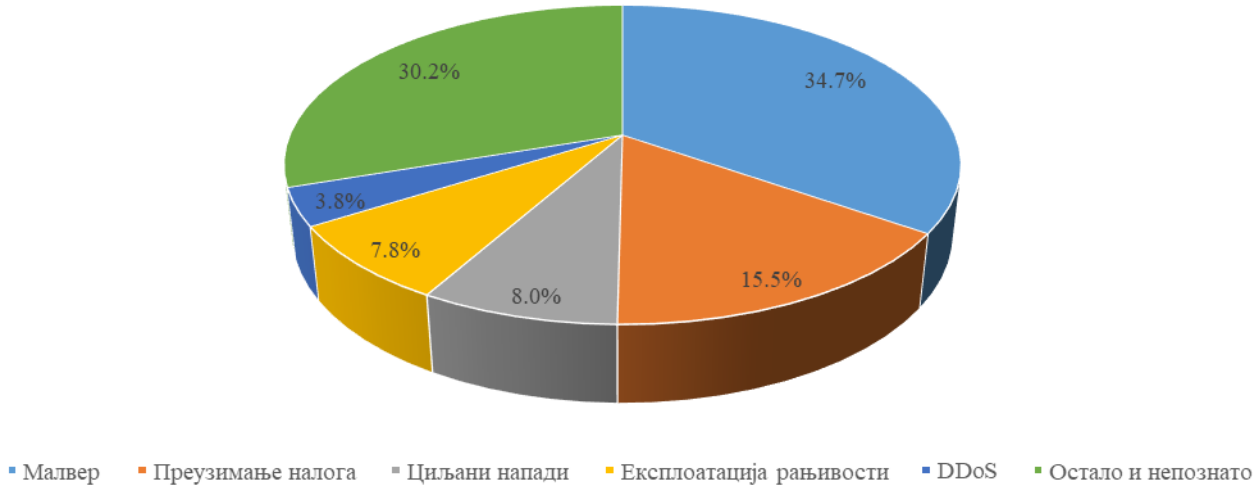


Dijagram 3 Ukupna šteta od sajber kriminala

Ista kompanija u svom izveštaju iznosi podatke o nedostatku radne snage, sa procenama da je u ovom trenutku na svetskom nivou nepopunjeno 3,5 miliona radnih mesta u oblasti informacione bezbednosti, od čega 700.000 samo u SAD. Ilustrativan je podatak da je u trenutku pisanja tog izveštaja u SAD bilo 106.000 otvorenih ponuda za posao za stručnjake sa CISSP sertifikatom (eng. *Certified Information Systems Security Professional*), dok je ukupan broj takvih sertifikata izdatih u SAD nešto preko 90.000. Takođe je identifikovan i problem zadržavanja radne snage, a posebno najkvalitetnije i najobučenije, sa podatkom da 24% glavnih službenika za informacionu bezbednost (CISO) u 500 najvećih kompanija promeni posao nakon godinu dana.

Kako bi se odgovorilo na pretnje u sajber prostoru koje se iz dana u dan povećavaju, neophodno je kontinuirano unapređivati strateški, institucionalni i pravni okvir u oblasti informacione bezbednosti koja, pre sve, treba da obezbedi preventivno delovanje na ove pretnje.

Prema podacima sa sajta *hackmageddon.com*, na globalnom nivou 2022. godine najzastupljeniji tip napada bio je korišćenje malvera, dok su manje zastupljeni (ali sa značajnim procentom) bili preuzimanje naloga, ciljani napadi, iskorišćavanje ranjivosti i distribuirano ometanje servisa (DDoS).



Dijagram 4 Zastupljenost različitih tipova incidenata u svetu

Agencija EU za sajber bezbednost - ENISA (eng. *The European Union Agency for Cybersecurity*) objavila je u martu 2023. godine studiju ***Utvrđivanje pretnji i izazova informacione bezbednosti za 2030. godinu***, koja sadrži predviđanja budućih pretnji i moguće protivmere. Primarni cilj studije je da identifikuje i prikupi informacije o budućim pretnjama koje bi mogle da utiču na infrastrukturu i usluge Evropske unije, kao i na bezbednost građana i društva u celini. U izradu studije

uključeni su futuristi, sociolozi, poslovni lideri, stručnjaci za informacionu bezbednost i drugi, a ciljna grupa su nacionalni organi za informacionu bezbednost, donosioci odluka u Evropskoj uniji i zemljama članicama, timovi za reagovanje, stručnjaci u ovoj oblasti i sve druge zainteresovane strane.

Studija je identifikovala 21 pretnju, od kojih je izdvojeno deset najznačajnijih:

- kompromitacija lanca snabdevanja,
- napredne kampanje dezinformisanja,
- povećanje digitalnog nadzora/gubitak privatnosti,
- ljudske greške i eksploatacija nasleđenih sistema,
- ciljani napadi poboljšani zloupotrebom podataka sa pametnih uređaja,
- nedostatak analize i kontrole infrastrukture i objekata u svemiru,
- napredne hibridne pretnje,
- nedostatak obučene radne snage,
- prekogranični pružaoci IKT usluga kao jedinstvena tačka prekida (eng. *single point of failure*),
- zloupotreba veštačke inteligencije.

Prateći stanje u ovoj oblasti Republika Srbija je usvojila Zakon o informacionoj bezbednosti 28. januara 2016. godine, koji je delimično preneo Direktivu 2016/1148 o merama za visok zajednički nivo bezbednosti mrežnih i informacionih sistema u Evropskoj uniji[4] (eng. *Network and Information Security Directive - NIS Directive*, u daljem tekstu: NIS direktiva), s obzirom da je usvojen pre donošenja te direktive.

Zakon pojam informacione bezbednosti definiše kao 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. Predmetni zakon predstavlja okvir za uređenje bezbednosti informaciono-komunikacionih sistema u Republici Srbiji. Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

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.

Pored toga, ovim zakonom se u okviru Regulatornog tela za elektronske komunikacije i poštanske usluge (u daljem tekstu RATEL) uspostavlja Nacionalni centar za prevenciju i zaštitu od bezbednosnih rizika u IKT sistemima u Republici Srbiji (u daljem tekstu: Nacionalni CERT), koji prati stanje o incidentima o nacionalnom nivou, obaveštava relevantna lica o rizicima i incidentima, reaguje po prijavljenim incidentima, izrađuje analize rizika i incidenata i podiže svest društva o značaju informacione bezbednosti. Jedna od važnih funkcija Nacionalnog CERT-a je i saradnja sa istim institucijama iz drugih zemalja. Imajući u vidu da incidenti u IKT sistemima najčešće imaju prekogranični karakter, odnosno da se dešavaju na teritoriji više zemalja, međusobna saradnja CERT-ova je od izuzetnog značaja, kako bi se međusobnom razmenom informacija uspešno odgovorilo na incidente. Od 1. novembra 2017. godine Nacionalni CERT je uvršten u spisak međunarodne organizacije za saradnju i razmenu informacija iz oblasti informacione bezbednosti *Trusted Introducer*, a nalazi se i na listi CERT timova Agencije EU za sajber bezbednost - ENISA.

U okviru Kancelarije za informacione tehnologije i elektronsku upravu formiran je Sektor za informacionu bezbednost koji, u skladu sa Zakonom, sprovodi aktivnosti CERT-a republičkih organa.

---

[4] 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, dostupna na adresi: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148

U cilju sprovođenja Zakona i u Ministarstvu unutrašnjih poslova formiran je Centar za reagovanje na napade na informacioni sistem MUP-a (CERT MUP) koji se od jula 2016. godine nalazi na listi CERT timova Agencije EU za sajber bezbednost - ENISA, a u novembru 2018. godine dobio je i akreditaciju od strane servisa *Trusted Introducer*.

Iako se sa primenom Zakona započelo odmah po usvajanju, utvrđeno je da je neophodno izvršiti dodatne izmene i dopune zakonske regulative radi usklađivanja sa NIS direktivom koja je u međuvremenu usvojena, ali i radi unapređenja nekih od postojećih rešenja u cilju efikasnijeg sprovođenja zakona u praksi. Zbog toga su u oktobru 2019. godine usvojene izmene i dopune Zakona o informacionoj bezbednosti[5] koji je u potpunosti usklađen sa navedenom Direktivom.

Izmenama i dopunama Zakona o informacionoj bezbednosti, koji je usvojen u oktobru 2019. godine uređene su novine koje se tiču:

- nadležnosti i potrebnih kapaciteta Nacionalnog CERT-a;
- uključivanja Narodne banke Srbije u rad Tela za koordinaciju poslova informacione bezbednosti;
- uspostavljanja Evidencije operatora IKT sistema od posebnog značaja;
- uspostavljanja obaveze dostavljanja statističkih podataka o incidentima koji se dese u IKT sistemima od posebnog značaja na godišnjem nivou;
- saradnje CERT-ova u Republici Srbiji;
- zaštite dece pri korišćenju informaciono-komunikacionih tehnologija;
- klasifikovanja incidenata i postupanja nadležnih organa u zavisnosti od nivoa opasnosti incidenta.

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 sprovodi se od 2019. godine i pokazuje, pored poštovanja zakonskih odredbi, nedostatak kapaciteta za adekvatno reagovanje na incidente.

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

U cilju boljeg razumevanja postojećeg stanja u oblasti informacione bezbednosti, značajno je sagledati incidente koji su prijavljeni Nacionalnom CERT-u u prethodnih nekoliko godina. Ova statistika može biti značajan pokazatelj da li su postojeće preventivne mere dovoljne i u kom pravcu je potrebno unapređivati pravni i institucionalni okvir. Zakon o informacionoj bezbednosti, obavezuje operatore IKT sistema od posebnog značaja da dostavljaju obaveštenja o incidentima koji značajno narušavaju informacionu bezbednost IKT sistema. Na osnovu dobijenih obaveštenja o incidentima Nacionalni CERT izrađuje godišnje statističke izveštaje koji su javno dostupni putem veb prezentacije.

Incidenti su svrstani u 10 grupa:

- instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl.malware),
- neovlašćeno prikupljanje podataka,
- prevara,
- pokušaj upada u IKT sistem,
- upad u IKT sistem,
- nedostupnost ili ograničena dostupnost IKT sistema,
- ugrožavanje bezbednosti podataka,
- operativni incidenti,
- incidenti fizičko-tehničke bezbednosti i

[5] "Službeni glasnik RS", br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019., dostupan na adresi: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg

- ostali incidenti.

U 2022. godini statistički najzastupljeniji bili su incidenti iz grupe Neovlašćeno prikupljanje podataka sa preko sedam i po miliona prijavljenih slučajeva, dok su sledeći po brojnosti incidenti iz grupe Pokušaji upada u IKT sistem sa gotovo tri miliona prijava. Broj prijava u ostalim grupama je znatno manji pa tako u grupi Prevare ima preko 58 hiljada, u grupi Instaliranje zlonamernog softera u okviru IKT sistema blizu 55 hiljada, a u grupi Operativni incidenti preko 13 hiljada prijava. Ukupan broj prijava u ostalih pet grupa je oko šest hiljada.

Dijagram 5 Broj prijavljenih incidenata u Srbiji po grupama u 2022. godini

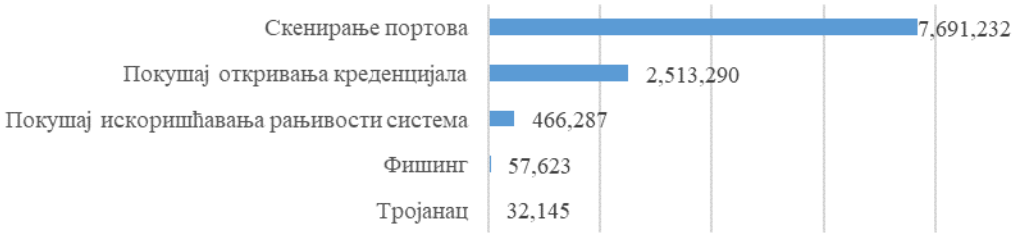
Posmatrano pojedinačno prema vrsti incidenta, u 2022. godini najviše prijava odnosilo se na skeniranje portova koje je uočeno u preko 7 miliona slučajeva i koje ne nanosi direktnu štetu žrtvi, ali predstavlja indikativne aktivnosti napadača u fazi izviđanja. Praksa napadača je da ovakve napade pokreću prema velikom broju IP adresa u pokušaju da nađu potencijalne žrtve koje imaju nezaštićene portove, pa se na taj način i IP adrese operatora kritične infrastrukture nađu u tom opsegu.

Na drugom mestu po brojnosti nalazi se pokušaj otkrivanja kredencijala koji podrazumeva pokušaj pristupa sistemu žrtve uzastopnim isprobavanjem velikog broja različitih kombinacija slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke. Ova vrsta napada oslanja se na nedostatak svesti korisnika prilikom kreiranja lozinki za pristup sistemu i veoma je popularna među napadačima jer zloupotrebom legitimnog naloga može biti omogućen pristup čitavom IKT sistemu.

Pokušaj iskorišćavanja ranjivosti sistema je na trećem mestu, a ova vrsta napada moguća je ukoliko u sistemu postoje ranjivosti.

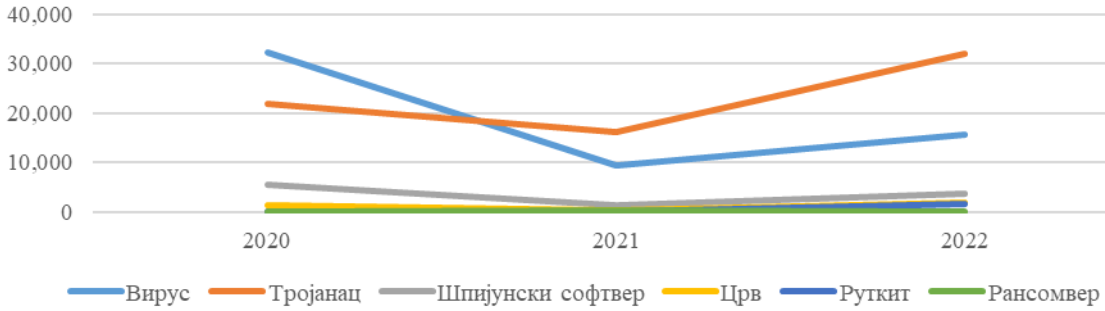
Na četvrtom mestu po brojnosti nalaze se fišing napadi, koji su tokom 2022. godine često bili usmereni na korisnike poštanskih usluga i platformi za e-trgovinu preko nekoliko velikih fišing kampanja.

Na petom mestu su trojanci, koji po pokretanju mogu da preuzmu druge pretnje sa Interneta, ubacuju druge tipove malvera na ugrožene računare, komuniciraju sa udaljenim napadačima, beleže sve što se kuca na tastaturi i šalju napadačima, kao i da na druge načine budu deo kompleksnijih sajber napada.



Dijagram 6 Najčešće prijavljeni incidenti u Srbiji u 2022. godini

Pregledom broja incidenata po vrstama za jednu godinu može se steći slika o trenutnom stanju, ali za dublju analizu potrebno je posmatrati trendove u nekom vremenskom periodu. Trendovi za svaku grupu incidenata predstavljeni su na narednim dijagramima.

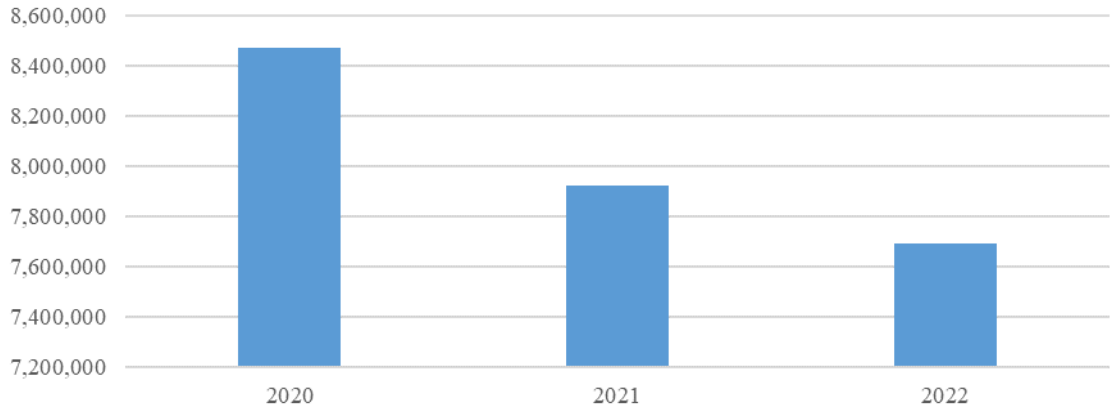


Dijagram 7 Incidenti u grupi Instaliranje zlonamernog softvera u okviru IKT sistema

U grupi Instaliranje zlonamernog softvera u okviru IKT sistema prate se podaci za šest vrsta zlonamernog softvera (malvera): viruse, trojance, crve, rutkit, ransomver i špijunski softver. Nakon drastičnog pada broja prijava slučajeva incidenata kod kojih je korišćen zlonamerni softver u 2021. godini u odnosu na prethodnu godinu, 2022. godine je došlo do značajnog porasta broja incidenta koji spadaju u ovu grupu, a ukupan broj incidenata u ovoj grupi gotovo se izjednačio sa brojem zabeleženim 2020. godine.

Trojanci su najčešći tip malvera koji je korišćen u poslednje dve godine sa udelom od preko 50% od svih zlonamernih softvera. Karakteristika trojanaca je da pokušavaju da navedu korisnike da ih pokrenu tako što se pretvaraju da su korisni programi, pa za njihovu uspešnu distribuciju napadači uključuju i metode socijalnog inženjeringa.

Dijagram 8 Incidenti u grupi Neovlašćeno prikupljanje podataka (osim skeniranja portova)



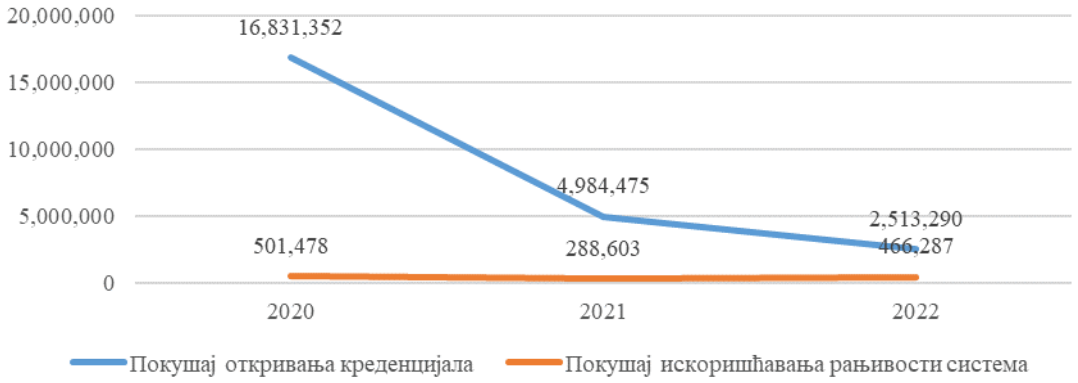
Dijagram 9 Incidenti tipa Skeniranje portova iz grupe Neovlašćeno prikupljanje podataka

Neovlašćeno prikupljanje podataka obuhvata socijalni inženjering, kompromitovanje ili curenje podataka, presretanje podataka između računara i servera i skeniranje portova. Na dijagramima se može primetiti indikativni trend povećanja broja napada iz ove grupe, osim skeniranja portova. Socijalni inženjering je u 2020. i 2021. godini bio na relativno bliskom nivou, da bi u 2022. godini bilo registrovano preko četiri puta više ovakvih incidenata. Kompromitovanje ili curenje podataka je imalo veliki skok u broju prijava 2021. u odnosu na 2020. godinu i taj broj se zadržao i u 2022. godini, dok je broj registrovanih slučajeva presretanja podataka između računara i servera imao enorman rast sa manje od 10 zabeleženih slučajeva u 2020. i 2021. godini, na preko 600 slučajeva u 2022. godini.

Prijavljeni slučajevi skeniranja portova prikazani su na posebnom dijagramu zbog nesrazmerne razlike u broju u odnosu na druge vrste incidenata iz ove grupe, ali ovo je i jedini primer u ovoj grupi da postoji konstantan opadajući trend. Ovako veliki broj zabeleženih slučajeva posledica je automatizovanih procesa za ispitivanje dostupnih servisa na udaljenim računarima, što ne mora nužno biti vođeno malicioznim namerama ali se vrši bez eksplicitne saglasnosti operatora IKT sistema.

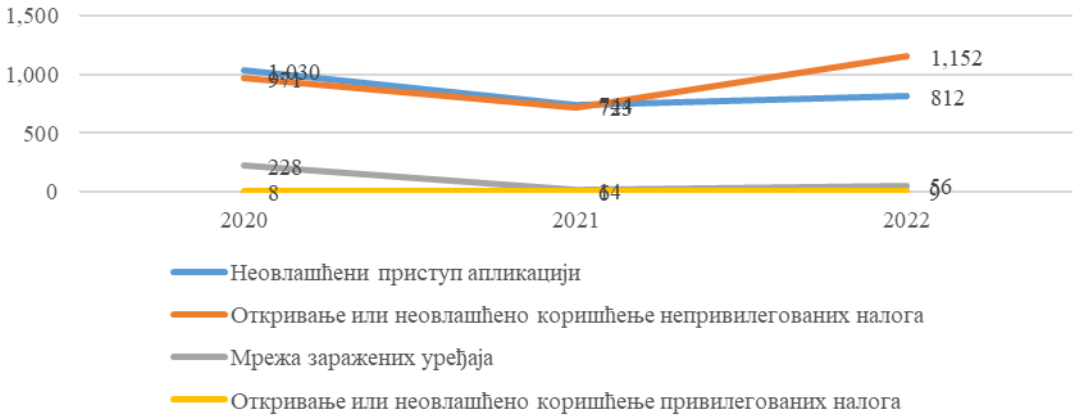
Dijagram 10 Incidenti u grupi Prevara

U grupi Prevara nalaze se fišing i neovlašćeno korišćenje resursa i drugi oblici prevara. Slično kao kod drugih tipova incidenata koji obuhvataju metode socijalnog inženjeringa, i kod fišinga je u 2021. godini došlo do pada broja zabeleženih slučajeva, da bi u 2022. godini broj prijava drastično porastao. Sličan trend može se videti i za druge slučajeve neovlašćenog korišćenja resursa (kao što je kriptodžeking) ali u manjem broju i sa procentualno manjim oscilacijama.



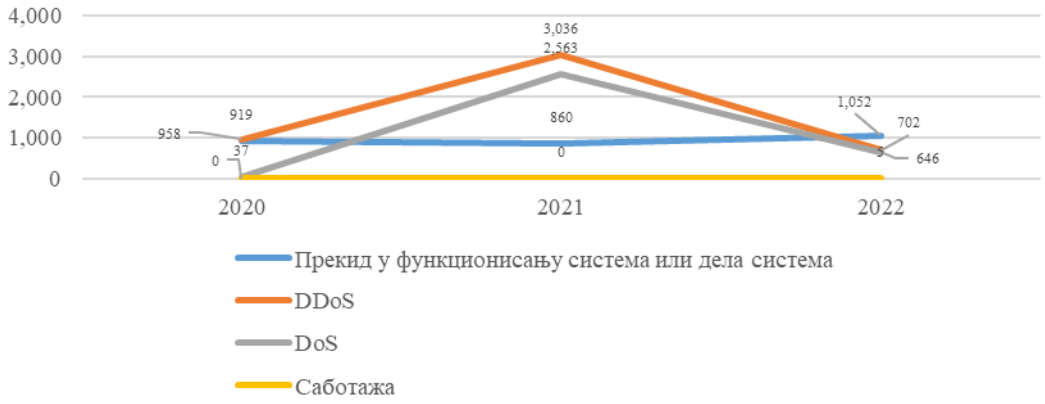
Dijagram 11 Incidenti u grupi Pokušaj upada u IKT sistem

Da bi upali u neki IKT sistem napadači pokušavaju da otkriju validne kredencijale ili da iskoriste ranjivosti sistema. Za otkrivanje kredencijala najčešće se primenjuju tehnike brutalne sile ili rečnika koje podrazumevaju da napadači pokušavaju da se prijave na sistem sa kredencijalima koje unose redom prema određenom šablonu sve dok ne unesu ispravan, što podrazumeva ogroman broj pokušaja i zato su ovi brojevi ovako veliki (mada se uočava trend opadanja broja pokušaja). Drugi tip incidenta u ovoj grupi, iskorišćavanje ranjivosti sistema, takođe pokazuje već viđen tren da posle smanjenja broja prijava u 2021. godini dolazi do ponovnog povećanja u 2022. godini i vraćanja približno na nivo iz 2020. godine.



Dijagram 12 Incidenti u grupi Upad u IKT sistem

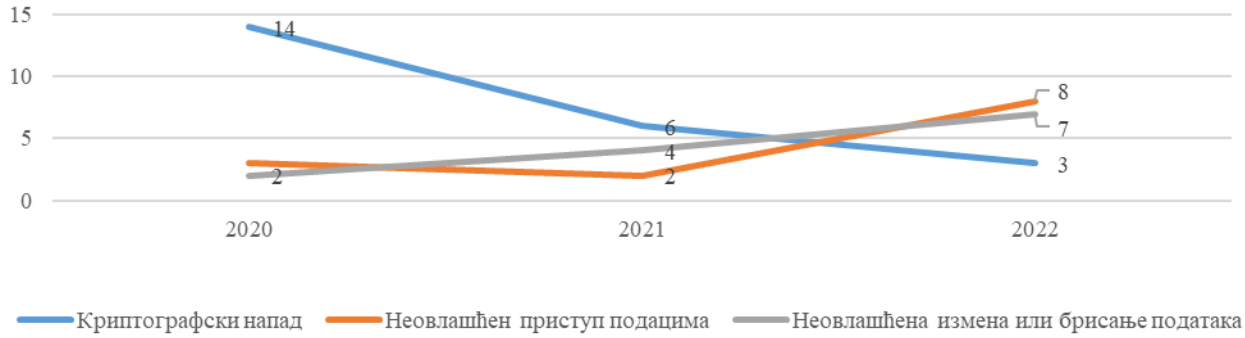
Neovlašćeni pristup aplikaciji, otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga, otkrivanje ili neovlašćeno korišćenje privilegovanih naloga i mreža zaraženih uređaja su vrste incidenata koje pripadaju grupi Upad u IKT sistem. U ovoj grupi u 2022. godini prijavljeno je najviše otkrivanja ili neovlašćenog korišćenja neprivilegovanih naloga, sa trendom da je zabeležen pad broja prijavljenih slučajeva 2021. godine u odnosu na prethodnu godinu i rast 2022. godine.



Dijagram 13 Incidenti u grupi Nedostupnost ili ograničena dostupnost IKT sistema

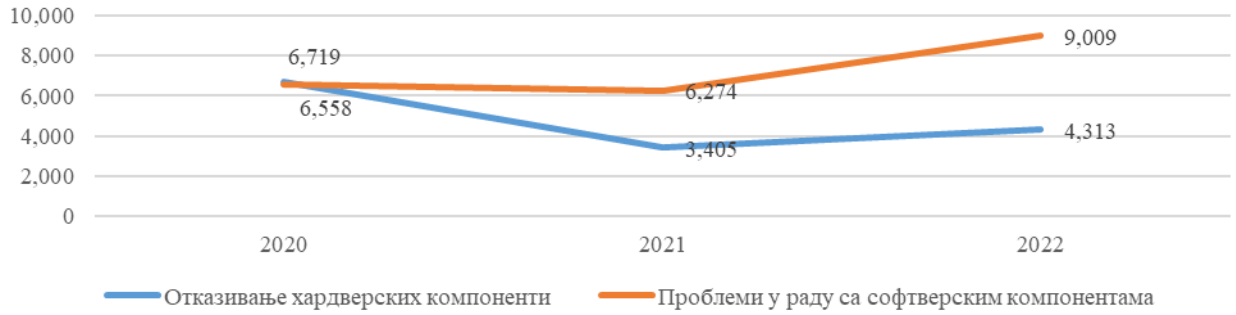
Neovlašćeno otkrivanje ili korišćenje privilegovanih naloga, koje predstavlja mnogo ozbiljniji incident jer u slučaju uspešnosti napadači imaju mogućnost pristupa osetljivim podacima, zabeleženo je u približno istom broju sve tri godine.

Grupa Nedostupnost ili ograničena dostupnost IKT sistema uključuje četiri tipa incidenta: prekid u funkcionisanju sistema ili dela sistema (eng. *outage*), distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (eng. *distributed denial-of-service - DDoS*), napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (eng. *Denial-of-Service - DoS*) i sabotažu. Za DoS i DDoS napade primetan je obrnut trend u odnosu na pretežan trend kod drugih vrsta napada, u smislu da je u 2021. godini uočen nagli skok broja prijavljenih napada, a u 2022. godini nagli pad u odnosu na prethodnu godinu. Takođe se može uočiti da u 2020. i 2021. godini nije zabeležen niti jedan slučaj sabotaže, dok je u 2022. godini prijavljeno pet takvih slučajeva.



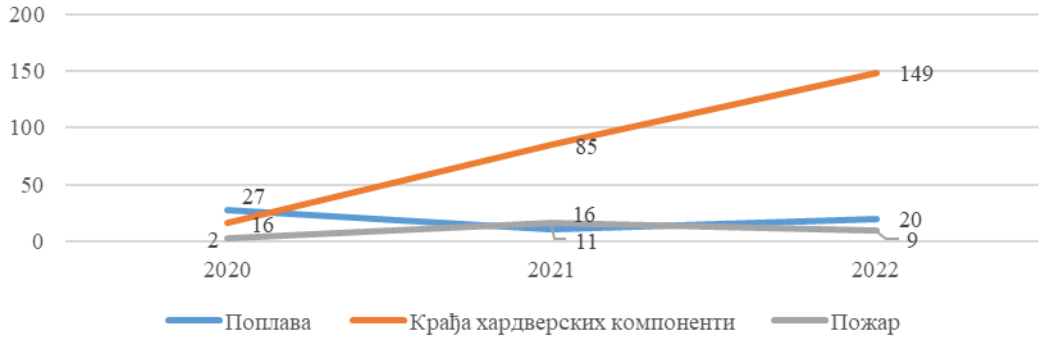
Dijagram 14 Incidenti u grupi Ugrožavanje bezbednosti podataka

Ugrožavanje bezbednosti podataka obuhvata kriptografski napad, neovlašćen pristup podacima i neovlašćene izmene ili brisanje podataka. Ukupan broj ovih napada nije veliki, a može se primetiti blagi trend rasta broja slučajeva neovlašćenog pristupa podacima i neovlašćene izmene ili brisanja podataka i trend pada broja kriptografskih napada.



Dijagram 15 Incidenti u grupi Operativni incidenti

Operativni incidenti su oni koji dovode do zastoja u pružanju usluga, odnosno prekida koji na bilo koji način ugrožavaju poslovni proces izazvanih otkazivanjem hardverskih komponenti ili problema u radu sa softverskim komponentama. U 2020. godini broj zabeleženih problema sa hardverskim i sa softverskim komponentama bio je približno isti, dok je u poslednje dve godine prijavljen približno dvostruko veći broj problema sa softerskim komponentama nego sa hardverom.

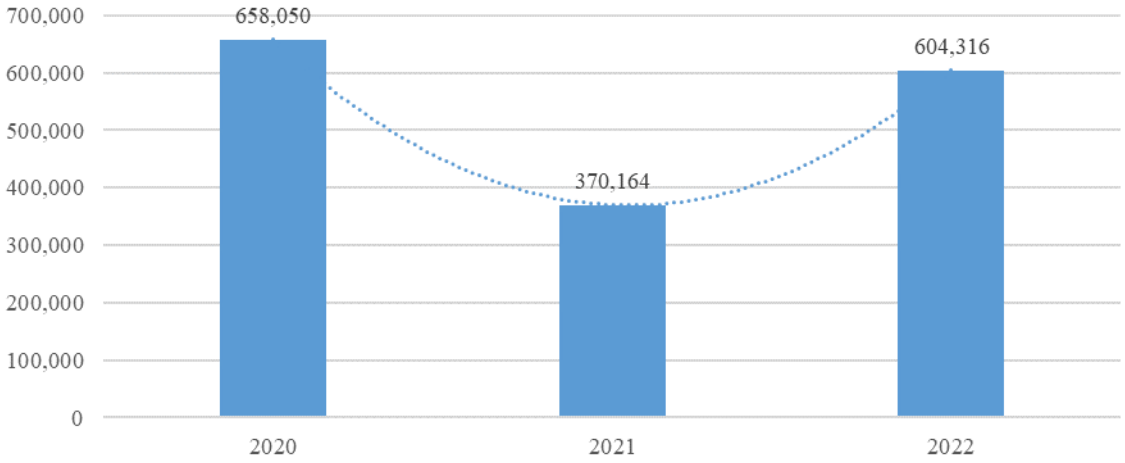


Dijagram 16 Incidenti u grupi Incidenti fizičko-tehničke bezbednosti

U grupu Incidenata fizičko-tehničke bezbednosti spadaju poplave, požari i krađe. Može se konstatovati da je zbir požara i poplava u zbiru prilično konstantan (po 29 u 2020. i 2022. godini i 27 u 2021. godini), ali je broj prijavljenih krađa praktično jedini tip incidenta koji beleži linearni trend rasta u protekle tri godine.

U ostale incidente svrstani su svi oni koji ne spadaju u navedene kategorije, kao što su detekcija potencijalno nebezbednih aplikacija, neodobrene platne transakcije ili lažni profili na društvenim mrežama.

Ukupan broj prijavljenih incidenata u 2020. godini bio je 25.958.850, u 2021. godini 13.279.007, a u 2022. godini 10.808.838. Gledajući samo ove brojeve mogao bi se steći utisak da postoji generalan trend smanjenja broja incidenata. Međutim, treba imati u vidu da je u 2020. godini broj incidenata na globalnom nivou eruptirao kao posledica pandemije i izmenjenih okolnosti poslovanja pa ni Srbija nije bila izuzeta od tog trenda (na žalost, statistika koja bi pokazala ovaj skok nije vođena u Srbiji pre 2020. godine). Sledeća godina donela je značajno smirivanje, pa poređenje 2021. i 2022. godine može bolje pokazati pravi trend. Posmatrajući trend prijavljenih skeniranja portova (8.469.448 u 2020. godini, 7.924.368 u 2021. godini i 7.691.232 u 2022. godini) i broj pokušaja otkrivanja kredencijala (16.831.352 u 2020. godini, 4.984.475 u 2021. godini i 2.513.290 u 2022. godini) očigledno je da ove dve vrste incidenata, koje u svakoj od ove tri godine zajedno čine između 94,4% i 97,4% od ukupnog broja incidenata, beleže značajno smanjenje nakon prve godine pandemije i trebaju biti tretirane zasebno zbog svoje procentualne zastupljenosti. Ako se iz ukupnog broja incidenata izuzmu ove dve vrste, dobija se sledeći dijagram broja incidenata po godinama:



Dijagram 17 Ukupan broj incidenata po godinama bez skeniranja portova i pokušaja otkrivanja kredencijala

Ako se uzme u obzir da je 2020. godina bila specifična i uzme u obzir odnos broja incidenata u 2021. i 2022. godini, uočava se značajan i zabrinjavajući rast. Na globalnom nivou, prognoze su da će broj incidenata značajno rasti u narednom periodu (nije nam poznata niti jedna analiza koja zaključuje da će broj incidenata opadati), ali takođe i njihova sofisticiranost. Posebno su alarmantna predviđanja da će se nastaviti trend rasta prosečne štete po incidentu, što znači da će ukupna suma štete nanete incidentima rasti u dosta većem procentu od rasta broja incidenata. Ovakvi trendovi neće mimoići ni Srbiju pa se može očekivati da se i u narednim godinama nastavi rast broja prijavljenih incidenata, ali i rast nanete štete.

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.

Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine predstavlja međusektorsku strategiju kojom se utvrđuju ciljevi i mere za razvoj informacionog društva i informacione bezbednosti. U delu koji se odnosi na informacionu bezbednost Strategija je usklađena sa Direktivom o mrežnoj i informacionoj bezbednosti EU (eng. *Network and Information Security Directive - NIS Directive*), koja predviđa obavezu donošenja nacionalne strategije za informacionu bezbednost kojom će se definisati strateški ciljevi i prioriteti koji se odnose na mrežnu i informacionu bezbednost.

Strategijom je definisan poseban cilj ***Unapređenje informacione bezbednosti građana, javne uprave i privrede***, koji se ostvaruje kroz realizaciju sledećih mera:

- podizanje svesti i znanja u oblasti informacione bezbednosti građana, javnih službenika i privrede,
- podizanje kapaciteta IKT sistema od posebnog značaja za primenu mera zaštite,
- podizanje kapaciteta Nacionalnog CERT-a, CERT-a organa vlasti i CERT-ova samostalnih operatora IKT,
- podizanje kapaciteta inspekcije za informacionu bezbednost,
- podsticanje javno-privatnog partnerstva u oblasti informacione bezbednosti i
- unapređenje regionalne i međunarodne saradnje.

Akcioni plan za realizaciju Strategije razvoja informacionog društva i informacione bezbednosti za period od 2024. do 2026. godine meri ostvarenost ovog posebnog cilja kroz Globalni indeks informacione bezbednosti (eng. *Global Cyber Security Indeks*) koji meri osam indikatora: poziciju

države u globalnim okvirima u ovoj oblasti, indeks bezbednosti u sajber prostoru, zakone, tehničku razvijenost, organizaciju, kapacitete, saradnju i poziciju države u regionalnim okvirima u ovoj oblasti. U poslednjem izdanju „Globalnog indeks ainformacione bezbednosti“, Republika Srbija našla se u prvoj od pet grupa država koja obuhvata zemlje sa najvišim nivoom razvoja u oblasti informacione bezbednosti. Međunarodna telekomunikaciona unija vrednovala je pet ključnih komponenti razvoja, i to pravni okvir, tehničke mere, organizacione mere, jačanje kapaciteta i međunarodnu saradnju. Republika Srbija prepoznata je kao jedna od vodećih zemalja u svim ovim aspektima čime je potvrđen značajan doprinos naše zemlje u osiguravanju visokog nivoa informacione bezbednosti.

U okviru mere *Podizanje svesti i znanja u oblasti informacione bezbednosti građana, javnih službenika i privrede* realizovane su sledeće aktivnosti:

- U saradnji sa nadležnim Ministarstvom kreirane su i sprovedene dve vrste obuka namenjene predstavnicima ministarstava. Teorijsku obuku pod nazivom „Primena Modela akta o bezbednosti” pohađalo je ukupno 27 zaposlenih lica iz 9 ministarstava, a dvodnevnu tehničku obuku „Detekcija i odbrana IKT sistema od sajber napada” pohađalo je ukupno 28 zaposlenih iz 8 ministarstava. Takođe, u saradnji sa Institutom za standardizaciju i Ministarstvom unutrašnjih poslova održan je vebinar pod nazivom „Od ZIB-a do standarda” namenjen predstavnicima sudstva i pravosudnih organa, koji je pohađalo ukupno 78 učesnika.
- U saradnji sa Radio televizijom Srbije organizovana je medijska kampanja namenjena podizanju svesti o značaju informacione bezbednosti u okviru koje su emitovani edukativni spotovi na temu bezbednosti dece na internetu. Takođe je u 10 epizoda realizovana i emisija „Porodična mreža” u cilju podizanja svesti o značaju informacione bezbednosti, o rizicima i merama zaštite, u kojoj su aktivno učešće imali roditelji sa decom.
- U toku 2022. godine sproveden je Javni poziv za dodelu sredstava za organizovanje regionalnih konferencija na temu razmene iskustva u oblasti podizanja nivoa digitalne pismenosti, digitalnih kompentencija i realizaciju programa koji za cilj imaju podizanje digitalnih kompetencija žena iz ruralnih oblasti.
- Izrađen je Vodič za sajber bezbednost malih i srednjih preduzeća u saradnji sa Nacionalnim CERT-om Republike Srbije. Vodič je namenjen malim i srednjim preduzećima i sadrži uputstva o tome kako se zaštititi od najčešćih pretnji po informacionu bezbednost s kojima mala i srednja preduzeća mogu da se susretnu u svom radu, a zasnovan je na dokazanim primerima dobre prakse privatnog i javnog sektora.
- Nacionalni CERT Republike Srbije kreirao je platformu za podizanje svesti i znanja iz oblasti informacione bezbednosti, koja je dostupna na adresi: https://learn.cert.rs/Home/Home?mostrarTour=True.

U okviru mere *Unapređenje saradnje i podizanje kapaciteta IKT sistema od posebnog značaja za primenu mera zaštite*:

- održane su obuke i vežbe za predstavnike pravosudnih organa i operatora IKT sistema od posebnog značaja u oblasti energetike;
- pripremljene su smernice za dostizanje neophodnog nivoa ispunjenosti zahteva (eng. *common criteria*) za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;
- u oktobru 2022. godine od strane Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), kao Nacionalnog CERT-a, organizovana je Nacionalna konferencija „Budimo sajber svesni”, kojom je obeležen oktobar kao međunarodni mesec informacione bezbednosti na kojoj su prezentovana aktuelna dešavanja u sajber prostoru, načini unapređenja saradnje i razmene informacija o sajber pretnjama, predstavljeni su načini zaštite kritične infrastrukture, kao i značaj javno-privatnog partnerstva u ovoj oblasti;
- tokom novembra 2022. godine održana je konfrencija u organizaciji Registra nacionalnog Internet domena Srbije na kojoj su nastavljeni razgovori povodom podizanja svesti i edukacije

o informacionoj bezbednosti i prezentovani su rezultati projekata Sajber heroj i digitalne kampanje Zaštiti se;

- u okviru baze Nacionalnog CERT-a kreiran je deo za razmenu podataka između Nacionalnog CERT-a i IKT sistema od posebnog značaja i uspostavljena je platforma za razmenu podataka *MISP - Malware Information Sharing Platform*);
- u toku je priprema obrazaca za samoprocenu IKT sistema od posebnog značaja kao i za proveru stepena razvijenosti informacione bezbednosti u Republici Srbiji.

U okviru mere *Podizanje kapaciteta Nacionalnog CERT-a, CERT-a organa vlasti i CERT-ova samostalnih operatora IKT sistema*:

- izrađene su smernice za postupanje u slučaju incidenata koji su visokog i veoma visokog nivoa opasnosti;
- uspostavljena je saradnja između Ministarstva, Nacionalnog CERT-a i Sektora za vanredne situacije u okviru Ministarstva unutrašnjih poslova radi prepoznavanja mehanizama saradnje u slučaju incidenta veoma visokog nivoa opasnosti;
- uspostavljen je CERT Ministarstva odbrane i upisan u Evidenciju IKT sistema od posebnog značaja;
- kontinuirano se vrši pohađanje obuka zaposlenih u Nacionalnom CERT-u u skladu sa planom stručnog usavršavanja RATEL-a

Podizanje kapaciteta inspekcije za informacionu bezbednost vrši se kroz brojne obuke među kojima su najznačajnije:

- Obuka koju je organizovalo Akreditaciono telo Srbije uz učešće EU eksperata vezano za eIDAS regulativu (eng. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*);
- Obuke za korišćenje softvera eInspektor;
- Učestvovanje na Tehničkom kolokvijumu za CERT-ove Zapadnog Balkana koju je organizovao Ženevski centar za upravljanje bezbednosnim sektorom (eng. *Geneva Centre for Security Sector Governance - DCAF*) u saradnji sa Albanskom nacionalnom agencijom za elektronsku sertifikaciju i informacionu bezbednost (AKCESK) u okviru regionalnog projekta;
- Obuka Instituta za standardizaciju za članove komisija za standarde i srodne dokumente;
- NFC radionica koju je organizovala Agencija Evropske Unije za sajber bezbednost – ENISA.

Mera *Podsticanje javno-privatnog partnerstva u oblasti informacione bezbednosti* realizuje se kroz sledeće aktivnosti:

- U okviru fondacije „Mreža za sajber bezbednost” (nekadašnja Petnička grupa), koja povezuje privredu i donosioce odluka o politikama kroz platformu za diskusiju i sprovođenje aktivnosti usmerenih ka unapređenju informacione bezbednosti u Srbiji, realizuje se program „Sajber heroj” u okviru koga se realizuje takmičenje u oblasti informacione bezbednosti *Serbian Cybersecurity Challenge*. 2022. godine nacionalni tim Srbije učestvovao je na međunarodnom takmičenju *European Cyber Security Challenge* (ECSC 2022). Pored toga, na poziv Agencije Evropske Unije za sajber bezbednost – ENISA, dva predstavnika iz Srbije bili su kandidati za Tim Evrope na takmičenju kontinenata.
- Zaključeni su sporazumi o saradnji sa Savezom slepih Beograd i Savezom gluvih Beograd - postignut je dogovor o održavanju prezentacija na temu bezbednosti dece na internetu.

Unapređenje regionalne i međunarodne saradnje sprovodi se kroz brojne aktivnosti prdviđene akcionim planom među kojima se izdvajaju:

- U okviru inicijative „Otvoreni Balkan” zaključen je Sporazum o povezivanju šema elektronske identifikacije građana Zapadnog Balkana između Srbije, Albanije i Severne Makedonije, čime

su države međusobno priznale šeme elektronske identifikacije upisane u odgovarajuće registre. Zaključivanje ovog sporazuma podrazumeva da strane tehnički povežu svoje portale elektronske uprave tako da građani mogu da se elektronski identifikuju u skladu sa najnaprednijim standardima informacione bezbednosti.

- U septembru 2022. godine potpisan je Memorandum o razumevanju u oblasti informacione bezbednosti između Ministarstva informisanja i telekomunikacija Republike Srbije i Saveta za sajber bezbednost Ujedinjenih Arapskih Emirata. Saradnja predviđena ovim memorandumom se sprovodi kroz razne unapred dogovorene forme, uključujući obuku, tehničke konsultacije i razmenu stručnjaka u neophodnim oblastima. Oblasti saradnje predviđene memorandumom su: razmena informacija o rizicima po informacionu bezbednost, zajedničko informisanje i odgovor na incidente na polju informacione bezbednosti, podela informacija o širenju zlonamernih softvera, razmena podataka o indikatorima kompromitacije, pružanje informacija o mogućim uspešnim rešenjima u oblasti informacione bezbednosti, zajednička saradnja u organizovanju tehničkih radionica, konferencija, edukativnih poseta i obuka, zajednička koordinacija i saradnja u organizaciji i sprovođenju obuka u oblasti informacione bezbednosti.
- U novembru 2022. godine u Beogradu realizovana je *TAIEX* ekspertska misija koje se odnosi na sertifikaciju u oblasti informacione bezbednosti, kao i na ostala pitanja u vezi sa primenom Akta o sajber bezbednosti EU (Uredba 2019/881). TAIEX je instrument Evropske komisije za tehničku pomoć i razmenu informacija i podržava javnu administraciju u vezi sa usklađivanjem, primenom i sprovođenjem zakonodavstva EU, kao i olakšavanjem razmene najboljih praksi EU. Ekspertskoj misiji prisustvovali su predstavnici Kancelarije za informacione tehnologije i elektronsku upravu, Ministarstva odbrane, Ministarstva informisanja i telekomunikacija, Bezbednosno – informativne agencije, kao i predstavnici RATEL-a - Nacionalnog CERT-a. Ekspertska misija zatražena je u cilju pripreme za revidiranje propisa iz oblasti informacione bezbednosti u skladu sa najnovijim zakonodavstvom EU.
- U oktobru 2022. godine održan je seminar o *Predlog*u NIS 2 direktive Evropske unije, uporednoj praksi u vezi uređenja i rada agencija za informacionu bezbednost, promenama u standardu ISO 27001 i najboljim rešenjima u pogledu upravljanja kriznim situacijama u slučaju sajber incidenata. U vezi sa navedenim temama učesnici seminara predstavili su pravni i strateški okvir i praksu iz svog delokruga rada.
- U oktobru 2022. godine Ministarstvo je učestvovalo na međunarodnoj konferenciji *INSAFE AND INHOPE*, održanoj u Briselu.
- Nadležni organi RS sarađuju sa EU institucijama nadležnim za oblast informacione bezbednosti. Ministarstvo ostvaruje saradnju sa Međunarodnom unijom za telekomunikacije u pogledu izrade Globalnog indeksa sajber bezbednosti, kao i sa Agencijom Evropske Unije za sajber bezbednost ENISA učešćem u radnoj grupi za elektronsku identifikaciju i kvalifikovane usluge od poverenja. CERT-ovi iz Republike iz Srbije nalaze se na *Trusted Introducer* listi, a Nacionalni CERT i CERT MUP članovi su *Forum of Incident Response and Security Teams* organizacije.

I pored uspešnog sprovođenja aktivnosti predviđenih Strategijom razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine, zbog nedovoljnih kadrovskih i tehničkih kapaciteta nadležnih organa u oblasti informacione bezbednosti, kasni se u realizaciji pojedinih aktivnosti, kao što su: izrada smernica za dostizanje neophodnog nivoa ispunjenosti zahteva (eng. *common criteria*) za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema; razvoj, harmonizacija i proširenje specijalizovanih kurseva i programa informacione bezbednosti na univerzitetima i drugim visokoškolskim ustanovama; obuke za mala i srednja preduzeća o potrebi i načinu primene mera zaštite i važnosti kontinuiranog podizanja kapaciteta zaposlenih, u skladu sa nacionalnim i međunarodnim standardima. Zbog izmena evropskih direktiva u ovoj oblasti neophodno je izvršiti

harmonizaciju propisa i uskladiti odredbe Zakona o informacionoj bezbednosti sa NIS 2 Direktivom (eng. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive)* Usklađivanje propisa omogućiće nastavak saradnje sa međunarodnim telima i ispunjenje obaveza Republike Srbije u procesu pridruživanja Evropskoj uniji. Unapređenje pravnog okvira trebalo bi da poboljša ne samo međunarodnu saradnju, već i kapacitete svih entiteta nadležnih za obezbeđivanje informacione bezbednosti.

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

Analizirajući postojeći zakonski okvir i njegovu implementaciju, ciljeve postavljene Strategijom razvoja informacionog društva i informacione bezbednosti za period 2021.-2026. godine i pravce razvoja na globalnom i nivou Evropske unije, mogu se identifikovati sledeći problemi koji se mogu prevazići isključivo izmenom institucionalnog i pravnog okvira:

- neusklađenost Zakona o informacionoj bezbednosti sa evropskim propisima,
- nedostatak kapaciteta nadležnih organa,
- potreba za podizanjem operativnih kapaciteta za reagovanje na incidente, posebno na one od nacionalnog značaja,
- nedostatak sistemskog prikupljanja i razmene informacija,
- nepostojanje nacionalne platforme za brzu detekciju incidenata,
- nedostatak koordinacije za otkrivanje ranjivosti i
- nedovoljna koordinacija međunarodnih aktivnosti.

Neusklađenost Zakona o informacionoj bezbednosti sa evropskim propisima

Izmene i dopune Zakona o informacionoj bezbednosti 2019. godine odnosile su se na usklađivanje sa NIS Direktivom koja je u decembru 2022. godine zamenjena NIS 2 Direktivom.

Zbog toga je predstavljena uporedna analiza NIS i NIS 2 Direktive, kako bi se prepoznale razlike u pravnom okviru koje je neophodno prevazići. NIS Direktiva uvodi 19 definicija, dok je u NIS 2 Direktivi ovaj broj porastao na 41. Većina definicija iz NIS Direktive zadržana je i u NIS 2 Direktivi u istom ili praktično istom obliku, ali je nekoliko definicija termina pretrpelo suštinske promene.

Na primer, termin „incident" je u NIS Direktivi definisan kao bilo koji događaj koji ima stvarni neželjeni efekat na bezbednost mrežnih i informacionih sistema, dok je u NIS 2 Direktivi ovaj termin definisan kao događaj koji kompromituje dostupnost, autentičnost, integritet ili poverljivost skladištenih, prenošenih ili procesiranih podataka, ili usluga koje se nude ili kojima se pristupa putem mrežnih i informacionih sistema. Definicija termina „rukovanje incidentom" u NIS 2 Direktivi proširena je prevencijom, reagovanjem i oporavkom, uz detekciju, analizu i ograničavanje koji su već bili uključeni u definiciju ovog termina u NIS Direktivi.

NIS Direktiva je u svom Članu 5 propisivala kriterijume za određivanje operatora esencijalnih servisa:

- entitet pruža servis koji je neophodan za održavanje kritičnih društvenih i/ili ekonomskih aktivnosti;
- pružanje tog servisa zavisi od mrežnih i informacionih sistema; i
- incident bi imao značajne remetilačke efekte na pružanje tog servisa.

Ovi kriterijumi nisu zadržani u NIS 2 Direktivi, već je ova Direktiva entitete kojima su propisane posebne obaveze podelila na esencijalne i važne. U skladu sa ovom podelom, određeni su i sektori visoke kritičnosti i ostali kritični sektori u kojima se obavljaju delatnosti od posebnog značaja. NIS 2 Direktivom određeno je da u sektore visoke kritičnosti spadaju:

- energetika,

- saobraćaj,
- bankarstvo,
- infrastrukture finansijskih tržišta,
- zdravlje,
- pijaća voda,
- otpadne vode,
- digitalna infrastruktura,
- upravljanje IKT uslugama,
- javna administracija i
- svemir.

Uređeno je da u ostale kritične sektore spadaju:

- poštanske i kurirske usluge,
- upravljanje otpadom,
- proizvodnja i snabdevanje hemikalijama,
- proizvodnja, obrada i distribucija hrane,
- druge proizvodne delatnosti (proizvodnja medicinskih uređaja i in vitro dijagnostičkih medicinskih sredstava, računara, elektronskih i optičkih proizvoda, električne opreme, mašina i uređaja, motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz),
- pružanje digitalnih usluga i
- istraživanje.

Odredbama NIS 2 Direktive propisano je da se esencijalnim entitetima smatraju:

- entiteti koji prevazilaze veličinu srednjih preduzeća (imaju više od 250 zaposlenih i obrt od preko 50 miliona evra) i koji svoju delatnost obavljaju u nekom od visoko kritičnih sektora;
- pružaoci kvalifikovanih usluga od poverenja, pružaoci usluge registracije domena najvišeg nivoa i pružaoci usluga DNS bez obzira na veličinu;
- pružaoci usluga javnih elektronskih komunikacionih mreža ili javno dostupnih elektronskih komunikacionih usluga koji spadaju u preduzeća srednje veličine;
- organi državne uprave na centralnom nivou;
- svi drugi entiteti koji svoje delatnosti obavljaju u visoko kritičnim ili kritičnim sektorima, a koje je država članica identifikovala kao esencijalne jer su jedini pružaoci neke esencijalne usluge, jer bi prekid u pružanju usluga mogao imati značajan uticaj na javnu sigurnost, javnu bezbednost i javno zdravlje, jer bi prekid u pružanju usluga mogao imati značajan sistemski rizik, ili koji su kritični zbog specifične važnosti na nacionalnom ili regionalnom nivou;
- entiteti identifikovani kao kritični u skladu sa Direktivom 2022/2557;
- svi drugi entiteti identifikovani kao esencijalni u skladu sa Direktivom 2016/1148 (NIS Direktiva), ako država članica proceni da je to potrebno.

Važnim entitetima smatraju se entiteti koji svoje delatnosti obavljaju u visoko kritičnim ili kritičnim sektorima, a koji ne ispunjavaju kriterijume da budu identifikovani kao esencijalni. Takođe, važnim entitetima se smatraju i oni koje je država članica identifikovala kao važne jer su jedini pružaoci neke esencijalne usluge, jer bi prekid u pružanju usluga mogao imati značajan uticaj na javnu sigurnost, javnu bezbednost i javno zdravlje, jer bi prekid u pružanju usluga mogao imati značajan sistemski rizik, ili koji su kritični zbog specifične važnosti na nacionalnom ili regionalnom nivou.

NIS direktivom propisano je da se određivanje šta predstavlja značajan remetilački efekat prepusti zemljama članicama, pri čemu je Direktivom sugerisano da se u obzir uzme:

- broj korisnika servisa koji pruža taj entitet koji su pogođeni prekidom;
- zavisnost drugih sektora kojima pripadaju operatori esencijalnih servisa od servisa koji pruža taj entitet;
- uticaj koji bi incidenti mogli imati, u smislu obima i trajanja, na ekonomske i društvene aktivnosti ili javnu bezbednost;
- tržišni udeo tog entiteta;
- geografsko širenje u pogledu područja koje bi moglo biti pogođeno incidentom; i

- važnost entiteta za održavanje dovoljnog nivoa servisa, uzimajući u obzir dostupnost alternativnih mogućnosti za pružanje tog servisa.

U NIS 2 Direktivi nije zadržan pojam značajnog remetilačkog efekta, ali su uvedeni pojmovi značajne sajber pretnje i značajnog incidenta. Značajna sajber pretnja je kao pojam definisana u članu 3. NIS 2 Direktive kao sajber pretnja za koju se, na osnovu svojih tehničkih karakteristika, može pretpostaviti da ima potencijal da ozbiljno utiče na mrežne i informacione sisteme entiteta ili korisnike njegovih usluga nanošenjem znatne materijalne ili nematerijalne štete. Članom 23, kojim su propisane obaveze izveštavanja, definisano je da će se incident smatrati značajnim ako:

- je prouzrokovao ili ima kapacitet da prouzrokuje ozbiljne prekide pružanja usluga ili ozbiljne finansijske gubitke ugroženom entitetu, i
- je uticao ili ima kapacitet da utiče na druga fizička ili pravna lica putem nanošenja značajne materijalne ili nematerijalne štete.

NIS Direktiva obavezala je države članice da usvoje nacionalnu strategiju bezbednosti mrežnih i informacionih sistema koja mora uključivati sledeće:

- ciljeve i prioritete nacionalne strategije bezbednosti mrežnih i informacionih sistema;
- okvir upravljanja za postizanje ciljeva i prioriteta ove strategije, uključujući uloge i odgovornosti državnih organa i drugih relevantnih aktera;
- utvrđivanje mera koje se odnose na pripremljenost, reagovanje i oporavak, uključujući saradnju između javnog i privatnog sektora;
- programe obrazovanja, podizanja svesti i obuke;
- planove istraživanja i razvoja;
- plan procene rizika radi njihove identifikacije;
- spisak aktera uključenih u sprovođenje nacionalne strategije bezbednosti mrežnih i informacionih sistema.

U NIS 2 Direktivi takođe postoji obaveza za države članice da usvoje nacionalnu strategiju (ali se koristi izraz „nacionalna strategija informacione bezbednosti”), pri čemu je spisak obaveznih stavki ostao sličan, a dodate su i koordinacija i saradnja. Takođe, državama članicama je data obaveza da kao deo nacionalne strategije usvoje sledeće politike:

- rešavanje informacione bezbednosti u lancu snabdevanja;
- uključivanje i specifikaciju zahteva vezanih za bezbednost IKT proizvoda i usluga u javnim nabavkama;
- upravljanje ranjivostima;
- održavanje opšte dostupnosti, integriteta i poverljivosti javnog jezgra otvorenog interneta;
- promovisanje razvoja i integracije relevantnih naprednih tehnologija sa ciljem implementacije najsavremenijih mera za upravljanje rizikom u oblasti informacione bezbednosti;
- promovisanje i razvoj obrazovanja i obuka, veština, podizanja svesti i inicijativa za istraživanje i razvoj, kao i smernica o dobrim praksama i kontrolama sajber higijene;
- podrška akademskim i istraživačkim institucijama u razvoju, unapređenju i promociji primene alata za informacionu bezbednost;
- podrška dobrovoljnoj razmeni informacija;
- jačanje sajber otpornosti i osnove sajber higijene malih i srednjih preduzeća;
- promovisanje aktivne sajber zaštite.

Obe direktive propisuju obaveze za države članice da odrede nadležne organe (jedan ili više) i jedinstvenu tačku kontakta, kao i da uspostave Timove za hitno reagovanje na incidente - CSIRT (eng. *Computer emergency response team*) sa nadležnostima koje pokrivaju sektore od posebnog značaja.

NIS 2 Direktivom zadržane su odredbe o Grupi za saradnju i Mreži CSIRT-ova iz NIS Direktive, uz nešto proširen skup zadataka za ova dva tela.

NIS 2 Direktivom detaljnije su razrađene tehničke, operativne (dodatna vrsta mera koja nije bila pomenuta u NIS Direktivi) i organizacione mere za upravljanje rizicima po mrežne i informacione sisteme. U ove mere spadaju:

- politike u vezi analize rizika i bezbednosti informacionih sistema;
- rukovanje incidentima;
- kontinuitet poslovanja i upravljanje krizama;
- bezbednost lanca snabdevanja;
- bezbednost u nabavci, razvoju i održavanju mrežnih i informacionih sistema, uključujući otkrivanje i rukovanje ranjivostima;
- politike i procedure za procenu efikasnosti mera za upravljanje rizikom;
- praktikovanje osnovnih mera sajber higijene i obuke u cilju podizanja bezbednosne svesti;
- politike i procedure vezane za korišćenje kriptografskih metoda;
- bezbednost ljudskih resursa, politike kontrole pristupa i upravljanje asetima;
- korišćenje multifaktorske autentifikacije i drugih metoda jake autentifikacije i korišćenje bezbednih komunikacionih sistema, posebno u slučaju vanrednih situacija.

NIS 2 Direktiva zadržala je odredbe o obavezi izveštavanja o incidentima, pri čemu se ova obaveza odnosi i na esencijalne i na važne entitete.

U odnosu na NIS Direktivu, u novoj Direktivi uvedena je obaveza za države članice da odrede ili uspostave jedan ili više nadležnih organa odgovornih za upravljanje velikim incidentima i krizama. Ako se odredi više organa, mora se nedvosmisleno odrediti koja institucija koordinira njihov rad u slučaju velikih incidenata i kriza. Države članice takođe moraju usvojiti nacionalni plan za odgovor na velike incidente i krize koji mora sadržati:

- ciljeve zbog kojih se preduzimaju mere i aktivnosti,
- zadatke i odgovornosti nadležnih organa,
- procedure za reagovanje i njihovo uklapanje u opšti okvir za reagovanje u slučaju nacionalne krize, kao i kanale za razmenu informacija,
- mere koje je potrebno preduzeti radi pripreme, uključujući vežbe i obuke,
- organizacije iz javnog i privatnog sektora i infrastrukturu koja se angažuje,
- procedure i sporazume između nacionalnih nadležnih organa.

NIS 2 Direktivom propisani su slični zahtevi i proširen skup zadataka za CSIRT-ove (CERT-ove) u odnosu na NIS Direktivu. Dodatni zahtev u NIS 2 Direktivi je da su CSIRT-ovi u obavezi da obezbede poverljivost i pouzdanost svojih operacija, a zadaci za CSIRT-ove su sledeći:

- praćenje i analiziranje sajber pretnji, ranjivosti i incidenata na nacionalnom nivou i, na zahtev, pružanje pomoći esencijalnim i važnim entitetima,
- pružanje ranih upozorenja i drugih informacija o rizicima i incidentima esencijalnim i važnim entitetima, nadležnim organima i drugim subjektima od značaja,
- reagovanje na incidente i pružanje pomoći esencijalnim i važnim entitetima (gde je primenljivo),
- pružanje dinamičke analize rizika i incidenata i ukazivanje na trenutnu situaciju,
- pružanje esencijalnim i važnim entitetima usluge proaktivnog skeniranja mrežnih i informacionih sistema radi otkrivanja ranjivosti,
- učešće u Mreži CSIRT-ova,
- koordinacija aktivnosti usmerenih na koordinisano otkrivanje ranjivosti (gde je primenljivo), i
- doprinos primeni bezbednih alata za razmenu informacija.

Odredbe o koordinisanom otkrivanju ranjivosti su uvedene u NIS 2 Direktivu kao nova tema (koja nije postojala u NIS Direktivi). NIS 2 Direktivom propisano je da države članice treba da odrede CSIRT koji će biti koordinator ovih aktivnosti. Taj CSIRT treba da deluje kao posrednik od poverenja i olakša komunikaciju između onog ko prijavljuje ranjivost (bilo da je u pitanju pravno ili fizičko lice) i proizvođača potencijalno ranjivog proizvoda ili pružaoca potencijalno ranjive usluge. Zadaci ovog CSIRT-a uključuju:

- identifikaciju i uspostavljanje kontakta sa predmetnim stranama,
- pomoć strani koja prijavljuje ranjivost i
- dogovaranje o rokovima za objavljivanje, kao i upravljanje ranjivostima koje utiču na više entiteta.

Strani koja prijavljuje ranjivost mora biti zagarantovana anonimnost ako to želi.

NIS 2 Direktiva daje zadatak ENISA-i da razvije i održava Evropsku bazu ranjivosti, uključujući odgovarajući informacioni sistem, politike i procedure, kao i da preduzme neophodne tehničke i organizacione mere koje će garantovati bezbednost i integritet ove baze podataka. Baza podataka će biti dostupna svim značajnim entitetima, a sadržaće sledeće podatke:

- opis ranjivosti,
- obuhvaćene proizvode ili usluge i ozbiljnost ranjivosti u smislu okolnosti pod kojima ona može biti eksploatisana i
- dostupnost odgovarajuće zakrpe ili uputstvo za umanjenje rizika ako zakrpa ne postoji.

Novitet u NIS 2 Direktivi je uspostavljanje Evropske mreže za organizaciju veze za sajber krize (EU-CyCLONe). Svrha uspostavljanja ove mreže je podrška upravljanju velikim incidentima i krizama na operativnom nivou i osiguranje razmene relevantnih informacija između država članica i institucija EU. Zadaci ove mreže su:

- da poveća nivo pripremljenosti za upravljanje velikim incidentima i krizama;
- da razvije zajedničku svest o situaciji u vezi sa velikim incidentima i krizama;
- da proceni posledice i uticaj relevantnih velikih incidenata i kriza i predloži mere za ublažavanje;
- da koordinira upravljanje velikim incidentima i krizama i podrži donošenje odluka na političkom nivou u vezi sa njima;
- da raspravlja, na zahtev države članice, o nacionalnim planovima za reagovanje na velike incidente i krize.

Novi zadatak koji je ENISA dobila NIS 2 Direktivom je da, u saradnji sa Evropskom Komisijom i Grupom za saradnju, izradi izveštaj o stanju u EU u oblasti informacione bezbednosti i da ga predstavi Evropskom Parlamentu. Ovaj izveštaj se izrađuje svake druge godine i treba da obuhvati:

- procenu rizika na nivou EU;
- procenu razvoja kapaciteta u oblasti informacione bezbednosti u javnom i privatnom sektoru;
- procenu opšteg nivoa svesti o informacionoj bezbednosti i sajber higijeni među građanima i entitetima, uključujući mala i srednja preduzeća;
- zbirnu procenu nivoa zrelosti kapaciteta i resursa za informacionu bezbednost širom EU, kao i stepena do kojeg su usklađene nacionalne strategije informacione bezbednosti država članica.

Grupa za saradnju je NIS 2 Direktivom dobila zadatak da do 17. januara 2025. godine, uz pomoć Evropske Komisije, ENISA i Mreže CSIRT-ova, uspostavi metodologiju i organizacione aspekte partnerskih pregleda (eng. *peer reviews*), sa svrhom učenja iz tuđih iskustava, ojačavanja uzajamnog poverenja, postizanja visokog zajedničkog nivoa informacione bezbednosti i poboljšanja kapaciteta i politika država članica da implementiraju ovu Direktivu. Partnerski pregledi moraju biti dobrooljni i sprovođeni od strane najmanje dva eksperta u oblasti informacione bezbednosti koji nisu iz države članice u kojoj se vrši pregled. Partnerski pregledi moraju obuhvatiti makar jednu od sledećih procena:

- nivo implementacije mera za upravljanje rizicima u informacionoj bezbednosti i implementacije obaveza u vezi izveštavanja utvrđenih ovom Direktivom;
- nivo sposobnosti, uključujući raspoložive finansijske, tehničke i ljudske resurse, i efikasnost izvršavanja zadataka;
- operativne sposobnosti CSIRT-ova;
- nivo implementacije uzajamne pomoći;

- nivo implementacije razmene informacija;
- posebna pitanja prekogranične ili međusektorske prirode.

NIS 2 Direktivom je propisano da države članice mogu zahtevati od esencijalnih i važnih entiteta da koriste određene IKT proizvode, usluge i procese, koji su sertifikovani prema evropskim šemama sertifikacije za informacionu bezbednost usvojenim u skladu sa Aktom o sajber bezbednosti. Pored toga, Evropska Komisija ima ovlašćenja da dopuni ovu Direktivu precizirajući koje kategorije esencijalnih i važnih entiteta treba da koriste određene sertifikovane IKT proizvode, usluge i procese. Ako odgovarajuća evropska šema sertifikacije za informacionu bezbednost nije dostupna, Evropska Komisija može zahtevati od ENISA da pripremi ovu šemu.

Zbog navedenih izmena pravnog okvira Evropske unije stvara se jaz u propisima koje Republika Srbija, ne samo zbog obaveza preuzetih u procesu harmonizacije i priključenja Evropskoj uniji, već zbog unapređenja same oblasti, mora da prevaziđe. Stoga je neophodno izvršiti usklađivanje pravnog okvira i Zakon o informacionoj bezbednosti harmonizovati sa navedenom Direktivom.

Nedostatak kapaciteta nadležnih organa

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

Za ispunjavanje svih zakonom predviđenih nadležnosti neophodno je da Nacionalni CERT i ostali CERT-ovi osnovani u Republici Srbiji imaju adekvatne resurse. Postoji generalno mišljenje u stručnoj javnosti da se oblast informacione bezbednosti ne shvata dovoljno ozbiljno i da se moguće posledice od napada na IKT sisteme potcenjuju, odnosno ne pridaje im se dovoljna pažnja. Jedno od pitanja koje se često postavlja je mogućnost obezbeđenja neophodnih ljudskih resursa i adekvatna naknada za njihov rad, imajući u vidu situaciju na tržištu sa ovim kadrom nasuprot ograničenjima koja nameću propisi u javnom sektoru. U tom kontekstu potrebno je sagledati kapacitete (pre svega kadrovske ali i organizaciono-tehničke) nadležnog organa (u daljem tekstu: Ministarstvo). Kao i kod drugih državnih i ostalih organa, i Ministarstvo se suočava sa problemom da privuče i zadrži dovoljno stručan kadar koji će se baviti informacionom bezbednošću.

Problem sa kadrovima se posebno odnosi na poslove inspekcije za informacionu bezbednost, odnosno na činjenicu da trenutno inspekcija broji dva inspektora. Zakonom o informacionoj bezbednosti predviđeno je da ova inspekcija vrši nadzor nad primenom zakona i nad radom IKT sistema od posebnog značaja. Imajući u vidu broj IKT sistema od posebnog značaja jasno je da dva inspektora ne mogu blagovremeno da sprovede nadzor nad većim brojem IKT sistema od posebnog značaja. Zakonom je predviđeno da inspektor ima ovlašćenja da naloži otklanjanje utvrđenih nepravilnosti i da zabrani korišćenje postupaka ili tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost, kao i da ostavi rok za primenu naloženih mera. S obzirom da je ovo način da se primene neke mere neophodne za suzbijanje incidenata, u slučaju odsustva inspektora ne postoji alternativni način za nalaganje tih mera.

Nedostatak operativnih kapaciteta za reagovanje na incidente

U Republici Srbiji su u poslednjih nekoliko godina razvijani kapaciteti za reagovanje na incidente u nekoliko organa uprave, ali u većini organizacija, kako u javnom sektoru tako i generalno u onima koje su nadležne za upravljanje IKT sistemima koji pripadaju kritičnoj infrastrukturi, nema dovoljno izgrađenih kapaciteta, pa uglavnom zavise od trećih lica. Nacionalni CERT 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, dok se nadležnosti CERT-a organa vlasti u Kancelariji za informacione tehnologije i elektronsku upravu

odnose, pre svega, na zaštitu informaciono-komunikacionih sistema jedinstvene informaciono-komunikacione mreže elektronske uprave.

Imajući ovo u vidu, čak ni zakonski nije pokrivena operativna pomoć drugim IKT sistemima od posebnog značaja, osim onih koji se nalaze u okviru sistema elektronske uprave. U prethodnom periodu izvršeno je nekoliko ozbiljnih napada na IKT sisteme u javnom sektoru u Srbiji (pomenimo samo napade na JKP Informatika iz Novog Sada i na Republički geodetski zavod) koji su zahtevali angažovanje nekih operativnih timova iz javnog sektora kojima ovakve intervencije nisu u nadležnosti, ali i specijalizovanih privatnih kompanija. Ovakvi primeri jasno ukazuju da postoji potreba za uspostavljanjem operativnog tima koji bi imao nadležnost, ali i znanje, da operativno reaguje u slučajevima incidenata u IKT sistemima od posebnog značaja kada operator ugroženog IKT sistema nema sopstvene kapacitete za rešavanje incidenta.

Takođe, jedan od identifikovanih problema je nepostojanje obaveznih vežbi na kojima bi se preispitivale i uvežbavale procedure za reagovanje u slučaju incidenta. Ovakve vežbe su ustaljena praksa u razvijenim zemljama, dok se u Srbiji nisu organizovale u značajnoj meri. Izuzetak su sajber vežbe „Sajber Tesla" koje se od 2016. godine u Republici Srbiji organizuju na godišnjem nivou 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. Jedan od identifikovanih problema prilikom organizacije ovakvih vežbi je redovan izostanak donosioca odluka, odnosno delegiranje niže rangiranih službenika u svojstvu zamene.

Nedostatak sistemskog prikupljanja i razmene informacija

Nacionalni CERT ima nadležnost da prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i o 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. Nacionalni CERT je i tačka kontakta sa drugim sličnim organizacijama van Srbije i sa međunarodnim organizacijama i udruženjima. U međunarodnoj praksi nacionalni CERT-ovi dobijaju poseban položaj i pristup informacijama u vezi informacione bezbednosti koje nisu javno objavljene, kako bi mogli da ih distribuiraju do subjekata kojima su ove informacije potrebne. Po ovom pitanju Nacionalni CERT je već sproveo određene aktivnosti, kao što su one na implementaciji MISP platforme. Ove aktivnosti svakako treba nastaviti ali je potrebno uključiti veći broj subjekata.

Prijava incidenata je jedan od važnih oblika prikupljanja informacija. Može se konstatovati da se poboljšava disciplina po pitanju poštovanja ove zakonske obaveze ali se ne može reći da se ona u potpunosti poštuje, jer je izvesno da se mnogi incidenti ne prijavljuju, a otkrivaju se u medijima ili putem drugih kanala komunikacije. Razlozi za neprijavljivanje su razni – neobaveštenost da je prijavljivanje obavezno, nedovoljna svest o značaju prijavljivanja, strah od ugrožavanja reputacije, zauzetost drugim poslovima, ili jednostavna nebriga. Potrebno je u kontinuitetu podsticati prijavljivanje incidenata, posebno ako bi to obezbedilo i određeni nivo pristupa sistemu za razmenu informacija.

Nizak stepen prevencije i zaštite IKT sistema od posebnog značaja

Zakonom o informacionoj bezbednosti definisano je da su IKT sistemi od posebnog značaja sistemi koji se koriste u obavljanju poslova u organima vlasti, za obradu posebnih vrsta podataka o ličnosti, u obavljanju delatnosti od opšteg interesa i drugih delatnosti u određenim sektorima (energetika, saobraćaj, zdravstvo, bankarstvo i finansijska tržišta, digitalna infrastruktura, dobra od opšteg interesa, usluge informacionog društva i ostale oblasti) i u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje prethodno navedenih delatnosti.

IKT sistemi od posebnog značaja po ovom Zakonu imaju obavezu da se upišu u evidenciju operatora IKT sistema od posebnog značaja, preduzmu mere zaštite ovog sistema, donesu akt o bezbednosti, vrše periodičnu proveru usklađenosti primenjenih mera zaštite sa usvojenim aktom o bezbednosti, urede odnos sa trećim licima u skladu sa zakonom ako njima poveravaju aktivnosti u

vezi sa IKT sistemom od posebnog značaja, dostavljaju obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema i dostavljaju statističke podatke o incidentima u IKT sistemu.

Ugrožavanje IKT sistema od posebnog značaja moglo bi da izazove posledice po funkcionisanje organizacija koje njima upravljaju, ali i na prava i interese građana i privrede, kao i na nacionalnu i javnu bezbednost. Identifikovani problemi sa kojima se suočavaju IKT sistemi od posebnog značaja odnose se na nedostatak dovoljnog broja zaposlenih (posebno onih sa adekvatim znanjem), neodgovarajuću opremu i nedovoljno razvijenu svest rukovodstva o značaju informacione bezbednosti. Ovi problemi su posebno izraženi u javnom sektoru. U privatnom sektoru postoji izdvajanje većih finansijskih sredstava za informacionu bezbednost.

Nedostatak kapaciteta za reagovanje na incidente u državnim institucijama

I pored obaveze predviđene Zakonom o informacionoj bezbednosti, nisu sve institucije u javnom sektoru razvile kapacitete za reagovanje na incidente. Organi uprave imaju problem sa privlačenjem i zadržavanjem kadra za ove poslove, o čemu se posebno mora voditi računa u budućnosti. Čak i institucije koje su formalno uspostavile svoje organizacione celine i radile na izgradnji njihovih kapaciteta moraju kontinuirano da unapređuju svoje kapacitete, dok oni koji svoje kapacitete još uvek nisu izgradile mogu dobiti, i dobijaju je, od strane onih koji su odmakli u ovom procesu.

Nacionalni CERT, koji je osnovan 2017. godine, i dalje ima potrebe za podizanjem kapaciteta bez obzira što je u prethodnom periodu dosta učinjeno po pitanju angažovanja novih zaposlenih, nabavke opreme i opremanja prostora. Saradnja sa CERT-om organa vlasti i CERT-ovima samostalnih operatora IKT sistema je uspostavljena i redovna, ali može biti poboljšana kroz intenzivniju razmenu znanja i iskustava i brzu pomoć u slučaju incidenata.

Radi efikasnijeg reagovanja u slučaju ozbiljnijih incidenata, posebno onih od nacionalnog značaja, potrebno je uspostaviti odgovarajuće protokole i procedure za saradnju, odrediti osobe za kontakt i oranizovati redovne vežbe.

CERT organa vlasti je prevashodno usmeren na zaštitu u okviru jedinstvene informaciono-komunikacione mreže elektronske uprave. Značajan broj organa javne vlasti povezan je na mrežu elektronske uprave i od velike koristi bi bilo podizanje njihovih kapaciteta za reagovanje u slučaju incidenta i poboljšanje razmene informacija sa CERT-om organa vlasti.

Nedostatak koordinacije za otkrivanje ranjivosti

Ovaj aspekt poslednjih godina dobija sve više na značaju na globalnom nivou. Mnogi istraživači i stručnjaci rade na otkrivanju ranjivosti i njihovom otklanjanju pre nego što ih otkriju kriminalci i zlonamerni korisnici. U takvim situacijama češće se događa da kriminalci dobiju otvorenu mogućnost da ugroze određeni IKT sistem nego da organizacija uspe da za kratko vreme otkloni ranjivost, pa je uspostavljanje modela za sistematično obaveštavanje o ranjivostima način da se ovi problemi otklone.

Nedovoljna koordinacija međunarodnih aktivnosti

Republika Srbija aktivno učestvuje u mnogim međunarodnim organizacijama i procesima u oblasti informacione bezbednosti, kako na globalnom tako i na regionalnom nivou, kao i u bilateralnim aktivnostima. Između ostalog, Republika Srbija učestvuje u radu Otvorene radne grupe UN za pitanja informacione bezbednosti, imala je predstavnika u petoj Grupi vladinih eksperata UN, aktivno učestvuje u radu Neformalne radne grupe OEBS osnovane odlukom Stalnog saveta broj 1039, sponzor je implementacije Mere OEBS za izgradnju poverenja broj 9, član je Globalnog foruma za sajber ekspertizu i ima imenovane predstavnike u svih pet radnih grupa ovog Foruma. Institucije iz Republike Srbije često učestvuju u aktivnostima koje se realizuju u okviru međunarodnih projekata iz oblasti informacione bezbednosti, uključujući obuke, radionice, sastanke i konferencije.

Dosadašnja praksa podrazumevala je angažovanje predstavnika iz nekoliko institucija iz javnog sektora u međunarodnim organizacijama i telima. Takva praksa nije problem sama po sebi, ali može dovesti do nekonzistentnog stava različitih predstavnika zbog manjka informacija o poziciji Srbije ili aktivnostima predstavnika u drugim organizacijama. Značajno bi bilo uspostavljanje obaveznih konsultacija predstavnika Srbije u međunarodnim organizacijama u oblasti informacione bezbednosti, uzimajući u obzir nadležnosti Ministarstva spoljnih poslova.

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

Izmene Zakona o informacionoj bezbednosti inicirane su pre svega zbog usklađivanja sa evropskom NIS 2 Direktivom (eng. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive) usvojenoj 14. decembra 2022. godine, ali i u delu sertifikacije IKT sistema sa Aktom o sajber bezbednosti - Uredba 2019/881 (eng. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) usvojenoj 17. aprila 2019. godine.

Pored toga, na osnovu dosadašnje primene Zakona utvrđene su i druge potrebe koje zbog nedovoljne implementacije svih zakonskih rešenja zahtevaju ne samo izmenu pravnog, već i institucionalnog okvira. Zbog toga će posebno biti predstavljene najpre promene važećeg institucionalnog okvira uređenog Zakonom, a zatim i druge izmene, kao rezultat harmonizacije sa evropskim pravnim okvirom.

Predlozi izmena institucionalnog okvira

Nedostatak kapaciteta nadležnih organa u oblasti informacione bezbednosti zahteva i izmenu institucionalnog okvira. U cilju pronalaženja najboljeg modela analizirani su primeri institucionalnog okvira tri evropske zemlje: Savezne Republike Nemačke, Velikog Vojvodstva Luksemburg i Kraljevine Holandije koji su predstavljeni u nastavku.

Savezna Republika Nemačka

Za oblast informacione bezbednosti na federalnom nivou u Nemačkoj je nadležno federalno Ministarstvo unutrašnjih poslova (Ministarstvo unutrašnjih poslova i zajednice). Međutim, Nemačka je zemlja sa jakim federalizmom i nadležnosti federalnih jedinica su veoma široke, pa je regulisanje oblasti informacione bezbednosti predstavljalo veliki izazov za ovu državu, što je čak dovelo i do izmena Ustava.

Prvu strategiju informacione bezbednosti Nemačka je usvojila 2011. godine, 2016. godine je usvojila izmene te strategije, a 2021. godine je usvojila novu Strategiju informacione bezbednosti za Nemačku. U novoj Strategiji definisana su četiri principa:

- Uspostavljanje informacione bezbednosti kao zajedničkog zadatka za Vladu, privatni sektor, istraživačku zajednicu i društvo u celini,
- Osnaživanje digitalnog suvereniteta Vlade, privatnog sektora, istraživačke zajednice i društva u celini,
- Ostvarivanje bezbedne digitalne transformacije i
- Postavljanje merljivih i transparentnih ciljeva.

Nadležnost pružanja informacione bezbednosti na nacionalnom nivou ima Federalna kancelarija za informacionu bezbednost (Bundesamt für Sicherheit in der Informationstechnik, BSI). Ova Kancelarija uspostavljena je 1991. godine i pripada nemačkom federalnom Ministarstvu unutrašnjih poslova, a nadležnosti su joj dodeljene Aktom o Federalnoj kancelariji za informacionu bezbednost koji je regulisao oblast informacione bezbednosti u Nemačkoj na nacionalnom nivou. Sedište Kancelarije je u Bonu, a trenutno ima preko 1400 zaposlenih.

Nakon usvajanja NIS Direktive EU, u Nemačkoj je njihov pravni sistem usklađen amandmanima na Akt o Federalnoj kancelariji za informacionu bezbednost i na nekoliko drugih zakona u oblasti javnih servisa. Neke od nadležnosti koje ima BSI kako bi ispunila svoje zadatke su:

- Prevencija pretnji po bezbednost federalnih IKT sistema,
- Testiranje i procena bezbednosti IKT sistema i komponenti i izdavanje bezbednosnih sertifikata, i
- Razvoj tehničkih bezbednosnih standarda za federalne IKT sisteme.

Nove izmene pravnog okvira napravljene su 2021. godine usvajanjem u Bundestagu Akta o IT bezbednosti Nemačke 2.0 (prva verzija usvojena je 2015. godine) kojima je Federalna kancelarija za informacionu bezbednost dobila nove i ojačala postojeće nadležnosti u sledećim oblastima:

- Detekcija i odbrana – povećane nadležnosti u detekciji bezbednosnih ranjivosti i odbrani od sajber napada, ovlašćenja za postavljanje obavezujućih minimalnih standarda za federalne institucije, monitoring implementacije postavljenih standarda, postavljanje pravila za bezbednu digitalizaciju;
- Bezbednost u mobilnim mrežama – uređenje zabrane korišćenja kritičnih komponenti, bezbednosni zahtevi za operatore mobilnih servisa, obaveza sertifikacije kritičnih komponenti, primena informacione bezbednosti u 5G mobilnim mrežama;
- Zaštita potrošača – savetovanja potrošača o bezbednosnim pitanjima (nova funkcija Kancelarije), uvođenje oznake „IT Security Mark“ na proizvodima;
- Bezbednost poslovanja – proširenje kritične infrastrukture na oblast odlaganja smeća, obaveza implementacije bezbednosnih mera za organizacije od posebnog javnog interesa (koje ne pripadaju kritičnoj infrastrukturi);
- Nacionalna sajberbezbednosna sertifikacija – nadležnosti Nacionalnog autoriteta za sajberbezbednosnu sertifikaciju (u skladu sa Aktom o sajber bezbednosti EU).

Organizaciona struktura Federalne kancelarije za informacionu bezbednost sastavljena je od osam direktorata:

- Centralni poslovi,
- Tehnički centar izvrsnosti,
- Tehnologije informacionih uverenja i upravljanje IT,
- Operativna informaciona bezbednost,
- Standardizacija, sertifikacija i informaciona bezbednost telekomunikacionih mreža,
- Informaciona bezbednost za digitalizaciju i elektronske identitete,
- Konsultacije za institucije Federacije, federalnih jedinica i lokalnih vlasti i
- Informaciona bezbednost za privatni sektor i društvo.

Svaki od direktorata organizovan je kroz niže organizacione jedinice. Kancelarijom upravlja predsednik, kojem su direktno podređene još tri organizacione jedinice:

- Biro za strateške komunikacije i medije,
- Jedinica za stratešku kontrolu i interne provere i
- Jedinica za stratešku i izvršnu podršku.

U okviru Kancelarije deluju neke od najznačajnijih organizacionih celina za sajber odbranu:

- Nacionalni centar za sajber odbranu – platforma za saradnju i razmenu informacija o sajber pretnjama i za usklađivanje aktivnosti Vlade na prevenciji i suzbijanju sajber napada; u radu Nacionalnog centra učestvuju predstavnici policije, službi bezbednosti (vojnih i civilnih), federalne kancelarije za civilnu zaštitu i pomoć u vanrednim situacijama i vojne sajber komande;
- Savez za informacionu bezbednost – javno-privatno partnerstvo u oblasti informacione bezbednosti u kojem učestvuje preko 4000 kompanija;
- Federalni CERT (CERT-Bund) – centralna tačka kontakta za preventivne i reaktivne mere u slučajevima sajber incidenata u federalnim institucijama; i
- IT Situacioni centar – nadležan za koordinaciju odgovora u slučajevima sajber incidenata.

Savet za informacionu bezbednost formiran je 2011. godine na osnovu Strategije za informacionu bezbednost Nemačke i sa ciljem da unapredi saradnju na nivou federalne Vlade u oblasti informacione bezbednosti. Izmene Strategije iz 2016. godine definisale su permanentnu ulogu ovog Saveta kao savetodavnog organa federalne Vlade. Sastancima Saveta rukovodi Glavni službenik za informisanje (CIO) federalne Vlade. Savet ima obavezu da Vladi podnosi izveštaje o strateškim pitanjima u oblasti informacione bezbednosti o kojima raspravlja. Od 2018. godine uspostavljena je i posebna radna grupa sa zadatkom da pomaže Savetu u radu.

Problem sa kojim se suočavaju sve zemlje, pa i Nemačka, jeste pravljenje razlike između unutrašnje bezbednosti, koja je tradicionalno u nadležnosti policije, i spoljne bezbednosti, koja je tradicionalno u nadležnosti vojske. U sajber prostoru ova granica nije sasvim jasna, a sve veća upotreba sajber prostora za vojne aktivnosti nameće potrebu da se određene aktivnosti definišu i sprovedu. Iz tog razloga Nemačka je 2017. godine definisala sajber i informacioni vojni domen, pored postojećih kopnenog, pomorskog i vazdušnog, i uspostavila novu službu nadležnu za ovaj domen. Prema raspoloživim podacima u ovoj službi je 2020. godine bilo zaposleno preko 14.000 civilnog i vojnog osoblja. Takođe, iz razloga specifičnosti sajber prostora po pitanju unutrašnje i spoljne bezbednosti, dogovorom nemačkih političkih partija je 2018. godine odlučeno da se formira zajednička agencija Ministarstva odbrane i Ministarstva unutrašnjih poslova sa zadatkom da sprovodi kreativne i inovativne projekte iz oblasti informacione bezbednosti. Na osnovu ovog dogovora, 2020. godine formirana je Sajber agencija (Agentur für Innovation in der Cybersicherheit ili Cyberagentur) u formi kompanije sa ograničenom odgovornošću (GmbH) čiji je jedini akcionar federalna Vlada. Ova Agencija ima oko 100 zaposlenih (prema raspoloživim podacima) i ne sprovodi samostalno istraživanja, već u saradnji sa akademijom i industrijom sprovodi inovativne projekte za koje se proceni da su od izuzetnog nacionalnog značaja (posebno ih interesuju teme kao što su pouzdane i otporne informacione tehnologije, interakcija čoveka i tehnologije, veštačka inteligencija, nano i kvantna tehnologija, svemirska i pomorska bezbednost, bionika, interfejsi mozak-računar, prediktivna analitika, kriptografija ili autonomni sistemi). Agencija je za svoje aktivnosti dobila inicijalni budžet od 280 miliona evra od kojih je veći deo već uložila u istraživačke projekte.

Još jedna značajna platforma koju je pokrenulo nemačko Ministarstvo odbrane je Sajber inovacioni hab, sa namerom da privuče mlade i kreativne umove da kroz startap-ove i okruženje koje više odgovara njihovom načinu razmišljanja realizuju projekte od značaja za odbranu. Sajber inovacioni hab je u suštini platforma za realizaciju projekata, a formalno je organizovan kao ogranak kompanije koja pruža IT usluge za nemačku armiju, koja donosi krajnju odluku koji projekti će se finansirati.

Veliko Vojvodstvo Luksemburg

Dokument javnih politika u oblasti informacione bezbednosti u Luksemburgu je nacionalna strategija informacione bezbednosti. Do sada je Luksemburg usvojio četiri strategije, a poslednja se odnosi na period od 2021. do 2025. godine. Svaka od strategija donosila je određena unapređenja, pa je tako prva strategija inicirala osnivanje Vladinog CERT-a, druga uspostavljanje Nacionalne agencije za bezbednost informacionih sistema (fra. *Agence nationale de la sécurité des systèmes d'information - ANSSI*), treća formiranje Centra za kompetencije u oblasti informacione bezbednosti (eng. *Cybersecurity Competence Center - C3*), uspostavljanje metodologije za analizu rizika *MONARC* i formiranje Međuministarskog koordinacionog komiteta za sajber prevenciju i informacionu bezbednost (Comité interministériel de coordination en matière de cyberprévention et de cybersécurité), dok četvrta predviđa formiranje *SOC* za kritičnu infrastrukturu, formiranje Nacionalnog centra za filtriranje *DDoS* napada, razvoj platforme za analizu i upravljanje rizicima *SERIMA* namenjene operatorima esencijalnih servisa i drugo. Institucija nadležna za izradu i koordinaciju strategije je Visoki komesarijat za nacionalnu zaštitu (HCPN).

Luksemburg je u maju 2019. godine transponovao NIS Direktivu EU u svoje zakonodavstvo i odredio Regulatorni institut Luksemburga *ILR* za jedinstvenu tačku kontakta i nadležni organ za sektore energetike, transporta, zdravlja, pijaće vode i digitalne infrastrukture, dok je Komisija za

nadzor sektora finansija *CSSF* nadležni organ za sektore infrastrukture finansijskih tržišta i kreditnih institucija.

Luksemburg nema centralni organ koji bi objedinjavao nadležnosti u oblasti informacione bezbednosti, nego su nadležnosti date različitim institucijama. Strateške nadležnosti imaju dve institucije: Telo za informacionu bezbednost *CSB* i Međuministarski koordinacioni komitet za sajber prevenciju i informacionu bezbednost (CIC-CPCS). Nadležnost nad koordinacijom aktivnosti ova dva tela i zadatak strateškog vođstva ima Visoki komesarijat za nacionalnu zaštitu.

Telo za informacionu bezbednost formirano je 2011. godine sa zadatkom da implementira i nadzire izvršavanje prve nacionalne strategije, a od 2019. godine nalazi se u nadležnosti Ministarstva države.

Međuministarski koordinacioni komitet za sajber prevenciju i informacionu bezbednost uspostavljen je 2017. godine sa ciljem da se, u saradnji sa Telom za informacionu bezbednost, angažuje na koordinaciji operativnih aktivnosti. U radu Komiteta učestvuju predstavnici sledećih institucija:

- Ministarstvo države,
- Visoki komesarijat za nacionalnu zaštitu,
- Odbrana Luksemburga (Direktorat za odbranu i Oružane snage Luksemburga),
- Ministarstvo privrede,
- ekonomska interesna grupa SECURITYMADEIN.LU,
- Vladin centar za informacione tehnologije (CTIE),
- Državna obaveštajna služba,
- Nacionalna agencija za bezbednost informacionih sistema (ANSSI) i
- Vladin CERT (GovCERT).

Radom komiteta predsedava Visoki komesar za nacionalnu zaštitu. Zadaci koji su postavljeni pred ovaj Komitet su:

- obezbeđenje konzistentnosti akcija i inicijativa,
- koordinacija implementacije inicijativa koje dolaze od EU ili sa drugih međunarodnih nivoa,
- nadzor nad implementacijom ovih inicijativa,
- davanje saveta Vladi po pitanjima informacione bezbednosti i
- diskusija o stavovima nacionalnih predstavnika.

Visoki komesarijat za nacionalnu zaštitu je telo koje je postojalo tokom Hladnog rata kao kancelarija Komiteta za nacionalnu zaštitu (sa zadacima vezanim za zaštitu organa vlasti i stanovništva, prikupljanje obaveštajnih podataka, sprovođenje psiholoških operacija i slično) i potom ukinuto, ali je reaktivirano nakon terorističkih napada 11. septembra 2001. sa novim nadležnostima u oblasti zaštite kritične infrastrukture i od 2016. godine uvršteno u sastav Ministarstva države. Visoki komesarijat je nadležan za prevenciju i upravljanje sajber krizama i za planiranje odgovora na vanredne situacije u oblasti informacione bezbednosti. Za sajber diplomatiju nadležno je Ministarstvo spoljnih i evropskih poslova.

Nacionalna agencija za bezbednost informacionih sistema (ANSSI) je nadležna za sisteme u državnim organima. Ova Agencija je formirana 2015. godine i sastavni je deo Visokog komesarijata za nacionalnu zaštitu kao regulatorni organ. Neke od nadležnosti ANSSI su:

- izrada politika i vodiča za zaštitu klasifikovanih i neklasifikovanih informacija,
- obezbeđenje primene mera zaštite informacionih sistema,
- sertifikacija načina obrade neklasifikovanih informacija,
- funkcije Nacionalnog i Vladinog CERT-a i
- nadležni organ za TEMPEST.

ANSSI je do 2018. godine bio i nadležni organ za odobravanje kriptografskih proizvoda, kada su te nadležnosti prenete na Vladin centar za informacione tehnologije (CTIE). ANSSI je do te godine bio i telo nadležno za upravljanje sajber incidentima, kada je ta uloga preneta na Vladin CERT. Vladin centar za informacione tehnologije (CTIE) je osnovan 2009. godine i predstavlja centralni organ za

poslove vezane za informacione tehnologije za ministarstva i državnu administraciju. CTIE je takođe i nadležni organ za distribuciju kriptografskog materijala i nadležni organ za kriptografsku akreditaciju, a u nadležnosti mu spadaju i zaštićena komunikacija i razmena informacija između državnih organa.

Vladin CERT (GovCERT) je osnovan 2013. godine sa zadatkom da rešava sve ozbiljnije sajber incidente u IKT sistemima Vlade. Od 2015. godine GovCERT je od ANSSI preuzeo nadležnosti upravljanja sajber incidentima i objedinio uloge Nacionalnog i Vladinog CERT-a, a od 2018. godine mu je, pored postojećih, poverena i funkcija Vojnog CERT-a (MilCERT) i smešten je u Visoki komesarijat za nacionalnu zaštitu. U okviru nadležnosti Nacionalnog CERT-a, GovCERT je zvanična nacionalna tačka kontakta sa CERT-ovima drugih zemalja i tačka za kontakt i razmenu informacija sa sektorskim CERT-ovima u Luksemburgu. GovCERT, u okviru svojih nadležnosti kao Vojni CERT, deluje kao zvanična tačka kontakta za vojne CERT-ove drugih zemalja, ali i prati i reaguje na incidente u IKT sistemima Oružanih snaga.

Ekonomska interesna grupa Security Made in Lëtzebuerg (poznatija kao SECURITYMADEIN.LU) je osnovana 2010. godine sa mandatom od Ministarstva privrede (koje i nadzire njen rad) da sprovodi istraživanja na međunarodnom nivou, deli informacije o pretnjama, implementira mrežu senzora za rana upozorenja i deluje kao hab za ekonomske aktivnosti u ovoj oblasti. Finansijska sredstva za rad grupe obezbeđuje država. SECURITYMADEIN.LU u svom sastavu ima tri organizacione jedinice: Centar za reagovanje na kompjuterske incidente (eng. *Computer Incident Response Center Luxembourg - CIRCL*), Servise podizanja bezbednosne svesti u sajber svetu i bezbednosna poboljšanja (CASES) i Centar za kompetencije u oblasti informacione bezbednosti (C3).

Možda i najpoznatija organizacija iz oblasti informacione bezbednosti iz Luksemburga je CIRCL koji je nadležan za privatni sektor, lokalnu samoupravu i nevladine organizacije. CIRCL je globalno poznat po svojoj platformi za deljenje informacija o pretnjama MISP, a od drugih inicijativa u kojima učestvuje vredi pomenuti zajednicu CERT.LU koja obezbeđuje razmenu informacija i saradnju privatnih CERT-ova sa CIRCL i GovCERT.

Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES) obezbeđuje publikacije, edukativni materijal, primere najboljih praksi i razne alate vezane za informacionu bezbednost (između ostalog, metod za analizu rizika MONARC).

Centar za kompetencije u oblasti informacione bezbednosti (C3) aktivnosti realizuje kroz davanje mišljenja, treniranje i testiranje, pretežno za privatni sektor.

Nacionalni autoritet za sertifikaciju u oblasti informacione bezbednosti je Institut za standardizaciju, akreditaciju, sigurnost i kvalitet proizvoda i usluga (ILNES).

Luksemburg ima usvojen plan za reagovanje u slučaju sajber krize (fra. *Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information - PIU Cyber*) za čiju ralizaciju je odgovoran direktno premijer. Ovaj plan je razvijen od strane Visokog komesarijata za nacionalnu zaštitu i ima četiri glavna cilja:

- usvajanje zaštitnih i preventivnih mera,
- definisanje uloge entiteta za upravljanje krizama,
- definisanje mera, postupaka i aktera u slučajevima vanrednih situacija i
- uzbunjivanje i informisanje javnosti.

Plan predviđa uspostavljanje četiri *ad-hoc* jedinice za rešavanje krize: jedinice za krizu, operativne jedinice, jedinice za procenu sajber rizika i jedinice za komunikacije i informisanje. Plan uključuje zadatke svake od ovih jedinica, njihov sastav, subordinaciju, izveštavanje i sve ostale elemente koji su potrebni za uspešno rešavanje krize.

<u>Kraljevina Holandija</u>

Holandija je prvu strategiju informacione bezbednosti usvojila 2011. godine, a trenutno važeća je strategija usvojena za period od 2022. do 2028. godine. Nova Strategija usmerava aktivnosti u četiri glavna smera:

- poboljšanje društvene otpornosti kroz zajedničke napore javnog, privatnog i nevladinog sektora,
- podsticanje bezbednosti digitalnih proizvoda i usluga u skladu sa propisima EU,
- suzbijanje sajber pretnji koje potiču od država i kriminalaca kroz poboljšanje prikupljanja i deljenja informacija, i u javnom i privatnom sektoru i
- obezbeđenje kvalitetne radne snage u oblasti informacione bezbednosti, obrazovanje i podizanje svesti građana.

Jedna od najvažnijih aktivnosti planirana Strategijom je spajanje nekoliko organizacija sa preklapajućim nadležnostima - NCSC, Centra za digitalno poverenje (DTC) i CSIRT-a provajdera digitalnih servisa (CSIRT-DSP) u jednu organizaciju, koja će postati jedinstveni nacionalni autoritet za informacionu bezbednost. Holandija je ovom Strategijom iskazala snažnu posvećenost objedinjavanju postojećih kapaciteta i neophodnost brze spoznaje informacija o pretnjama i ranjivostima i reagovanja na ove informacije. Strategijom je čak naglašena potreba suzbijanja fragmentacije u deljenju informacija kad god je moguće i potreba za restriktivnošću u formiranju novih CERT-ova. U tom cilju, novi autoritet (za koji se očekuje da će biti uspostavljen tokom 2024. godine) radiće u saradnji sa javnim i privatnim sektorom i pružati informacije o bezbednosti svim sektorima, organizacijama koje spadaju i koje ne spadaju u kritičnu infrastrukturu i generalnoj javnosti.

U Holandiji je prepoznato više od 20 institucija sa individualnom i kolektivnom odgovornošću u oblasti informacione bezbednosti. Na političkom i strateškom nivou najvažnije telo je Savet za informacionu bezbednost.

Savet za informacionu bezbednost formiran je 2011. godine kao telo koje treba da poveže različite aktere iz javnog i privatnog sektora i sa mandatom da savetuje Vladu i privatni sektor, postavi nacionalne prioritete, proceni potrebe za istraživanjem i razvojem i obezbedi razmenu znanja u okviru javnog i privatnog sektora. Za rad Saveta nadležno je Ministarstvo bezbednosti i pravde, a u radu Saveta učestvuju predstavnici iz javnog i privatnog sektora. Javni sektor je zastupljen sa 15 predstavnika iz sledećih institucija:

- Nacionalni koordinator za bezbednost i suzbijanje terorizma (u sastavu Ministarstva bezbednosti i pravde),
- Ministarstvo ekonomskih poslova,
- Ministarstvo odbrane,
- Generalni obaveštajni i bezbednosni servis,
- Agencija za nacionalne policijske servise i
- Generalni odbor tužilaca.

Iz privatnog sektora u radu Saveta učestvuju predstavnici vodećih provajdera telekomunikacionih usluga, vodećih snabdevača IKT opremom, korisnika IT usluga, malih i srednjih preduzeća, operatora kritične infrastrukture i akademskih institucija. Radom Saveta kopredsedavaju Nacionalni koordinator za bezbednost i suzbijanje terorizma i predstavnik privatnog sektora (koji se periodično menja).

Nacionalni centar za informacionu bezbednost (NCSC) formiran je 2012. godine sa zadatkom da unapredi razumevanje razvoja, pretnji i trendova u oblasti informacione bezbednosti i preuzme odgovornost u rešavanju sajber incidenata i upravljanju sajber krizama. U sastav NCSC prilikom osnivanja inkorporiran je postojeći Vladin CERT (GOVCERT.NL). U nadležnost NCSC spada pružanje usluga Vladi i IKT sistemima kritične infrastrukture u javnom i privatnom sektoru, kao i unapređenje javno-privatnog partnerstva. NCSC je organizaciono smešten u Direktoratu za informacionu bezbednost Ministarstva bezbednosti i pravde, a direktno je potčinjen Nacionalnom koordinatoru za bezbednost i suzbijanje terorizma. NCSC čine tri tima sa nadležnostima za reagovanje na incidente,

edukaciju i razvoj. U Direktoratu za informacionu bezbednost postoji i posebno Odeljenje za politike u čijoj je nadležnosti razvoj politika i strategija u oblasti informacione bezbednosti.

Nadležnost NCSC obuhvata postupanje sa pretnjama i incidentima, podizanje bezbednosne svesti, davanje saveta, reagovanje u slučaju krize i pružanje platforme za saradnju. NCSC je takođe veoma aktivan u međunarodnoj saradnji i nacionalna tačka kontakta Holandije. NCSC ima ključnu koordinacionu ulogu u slučaju ozbiljnog sajber incidenta ili sajber krize. Da bi uspešno ostvario ovaj zadatak, NCSC kontinualno prati stanje, vrši procene ugroženosti i mogućih posledica i reaguje u slučaju potrebe. Jedna od najvažnijih aktivnosti NCSC je upravo prikupljanje informacija, kako od javnog i privatnog sektora u Holandiji tako i od međunarodnih partnera.

U slučaju ozbiljnog sajber incidenta ili sajber krize NCSC aktivira Odbor za IKT odgovor (IRB) i daje podršku njegovim aktivnostima kroz pribavljanje i distribuciju informacija i administrativnu podršku. S obzirom da je u Holandiji veliki deo kritične infrastrukture u privatnom sektoru, u radu IRB učestvuju, pored predstavnika institucija Vlade, i predstavnici provajdera telekomunikacionih usluga, energetskog i finansijskog sektora, a po potrebi se mogu uključiti i drugi eksperti. Radom IRB rukovodi predstavnik Ministarstva ekonomskih poslova. Primarni zadatak IRB je da savetuje nacionalna tela za upravljanje krizama o merama koje treba preduzeti, ali takođe i da služi kao telo koje u slučaju krize spaja tehnički i administrativni nivo.

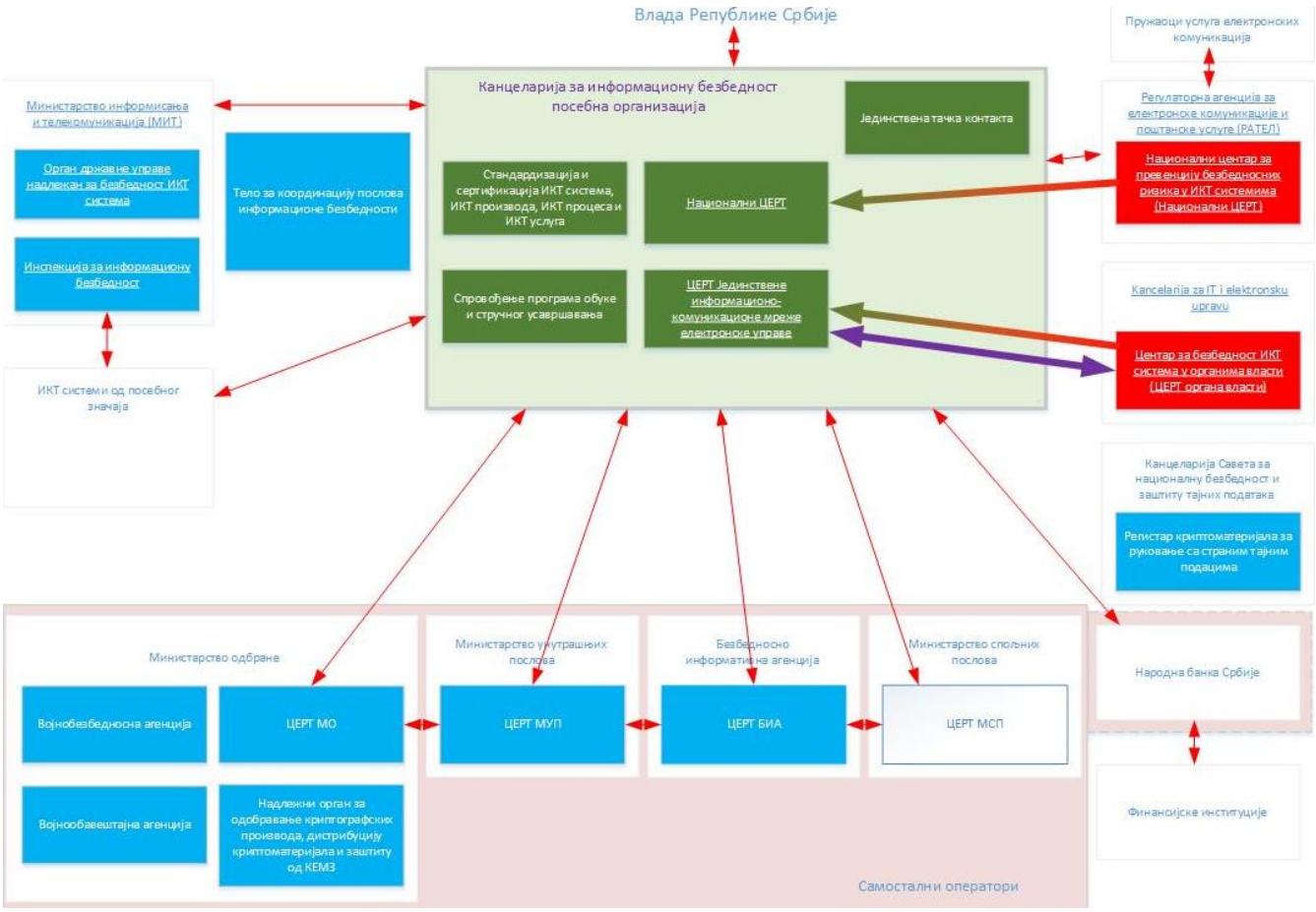
Holandija je 2012. godine prepoznala sajber prostor kao peti domen vojnih operacija (pored zemlje, mora, vazduha i svemira) i definisala šest oblasti razvoja sajber kapaciteta: odbrana, napad, obaveštajne aktivnosti, adaptivnost, inovacije i saradnja. Zajednička komanda za upravljanje informacijama (JIVC) formirana je 2013. godine, a u njen sastav ušao je i CERT odbrane (DefCERT) formiran godinu dana ranije. Nadležnosti DefCERT su u domenu bezbednosti IKT sistema Ministarstva odbrane i Oružanih snaga Holandije, podrške vojnim operacijama, procene pretnji i ranjivosti, davanja saveta i slično, ali takođe i podrška državnim organima u zajedničkom odgovoru na sajber pretnje. DefCERT i NCSC su potpisali memorandum o razumevanju i intenzivno sarađuju kroz razmenu informacija i uzajamnu podršku.

Odbrambena sajber komanda je formirana 2014. godine sa primarnim fokusom na uspostavljanje odbrambenih, napadačkih i obaveštajnih kapaciteta u sajber prostoru. U sastav Odbrambene sajber komande prilikom uspostavljanja ušle su organizacione jedinice ostalih službi, čime je uspostavljena jedinstvena celina u odbrambenom sistemu Holandije nadležna za ovu oblast.

Predlozi unapređenja institucionalnog okvira u Republici Srbiji

Analiza postojećeg institucionalnog okvira pokazuje rasipanje kapaciteta nadležnih organa za preventivno i blagovremeno reagovanje na incidente u sajber prostoru.

U skladu sa navedenim modelima evropskim zemalja prilikom izrade Nacrta analizirana su tri modela institucionalne promene koji su dati u nastavku teksta.



Dijagram 19 Institucionalni okvir - model 1

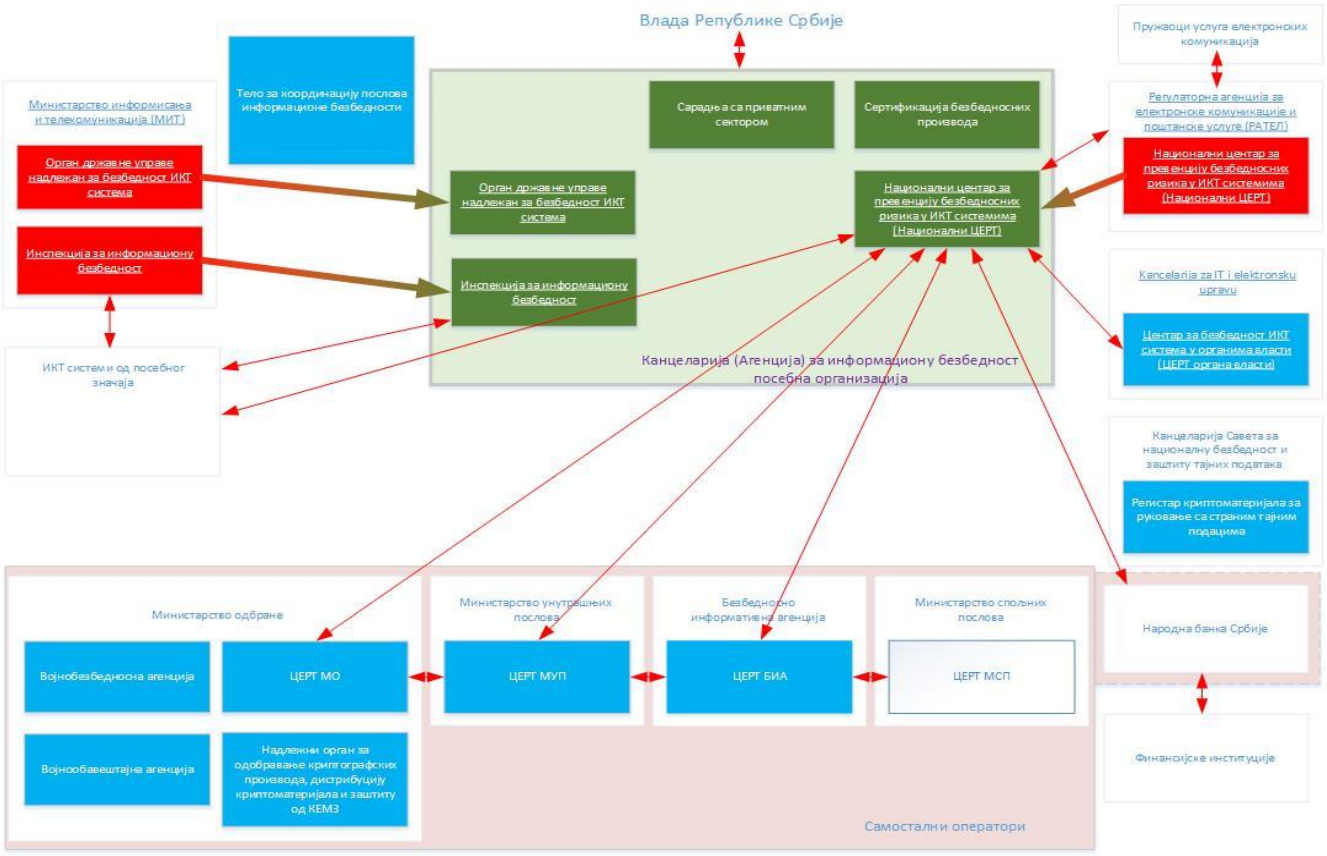
Novina:

- Formira se posebna organizacija - Kancelarija za informacionu bezbednost koja postaje jedinstvena tačka kontakta
- Na novu Kancelariju prenose se nadležnosti Nacionalnog CERT-a i Vladinog CERT-a (i postojeće organizacione jedinice i zaposleni).

Prednosti ovakvog modela institucionalnog okvira su u uspostavljanju jedinstvene, prepoznatljive institucije (posebne organizacije), grupisanju postojećih kapaciteta, stvaranju uslova za bolju i bržu razmenu informacija, kao i uslova za konkretnu pomoć drugim organima državne uprave u slučaju sajber incidenata (na primer MSP-u ili Kancelariji za IT i eUpravu). Nedostatak ovakvog modela institucionalnog okvira su potencijalni problem za ceo javni sektor u slučaju nedovoljnih kapaciteta nove Kancelarije i nedostatak podrške da se prihvati prenos svojih nadležnosti i zaposlenih u novu Kancelariju.

Drugim modelom:

- Formira se posebna organizacija - Kancelarija za informacionu bezbednost koja postaje Nadležni organ i jedinstvena tačka kontakta
- Na novu Kancelariju prenose se nadležnosti Inspekcije za informacionu bezbednost i Nacionalnog CERT-a.



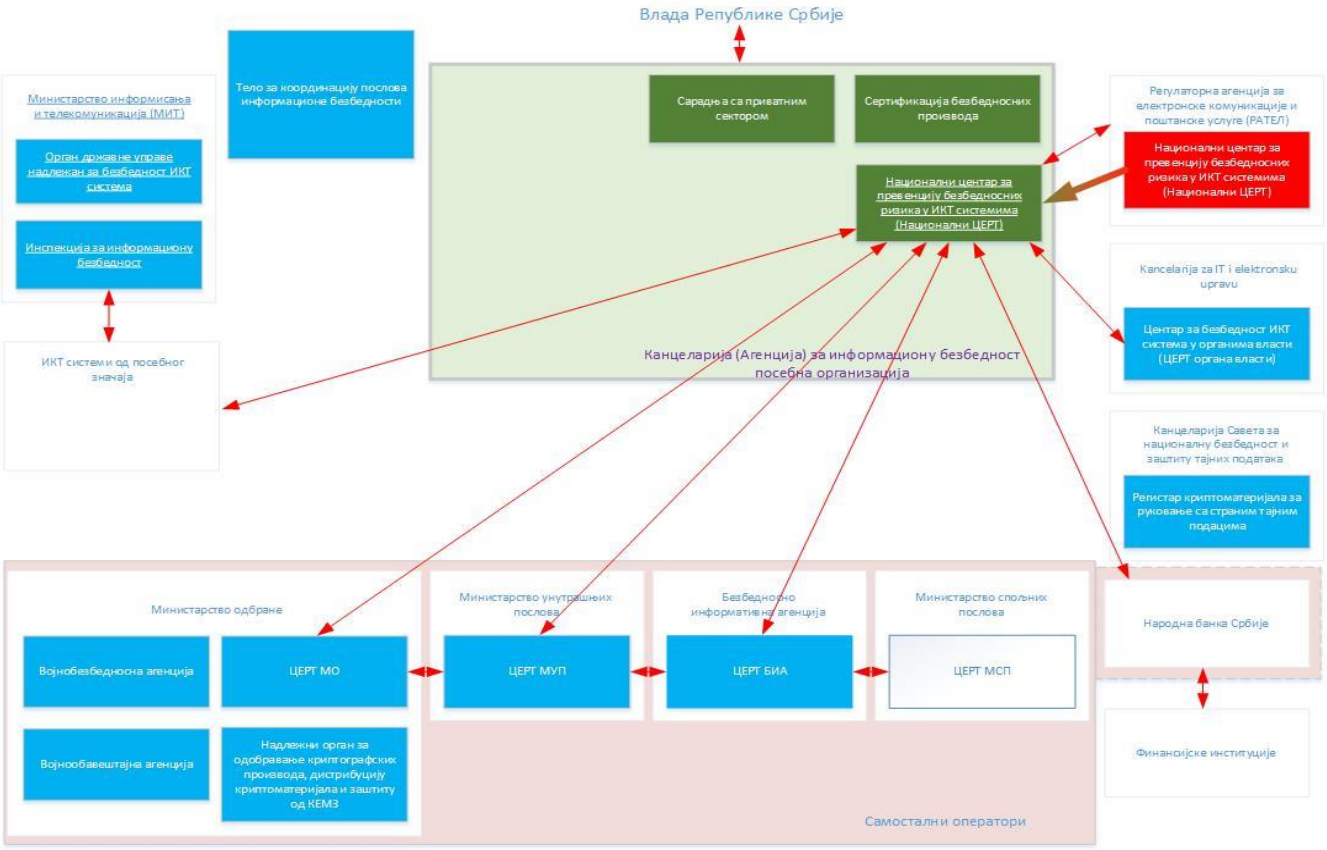
Dijagram 20 Institucionalni okvir - model 2

Prednosti ovakvog modela institucionalnog okvira su u povećanju kapaciteta za podršku IKT sistemima od posebnog značaja i stvaranje uslova za bolju i bržu razmenu informacija. Nedostatak ovakvog modela institucionalnog okvira su ograničene mogućnosti za saradnju po pitanju operativnih aktivnosti, kao i nedostatak političke podrške da se prihvati prenos svojih nadležnosti i zaposlenih u novu Kancelariju.

Trećim modelom:

- Formira se posebna organizacija - Kancelarija (Agencija) na koju se prenose nadležnosti Nacionalnog CERT-a.

Prednosti ovakvog modela institucionalnog okvira je u bržoj implementaciji modela koja ne zahteva velike promene, dok su nedostaci ovakvog modela institucionalnog okvira u formiranju još jedne posebne organizacije koja će se delimično baviti pitanjima informacione bezbednosti.



Dijagram 21 Institucionalni okvir - model 3

Nakon analize modela i praksi evropskih zemalja odlučeno je da se prihvati prvi model.

U Predlogu zakona predloženo je u članu 28. osnivanje Kancelarija za informacionu bezbednost, kao posebne organizacije u smislu zakona kojim se uređuje položaj državne uprave radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika i incidenata u IKT sistemima u Republici Srbiji. Kancelarija ima svojstvo pravnog lica. Radom Kancelarije rukovodi direktor koga imenuje Vlada, u skladu sa zakonom kojim se uređuje položaj državnih službenika, a koga predsedniku Vlade predlaže ministar nadležan za poslove informacione bezbednosti.. Kancelarija ima zamenika direktora, koji mora biti lice odgovarajuće stručnosti, koji se postavlja u skladu sa propisima kojim se uređuje položaj državnih službenika i ima ovlašćenja u skladu sa propisima o državnoj upravi.

Nadzor nad radom Kancelarije u vršenju poslova sprovodi Ministarstvo, u skladu sa zakonom kojim se uređuje državna uprava.

Nadležnosti Kancelarije za informacionu bezbednost uređene su članovima 30-34. Kancelarija za informacionu bezbednost uspostavlja se i poslove iz svoje nadležnosti propisane ovim zakonom počinje da obavlja 1. januara 2027. godine.

Poslove Kancelarije za informacionu bezbednost propisane ovim zakonom obavlja Kancelarija za informacione tehnologije i elektronsku upravu u periodu koji počinje danom nastupanja 12 meseci od dana stupanja na snagu ovog zakona i koji traje do 1. januara 2027. godine.

Regulatorno telo za elektronske komunikacije i poštanske usluge obavlja poslove Nacionalnog CERT-a utvrđene ovim zakonom do isteka perioda od 12 meseci od dana stupanja na snagu ovog zakona.

Ministarstvo i dalje vodi evidenciju operatora IKT sistema od posebnog značaja i vrši nadzor nad radom novoosnovane Kancelarije. Na ovaj način udružuju se postojeći kapaciteti dva CERT-a, što bi u značajnoj meri trebalo da poboljša koordinaciju i reagovanje na incidente.

Usklađivanje sa evropskim propisima

Direktiva EU 2022/2555 o merama za visok zajednički nivo informacione bezbednosti širom Unije utvrđuje mere koje imaju za cilj postizanje visokog zajedničkog nivoa informacione bezbednosti unutar EU kako bi se poboljšalo funkcionisanje unutrašnjeg tržišta. Ovom Direktivom dati su amandmani na Uredbu EU 910/2014 o elektronskoj identifikaciji i uslugama od poverenja (eIDAS) i na Direktivu EU 2018/1972 o kodeksu elektronskih komunikacija.

Direktivom se:

- utvrđuje obaveza za sve države članice da usvoje nacionalnu strategiju o bezbednosti mrežnih i informacionih sistema, da imenuju nacionalne nadležne organe (kompetentne autoritete), organe nadležne za upravljanje sajber krizama, jedinstvene tačke kontakta i CSIRT-ove;
- utvrđuju obaveze po pitanjima mera za upravljanje rizikom i izveštavanje za entitete određene kao esencijalne ili važne u skladu sa ovom Direktivom, kao i za entitete identifikovane kao kritične u skladu sa Direktivom EU 2022/2557 (CER Direktiva);
- utvrđuju pravila i obaveze u vezi deljenja informacija; i
- utvrđuju obaveze država članica EU po pitanjima primene ove Direktive i nadzora nad primenom.

Predlogom Zakona o informacionoj bezbednosti (u daljem tekstu: Predlog zakona):

- *uređuju se mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima;*
- *uređuju se odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema;*
- *uređuju se postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti; i*
- *određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.*
- *kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.*

Direktiva NIS 2 je primenljiva na entitete koji se smatraju preduzećima najmanje srednje veličine i koji svoje delatnosti obavljaju unutar Evropske Unije u sektorima koji su određeni kao visoko kritični ili kritični. Pored toga, ova Direktiva primenjuje se i na entitete, bez obzira na njihovu veličinu, koji su identifikovani kao kritični u skladu sa Direktivom 2022/2557 ili koji pružaju usluge registracije imena domena, kao i na sve druge entitete iz visoko kritičnih ili kritičnih sektora, bez obzira na njihovu veličinu:

- koji pružaju usluge javnih elektronskih komunikacionih mreža, usluge od poverenja, usluge registracije domena najvišeg nivoa ili usluge DNS;
- koji su jedini pružaoci neke esencijalne usluge u državi članici;
- čiji bi prekid u pružanju usluga mogao imati značajan uticaj na javnu sigurnost, javnu bezbednost i javno zdravlje;
- čiji bi prekid u pružanju usluga mogao imati značajan sistemski rizik;
- koji su kritični zbog specifične važnosti na nacionalnom ili regionalnom nivou;
- koji spadaju u državne organe na centralnom nivou, ili spadaju u državne organe na regionalnom nivou ako bi prekid pružanja njihovih usluga imao značajan uticaj na kritične društvene ili ekonomske aktivnosti.

Ova Direktiva ne primenjuje se na državne organe nadležne za nacionalnu bezbednost, javnu bezbednost, odbranu i sprovođenje zakona. Direktivom su definisane dve kategorije entiteta: esencijalni i važni.

Esencijalnim entitetima smatraju se:

- entiteti koji prevazilaze veličinu srednjih preduzeća (imaju više od 250 zaposlenih i obrt od preko 50 miliona evra) i koji svoju delatnost obavljaju u nekom od visoko kritičnih sektora;
- pružaoci kvalifikovanih usluga od poverenja, pružaoci usluge registracije domena najvišeg nivoa i pružaoci usluga DNS bez obzira na veličinu;
- pružaoci usluga javnih elektronskih komunikacionih mreža ili javno dostupnih elektronskih komunikacionih usluga koji spadaju u preduzeća srednje veličine;
- organi državne uprave na centralnom nivou;
- svi drugi entiteti koji svoje delatnosti obavljaju u visoko kritičnim ili kritičnim sektorima, a koje je država članica identifikovala kao esencijalne jer su jedini pružaoci neke esencijalne usluge, jer bi prekid u pružanju usluga mogao imati značajan uticaj na javnu sigurnost, javnu bezbednost i javno zdravlje, jer bi prekid u pružanju usluga mogao imati značajan sistemski rizik, ili koji su kritični zbog specifične važnosti na nacionalnom ili regionalnom nivou;
- entiteti identifikovani kao kritični u skladu sa Direktivom 2022/2557;
- svi drugi entiteti identifikovani kao esencijalni u skladu sa Direktivom 2016/1148 (NIS Direktiva), ako država članica proceni da je to potrebno.

Važnim entitetima smatraju se entiteti koji svoje delatnosti obavljaju u visoko kritičnim ili kritičnim sektorima, a koji ne ispunjavaju kriterijume da budu identifikovani kao esencijalni. Takođe, važnim entitetima se smatraju i oni koje je država članica identifikovala kao važne jer su jedini pružaoci neke esencijalne usluge, jer bi prekid u pružanju usluga mogao imati značajan uticaj na javnu sigurnost, javnu bezbednost i javno zdravlje, jer bi prekid u pružanju usluga mogao imati značajan sistemski rizik, ili koji su kritični zbog specifične važnosti na nacionalnom ili regionalnom nivou. U sektore visoke kritičnosti spadaju:

- energetika,
- saobraćaj,
- bankarstvo,
- infrastrukture finansijskih tržišta,
- zdravlje,
- pijaća voda,
- otpadne vode,
- digitalna infrastruktura,
- upravljanje IKT uslugama,
- javna administracija i
- svemir.

U ostale kritične sektore spadaju:

- poštanske i kurirske usluge,
- upravljanje otpadom,
- proizvodnja i snabdevanje hemikalijama,
- proizvodnja, obrada i distribucija hrane,
- druge proizvodne delatnosti (proizvodnja medicinskih uređaja i *in vitro* dijagnostičkih medicinskih sredstava, računara, elektronskih i optičkih proizvoda, električne opreme, mašina i uređaja, motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz),
- pružanje digitalnih usluga i
- istraživanje.

Predlogom zakona definisani su operatori prioritetnih IKT sistema od posebnog značaja koji su pandan esencijalnim entitetima, i operatori važnih IKT sistema od posebnog značaja koji su pandan važnim entitetima iz NIS 2 Direktive. Članom 5. Predloga zakona propisano je da su operatori prioritetnih IKT sistema od posebnog značaja:

- *organi;*
- *subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura;*

- *pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:*
  - *energetika,*
  - *saobraćaj,*
  - *bankarstvo i finansijska tržišta,*
  - *zdravstvo,*
  - *voda za piće,*
  - *otpadne vode,*
  - *digitalna infrastruktura,*
  - *upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema od posebnog značaja,*
  - *ostale oblasti (upravljanje nuklearnim objektima, pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a, upravljanje registrom domena najvišeg nivoa sa izuzetkom operatora korenskih servera imena, pružanje usluga mreže za isporuku sadržaja, obavljanje delatnosti elektronskih komunikacija, tačka za razmenu internet saobraćaja, oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti).*

Članom 6. Predloga zakona propisano je da su operatori važnih IKT sistema od posebnog značaja:

- *naučnoistraživačke institucije;*
- *pravna i fizička lica u svojstvu registrovanog subjekta i organi koji ne spadaju u operatore prioritetnih IKT sistema od posebnog značaja prema kriterijumima za određivanje operatora;*
- *pravna lica koja su definisana kao operatori IKT sistema od posebnog značaja u skladu sa postojećim Zakonom o informacionoj bezbednosti;*
- *pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:*
  - *poštanske usluge;*
  - *upravljanje otpadom;*
  - *proizvodnja i snabdevanje hemikalijama;*
  - *proizvodnja, prerada i distribucija hrane;*
  - *proizvodnja računara, elektronskih i optičkih proizvoda;*
  - *proizvodnja električne opreme;*
  - *proizvodnja mašina i uređaja;*
  - *proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz;*
  - *proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava;*
  - *usluge informacionog društva u smislu zakona o elektronskoj trgovini;*
  - *proizvodnja, promet i prevoz naoružanja i vojne opreme.*

Evidenciju prioritetnih i važnih IKT sistema od posebnog značaja uspostavlja i vodi ministarstvo nadležno za poslove informacione bezbednosti.

NIS 2 Direktiva daje definicije 41 termina.

U Predlogu zakona dato je objašnjenje 58 termina, od kojih 34 (identično ili u istom smislu) postoje i u NIS 2 Direktivi. Termini iz Predloga zakona koji imaju svoj pandan u NIS 2 Direktivi su:

- *informaciono-komunikacioni sistem*
- *operator IKT sistema*
- *informaciona bezbednost*
- *rizik*
- *ranjivost*
- *izbegnuti incident*
- *pretnja*
- *ozbiljna pretnja*
- *incident*
- *upravljanje incidentom*
- *kriza informacione bezbednosti*
- *organ*
- *usluga informacionog društva*
- *pružalac usluge informacionog društva*
- *mreža za isporuku sadržaja*
- *tačka za razmenu internet saobraćaja*
- *sistem naziva domena (DNS)*
- *pružalac usluge DNS-a*
- *usluga od poverenja*
- *pružalac usluge od poverenja*
- *kvalifikovana usluga od poverenja*
- *pružalac kvalifikovane usluge od poverenja*
- *usluge računarstva u klaudu*
- *usluga centra za upravljanje i čuvanje podataka*
- *naučnoistraživačka organizacija*
- *javna elektronska komunikaciona mreža*
- *elektronska komunikaciona usluga*
- *pružalac upravljanih usluga*
- *pružalac upravljanih bezbednosnih usluga*
- *registar naziva domena najvišeg nivoa*
- *pružalac usluge registracije naziva domena*
- *IKT proizvod*
- *IKT usluga*
- *IKT proces*

Termini koji su definisani u Predlogu zakona, a nisu u NIS 2 Direktivi su:

- *tajnost*
- *integritet*
- *raspoloživost*
- *autentičnost*
- *poverljivost*
- *neporecivost*
- *upravljanje rizikom*
- *jedinstveni sistem za prijem obaveštenja o incidentima*
- *mere zaštite IKT sistema*
- *tajni podatak*
- *IKT sistem za rad sa tajnim podacima*
- *služba bezbednosti*
- *samostalni operatori IKT sistema*
- *CERT*

- *kompromitujuće elektromagnetno zračenje (KEMZ)*
- *kriptobezbednost*
- *kriptozaštita*
- *kriptografski proizvod*
- *kriptomaterijali*
- *bezbednosna zona*
- *informaciona dobra*
- *TLP (Traffic Light Protocol)*

Posebno je zanimljivo definisanje dva centralna termina ova dva dokumenta: informacione bezbednosti i sajber bezbednosti. U Predlogu zakona termin „informaciona bezbednost" ima definiciju identičnu definiciji termina „bezbednost mrežnih i informacionih sistema (security of network and information systems)" u NIS 2 Direktivi, ali u Predlogu (niti u bilo kojem drugom pravnom dokumentu u Srbiji) ne postoji definicija sajber bezbednosti, a takođe ni u NIS 2 Direktivi ne postoji definicija informacione bezbednosti. Mada nije eksplicitno definisan ni u NIS 2 Direktivi (ni u prethodnoj NIS Direktivi) ni u Aktu o sajber bezbednosti, pod terminom „informaciona bezbednost" u Evropskoj Uniji se podrazumeva očuvanje poverljivosti, integriteta i raspoloživosti, u skladu sa definicijom iz pregleda sajber bezbednosti i srodnih termina koji je objavila ENISA[6] i definicijom iz standarda ISO 27000[7].

Definicija termina „sajber bezbednost" je u NIS 2 Direktivi referencirana na definiciju iz Akta o sajber bezbednosti (Uredba EU 2019/881), prema kojoj „sajber bezbednost označava aktivnosti neophodne za zaštitu mrežnih i informacionih sistema, korisnika tih sistema i drugih osoba na koje utiču sajber pretnje". Ova definicija može u određenoj meri da se uporedi sa definicijom termina „mere zaštite IKT sistema" iz Predlog zakona, prema kojoj su to „tehničke, organizacione, administrativne i fizičke mere za upravljanje bezbednosnim rizicima IKT sistema". Ipak, za ove dve definicije ne može se tvrditi da imaju isti smisao, pa su zato u prethodnom nabrajanju svrstane u grupe termina čije definicije nemaju svoj pandan u drugom aktu.

NIS 2 Direktiva nalaže državama članicama da usvoje nacionalnu strategiju informacionu bezbednosti i daje okvir tema koje trebaju biti obuhvaćene strategijom.

Predlogom zakona nisu propisane odredbe u vezi strategije, ali je Zakon prepoznat u Strategiji razvoja informacionog društva i informacione bezbednosti za period 2021-2026. godine.

NIS 2 Direktivom je propisano da države članice moraju odrediti jedan ili više nadležnih organa (sa nadležnostima u određenim sektorima kojima pripadaju operatori esencijalnih servisa), kao i jedinstvenu tačku kontakta za komunikaciju sa nadležnim organima drugih zemalja članica i učešće u Grupi za saradnju. Ako je nacionalnim zakonodavstvom definisan samo jedan nadležni organ, onda je taj organ istovremeno i jedinstvena tačka kontakta.

Članom 26. Predloga zakona propisano je da nadležni organ bude ministarstvo nadležno za poslove informacione bezbednosti. U okviru svojih nadležnosti ovo ministarstvo:

- *priprema i predlaže propise i planska dokumenata;*
- *vodi evidenciju operatora IKT sistema od posebnog značaja;*
- *vrši nadzor nad radom Kancelarije za informacionu bezbednost;*

---

[6] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

- *vrši inspekcijski nadzor nad primenom ovog zakona i radom operatora IKT sistema od posebnog značaja;*
- *ostvaruje međunarodnu saradnju u okviru svojih nadležnosti.*

Ipak, ovo ministarstvo nije određeno za jedinstvenu tačku kontakta, već je članom 34. Predlogo zakona propisano da jedinstvena tačka kontakta bude Kancelarija za informacionu bezbednost.

Svaka država članica treba da odredi ili uspostavi jedan ili više nadležnih organa odgovornih za upravljanje velikim incidentima i krizama. Ako se odredi više organa, mora se nedvosmisleno odrediti koja institucija koordinira njihov rad u slučaju velikih incidenata i kriza. Države članice takođe moraju usvojiti nacionalni plan za odgovor na velike incidente i krize koji mora sadržati:

- ciljeve zbog kojih se preduzimaju mere i aktivnosti,
- zadatke i odgovornosti nadležnih organa,
- procedure za reagovanje i njihovo uklapanje u opšti okvir za reagovanje u slučaju nacionalne krize, kao i kanale za razmenu informacija,
- mere koje je potrebno preduzeti radi pripreme, uključujući vežbe i obuke,
- organizacije iz javnog i privatnog sektora i infrastrukturu koja se angažuje,
- procedure i sporazume između nacionalnih nadležnih organa.

Incidenti u IKT sistemima od posebnog značaja klasifikovani su u Članu 16. Predlog zakona u četiri kategorije: nizak, srednji, visok i veoma visok. Kancelarija za informacionu bezbednost upravlja odgovorom na incidente niskog, srednjeg i visokog nivoa u saradnji sa operatorima IKT sistema od posebnog značaja, ministarstvom nadležnim za poslove informacione bezbednosti, Telom za koordinaciju poslova informacione bezbednosti i drugim nadležnim organima po potrebi. Incidenti veoma visokog nivoa smatraju se krizom informacione bezbednosti i u tom slučaju rukovođenje i koordinaciju sprovođenja mera i zadataka preduzima Vlada, koja na predlog ministarstva nadležnog za poslove informacione bezbednosti, a po pribavljenom mišljenju Kancelarije za informacionu bezbednost, donosi odluku o proglašenju krize informacione bezbednosti i zadužuje organe da postupaju prema predloženim merama u skladu sa svojim nadležnostima.

Predlogo zakona predviđena je izrada Plan za reagovanje u slučaju incidenta visokog nivoa i kriza informacione bezbednosti.

NIS 2 Direktivom je određeno da svaka zemlja članica mora uspostaviti jedan ili više CSIRT-ova koji moraju pokrivati sve sektore kojima pripadaju operatori esencijalnih servisa i servise koje pružaju operatori digitalnih servisa i biti odgovorni za postupanje sa incidentima.

Članom 28. Predlogo zakona propisano je uspostavljanje Kancelarije za informacionou bezbednost kao posebne organizacije u smislu zakona kojim se uređuje položaj državne uprave i radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika i incidenata u IKT sistemima u Republici Srbiji. Član 30. propisisuje nadležnosti Kancelarije za informacionu bezbednost:

1) vrši prevenciju i zaštitu od bezbednosnih rizika na nacionalnom nivou u skladu sa ovim zakonom (poslovi Nacionalnog CERT-a);

2) preduzima preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave u skladu sa ovim zakonom (poslovi CERT-a organa vlasti);

3) obavlja saradnju na nacionalnom nivou u oblasti informacione bezbednosti;

4) vrši poslove jedinstvene tačke kontakta;

5) vrši poslove sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga, izuzev sistema, proizvoda, procesa i usluga za potrebe odbrane i bezbednosti;

6) propisuje minimalne mere zaštite IKT sistema organa, uvažavajući načela iz člana 3. ovog zakona, mere zaštite iz člana 10. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada;

7) u saradnji sa nadležnim organima i drugim subjektima iz javnog, akademskog, privrednog i nevladinog sektora učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti;

8) obavlja saradnju i razmenu informacija na međunarodnom nivou u oblasti informacione bezbednosti u cilju praćenja i usaglašavanja sa međunarodnim propisima i standardima;

9) vrši stručni nadzor nad radom operatora IKT sistema od posebnog značaja;

10) vodi bazu ranjivosti IKT proizvoda i IKT usluga;

11) izveštava Ministarstvo na kvartalnom nivou o preduzetim aktivnostima;

12) obavlja druge poslove u skladu sa ovim zakonom.

Kancelarija za informacionu bezbednost uspostavlja se i poslove iz svoje nadležnosti propisane ovim zakonom počinje da obavlja 1. januara 2027. godine.

Poslove Kancelarije za informacionu bezbednost propisane ovim zakonom obavljaće Kancelarija za informacione tehnologije i elektronsku upravu u periodu koji počinje danom nastupanja 12 meseci od dana stupanja na snagu ovog zakona i koji traje do 1. januara 2027. godine.

Regulatorno telo za elektronske komunikacije i poštanske usluge obavlja poslove Nacionalnog CERT-a utvrđene ovim zakonom do isteka perioda od 12 meseci od dana stupanja na snagu ovog zakona..

Nadzor nad radom Kancelarije za informacionu bezbednost vrši ministarstvo nadležno za informacionu bezbednost.

Predlog zakona, kao i postojeći Zakon o informacionoj bezbednosti, prepoznaje samostalne operatore IKT sistema (ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije) koji pokrivaju svoje IKT sisteme i na koje se ne primenjuju odredbe o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost i odredbe o dostavljanju statističkih podataka o incidentima. Samostalni operator IKT sistema ima obavezu da:

1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja;

2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata;

3) donese akt o bezbednosti IKT sistema;

4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima;

6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima. Predlogom zakona su prepoznati i Posebni CERT-ovi za prevenciju rizika u IKT sistemima koji obavljaju poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

NIS 2 Direktivom je propisano da CSIRT -ovi moraju ispunjavati sledeće zahteve:

- moraju obezbediti visok nivo dostupnosti svojih komunikacionih servisa izbegavanjem jedinstvene tačke prekida i imati uvek na raspolaganju više načina da budu kontaktirani i da oni kontaktiraju druge;
- zaposleni i informacioni sistemi koje koriste moraju biti smešteni na bezbednim lokacijama;
- moraju biti opremljeni odgovarajućim sistemima za upravljanje i prosleđivanje zahteva;
- moraju obezbediti poverljivost i pouzdanost svojih operacija;
- moraju biti popunjeni adekvatnim brojem i kvalitetom zaposlenih;
- moraju imati osiguran kontinuitet rada infrastrukture, uključujući redundantni prostor i opremu.

Poslovi CSIRT-ova moraju obuhvatiti:

- praćenje i analiziranje sajber pretnji, ranjivosti i incidenata na nacionalnom nivou i, na zahtev, pružanje pomoći esencijalnim i važnim entitetima,
- pružanje ranih upozorenja i drugih informacija o rizicima i incidentima esencijalnim i važnim entitetima, nadležnim organima i drugim subjektima od značaja,
- reagovanje na incidente i pružanje pomoći esencijalnim i važnim entitetima (gde je primenljivo),
- pružanje dinamičke analize rizika i incidenata i ukazivanje na trenutnu situaciju,
- pružanje esencijalnim i važnim entitetima usluge proaktivnog skeniranja mrežnih i informacionih sistema radi otkrivanja ranjivosti,
- učešće u Mreži CSIRT-ova,
- koordinaciju aktivnosti usmerenih na koordinisano otkrivanje ranjivosti (gde je primenljivo), i
- doprinos primeni bezbednih alata za razmenu informacija.

Takođe, propisano je da CSIRT-ovi promovišu usvajanje i upotrebu uobičajenih ili standardizovanih praksi, klasifikacionih šema i taksonomija u vezi sa:

- procedurama za rešavanje incidenata,
- upravljanjem krizama i
- koordinisanim otkrivanjem ranjivosti.

Članom 31. Predloga zakona propisano je da Kancelarija za informacionu bezbednost u okviru poslova Nacionalnog CERT-a ima sledeći delokrug rada:

1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji kao i javnost.

2) prati stanje o incidentima u Republici Srbiji;

3) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o pretnjama, ranjivostima i incidentima;

4) reaguje bez odlaganja 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;

5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu;

6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora;

7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom;

8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje;

9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija;

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

11) vodi Evidenciju posebnih CERT-ova;

12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima;

13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima.

Pored toga, Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za:

- *upravljanje incidentima,*
- *klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata,*
- *upravljanje kriznim situacijama i*
- *koordinisano otkrivanje ranjivosti.*

Članom 32. Predloga zakona propisano je da Kancelarija za informacionu bezbednost obavlja sledeće poslove u okviru poslova CERT-a Jedinstvene informaciono-komunikacione mreže elektronske uprave:

- *vrši zaštitu mreže eUprave,*
- *obavlja koordinaciju i saradnju sa operatorima IKT sistema koje povezuje mreža eUprave u prevenciji incidenata,*

- *aktivno učestvuje u otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata,*
- *vrši proaktivno skeniranje mreže operatora IKT sistema od posebnog značaja koji su korisnici mreže, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora,*
- *u slučaju otkrivene ranjivosti:*
  - *obavesti operatore IKT sistema koji su korisnici mreže eUprave o tome,*
  - *nalaže operatorima IKT sistema od posebnog značaja koji su korisnici mreže da preduzmu adekvatne mere zaštite u cilju sprečavanja, smanjenja i otklanjanja posledica indicenta,*
- *izdaje stručne preporuke za zaštitu IKT sistema organa, osim IKT sistema za rad sa tajnim podacima,*
- *donosi akt kojim se uređuje postupanje operatora IKT sistema od posebnog značaja koji koriste mreže u slučaju incidenta,*
- *u saradnji sa nadležnim organima vrši procenu potrebe za stručnim usavršavanjem zaposlenih u operatorima IKT sistema od posebnog značaja koji koriste mrežu,*
- *planira i organizuje proceduralne i praktične vežbe u oblasti informacione bezbednosti za zaposlene u operatorima IKT sistema od posebnog značaja koji koriste mrežu,*
- *izrađuje predloge za unapređenje bezbednosnih karakteristika mreže eUprave,*
- *izrađuje analize rizika i incidenata u okviru mreže eUprave,*
- *obavlja druge poslove u skladu sa zakonom u cilju unapređenja informacione bezbednosti mreže eUprave.*

Odredbe o koordinisanom otkrivanju ranjivosti su uvedene u NIS 2 Direktivu kao nova tema (koja nije postojala u NIS Direktivi). NIS 2 Direktivom propisano je da države članice treba da odrede CSIRT koji će biti koordinator ovih aktivnosti. Taj CSIRT treba da deluje kao posrednik od poverenja i olakša komunikaciju između onog ko prijavljuje ranjivost (bilo da je u pitanju pravno ili fizičko lice) i proizvođača potencijalno ranjivog proizvoda ili pružaoca potencijalno ranjive usluge. Zadaci ovog CSIRT-a uključuju:

- identifikaciju i uspostavljanje kontakta sa predmetnim stranama,
- pomoć strani koja prijavljuje ranjivost i
- dogovaranje o rokovima za objavljivanje, kao i upravljanje ranjivostima koje utiču na više entiteta.

Strani koja prijavljuje ranjivost mora biti zagarantovana anonimnost ako to želi.

NIS 2 Direktiva daje zadatak ENISA-i da razvije i održava Evropsku bazu ranjivosti, uključujući odgovarajući informacioni sistem, politike i procedure, kao i da preduzme neophodne tehničke i organizacione mere koje će garantovati bezbednost i integritet ove baze podataka. Baza podataka će biti dostupna svim značajnim entitetima, a sadržaće sledeće podatke:

- opis ranjivosti,
- obuhvaćene proizvode ili usluge i ozbiljnost ranjivosti u smislu okolnosti pod kojima ona može biti eksploatisana i
- dostupnost odgovarajuće zakrpe ili uputstvo za umanjenje rizika ako zakrpa ne postoji.

Članom 36. Predloga zakona propisano je organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-uspostavlja i održava bazu ranjivosti IKT proizvoda i IKT usluga u Republici Srbiji i omogućava fizičkim i pravnim licima, kao i proizvođačima, dobavljačima i pružaocima usluge u IKT sistemu, da na dobrovoljnoj bazi prijave ranjivosti u IKT proizvodima ili IKT uslugama, a koje se mogu prijaviti anonimno.. Baza ranjivosti IKT proizvoda i IKT usluga sadrži:

- *podatke o ranjivosti i*
- *podatke o IKT proizvodima ili IKT uslugama na koje ranjivost utiče.*

Organ, odnosno organizacija iz stava 1. ovog člana propisuje sadržaj, procedure verifikacije ranjivosti, procedure za upravljanje tehničkim ranjivostima IKT proizvoda i IKT usluga, način upisa i vođenja registra.

NIS 2 Direktivom je propisano da nadležni organ, jedinstvena tačka kontakta i CSIRT-ovi jedne države članice međusobno sarađuju u cilju ispunjavanja obaveza koje su im postavljene ovom Direktivom. Ovo se posebno odnosi na razmenu informacija o incidentima, izbegnutim incidentima i pretnjama. Takođe, propisana je razmena informacija između nadležnih organa uspostavljenih ovom Direktivom i Direktivom 2022/2557.

Predlog zakona propisuje saradnju Kancelarije sa, ministarstvom nadležnim za informacionu bezbednost, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema.

Jedan od oblika saradnje na nacionalnom nivou propisan Predlogom zakona je kroz aktivnosti Tela za koordinaciju poslova informacione bezbednosti, koje je koordinaciono telo Vlade i u čiji sastav ulaze predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, organa nadležnog za projektovanje, usklađivanje, razvoj i funkcionisanje sistema elektronske uprave, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge.

Esencijalni i važni entiteti moraju sprovoditi odgovarajuće i proporcionalne tehničke, operativne i organizacione mere za upravljanje rizicima po mrežne i informacione sisteme koje koriste za pružanje svojih usluga. Ove mere moraju obuhvatiti najmanje:

- politike u vezi analize rizika i bezbednosti informacionih sistema;
- rukovanje incidentima;
- kontinuitet poslovanja i upravljanje krizama;
- bezbednost lanca snabdevanja;
- bezbednost u nabavci, razvoju i održavanju mrežnih i informacionih sistema, uključujući rukovanje i otkrivanje ranjivostima;
- politike i procedure za procenu efikasnosti mera za upravljanje rizikom;
- praktikovanje osnovnih mera sajber higijene i obuke u cilju podizanja bezbednosne svesti;
- politike i procedure vezane za korišćenje kriptografskih metoda;
- bezbednost ljudskih resursa, politike kontrole pristupa i upravljanje asetima;
- korišćenje multifaktorske autentifikacije i drugih metoda jake autentifikacije i korišćenje bezbednih komunikacionih sistema, posebno u slučaju vanrednih situacija.

Operator IKT sistema od posebnog značaja dužan je da donese akt o proceni rizika za IKT sisteme kojima upravlja, kojim se vrši procena rizika za IKT sistem od posebnog značaja s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj. Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema, kojim se određuju se mere zaštite, a naročito principi, 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.

Ovim merama se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i smanjenje štete od incidenata, a one se odnose na:

- *uspostavljanje organizacione strukture, sa utvrđenim poslovima, znanjima, kompetencijama, iskustvom i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema;*
- *prikupljanje podataka o pretnjama po informacionu bezbednost IKT sistema;*
- *postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja;*
- *obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne obuke za zaposlene odgovorne za upravljanje informacionom bezbednosti radi obezbeđivanja kontinuirane edukacije;*
- *obezbeđivanje dovoljno resursa za adekvatno upravljanje informacionom bezbednošću;*
- *zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema;*
- *identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu;*
- *klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. ovog zakona;*
- *zaštitu nosača podataka;*
- *ograničenje pristupa podacima i sredstvima za obradu podataka;*
- *odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža;*
- *utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju;*
- *predviđanje upotrebe kriptografskih kontrola i drugih tehnika za sakrivanje podataka radi zaštite poverljivosti, autentičnosti i integriteta podataka;*
- *primena mera zaštite radi sprečavanja oticanja podataka;*
- *fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu;*
- *zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem;*
- *obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka;*
- *primenu odgovarajućih procedura i mera zaštite prilikom korišćenja usluge računarstva u klaudu;*
- *praćenje IKT sistema u cilju otkrivanja ranjivosti i pretnji*
- *ograničenje pristupa internet stranicama koje mogu potencijalno da naruše bezbednost IKT sistema;*
- *zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera;*
- *zaštitu od gubitka podataka redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za razmenu podataka;*
- *čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema;*
- *obezbeđivanje integriteta softvera i operativnih sistema;*
- *zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;*
- *obezbeđivanje zaštite IKT sistema prilikom sprovođenja revizorskog testiranja;*
- *zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove;*
- *bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema;*
- *ispunjenje zahteva za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;*
- *zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema;*
- *procedure za čuvanje i brisanje informacija u IKT sistemima, u skladu sa propisima;*

- *zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga;*
- *održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;*
- *prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, kao i primenu mera sanacije posledica incidenta;*
- *mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje su definišu Planom kontinuiteta obavljanja posla;*
- *usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite;*
- *upotrebu multifaktorske autentikacije ili rešenja kontinuirane provere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije, te bezbednih komunikacionih sistema u hitnim slučajevima unutar operatora IKT sistema.*

NIS 2 Direktiva određuje da operatori esencijalnih i važnih servisa, bez nepotrebnog odlaganja, obaveste nadležni organ ili CSIRT o incidentima koji imaju ili mogu imati značajan uticaj na kontinuitet servisa koji pružaju, sa dovoljno informacija da se može odrediti da li postoji i prekogranični uticaj. Parametri koji određuju da je incident značajan su:

- incident je prouzrokovao ili ima kapacitet da prouzrokuje ozbiljne prekide pružanja usluga ili ozbiljne finansijske gubitke ugroženom entitetu, i
- incident je uticao ili ima kapacitet da utiče na druga fizička ili pravna lica putem nanošenja značajne materijalne ili nematerijalne štete.

Predlogom zakona propisano je da operatori IKT sistema od posebnog značaja imaju obavezu da putem jedinstvenog sistema za prijem obaveštenja o incidentima prijave incidente koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (odnosno Narodnoj banci Srbije, Komisiji za hartije od vrednosti ili Regulatornom telu za elektronske komunikacije i poštanske usluge ako su u pitanju operatori IKT sistema koji spadaju u njihovu nadležnost).

Članom 13. Predloga zakona propisani su kriterijumi za određivanje incidenata koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti:

- *koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;*
- *koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period;*
- *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;*
- *koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;*
- *koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose;*
- *koji su nastali kao posledica incidenta u prioritetnom IKT sistemu od posebnog značaja, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge prioritetnog IKT sistema od posebnog značaja koji priprada oblasti digitalne infrastrukture;*
- *incidente koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima.*

Države članice mogu zahtevati od esencijalnih i važnih entiteta da koriste određene IKT proizvode, usluge i procese koji su sertifikovani prema evropskim šemama sertifikacije za informacionu bezbednost usvojenim u skladu sa Aktom o sajber bezbednosti (Uredba EU 2019/881).

Članom 30. Predloga zakona propisano je da Kancelarija za informacionu bezbednost, između ostalog, obavlja poslove standardizacije i sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga. U Nacrtu zakona, osim navođenja u ovom članu, nema bližih odrednica vezanih za ovu nadležnost.

Sa druge strane, u Predlogu zakona zadržano je čitavo poglavlje iz postojećeg Zakona o informacionoj bezbednosti sa osam članova koji detaljno obrađuju kriptobezbednost i zaštitu od kompromitujućeg elektromagnetnog zračenja. Predlogom zakona, kao i postojećim Zakonom o informacionoj bezbednosti, propisano je da je za ove poslove nadležno ministarstvo nadležno za poslove odbrane.

NIS 2 Direktiva propisuje da države članice obezbede nadzor nad sprovođenjem i preduzmu neophodne mere za obezbeđenje usklađenosti sa ovom Direktivom.

Predlogom zakona predviđeno je da 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) vrši inspekcija za informacionu bezbednost. Poslove inspekcije za informacionu bezbednost obavlja ministarstvo nadležno za informacionu bezbednost preko inspektora za informacionu bezbednost.

Ovlašćenja u vezi nadzora nad sprovođenjem ove Direktive u sistemima esencijalnih entiteta su:

- inspekcije na licu mesta i nadzor van lokacije, uključujući nasumične provere koje sprovode obučeni stručnjaci;
- redovne i ciljane bezbednosne revizije koje sprovodi nezavisno telo ili nadležni organ;
- vanredne revizije, uključujući one koje se sprovode zbog značajnog incidenta ili kršenja ove Direktive;
- bezbednosna skeniranja zasnovana na kriterijumima za procenu rizika, u saradnji sa predmetnim subjektom;
- zahtevi za informacijama neophodnim za procenu mera za upravljanje rizikom;
- zahtevi za pristup podacima, dokumentima i informacijama neophodnim za obavljanje nadzornih zadataka;
- zahtevi za dokazima o primeni politika informacione bezbednosti.

Države članice će obezbediti da njihovi nadležni organi prema esencijalnim entitetima imaju ovlašćenje najmanje da:

- izdaju upozorenja o kršenju ove Direktive;
- usvoje obavezujuća uputstva, uključujući ona u vezi sa merama neophodnim za sprečavanje ili otklanjanje incidenta, kao i vremenske rokove za sprovođenje tih mera i izveštavanje o njihovoj primeni;
- narede predmetnim subjektima da prestanu sa kršenjem odredbi ove Direktive;
- narede predmetnim subjektima da obezbede da su njihove mere za upravljanje rizikom informacione bezbednosti i izveštavanja u skladu sa ovom Direktivom;
- nalože predmetnim subjektima da fizičkim ili pravnim licima kojima pružaju usluge pruže obaveštenja o aktuelnoj pretnji, prirodi pretnje, kao i o svim mogućim merama koje mogu preduzeti ta fizička ili pravna lica kao odgovor na tu pretnju;
- nalože predmetnim subjektima da u razumnom roku sprovedu preporuke date kao rezultat revizije bezbednosti;
- Odrede službenika za praćenje usklađenosti predmetnih subjekata sa naloženim merama za upravljanje rizikom i izveštavanje;
- narede predmetnim subjektima da na određen način objave aspekte kršenja ove Direktive;
- nametnu ili zatraže izricanje administrativne kazne.

Ovlašćenja u vezi nadzora nad sprovođenjem ove Direktive u sistemima važnih entiteta su:

- inspekcije na licu mesta i nadzor van lokacije koje sprovode obučeni stručnjaci;
- ciljane bezbednosne revizije koje sprovodi nezavisno telo ili nadležni organ;
- bezbednosna skeniranja zasnovana na kriterijumima za procenu rizika, u saradnji sa predmetnim subjektom;
- zahtevi za informacijama neophodnim za procenu mera za upravljanje rizikom;
- zahtevi za pristup podacima, dokumentima i informacijama neophodnim za obavljanje nadzornih zadataka;
- zahtevi za dokazima o primeni politika informacione bezbednosti.

Države članice će obezbediti da njihovi nadležni organi prema važnim entitetima imaju ovlašćenje najmanje da:

- izdaju upozorenja o kršenju ove Direktive;
- usvoje obavezujuća uputstva ili nalog za otklanjanje uočenih nedostataka;
- narede predmetnim subjektima da prestanu sa kršenjem odredbi ove Direktive;
- narede predmetnim subjektima da obezbede da su njihove mere za upravljanje rizikom informacione bezbednosti i izveštavanja u skladu sa ovom Direktivom;
- nalože predmetnim subjektima da fizičkim ili pravnim licima kojima pružaju usluge pruže obaveštenja o aktuelnoj pretnji, prirodi pretnje, kao i o svim mogućim merama koje mogu preduzeti ta fizička ili pravna lica kao odgovor na tu pretnju;
- nalože predmetnim subjektima da u razumnom roku sprovedu preporuke date kao rezultat revizije bezbednosti;
- narede predmetnim subjektima da na određen način objave aspekte kršenja ove Direktive;
- nametnu ili zatraže izricanje administrativne kazne.

Predlogom zakona propisano je da inspektor za informacionu bezbednost ima ovlašćenja da:

- *naloži otklanjanje utvrđenih nepravilnosti i za to utvrdi razuman rok;*
- *zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok;*
- *zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje mreže u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika;*
- *naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način;*
- *naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama.*

Izmene Zakona neophodne su i zbog donošenja Uredbe 881/2019 Parlamenta i Saveta EU o Agenciji Evropske Unije za sajber bezbednost (ENISA) (eng. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) koja je usvojena 17. aprila 2019. godine. Uredbom su proširene nadležnosti ENISA. Ova Uredba značajna je za sertifikaciju u oblasti informacione bezbednosti koju je potrebno predvideti izmenama Zakona.

Šema sajberbezbednosne sertifikacije EU predstavlja sveobuhvatan set pravila, tehničkih zahteva, standarda i procedura koji je uspostavljen na nivou EU i koji se odnosi na sertifikaciju ili procenu usaglašenosti određenih IKT proizvoda, servisa i procesa. Šema nacionalne sajberbezbednosne sertifikacije odnosi se na sveobuhvatan set pravila, tehničkih zahteva, standarda i procedura razvijenih i usvojenih od strane nacionalnih autoriteta i koji se odnose na sertifikaciju ili procenu usaglašenosti IKT proizvoda, servisa i procesa koji spadaju u okvir te šeme. Evropski

sajberbezbednosni sertifikat je dokument izdat od strane relevantne organizacije kojim se potvrđuje da je određeni IKT proizvod, servis ili proces proveren na ispunjavanje specifičnih bezbednosnih zahteva postavljenih u šemi sajberbezbednosne sertifikacije EU.

IKT proizvod predstavlja element ili grupu elemenata mrežnog ili informacionog sistema. IKT servis označava servis koji se u potpunosti ili uglavnom odnosi na prenos, skladištenje, preuzimanje ili obradu informacija u mrežnom ili informacionom sistemu. IKT proces predstavlja set aktivnosti koje se obavljaju u svrhu dizajna, razvoja, isporuke ili održavanja IKT proizvoda ili IKT servisa.

Razlog za uspostavljanje okvira za sajberbezbednosnu sertifikaciju je poboljšanje uslova za funkcionisanje internog tržišta kroz povećanje nivoa informacione bezbednosti i uspostavljanje jedinstvenog pristupa sajberbezbednosnoj sertifikaciji na nivou EU. ENISA je Uredbom dobila obavezu da do 28. juna 2020. godine objavi program rada po pitanjima sajberbezbednosne sertifikacije. Komisija može od ENISA tražiti da na osnovu tog programa napravi šemu sajberbezbednosne sertifikacije za kandidata ili da preuredi postojeću šemu sajberbezbednosne sertifikacije EU.

Šema treba da obezbedi ispunjenje sledećih ciljeva:

- Zaštitu skladištenih, prenošenih ili na drugi način obrađivanih podataka od slučajnog ili namernog skladištenja, obrade, pristupa ili objavljivanja tokom celog životnog ciklusa IKT proizvoda, servisa ili procesa;
- Zaštitu skladištenih, prenošenih ili na drugi način obrađivanih podataka od slučajnog ili namernog uništenja, gubljenja, izmene ili nedostupnosti tokom celog životnog ciklusa IKT proizvoda, servisa ili procesa;
- Pristup podacima, servisima ili funkcijama samo od strane autorizovanih osoba, programa ili mašina i samo u meri u kojoj im je pristup odobren;
- Identifikaciju i dokumentaciju poznatih zavisnosti i ranjivosti;
- Beleženje svih pristupa, korišćenja i obrade podataka, servisa ili funkcija sa svim potrebnim informacijama;
- Omogućavanje provere beleški o pristupima, korišćenju i obradi podataka, servisa ili funkcija;
- Verifikaciju da IKT proizvodi, servisi i procesi ne sadrže poznate ranjivosti;
- Blagovremeno vraćanje dostupnosti i pristupa podacima, servisima i funkcijama u slučaju fizičkog ili tehničkog incidenta;
- Bezbednost IKT proizvoda, servisa i procesa po definiciji i po dizajnu; i
- Isporuka IKT proizvoda, servisa i procesa sa ažurnim hardverom i softverom bez javno poznatih ranjivosti i sa mehanizmima za bezbednosno ažuriranje.

Srazmerno riziku pridruženom nameni i svrsi korišćenja i u skladu sa verovatnoćom i uticajem mogućeg sajber incidenta, IKT proizvodima, servisima i procesima može se dodeliti nivo uverenja „osnovni”, „znatan” ili „visok”. „Osnovni” nivo daje uverenje da IKT proizvod, servis ili proces ispunjava odgovarajuće bezbednosne zahteve u pogledu minimizacije osnovnih rizika od sajber incidenata i napada, a provera ispunjenosti ovih zahteva mora uključivati najmanje pregled tehničke dokumentacije. Nivo „znatan” daje uverenje da IKT proizvod, servis ili proces, pored kriterijuma za nivo „osnovni”, ispunjava odgovarajuće bezbednosne zahteve u pogledu minimizacije poznatih rizika od sajber incidenata i napada i rizike od sajber incidenata i napada sprovedenih od strane aktera sa ograničenim veštinama i resursima, a provera ispunjenosti ovih zahteva mora uključivati najmanje proveru da ne postoje javno poznate ranjivosti i proveru da su neophodne bezbednosne funkcionalnosti korektno implementirane. Nivo „visok” daje uverenje da IKT proizvod, servis ili proces ispunjava odgovarajuće bezbednosne zahteve u pogledu minimizacije rizika od najsavremenijih sajber napada sprovedenih od strane aktera sa značajnim veštinama i resursima, a provera ispunjenosti ovih zahteva mora uključivati najmanje proveru da ne postoje javno poznate ranjivosti, proveru da su neophodne i najsavremenije bezbednosne funkcionalnosti korektno implementirane i primenu penetracionih testiranja radi procene otpornosti na napade od strane aktera sa značajnim veštinama.

Za nivo uverenja „osnovni”, proizvođačima je dozvoljeno da vrše samoprocenu usaglašenosti i da samostalno izdaju uverenje, pri čemu snose potpunu odgovornost za saglasnost sa zahtevima.

Svaka zemlja članica EU u obavezi je da odredi jedan ili više nacionalnih autoriteta za sajberbezbednosnu sertifikaciju i da o tome obavesti Komisiju (ako ih je više, svaki treba da ima svoju zasebnu nadležnost). Na nivou EU formiraće se Grupa za evropsku sajberbezbednosnu sertifikaciju (ECCG) sastavljena od predstavnika nacionalnih autoriteta za sajberbezbednosnu sertifikaciju ili drugih nacionalnih autoriteta koja će, između ostalog, imati sledeće zadatke:

- Da savetuje i pruži pomoć Komisiji u osiguranju dosledne implementacije programa sajberbezbednosne sertifikacije;
- Da pruži pomoć, savetuje i sarađuje sa ENISA u pripremi šema sertifikacije;
- Da olakša saradnju između nacionalnih autoriteta za sajberbezbednosnu sertifikaciju kroz izgradnju kapaciteta i razmenu informacija;
- Da olakša prilagođenje šema sajberbezbednosne sertifikacije EU međunarodno prepoznatim standardima itd.

Nacionalne šeme informacione bezbednosne sertifikacije koje ne spadaju u okvir šeme sajberbezbednosne sertifikacije EU mogu da nastave sa izdavanjem sertifikata i nakon stupanja na snagu šeme sajberbezbednosne sertifikacije EU, dok one nacionalne šeme koje spadaju pod ovaj okvir ne smeju više izdavati sertifikate.

Predlogom Zakona u članu 30. su poslovi sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga povereni novoosnovanoj Kancelariji za informacionu bezbednost.

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

Novi Zakon o informacionoj bezbednosti imaće neposredan uticaj na:

- IKT sisteme od posebnog značaja;
- Nacionalni CERT;
- CERT organa vlasti - Jedinstvene informaciono-komunikacione mreže elektronske uprave;
- nove IKT sisteme od posebnog značaja;
- CERT-ove samostalnih operatora IKT sistema.

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

Izmene nacionalnog okvira treba da budu usmerene ka postizanju razvijenog informacionog društva i elektronske uprave u službi građana i privrede, kao i unapređenu informacionu bezbednost građana, javne uprave i privrede, što se postiže:

- poboljšanjem postojećih i izgradnjom nedostajućih kapaciteta,
- uspostavljanjem okvira za pravovremenu i efikasnu razmenu informacija na svim nivoima, a posebno između nadležnog organa za informacionu bezbednost i organa bezbednosti i odbrane,
- koordinisanom i usklađenom međunarodnom saradnjom,
- usaglašenim modelom obrazovanja i definisanjem profila ljudskih resursa u oblasti informacione bezbednosti,
- efikasnom preventivnom i reaktivnom zaštitom kritične informaciono-komunikacione infrastrukture,
- podsticanjem istraživačkih i razvojnih kapaciteta i realizacijom zajedničkih projekata javnog, privatnog i akademskog sektora,

- poboljšanjem informacione bezbednosti IKT sistema koji ne spadaju u kritičnu infrastrukturu i stanovništva u celini,
- uspostavljanjem okvira za bezbednosnu sertifikaciju,
- usklađivanjem sa najboljim praksama, a naročito sa legislativom Evropske unije.

Novi Zakon o informacionoj bezbednosti treba da se donese prvenstveno radi potpunog usklađivanja sa EU regulativom u ovoj oblasti, 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, kao i podizanju informacione bezbednosti društva u celini.

Kada je reč o efektima na građane, treba istaći da se primenom zakona očekuje sledeće:

- veća pouzdanost usluga koje građani koriste putem informaciono-komunikacionih sistema od posebnog značaja;
- zaštita podataka građana koji se obrađuju u IKT sistemima od posebnog značaja;
- stvaranje mehanizama za podizanje svesti građana o značaju informacione bezbednosti;
- uspostavljanje kanala putem kojih će građani moći da komuniciraju sa organima u slučaju problema i štete koji su nastali usled narušavanja informacione bezbednosti;
- obaveštavanje korisnika u slučaju incidenata koji značajno ugrožavaju IKT sisteme od posebnog značaja čije usluge koriste i dobijanje instrukcija koje mere treba da preduzmu radi prevencije i saniranja potencijalne štete.

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).

Novim zakonom uspostavlja se nova posebna organizacija Kancelarija za informacionu bezbednost, što će doprineti boljoj koordinaciji između Ministarstva i Kancelarije (u kojoj se objedinjavaju poslovi Nacionalnog CERT-a i CERT-a organa vlasti) sa jedne strane, ali i poboljšanju saradnje sa posebnim CERT-ovima i IKT sistemima od posebnog značaja sa druge strane.

Takođe se predviđa jačanje kapaciteta Nacionalnog CERT-a i to tehnoloških, ljudskih i organizacionih kapaciteta, što će Nacionalnom CERT-u 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.

Preciznijim regulisanjem pojmova (definicija) stvaraju se bolji uslovi za prepoznavanje i razumevanje sajber pretnji.

Davanjem većeg značaja CERT-ovima i redefinisanjem obaveza operatora informaciono-komunikacionih sistema od posebnog značaja olakšava se njihovo delovanje i pruža adekvatniji odgovor na incidente.

Izrada nacionalnog plana delovanja u slučaju velikih incidenata uticaće na brže i efikasnije reagovanje na sajber pretnje.

Unapređenje institucionalnog okvira i poboljšanje mehanizama reagovanja na incidente u sajber prostoru omogućiće ostvarivanje ciljeva, i to:

- bezbednost informaciono-komunikacionih sistema koja se odnosi na rizike narušavanja funkcionisanja organa uprave, 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.

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?

Predlog zakona u potpunosti je usklađen sa Strategijom razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine. Opštim ciljem Strategije ***Razvijeno informaciono društvo i elektronska uprava u službi građana i privrede i unapređena informaciona bezbednost građana, javne uprave i privrede*** prepoznat je značaj informacione bezbednosti za društvo u celini. Poseban cilj ***Unapređenje informacione bezbednosti građana, javne uprave i privrede*** ostvaruje se kroz realizaciju sledećih mera:

- podizanje svesti i znanja u oblasti informacione bezbednosti građana, javnih službenika i privrede,
- podizanje kapaciteta IKT sistema od posebnog značaja za primenu mera zaštite,
- podizanje kapaciteta Nacionalnog CERT-a, CERT-a organa vlasti i CERT-ova samostalnih operatora IKT,
- podizanje kapaciteta inspekcije za informacionu bezbednost,
- podsticanje javno-privatnog partnerstva u oblasti informacione bezbednosti i
- unapređenje regionalne i međunarodne saradnje.

U okviru mere *Unapređenje saradnje i podizanje kapaciteta IKT sistema od posebnog značaja za primenu mera zaštite* predviđena je posebna aktivnost **Usklađivanje propisa sa regulativom EU u oblasti informacione bezbednosti**, što i jeste ključni razlog donošenja novog Zakona o informacionoj bezbednosti. Praćenjem evropskih tokova u ovoj oblasti ne vrši se samo harmonizacija propisa, već i unapređenje institucionalnog okvira i poboljšanje mehanizama reagovanja na incidente u sajber prostoru, kao i preventivnog delovanja radi očuvanja informacione bezbednosti.

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

Osnovni pokazatelji učinka donošenja Zakona ogledaju se u sledećem:

- utvrđeni su načini i mehanizmi za podizanje kapaciteta IKT sistema od posebnog značaja
- unapređena je platforma za razmenu informacija između Nacionalnog CERTa i IKT sistema od posebnog značaja sa mehanizmom za brzo reagovanje
- poboljšana je saradnja između CERT-ova u Republici Srbiji i koordinisan je odgovor na krizne situacije
- broj uspostavljenih CERT-ova samostalnih operatora se povećava
- broj obučenih zaposlenih u CERT-u organa vlasti i u samostalnim operatorima IKT se povećava
- broj zaposlenih inspektora za informacionu bezbednost se povećava
- bolje je upravljanje rizikom.

Pokazatelj	Bazna godina i vrednost	2024	2025	2026
Broj organizovanih sajber vežbi	2023 (1)	2	3	4
Dodat broj novih funkcionalnosti platformi za	2023	1	2	3

razmenu podataka o incidentima	(0)				
Broj sastanaka CERT-ova godišnje	(3)	2023	4	5	6
Broj polaznika obuka	(20)	2022 0	3	40	50
Broj zaposlenih inspektora	(2)	2023	3	4	5
Broj adekvatno sačinjenih akata o proceni rizika	(0)	2023 00	1	200	300

Usvajanje NIS 2 Direktive u decembru 2022. godine je bio je podsticaj da se napravi analiza sadašnjeg pravnog i institucionalnog okvira, postave novi ciljevi. *Predlogom* zakona ostvaruje se napredak u odnosu na postojeće stanje, kako u domenu preciznijeg uređivanja oblasti, tako i u kreiranju funkcionalnijeg i efikasnijeg institucionalnog okvira.

Jedan od zadataka koje je Evropska unija postavila pred ENISA je i izrada okvira za sertifikaciju proizvoda, servisa i usluga, koji ima za cilj da se odredi nivo zaštite koji mogu da pruže određeni proizvodi, servisi i usluge i da se ojača poverenje u digitalne tehnologije i provajdere digitalnih servisa. *Predlogom* zakona uvodi se obaveza sertifikacije IKT sistema koja će se vršiti kada i evropske zemlje bliže regulišu ovo pitanje.

Bez obzira što je pozicija Srbije u međunarodnih okvirima sve bolja u ovom domenu, postoje značajne mogućnosti za poboljšanje. Međunarodnu saradnju su ostvarivali predstavnici Ministarstva informisanja i telekomunikacija, RATEL-a, Ministarstva spoljnih poslova, Ministarstva unutrašnjih poslova i Ministarstva odbrane, što će se verovatno nastaviti i u narednom periodu. Važno je da nastupi predstavnika Srbije u međunarodnim institucijama budu koordinisani kako bi mogli na najbolji način da obavljaju svoje poslove.

Pravovremeno otkrivanje i otklanjanje ranjivosti je stalni izazov na kojem zajednički radi više zemalja kako bi se pronašao adekvatan način rešavanja. Blagovremenim otkrivanjem pretnji jača se stepen informacione bezbednosti kao i poverenje u institucije koje se tom temom bave.

Predlog zakona uređuje okvir za postupanje u kriznim situacijama i zajednički odgovor CERT-ova.

Pored promocije i podrške učešću predstavnika institucija i organizacija iz Srbije na međunarodnim vežbama, radi uspostavljanja odgovarajućeg odgovora na incidente većih razmera neophodna je organizacija nacionalnih sajber vežbi. Ove vežbe treba da organizuje i sprovodi novoosnovana Kancelarija za informacionu bezbednost, a svrha vežbi treba da bude provera i uvežbavanje procedura za reagovanje.

Zbog toga je neophodno razvijati partnerske odnose sa akademskim institucijama koje imaju programe za informacionu bezbednost na osnovnom, master i doktorskom nivou studija. Kancelarija treba da podstiče naučne radove iz ovih oblasti i učešće akademskih institucija u međunarodnim projektima jer se na taj način stiču nova znanja i naši akademski ljudski resursi stimulišu da budu uključeni u najnovija dostignuća u ovoj oblasti.

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 Zakona o informacionoj bezbednosti potrebno je obezbediti u budžetu, za potrebe podizanja kapaciteta novoosnovane Kancelarije za informacionu bezbednost. S obzirom da Kancelarija za informacionu bezbednost preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad Kancelarije za informacione tehnologije i elektronsku upravu u delokrugu poslova CERT-a organa vlasti, kao i prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Regulatornog tela za elektronske komunikacije i poštanske usluge nastalu u obavljanju poslova Nacionalnog CERT-a, potrebno je izvršiti odgovarajući prenos finansijskih sredstava.

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 *Predlog* zakona predviđeno formiranje posebne organizacije i povećavanje kadrovskih i tehničkih kapaciteta u narednom periodu predviđa se povećavanje broja zaposlenih kao i kupovina neophodne opreme.

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

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 novim zakonom, 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 informisanja i telekomunikacija je početkom 2023. godine formiralo radnu grupu za izradu Nacrta Zakona o informacionoj bezbednosti koga su činili predstavnici relevantnih ministarstava, posebnih organizacija, agencija, akademske zajednice i privrede. Tokom pripreme Nacrta održano je nekoliko konsultacija sa različitim interesnim grupama. Sa privredom su održane

konsultacije 22. juna u Nacionalnoj alijansi za lokalni ekonomski razvoj na kojima su predstavljeni predlozi teksta Nacrta. Sastanku je prisustvovalo blizu 20 privrednih subjekata.

Ministarstvo informisanja i telekomunikacija sprovelo je javnu raspravu o Nacrtu Zakona o informacionoj bezbednosti u periodu od 27.jula do 30. avgusta 2023. godine, na osnovu zaključka Vlade. U okviru javne rasprave, održana su dva okrugla stola u Beogradu i Kragujevcu. U javnoj raspravi učestvovali predstavnici državnih organa, privrednog sektora, akademske zajednice, nevladinih organizacija i eminentni stručnjaci u ovoj oblasti.

Iako je tekst zakona neznatno izmenjen u odnosu na 2023. godinu, u 2024. godini iz proceduralnih razloga ponovljena je javna rasprava i to u periodu od 3. jula do 23. jula 2024. godine, na osnovu koje je Ministarstvo objavilo izveštaj o javnoj raspravi na sajtu Ministarstva i portalu „eKonsultacije“.

Donošenje zakona je prioritet imajući u vidu činjenicu da se istim vrši usklađivanje sa evropskom regulativom.

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 zakona, predviđeno je donošenje sledećih podzakonskih akata:

- Uredba kojom se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema od posebnog značaja;
- Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji;
- Podzakonski akt kojim se uređuju bliži uslove za prikupljanje, čuvanje, verifikaciju i objavljivanje tačnih i potpunih podataka o registraciji domena u posebnoj bazi podataka;
- Podzakonski akt kojim se bliže uređuju uslovi za proveru KEMZ i način procene rizika od oticanja podataka putem KEMZ;
- Podzakonski akt kojim se bliže uređuju uslovi koje moraju da ispunjavaju kriptografski proizvodi;
- Podzakonski akt kojim se bliže uređuje sadržaj zahteva za izdavanje odobrenja za kriptografski proizvod, uslove za izdavanje odobrenja za kriptografski proizvod, način izdavanja odobrenja i vođenja registra izdatih odobrenja za kriptografski proizvod;
- Podzakonski akt kojim se bliže uređuje vođenje registara kriptografskih proizvoda, kriptomaterijala, pravila i propisa i lica koja obavljaju poslove kriptozaštite;
- Uredbe o bližem sadržaju akta o bezbednosti IKT od posebnog značaja, načinu provere i sadržaj izveštaja o proveri, kao i dostavljanje izveštaja nadležnom organu;
- Uredbe o bližem uređenju mera zaštite IKT sistema od posebnog značaja;
- Uredba o postupku obaveštavanja o incidentima, obrascima za obaveštavanje, listi incidenata prema vrstama i klasifikaciji incidenata prema nivou opasnosti;
- Uredbe o načinu sprovođenja mera za bezbednost i zaštitu dece na internetu;
- Pravilnika o opštoj metodologiji za procenu rizika u IKT sistemima od posebnog značaja;
- Pravilnika o vrsti, formi i načinu dostavljanja statističkih podataka o incidentima u informaciono-komunikacionim sistemima od posebnog značaja;
- Pravilnika o sadržaju, načinu upisa i vođenju evidencije posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima;
- Pravilnika o sadržaju, proceduri verifikacije ranjivosti, , procedure za upravljanje tehničkim ranjivostima IKT proizvoda i IKT usluga, način upisa i vođenja registra.

Radi upoznavanja javnosti sa novim zakonskim rešenjima, Ministarstvo informisanja i telekomunikacija održavaće posebne skupove na kojima će upoznavati sva zainteresovana lica o

usvojenim odredbama. Poseban fokus će biti na operatore IKT sistema od posebnog značaja, kojima se ovim zakonom propisuju obaveze u cilju zaštite njihovih sistema. Očekuje se da će se ove aktivnosti početi da sprovode odmah po donošenju zakona, odnosno podzakonskih akta koje ovaj zakon predviđa, i da će trajati najmanje godinu dana, a po potrebi i duže.

Međuinstitucionalna saradnja između organa koji sprovode ovaj zakon uspostaviće se na više načina:

- Kroz rad Vladinog Tela za koordinaciju poslova informacione bezbednosti, koje okuplja sve organe čiji su poslovi od velikog značaja za informacionu bezbednost u Republici Srbiji;
- U postupku obaveštavanja o incidentima koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji, nadležni organi ostvaruju saradnju po pitanju razmene informacija, posebno ako je reč o incidentima koji predstavljaju krivično delo ili ugrožavaju odbranu i nacionalnu bezbednost Republike Srbije, odnosno kritičnu infrastrukturu.

Zakon predviđa i međusobnu saradnju CERT-ova (Nacionalnog CERT-a, CERT-a Jedinstvene informaciono-komunikacione mreže elektronske uprave, Posebnih CERT-ova i drugih CERT-ova).

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 obezbeđuju se u budžetu Republike Srbije kroz budžet Kancelarije za informacionu bezbednost, kao posebne organizacije koja će obavljati poslove Nacionalnog CERT-a i CERT-a organa vlasti. Kancelarija za informacionu bezbednost uspostavlja se i poslove iz svoje nadležnosti propisane ovim zakonom počinje da obavlja 1. januara 2027. godine. Poslove Kancelarije za informacionu bezbednost propisane ovim zakonom obavljaće Kancelarija za informacione tehnologije i elektronsku upravu u periodu koji počinje danom nastupanja 12 meseci od dana stupanja na snagu ovog zakona i koji traje do 1. januara 2027. godine. Regulatorno telo za elektronske komunikacije i poštanske usluge obavlja poslove Nacionalnog CERT-a utvrđene ovim zakonom do isteka perioda od 12 meseci od dana stupanja na snagu ovog zakona. Kancelarija za informacione tehnologije i elektronsku upravu preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Regulatornog tela za elektronske komunikacije i poštanske usluge nastalu u obavljanju poslova Nacionalnog CERT-a danom isteka perioda od 12 meseci od dana stupanja na snagu ovog zakona, potrebne za vršenje stručnih poslova utvrđenih ovim zakonom. Kancelarija za informacionu bezbednost počev od datuma prethodno navedenog preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Kancelarije za informacione tehnologije i elektronsku upravu nastalu u obavljanju poslova propisanih ovim zakonom iz nadležnosti Kancelarije za informacionu bezbednost.

IZJAVA O USKLAĐENOSTI PROPISA SA

PROPISIMA EVROPSKE UNIJE

1. Ovlašćeni predlagač propisa: Vlada

Obrađivač: Ministarstvo informisanja i telekomunikacija

2. Naziv propisa:

Predlog zakona o informacionoj bezbednosti

Draft 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:

2024-0

4. Usklađenost propisa sa propisima Evropske unije:

a) Navođenje odredbi primarnih izvora prava Evropske unije i ocene usklađenosti sa njima:

Consolidated version of the Treaty on the Functioning of the European Union

PART TNREE UNION POLICIES AND INTERNAL ACTIONS

TITLE VII COMMON RULES ON COMPETITION, TAXATION AND APPROXIMATION OF LAWS, CHAPTER 3 APPROXIMATION OF LAWS

Article 114 (eh Article 95 TES)

CELEX 12016E114

Potpuno usklađeno

b) Navođenje sekundarnih izvora prava Evropske unije i ocene usklađenosti sa njima:

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high sommon level of cybersecurity across the Union, amending Regulation (EU)

No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)- **potpuno usklađeno**

32022L2555

Direktiva (EU) 2022/2055 Evropskog parlamenta i Saveta od dana 14. decembra 2022. godine o merama za visok zajednički nivo sajber bezbednosti, izmeni Uredbe (EU) br. 910/2014 i Direktive (EU) br. 2018/1972 i stavljanju van snage Direktive (EU) 2016/1148

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

Nema.

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?
Ne.

7. Da li je propis preveden na neki službeni jezik Evropske unije?

Preveden je na engleski jezik.

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

Predlog zakona je prosleđen Evropskoj komisiji radi davanja mišljenja. Evropska komisija je u decembru 2024. godine dostavila svoje komentare i sugestije koji su inkorporirani u tekst Predloga zakona.

1. Naziv propisa Evropske unije : **Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)** **Direktiva (EU) 2022/2055 Evropskog parlamenta i Saveta od dana 14. decembra 2022. godine o merama za visok zajednički nivo sajber bezbednosti, izmeni Uredbe (EU) br. 910/2014 i Direktive (EU) br. 2018/1972 i stavljanju van snage Direktive (EU) 2016/1148**	2. „CELEX" oznaka EU propisa 32022L2555
3. Ovlašćeni predlagač propisa: Vlada	4. Datum izrade tabele:
Ministarstvo informisanja i telekomunikacija	10. februar 2025.
5. Naziv (nacrta, predloga) propisa čije odredbe su predmet analize usklađenosti sa propisom Evropske unije: **1. Predlog zakona o informacionoj bezbednosti** **2. Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju** **3. Zakon o inspekcijskom nadzoru** **4. Zakon o prekršajima** **5. Zakon o zaštiti podataka o ličnosti**	6. Brojčane oznake (šifre) planiranih propisa iz baze NPAA: 2024-0
7. Usklađenost odredbi propisa sa odredbama propisa EU: POTPUNO USKLAĐENO	

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.	***Subject matter***	1.1.	Predmet uređivanja Član 1.	PU		

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

	This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.		Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite, praćenje pravilne primene propisanih mera zaštite, kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.			
1.2.	To that end, this Directive lays down: (a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs); (b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557; (c) rules and obligations on cybersecurity information sharing; (d) supervisory and enforcement obligations on Member States.	1. 1.	Predmet uređivanja Član 1. Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite, praćenje pravilne primene propisanih mera zaštite, kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.	PU		
2.1.	***Scope*** This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union. Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.	1.5. 1.6.	Operatori prioritetnih IKT sistema od posebnog značaja Član 5. Operatori prioritetnih IKT sistema od posebnog značaja su operatori IKT sistema od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori prioritetnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u	PU		Razlikovanje operatora po veličini biće utvrđeno podzakonskim aktom iz člana 6. stav 3.

			sledećim oblastima: (1) Energetika - proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - kombinovana proizvodnja električne i toplotne energije; - snabdevanje električnom energijom; - prenos električne energije i upravljanje prenosnim sistemom; - distribucija električne energije i upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom; - skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - upravljanje organizovanim tržištem električne energije; - proizvodnja, distribucija i snabdevanje toplotnom energijom; - transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta; - istraživanje i proizvodnja nafte i prirodnog gasa; - proizvodnja derivata nafte; - skladištenje nafte i derivata nafte; - transport i upravljanje transportnim sistemom za prirodni gas; - skladištenje i upravljanje skladištem prirodnog gasa; - distribucija i upravljanje distributivnim sistemom za prirodni gas; - snabdevanje i javno snabdevanje prirodnim gasom; - proizvodnja i prerada uglja; - proizvodnja, skladištenje i prenos vodonika. (2) Saobraćaj - obavljanje javnog avio-prevoza uz važeću			

			operativnu dozvolu; - upravljanje aerodromom; - usluge kontrole letenja; - upravljanje javnom železničkom infrastrukturom; - poslovi železničkih preduzeća; - obavljanje prevoza putnika i tereta unutrašnjim vodama; - upravljanje lukama; - servis za upravljanje brodskim saobraćajem (VTS); - rečni informacioni servisi (RIS); - upravljanje putnom infrastrukturom; - upravljanje inteligentnim transportnim sistemima (ITS). (3) Bankarstvo i finansijska tržišta - poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; - poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala; - poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina. (4) Zdravstvo - pružanje zdravstvene zaštite; - rad nacionalnih referentnih laboratorija; - istraživanje i razvoj lekova; - proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu; - proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja. (5) Voda za piće - snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima			

			navedeni poslovi nisu pretežni deo njihove delatnosti. (6) Otpadne vode - sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (7) Digitalna infrastruktura - pružanje usluga računarstva u klaudu; - pružanje usluge centra za čuvanje i skladištenje podataka. (8) Upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema od posebnog značaja - pružanje upravljanih usluga; - pružanje upravljanih bezbednosnih usluga. (9) Ostale oblasti - upravljanje nuklearnim objektima; - pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena; - pružanje usluga mreže za isporuku sadržaja; - obavljanje delatnosti elektronskih komunikacija; - tačka za razmenu internet saobraćaja; - izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije; - oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti. 2) organi; 3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura. Operatori važnih IKT sistema od posebnog značaja Član 6. Operatori važnih IKT sistema od posebnog značaja su operatori IKT sistemi čiji bi prekid ili poremećaj u pružanju usluga mogao da ima značajan uticaj na javni interes, funkcionisanje drugih sektora ili bi			

			stvorio značajan sistemski rizik. Operatori važnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: - poštanske usluge u smislu zakona kojim se uređuje oblast poštanskih usluga; - upravljanje otpadom, u smislu zakona kojim se uređuje upravljanje otpadom, izuzev privrednih subjekata kojima navedeni posao nije pretežni deo njihove delatnosti; - upravljanje ambalažnim otpadom, u smislu zakona kojim se uređuje upravljanje ambalažnim otpadom; - proizvodnja i snabdevanje hemikalijama, u skladu sa zakonom kojim se uređuju hemikalije; - proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade; - proizvodnja računara, elektronskih i optičkih proizvoda; - proizvodnja električne opreme; - proizvodnja mašina i uređaja; - proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz; - proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava; - usluge informacionog društva u smislu zakona o elektronskoj trgovini; - proizvodnja, promet i prevoz naoružanja i vojne opreme. 2) naučnoistraživačke institucije; 3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne spadaju u operatore prioritetnih IKT sistema od posebnog značaja prema kriterijumima za određivanje operatora. Podzakonski akt kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema od posebnog značaja donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti.			

			Ministarstva u čijim nadležnostima su oblasti u kojima operatori prioritetnih i važnih IKT sistema od posebnog značaja obavljaju delatnosti, dužni su da u postupku izrade podzakonskog akta iz stava 3. ovog člana, dostave ministarstvu nadležnom za poslove informacione bezbednosti predloge sektorskih kriterijuma radi određivanja operatora IKT sistema od posebnog značaja.			
2.2.	Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where: (a)services are provided by: (i)providers of public electronic communications networks or of publicly available electronic communications services; (ii)trust service providers; (iii)top-level domain name registries and domain name system service providers; (b)the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities; (c)disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; (d)disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact; (e)the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State; (f)the entity is a public administration entity: (i)of central government as defined by a Member State in accordance with national law; or	1.5.	Operatori prioritetnih IKT sistema od posebnog značaja Član 5. Operatori prioritetnih IKT sistema od posebnog značaja su operatori IKT sistema od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori prioritetnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: (1) Energetika - proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - kombinovana proizvodnja električne i toplotne energije; - snabdevanje električnom energijom; - prenos električne energije i upravljanje prenosnim sistemom; - distribucija električne energije i upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom; - skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - upravljanje organizovanim tržištem električne energije;	PU		

	(ii)at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.		- proizvodnja, distribucija i snabdevanje toplotnom energijom; - transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta; - istraživanje i proizvodnja nafte i prirodnog gasa; - proizvodnja derivata nafte; - skladištenje nafte i derivata nafte; - transport i upravljanje transportnim sistemom za prirodni gas; - skladištenje i upravljanje skladištem prirodnog gasa; - distribucija i upravljanje distributivnim sistemom za prirodni gas; - snabdevanje i javno snabdevanje prirodnim gasom; - proizvodnja i prerada uglja; - proizvodnja, skladištenje i prenos vodonika. (2) Saobraćaj - obavljanje javnog avio-prevoza uz važeću operativnu dozvolu; - upravljanje aerodromom; - usluge kontrole letenja; - upravljanje javnom železničkom infrastrukturom; - poslovi železničkih preduzeća; - obavljanje prevoza putnika i tereta unutrašnjim vodama; - upravljanje lukama; - servis za upravljanje brodskim saobraćajem (VTS); - rečni informacioni servisi (RIS); - upravljanje putnom infrastrukturom; - upravljanje inteligentnim transportnim sistemima (ITS). (3) Bankarstvo i finansijska tržišta - poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;			

			- poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; - poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala; - poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina. (4) Zdravstvo - pružanje zdravstvene zaštite; - rad nacionalnih referentnih laboratorija; - istraživanje i razvoj lekova; - proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu; - proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja. (5) Voda za piće - snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (6) Otpadne vode - sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (7) Digitalna infrastruktura - pružanje usluga računarstva u klaudu; - pružanje usluge centra za čuvanje i skladištenje podataka. (8) Upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema od posebnog značaja - pružanje upravljanih usluga; - pružanje upravljanih bezbednosnih usluga. (9) Ostale oblasti - upravljanje nuklearnim objektima; - pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena;			

			- pružanje usluga mreže za isporuku sadržaja; - obavljanje delatnosti elektronskih komunikacija; - tačka za razmenu internet saobraćaja; - izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije; - oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti. 2) organi; 3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura.			
2.3.	Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.	1.5.2.3.	3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura	PU		
2.4.	Regardless of their size, this Directive applies to entities providing domain name registration services.	1.5.2.1.9.	(9) Ostale oblasti - upravljanje nuklearnim objektima; - pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena; - pružanje usluga mreže za isporuku sadržaja; - obavljanje delatnosti elektronskih komunikacija; - tačka za razmenu internet saobraćaja; - izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije; - oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti.	PU		
2.5.	Member States may provide for this Directive to apply to: (a)public administration entities at local level; (b)education institutions, in particular where they carry out critical research activities.	1.5.2.2. 1.6.2.2.	2) organi 2) naučnoistraživačke institucije	PU		

2.6.	This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.	1.2.1.1.25. 1.8.	25) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije Obaveze samostalnih operatora Član 8. Samostalni operator dužan je da: 1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja; 2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata; 3) donese akt o bezbednosti IKT sistema; 4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima; 6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima. Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama. Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost, odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja. Samostalni operatori, u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske	PU		

			uprave. 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.			
2.7.	This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.	1.2.1.1.25. 1.8.	25) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije Obaveze samostalnih operatora Član 8. Samostalni operator dužan je da: 1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja; 2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata; 3) donese akt o bezbednosti IKT sistema; 4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima; 6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima. Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama. Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost,	PU		

			odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja. Samostalni operatori, u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave. 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.			
2.8.	Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.	1.8.	25) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije Obaveze samostalnih operatora Član 8. Samostalni operator dužan je da: 1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja; 2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata; 3) donese akt o bezbednosti IKT sistema; 4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima; 6) formira sopstveni CERT radi upravljanja	PU		

			incidentima u svojim sistemima. Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama. Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost, odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja. Samostalni operatori, u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave. 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.			
2.9.	Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider.	2.37. 2.64.	Državni organ kao pružalac kvalifikovanih usluga od poverenja Član 37. Državni organ može pružati kvalifikovane usluge od poverenja ukoliko ispunjava uslove za pružanje usluga predviđene ovim zakonom. Ocenjivanje ispunjenosti uslova državnog organa za pružanje usluge od poverenja vrši ministarstvo, odnosno inspektor za elektronsku identifikaciju i usluge od poverenja, nakon podnetog zahteva. Izuzetno od stava 2. ovog člana ocenjivanje ispunjenosti uslova vrši se na osnovu interne kontrole u saradnji sa nadležnim ministarstvom samo u slučaju kada je pružalac kvalifikovane usluge od poverenja ministarstvo nadležno za poslove odbrane, uz obavezu dostavljanja izveštaja o izvršenoj internoj kontroli nadležnom ministarstvu. Nakon provere ispunjenosti uslova Vlada uredbom utvrđuje da državni organ može da obavlja	PU	Drugim zakonom (Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja) predviđeno je da se nadzor može vršiti nad entitetima iz paragrafa 7 i 8.	

			kvalifikovanu uslugu od poverenja koja je bila predmet ocenjivanja iz stava 2. ovog člana. Ministarstvo vrši upis državnog organa u registar iz člana 35. ovog zakona, na osnovu uredbe iz stava 4. ovog člana. Poslovi inspekcije za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju Član 64. Inspekcija za elektronsku identifikaciju i usluge od poverenja u elektronskom poslovanju vrši inspekcijski nadzor nad primenom ovog zakona i radom pružalaca usluga elektronske identifikacije i pružalaca usluga od poverenja (u daljem tekstu: pružaoci usluga) preko inspektora za elektronsku identifikaciju i usluge od poverenja (u daljem tekstu: inspektor). U okviru inspekcijskog nadzora pružalaca usluga inspektor utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim za sprovođenje ovog zakona.			
2.10.	This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.			NU	Tačan opseg ovih subjekata urediće se podzakonskim aktom.	
2.11.	The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.	1.2.1.1.25. 1.8.	25) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije Obaveze samostalnih operatora Član 8. Samostalni operator dužan je da: 1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja; 2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata; 3) donese akt o bezbednosti IKT sistema; 4) vrši proveru usklađenosti mera zaštite IKT	PU		

			sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima; 6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima. Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama. Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost, odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja. Samostalni operatori, u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave. 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.			
2.12.	This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU (27) and 2013/40/EU (28) of the European Parliament and of the Council and Directive (EU) 2022/2557.			NP		Odnos sa drugim propisima EU
2.13.	Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that			NP		Obaveza država članica u razmeni informacija sa Komisijom.

	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 that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.					
2.14.	Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof. The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data protection law and Union privacy law, in particular Directive 2002/58/EC.	1.4.	Obrada podataka o ličnosti Član 4. Na obradu podataka o ličnosti koja je neophodna za vršenje nadležnosti i ispunjenje obaveza iz ovog zakona primenjuju se odredbe ovog zakona, odredbe posebnih zakona kojima se uređuju određene oblasti, kao i odredbe zakona kojim se uređuje zaštita podataka o ličnosti.	PU		
3.1.	***Essential and important entities*** For the purposes of this Directive, the following entities shall be considered to be essential entities: (a)entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC; (b)qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size; (c)providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC; (d)public administration entities referred to in Article 2(2), point (f)(i); (e)any other entities of a type referred to in Annex I	1.5. 1.6.	Operatori prioritetnih IKT sistema od posebnog značaja Član 5. Operatori prioritetnih IKT sistema od posebnog značaja su operatori IKT sistema od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori prioritetnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: (1) Energetika - proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - kombinovana proizvodnja električne i toplotne energije; - snabdevanje električnom energijom;	PU		

	or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e); (f)entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive; (g)if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.		- prenos električne energije i upravljanje prenosnim sistemom; - distribucija električne energije i upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom; - skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - upravljanje organizovanim tržištem električne energije; - proizvodnja, distribucija i snabdevanje toplotnom energijom; - transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta; - istraživanje i proizvodnja nafte i prirodnog gasa; - proizvodnja derivata nafte; - skladištenje nafte i derivata nafte; - transport i upravljanje transportnim sistemom za prirodni gas; - skladištenje i upravljanje skladištem prirodnog gasa; - distribucija i upravljanje distributivnim sistemom za prirodni gas; - snabdevanje i javno snabdevanje prirodnim gasom; - proizvodnja i prerada uglja; - proizvodnja, skladištenje i prenos vodonika. (2) Saobraćaj - obavljanje javnog avio-prevoza uz važeću operativnu dozvolu; - upravljanje aerodromom; - usluge kontrole letenja; - upravljanje javnom železničkom infrastrukturom; - poslovi železničkih preduzeća; - obavljanje prevoza putnika i tereta unutrašnjim vodama; - upravljanje lukama; - servis za upravljanje brodskim			

			saobraćajem (VTS); - rečni informacioni servisi (RIS); - upravljanje putnom infrastrukturom; - upravljanje inteligentnim transportnim sistemima (ITS). (3) Bankarstvo i finansijska tržišta - poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; - poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala; - poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina. (4) Zdravstvo - pružanje zdravstvene zaštite; - rad nacionalnih referentnih laboratorija; - istraživanje i razvoj lekova; - proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu; - proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja. (5) Voda za piće - snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (6) Otpadne vode - sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (7) Digitalna infrastruktura - pružanje usluga računarstva u klaudu;			

			- pružanje usluge centra za čuvanje i skladištenje podataka. (8) Upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema od posebnog značaja - pružanje upravljanih usluga; - pružanje upravljanih bezbednosnih usluga. (9) Ostale oblasti - upravljanje nuklearnim objektima; - pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena; - pružanje usluga mreže za isporuku sadržaja; - obavljanje delatnosti elektronskih komunikacija; - tačka za razmenu internet saobraćaja; - izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije; - oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti. 2) organi; 3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura. Operatori važnih IKT sistema od posebnog značaja Član 6. Operatori važnih IKT sistema od posebnog značaja su operatori IKT sistemi čiji bi prekid ili poremećaj u pružanju usluga mogao da ima značajan uticaj na javni interes, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori važnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: - poštanske usluge u smislu zakona kojim se uređuje oblast poštanskih usluga; - upravljanje otpadom, u smislu zakona kojim se uređuje upravljanje otpadom, izuzev		

			privrednih subjekata kojima navedeni posao nije pretežni deo njihove delatnosti; - upravljanje ambalažnim otpadom, u smislu zakona kojim se uređuje upravljanje ambalažnim otpadom; - proizvodnja i snabdevanje hemikalijama, u skladu sa zakonom kojim se uređuju hemikalije; - proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade; - proizvodnja računara, elektronskih i optičkih proizvoda; - proizvodnja električne opreme; - proizvodnja mašina i uređaja; - proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz; - proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava; - usluge informacionog društva u smislu zakona o elektronskoj trgovini; - proizvodnja, promet i prevoz naoružanja i vojne opreme. 2) naučnoistraživačke institucije; 3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne spadaju u operatore prioritetnih IKT sistema od posebnog značaja prema kriterijumima za određivanje operatora. Podzakonski akt kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema od posebnog značaja donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti. Ministarstva u čijim nadležnostima su oblasti u kojima operatori prioritetnih i važnih IKT sistema od posebnog značaja obavljaju delatnosti, dužni su da u postupku izrade podzakonskog akta iz stava 3. ovog člana, dostave ministarstvu nadležnom za poslove informacione bezbednosti predloge sektorskih kriterijuma radi određivanja operatora IKT sistema od posebnog značaja.			
3.2.	For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as	1.6.2.3.	3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne	PU		

	essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).		spadaju u operatore prioritetnih IKT sistema od posebnog značaja prema kriterijumima za određivanje operatora.			
3.3.	By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.			NP		Nije potrebna zakonska odredba da bi se ovo realizovalo. Može da se realizuje primenom postojećeg zakonodavstva.
3.4.	For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities: (a)the name of the entity; (b)the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers; (c)where applicable, the relevant sector and subsector referred to in Annex I or II; and (d)where applicable, a list of the Member States where they provide services falling within the scope of this Directive. The entities referred to in paragraph 3 shall notify any changes to the details submitted pursuant to the first subparagraph of this paragraph without delay, and, in any event, within two weeks of the date of the change. The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph.	1.9.	Evidencija operatora IKT sistema od posebnog značaja Član 9. Ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Ministarstvo) uspostavlja i vodi evidenciju prioritetnih i važnih IKT sistema od posebnog značaja (u daljem tekstu: Evidencija) koja sadrži: 1) naziv, matični broj i sedište operatora IKT sistema od posebnog značaja; 2) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon administratora zaduženog za održavanje i upravljanje IKT sistemom 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, odnosno da li IKT sistem od posebnog značaja potpada pod prioritetan ili važan; 5) podatak o delatnosti operatora IKT sistema od posebnog značaja; 6) adresni opseg internet protokola (engl. „IP address range“) koji pripadaju IKT sistemu od posebnog značaja, a koji obuhvata podatke o javnim statičkim IP adresama; 7) veb stranice operatora IKT sistema od posebnog značaja; 8) broj lokacija na kojima se IKT sistem od posebnog značaja nalazi.	PU		

	Member States may establish national mechanisms for entities to register themselves.		Pored podataka iz stava 1. ovog člana, evidencija može da sadrži i druge dopunske podatke o IKT sistemu od posebnog značaja. Samostalni operatori IKT sistema izuzeti su od obaveze dostavljanja podataka iz stava 1. tač. 4), 5), 6) i 8) ovog člana. Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji donosi Ministarstvo. Operator IKT sistema od posebnog značaja dužan je da Ministarstvu dostavi podatke iz st. 1. i 2. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 4. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja. Operator IKT sistema od posebnog značaja dužan je da u slučaju promene podataka iz stava 1. ovog člana o tome obavesti Ministarstvo u roku od 15 dana od dana nastanka promene. Podaci iz stava 1. tač. 2) i 3) obrađuju se u svrhu izvršenja odredbi ovog zakona u pogledu dostavljanja obaveštenja i upozorenja značajnih za bezbednost IKT sistema od posebnog značaja, kao i radi uspostavljanja komunikacije i ostvarivanja saradnje u cilju otklanjanja štetnih posledica incidenata i preventivnog delovanja. Podaci iz stava 1. tač. 2) i 3) obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i čuvaju se do trenutka prestanka svrhe obrade ili do izvršene promene podataka u skladu sa stavom 5. ovog člana. Ministarstvo stavlja na raspolaganje ažurnu Evidenciju Kancelariji za informacionu bezbednost radi izvršenja odredbi ovog zakona u pogledu prikupljanja i razmene informacija o pretnjama, ranjivostima i incidentima i pružanja podrške, upozoravanja i savetovanja lica koja upravljaju IKT sistemima. Evidencija predstavlja tajni podatak u smislu zakona kojim se uređuje tajnost podataka.			
3.5.	By 17 April 2025 and every two years thereafter, the competent authorities shall notify: (a)the Commission and the Cooperation Group of the number of essential and important entities listed			NP	Obaveza Komisije i drugih tela EU.	

	pursuant to paragraph 3 for each sector and subsector referred to in Annex I or II; and (b)the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.					
3.6.	Until 17 April 2025 and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 5, point (b).			NP	Obaveza Komisije i drugih tela EU.	
4.1.	***Sector- specific Union legal acts*** Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.			NP	Ostvarljivo primenom opštih pravnih načela.	
4.2.	The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where: (a)cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or (b)the sector-specific Union legal act provides for immediate access, where appropriate automatic and			NP	U vezi je sa prethodnim članom.	

	direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.					
4.3.	3. The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA.			NP	Obaveza Komisije.	
5.1.	***Minimum harmonisation*** This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.			NP	Odredba o važenju propisa EU.	
6 (1)	***Definitions*** For the purposes of this Directive, the following definitions apply: (1)'network and information system' means: (a)an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; (b)any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or (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;	1.2.1.1.	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 i usluge 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 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.	PU		
6 (2)	(2)'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability,	1.2.1.3.	3) informaciona bezbednost predstavlja sposobnost informaciono- komunikacionih sistema i mreža da se odupru i/ili ublaže, uz određeni stepen pouzdanosti, svaki događaj koji bi mogao da ugrozi	PU		

	authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;		raspoloživost, integritet, autentičnost, neporecivost i poverljivost podataka koji se obrađuju, odnosno usluga koje se pružaju ili su dostupne putem tog IKT sistema;			
6 (3)	(3)‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;			NU	Nismo uveli u zakonsku terminologiju izraz sajber bezbednost. Krećemo se u okviru termina informacione bezbednosti koji podrazumeva i sajber bezbednost i bezbednost informacionih sistema i mreža.	
6 (4)	(4)‘national cybersecurity strategy ’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;			PU	Primenom propisa koji uređuju oblast usvajanja planskih dokumenata (među kojima su i strategije) i drugih zakona u efektu smo u skladu sa ovom odredbom. Nije potrebno da je dodatno propišemo i u sektorskom zakonu.	
6 (5)	(5)‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;	1.2.1.12.	12) izbegnuti incident predstavlja identifikovani događaj u IKT sistemu koji je mogao dovesti do značajnog ugrožavanja raspoloživosti, autentičnosti, integriteta ili poverljivosti podataka, usluga ili sistema, ali je pravovremenom intervencijom ili zaštitnim merama sprečeno ostvarivanje štetnih posledica;	PU		
6 (6)	(6)‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;	1.2.1.15.	15) incident je svaki događaj koji ugrožava raspoloživost, autentičnost, integritet, neporecivost ili poverljivost podataka koji se čuvaju, prenose ili obrađuju ili usluge koje se pružaju, odnosno koje su dostupne putem IKT sistema;	PU		
6 (7)	(7)‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;			NP	Termin koji se koristi za incidente koji pogađaju države članice EU.	
6 (8)	(8)‘incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;	1.2.1.18.	18) upravljanje incidentom podrazumeva preduzimanje svih radnji i postupaka čiji je cilj sprečavanje, otkrivanje, analiza i prekid incidenta, kao i preduzimanje drugih mera radi odgovora na incident i otklanjanja njegovih posledica;	PU		

6 (9)	(9)‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;	1.2.1.9.	9) rizik predstavlja mogućnost nastanka događaja ili uslova koji mogu ugroziti nivo informacione bezbednosti ili ispravno funkcionisanje IKT sistema, što se utvrđuje na osnovu procene verovatnoće događaja i veličine njegovog potencijalnog uticaja na nivo informacione bezbednosti;	PU		
6 (10)	(10)‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;	1.2.1.13.	13) pretnja predstavlja svaku okolnost, događaj ili radnju koja može da ugrozi, poremeti ili na drugi način štetno utiče na IKT sistem, korisnike sistema i druga lica sa jasnom verovatnoćom nastajanja štete u slučaju da izostane reakcija;	PU		
6 (11)	(11)‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage;	1.2.1.14.	14) ozbiljna pretnja predstavlja pretnju po informacionu bezbednost za koju se, s obzirom na njena tehnička svojstva, može pretpostaviti da ima potencijal da izazove značajne negativne posledice po IKT sistem, njegovog operatora ili korisnike usluga tog operatora uzrokujući značajnu materijalnu ili nematerijalnu štetu;	PU		
6 (12)	(12)‘ICT product’ means an ICT product as defined in Article 2, point (12), of Regulation (EU) 2019/881;	1.2.1.53.	53) IKT proizvod je element ili grupa elemenata u okviru informaciono-komunikacionog sistema;	PU		
6 (13)	(13)‘ICT service’ means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;	1.2.1.54.	54) IKT usluga je usluga koja se u potpunosti ili u većoj meri sastoji iz prenosa, čuvanja, preuzimanja ili obrade podataka korišćenjem IKT sistema;	PU		
6 (14)	(14)‘ICT process’ means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;	1.2.1.55.	55) IKT proces je skup aktivnosti koji se obavlja u cilju izrade, razvoja, korišćenja i održavanja IKT proizvoda ili IKT usluge;	PU		
6 (15)	(15)‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;	1.2.1.10.	10) ranjivost predstavlja slabost ili nedostatak u IKT proizvodima ili uslugama koji se mogu iskoristiti za realizaciju jedne ili više pretnji;	PU		
6 (17)	(17)‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;			PU		Oblast regulisanja drugih opštih propisa.
6 (18)	(18)‘internet exchange point’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous	1.2.1.37.	37) tačka za razmenu internet saobraćaja (engl. internet exchange point) je mrežna struktura koja pruža mogućnost povezivanja dve ili više nezavisnih mreža (autonomnih sistema) prvenstveno u svrhu olakšavanja razmene internet saobraćaja, i koja omogućuje međupovezivanje autonomnih sistema, u kom slučaju nije potrebno da internet saobraćaj između autonomnih sistema prođe kroz treći	PU		

	systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;		autonomni sistem, te koja takav saobraćaj ne menja i ne utiče na njega na drugi način;			
6 (19)	(19)‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;	1.2.1.38.	38) sistem naziva domena (DNS) je distribuirani, hijerarhijski organizovan sistem koji povezuje nazive domena sa odgovarajućim IP adresama koje se koriste za usmeravanje i povezivanje korisničkih uređaja sa uslugama i resursima na internetu;	PU		
6 (20)	(20)‘DNS service provider’ means an entity that provides: (a)publicly available recursive domain name resolution services for internet end-users; or (b)authoritative domain name resolution services for third-party use, with the exception of root name servers;	1.2.1.39.	39) pružalac usluge DNS-a je subjekat koji pruža usluge razrešavanja DNS upita korisnicima interneta ili pruža uslugu autoritativnih servera imena za nazive domena koje koriste treća lica, sa izuzetkom korenskih (engl. root) servera imena;	PU		
6 (21)	(21)‘top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;	1.2.1.51.	51) registar naziva domena najvišeg nivoa (engl. TLD name registry) je subjekt koji je odgovoran za upravljanje nazivom domena najvišeg nivoa (TLD) koji mu je dodeljen i koji donosi politike i pravila za domen, upravlja bazom registra, generiše datoteku zone i održava tehničku infrastrukturu servera imena za dodeljeni domen najvišeg nivoa;	PU		
6 (22)	(22)‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;	1.2.1.52.	52) pružalac usluge registracije naziva domena je registrator naziva domena ili drugi subjekt koji deluje u ime registratora;	PU		
6 (23)	(23)‘digital service’ means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council	1.2.1.37.	37) tačka za razmenu internet saobraćaja (engl. internet exchange point) je mrežna struktura koja pruža mogućnost povezivanja dve ili više nezavisnih mreža (autonomnih sistema) prvenstveno u svrhu olakšavanja razmene internet saobraćaja, i koja omogućuje međupovezivanje autonomnih sistema, u kom slučaju nije potrebno da internet saobraćaj između autonomnih sistema prođe kroz treći autonomni sistem, te koja takav saobraćaj ne menja i ne utiče na njega na drugi način;	PU		

6 (24)	(24)‘trust service’ means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;	1.2.1.40.	40) usluga od poverenja je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju	PU		
6 (25)	(25)‘trust service provider’ means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;	1.2.1.41.	41) pružalac usluge od poverenja je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju	PU		
6 (26)	(26)‘qualified trust service’ means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;	1.2.1.42.	42) kvalifikovana usluga od poverenja je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju	PU		
6 (27)	(27)‘qualified trust service provider’ means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;	1.2.1.43.	43) pružalac kvalifikovane usluge od poverenja je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju	PU		
6 (28)	(28)‘online marketplace’ means an online marketplace as defined in Article 2, point (n), of Directive 2005/29/EC of the European Parliament and of the Council			NU	Oblast je predmet uređivanja drugih zakona. Za sada nije definisan termin u pravnom sistemu RS.	
6 (29)	(29)‘online search engine’ means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council			NU	Oblast je predmet uređivanja drugih zakona. Za sada nije definisan termin u pravnom sistemu RS.	
6 (30)	(30)‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;	1.2.1.44.	usluge računarstva u klaudu (engl. „cloud computing service”) su digitalne usluge koje omogućavaju upravljanje na zahtev i široki daljinski pristup nadogradivom i elastičnom skupu deljivih računarskih resursa, uključujući i situacije kada su takvi resursi raspoređeni na nekoliko lokacija;	PU		
6 (31)	(31)‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;	1.2.1.45.	usluga centra za upravljanje i čuvanje podataka je usluga koja se pruža u okviru infrastrukture namenjene za centralizovano smeštanje, međupovezivanje i funkcionisanje računarske i mrežne opreme radi čuvanja, obrade i prenosa podataka (data centar), uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu uticaja na životnu sredinu;	PU		
6 (32)	(32)‘content delivery network’ means a network of geographically distributed servers for the purpose	1.2.1.36.	36) mreža za isporuku sadržaja (Content Delivery Network – CDN) označava mrežu geografski	PU		

	of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;		raspoređenih servera koja je osmišljena da obezbedi visoku dostupnost, pristupačnost i brzu isporuku digitalnog sadržaja i usluga korisnicima interneta, u ime pružalaca sadržaja i usluga;			
6 (33)	(33)‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;			NU	Oblast je predmet uređivanja drugih zakona. Za sada nije definisan termin u pravnom sistemu RS.	
6 (34)	(34)‘representative’ means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;			NU	Oblast je predmet uređivanja drugih zakona. Za sada nije definisan termin u pravnom sistemu RS.	
6 (35)	(35)‘public administration entity’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria: (a)it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; (b)it has legal personality or is entitled by law to act on behalf of another entity with legal personality; (c)it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;	1.2.1.23.	organ je državni organ, organ autonomne pokrajine, jedinica lokalne samouprave, organizacija i drugo pravno ili fizičko lice kome je povereno vršenje javnih ovlašćenja	PU		

	(d)it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;					
6 (36)	(36)‘public electronic communications network’ means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972;	1.2.1.47.	javna elektronska komunikaciona mreža je elektronska komunikaciona mreža u smislu zakona kojim se uređuju elektronske komunikacije;	PU		
6 (37)	(37)‘electronic communications service’ means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972;	1.2.1.48.	elektronska komunikaciona usluga je usluga u smislu zakona kojim se uređuju elektronske komunikacije;	PU		
6 (38)	(38)‘entity’ means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	1.2.1.2.	operator IKT sistema je fizičko lice u svojstvu registrovanog subjekta, pravno lice, organ ili organizaciona jedinica organa koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti;	PU		
6 (39)	(39)‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely;	1.2.1.49.	pružalac upravljanih usluga je subjekt koji pruža usluge u vezi sa postavljanjem, upravljanjem, radom i održavanjem IKT proizvoda, mreža, infrastrukture, aplikacija ili druge mreže i informacionog sistema putem pružanja pomoći ili aktivnog upravljanja koje se sprovodi u prostorijama korisnika usluge ili na daljinu;	PU		
6 (40)	(40)‘managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;	1.2.1.50.	pružalac upravljanih bezbednosnih usluga je pružalac upravljanih usluga koji sprovodi ili pruža pomoć u sprovođenju aktivnosti u vezi sa upravljanjem rizikom u oblasti bezbednosti.	PU		
6 (41)	(41)‘research organisation’ means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.	1.2.1.46.	naučnoistraživačka organizacija je organizacija u smislu zakona kojim se uređuju nauka i istraživanje	PU		
7.1.	***National cybersecurity strategy*** Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:			PU	Primenom opštih propisa za izradu planskih dokumenata osigurana je pravilna primena ove odredbe. Nije potrebno dodatno propisivati sektorskim propisom.	

	(a)objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II; (b)a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2; (c)a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts; (d)a mechanism to identify relevant assets and an assessment of the risks in that Member State; (e)an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors; (f)a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy; (g)a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate; (h)a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.					

7.2.	As part of the national cybersecurity strategy, Member States shall in particular adopt policies: (a)addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services; (b)on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products; (c)managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1); (d)related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables; (e)promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures; (f)promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities; (g)supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure; (h)including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;			PU	Primenom opštih propisa za izradu planskih dokumenata osigurana je pravilna primena ove odredbe. Nije potrebno dodatno propisivati sektorskim propisom.	

	(i)strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs; (j)promoting active cyber protection.					
7.3.	Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.			NP	Obavaza država članica prema Komisiji.	
7.4.	Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.			PU	Implementacija ove odredbe osigurana je primenom opštih propisa koji uređuju pitanja izrade planskih dokumenata u Republici Srbiji.	
8.1.	***Competent authorities and single points of contact*** Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).	1.26. 1.30.1.4.	Nadležni organ Član 26. Organ državne uprave nadležan za informacionu bezbednost je ministarstvo nadležno za poslove informacione bezbednosti. U okviru svojih nadležnosti Ministarstvo: 1) priprema i predlaže propise i planska dokumenta iz oblasti informacione bezbednosti u skladu sa ovim zakonom; 2) vodi evidenciju operatora IKT sistema od posebnog značaja; 3) vrši nadzor nad radom Kancelarije u vršenju poslova za koje je nadležna u skladu sa ovim zakonom; 4) 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; 5) ostvaruje međunarodnu saradnju u okviru svojih nadležnosti.	PU		

			Kancelarija u okviru svoje nadležnosti obavlja sledeće poslove i to: 4) vrši poslove jedinstvene tačke kontakta;			
8.2.	The competent authorities referred to in paragraph 1 shall monitor the implementation of this Directive at national level.	1.26. 1.27. 1.28. 1.29. 1.30.	Nadležni organ Član 26. Organ državne uprave nadležan za informacionu bezbednost je ministarstvo nadležno za poslove informacione bezbednosti. U okviru svojih nadležnosti Ministarstvo: 1) priprema i predlaže propise i planska dokumenta iz oblasti informacione bezbednosti u skladu sa ovim zakonom; 2) vodi evidenciju operatora IKT sistema od posebnog značaja; 3) vrši nadzor nad radom Kancelarije za informacionu bezbednost u vršenju poslova za koje je nadležna u skladu sa ovim zakonom; 4) 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; 5) ostvaruje međunarodnu saradnju u okviru svojih nadležnosti. Telo za koordinaciju poslova informacione bezbednosti Član 27. 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, poslove pravosuđa, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge.	PU		

			U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa, 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. Kancelarija za informacionu bezbednost Član 28. Radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika i incidenata u IKT sistemima u Republici Srbiji osniva se Kancelarija za informacionu bezbednost (u daljem tekstu: Kancelarija), kao posebna organizacija u smislu zakona kojim se uređuje položaj državne uprave. Kancelarija ima svojstvo pravnog lica. Radom Kancelarije rukovodi direktor koga imenuje Vlada, u skladu sa zakonom kojim se uređuje položaj državnih službenika, a koga predsedniku Vlade predlaže ministar nadležan za poslove informacione bezbednosti. Kancelarija ima zamenika direktora, koji mora biti lice odgovarajuće stručnosti, koji se postavlja u skladu sa propisima kojim se uređuje položaj državnih službenika i ima ovlašćenja u skladu sa propisima o državnoj upravi. Nadzor nad radom Kancelarije Član 29. Nadzor nad radom Kancelarije u vršenju poslova sprovodi Ministarstvo, u skladu sa zakonom kojim se uređuje državna uprava. Nadležnosti Kancelarije Član 30. Kancelarija u okviru svoje nadležnosti obavlja sledeće poslove i to: 1) vrši prevenciju i zaštitu od bezbednosnih rizika na nacionalnom nivou u skladu sa ovim zakonom (poslovi Nacionalnog CERT-a);		

			2) preduzima preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave u skladu sa ovim zakonom (poslovi CERT-a organa vlasti); 3) obavlja saradnju na nacionalnom nivou u oblasti informacione bezbednosti; 4) vrši poslove jedinstvene tačke kontakta; 5) vrši poslove sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga, izuzev sistema, proizvoda, procesa i usluga za potrebe odbrane i bezbednosti i IKT sistema za rad sa tajnim podacima; 6) propisuje minimalne mere zaštite IKT sistema organa, uvažavajući načela iz člana 3. ovog zakona, mere zaštite iz člana 10. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada; 7) u saradnji sa nadležnim organima i drugim subjektima iz javnog, akademskog, privrednog i nevladinog sektora učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti; 8) obavlja saradnju i razmenu informacija na međunarodnom nivou u oblasti informacione bezbednosti u cilju praćenja i usaglašavanja sa međunarodnim propisima i standardima; 9) vrši stručni nadzor nad radom operatora IKT sistema od posebnog značaja; 10) vodi bazu ranjivosti IKT proizvoda i IKT usluga; 11) izveštava Ministarstvo na kvartalnom nivou o preduzetim aktivnostima; 12) obavlja druge poslove u skladu sa ovim zakonom.			
8.3.	Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.	1.34.	Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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	PU		

			kapacitete; 3) mogu da imaju negativan uticaj na više od jedne države. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
8.4.	Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State.	1.34.	Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi	PU		

			poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
8.5.	Member States shall ensure that their competent authorities and 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.			PU	Odredba se implementira primenom opštih propisa i drugih neregulatornih aktivnosti.	
8.6.	Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto. Each Member State shall make public the identity of its competent authority. The Commission shall make a list of the single points of contact publicly available.			NP	Obaveza države članice prema Komisiji.	
9.1.	***National cyber management frameworks*** Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents			NP	Odnosi se na incidente koji pogađaju države članice. Ovim zakonom se uspostavljaju nadležni organi koji su formirani tako da stupanjem	

	and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.				Republike Srbije u članstvo EU mogu da preuzmu i implementaciju ove odredbe.	
9.2.	Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.	1.27.	Telo za koordinaciju poslova informacione bezbednosti Član 27. 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, poslove pravosuđa, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge. U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa, 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.	PU		
9.3.	Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive.	1.13 1.14. 1.15.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident.	PU		

			Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost.			

			Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa			

			zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi.			
9.4.	Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: (a)the objectives of national preparedness measures and activities; (b)the tasks and responsibilities of the cyber crisis management authorities; (c)the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;	1.13 1.14. 1.15.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 3) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje	PU		

	(d)national preparedness measures, including exercises and training activities; (e)the relevant public and private stakeholders and infrastructure involved; (f)national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.		usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog			

			značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave;		

			2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi.			
9.5.	Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.			NP	Organizovana mreža država članica EU	
10.1.	***Computer security incident response teams (CSIRTs)*** Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.	1.31.	Poslovi prevencije i zaštite od bezbednosnih rizika na nacionalnom nivou (Nacionalni CERT) Član 31. U okviru poslova prevencije i zaštite od bezbednosnih rizika i incidenata Kancelarija vrši poslove Nacionalnog CERT-a i to: 1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost. 2) prati stanje o incidentima u Republici Srbiji; 3) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o pretnjama, ranjivostima i	PU		

			incidentima; 4) reaguje bez odlaganja 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; 5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu; 6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora; 7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom; 8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje; 9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija; 10) podiže svest kod građana, privrednih subjekata i organa o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti; 11) vodi Evidenciju posebnih CERT-ova; 12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima; 13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za: 1) upravljanje incidentima; 2) klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata; 3) upravljanje kriznim situacijama; 4) koordinirano otkrivanje ranjivosti. Kancelarija je ovlašćena da vrši obradu podataka o licu koje prijavi incident, pri čemu obrada podataka			

			o licu 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. Kancelarija obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije. U okviru obavljanja poslova Nacionalnog CERT-a potrebno je obezbediti sledeće zahteve: 1) visok nivo dostupnosti komunikacionih kanala izbegavanjem jedinstvenih tačaka prekida i korišćenje više sredstava za dvosmerno kontaktiranje; 2) prostorije Nacionalnog CERT-a i informacioni sistemi za podršku treba da budu smešteni na sigurnim lokacijama; 3) upotrebu odgovarajućeg sistema za upravljanje zahtevima i njihovo usmeravanje, posebno kako bi se olakšala efikasna i efektivna razmena informacija; 4) obezbeđivanje poverljivosti i pouzdanosti svojih aktivnosti; 5) postojanje adekvatnih kadrovskih kapaciteta; 6) opremljenost redundantnim sistemima i rezervnim radnim prostorom kako bi se osigurao kontinuitet usluga.			
10.2.	Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).			PU	Implementacija se obezbeđuje drugim opštim propisima, alokacijom resursa, finansiranjem i drugim neregulatornim merama.	
10.3.	Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.			PU	Implementacija se obezbeđuje drugim opštim propisima, alokacijom resursa, finansiranjem i drugim neregulatornim merama.	

10.4.	The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.	1.33.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti.	PU		
10.5.	The CSIRTs shall participate in peer reviews organised in accordance with Article 19.			NP	Propisano na način da može da se realizuje samo među članicama EU. Ne postoje prepreke da CERT sudeluje u ovome prema postojećem zakonodavstvu Republike Srbije kada se za to stvore uslovi.	
10.6.	Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network.	1.33.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici	PU		

			Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti.			
10.7.	The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.	1.33. 1.34.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti. Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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;	PU		

			3) mogu da imaju negativan uticaj na više od jedne države. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
10.8.	The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.	1.34.	Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena	PU		

			podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
10.9.	Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.			NP	Obaveza država članica prema Komisiji.	
10.10.	Member States may request the assistance of ENISA in developing their CSIRTs.			NP	Pravo država članica u odnosu na ENISA-u.	
11.1.	***Requirements, technical capabilities and tasks of CSIRTs*** The CSIRTs shall comply with the following requirements: (a)the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for			PU	Sprovođenje odredbe osigurano primenom opštih propisa, alokacijom resursa, finansiranjem i drugim neregulatornim merama.	

	contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners; (b)the CSIRTs' premises and the supporting information systems shall be located at secure sites; (c)the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers; (d)the CSIRTs shall ensure the confidentiality and trustworthiness of their operations; (e)the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately; (f)the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services. The CSIRTs may participate in international cooperation networks.					
11.2.	Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.			PU	Sprovođenje odredbe osigurano primenom opštih propisa, alokacijom resursa, finansiranjem i drugim neregulatornim merama.	
11.3.	The CSIRTs shall have the following tasks: (a)monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems; (b)providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the	1.31.	Poslovi prevencije i zaštite od bezbednosnih rizika na nacionalnom nivou (Nacionalni CERT) Član 31. U okviru poslova prevencije i zaštite od bezbednosnih rizika i incidenata Kancelarija vrši poslove Nacionalnog CERT-a i to: 1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost. 2) prati stanje o incidentima u Republici Srbiji; 3) pruža rana upozorenja, uzbune i najave i	PU		

	competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time; (c)responding to incidents and providing assistance to the essential and important entities concerned, where applicable; (d)collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity; (e)providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact; (f)participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request; (g)where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1); (h)contributing to the deployment of secure information-sharing tools pursuant to Article 10(3). The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services. When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.		informiše relevantna lica o pretnjama, ranjivostima i incidentima; 4) reaguje bez odlaganja 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; 5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu; 6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora; 7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom; 8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje; 9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija; 10) podiže svest kod građana, privrednih subjekata i organa o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti; 11) vodi Evidenciju posebnih CERT-ova; 12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima; 13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za: 1) upravljanje incidentima; 2) klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata; 3) upravljanje kriznim situacijama; 4) koordinirano otkrivanje ranjivosti. Kancelarija je ovlašćena da vrši obradu podataka o			

			licu koje prijavi incident, pri čemu obrada podataka o licu 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. Kancelarija obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije. U okviru obavljanja poslova Nacionalnog CERT-a potrebno je obezbediti sledeće zahteve: 1) visok nivo dostupnosti komunikacionih kanala izbegavanjem jedinstvenih tačaka prekida i korišćenje više sredstava za dvosmerno kontaktiranje; 2) prostorije Nacionalnog CERT-a i informacioni sistemi za podršku treba da budu smešteni na sigurnim lokacijama; 3) upotrebu odgovarajućeg sistema za upravljanje zahtevima i njihovo usmeravanje, posebno kako bi se olakšala efikasna i efektivna razmena informacija; 4) obezbeđivanje poverljivosti i pouzdanosti svojih aktivnosti; 5) postojanje adekvatnih kadrovskih kapaciteta; 6) opremljenost redundantnim sistemima i rezervnim radnim prostorom kako bi se osigurao kontinuitet usluga.			
11.4.	The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.	1.33.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da	PU		

			prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti.			
11.5.	In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to: (a)incident-handling procedures; (b)crisis management; and (c)coordinated vulnerability disclosure under Article 12(1).	1.31.	Poslovi prevencije i zaštite od bezbednosnih rizika na nacionalnom nivou (Nacionalni CERT) Član 31. U okviru poslova prevencije i zaštite od bezbednosnih rizika i incidenata Kancelarija vrši poslove Nacionalnog CERT-a i to: 1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost. 2) prati stanje o incidentima u Republici Srbiji; 3) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o pretnjama, ranjivostima i incidentima; 4) reaguje bez odlaganja 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; 5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu; 6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora; 7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom; 8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje;	PU		

			9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija; 10) podiže svest kod građana, privrednih subjekata i organa o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti; 11) vodi Evidenciju posebnih CERT-ova; 12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima; 13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za: 1) upravljanje incidentima; 2) klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata; 3) upravljanje kriznim situacijama; 4) koordinirano otkrivanje ranjivosti. Kancelarija je ovlašćena da vrši obradu podataka o licu koje prijavi incident, pri čemu obrada podataka o licu 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. Kancelarija obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije. U okviru obavljanja poslova Nacionalnog CERT-a potrebno je obezbediti sledeće zahteve: 1) visok nivo dostupnosti komunikacionih kanala izbegavanjem jedinstvenih tačaka prekida i korišćenje više sredstava za dvosmerno kontaktiranje; 2) prostorije Nacionalnog CERT-a i informacioni sistemi za podršku treba da budu smešteni na sigurnim lokacijama; 3) upotrebu odgovarajućeg sistema za upravljanje zahtevima i njihovo usmeravanje, posebno kako bi se olakšala efikasna i efektivna razmena informacija; 4) obezbeđivanje poverljivosti i pouzdanosti svojih aktivnosti;			

			5) postojanje adekvatnih kadrovskih kapaciteta; 6) opremljenost redundantnim sistemima i rezervnim radnim prostorom kako bi se osigurao kontinuitet usluga. Preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave (CERT organa vlasti)			
12.1.	***Coordinated vulnerability disclosure and a European vulnerability database*** Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include: (a)identifying and contacting the entities concerned; (b)assisting the natural or legal persons reporting a vulnerability; and (c)negotiating disclosure timelines and managing vulnerabilities that affect multiple entities. Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall,	1.36.	Baza ranjivosti Član 36. Organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-a uspostavlja i održava bazu ranjivosti IKT proizvoda i IKT usluga u Republici Srbiji i omogućava fizičkim i pravnim licima, kao i proizvođačima, dobavljačima i pružaocima usluge u IKT sistemu, da na dobrovoljnoj bazi prijave ranjivosti u IKT proizvodima ili IKT uslugama, a koje se mogu prijaviti anonimno. Baza ranjivosti IKT proizvoda i IKT usluga sadrži: 1) podatke o ranjivosti; 2) podatke o ranjivostima IKT proizvoda ili IKT usluga. Organ, odnosno organizacija iz stava 1. ovog člana propisuje sadržaj, procedure verifikacije ranjivosti, procedure za upravljanje tehničkim ranjivostima IKT proizvoda i IKT usluga, način upisa i vođenja registra.	PU		

	where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.					
12.2.	ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include: (a)information describing the vulnerability; (b)the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited; (c)the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.			NP	Obaveze ENISA	
13.1.	***Cooperation at national level*** Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.			PU	Implementacija je osigurana primenom propisa koji uređuju saradnju državnih organa i međunarodnu saradnju.	
13.2.	Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats	1.13 1.14.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni	PU		

	and near misses pursuant to Article 30.	1.15.	su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni			

			su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture.			

			Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi.			
13.3.	Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive.	1.13 1.14. 1.15.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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	PU		

			usluga, ili traju duži vremenski period; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti			

			finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu			

			Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi.			
13.4.	In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.	1.33. 1.34.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol” (TLP), i poštujući propise o zaštiti podataka o ličnosti. Međunarodna saradnja i poslovi jedinstvene tačke	PU		

			kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.		
13.5.	Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as			PU	Implementacija osigurana primenom propisa o saradnji državnih organa i međunarodnoj saradnji.	

	well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.					
13.6.	Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.	1.2.1.17.	jedinstveni sistem za prijem obaveštenja o incidentima je informacioni sistem u koji se unose podaci o incidentima i izbegnutim incidentima u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti;	PU		
14.1.	***Cooperation Group*** In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.	1.27.	Telo za koordinaciju poslova informacione bezbednosti Član 27. 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, poslove pravosuđa, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge. U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa, privrede, akademske zajednice i nevladinog sektora. Odlukom kojom osniva Telo za koordinaciju Vlada određuje i njegov sastav, zadatke, rok u kome ono	PU		

			podnosi izveštaje Vladi i druga pitanja koja su vezana za njegov rad.			
14.2.	The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.			PU	Osigurano primenom odredbi koje uređuju način rada i nadležnosti Vladinih tela.	
14.3.	The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation. Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work. The Commission shall provide the secretariat.			NP	Odnosi se samo na tela koja se osnuju na nivou EU.	
14.4.	The Cooperation Group shall have the following tasks: (a)to provide guidance to the competent authorities in relation to the transposition and implementation of this Directive; (b)to provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure, as referred to in Article 7(2), point (c); (c)to exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities pursuant to Article 2(2), points (b) to (e); (d)to exchange advice and cooperate with the Commission on emerging cybersecurity policy			NP	Odnosi se samo na tela koja se osnuju na nivou EU.	

	initiatives and the overall consistency of sector-specific cybersecurity requirements; (e)to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive; (f)to exchange best practices and information with relevant Union institutions, bodies, offices and agencies; (g)to exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity; (h)where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations; (i)to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1); (j)to discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions as referred to in Article 37; (k)upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance as referred to in Article 37; (l)to provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues; (m)to exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe; (n)to contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;					

	(o)to organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges; (p)to discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA; (q)to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6); (r)to prepare reports for the purpose of the review referred to in Article 40 on the experience gained at a strategic level and from peer reviews; (s)to discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware. The Cooperation Group shall submit the reports referred to in the first subparagraph, point (r), to the Commission, to the European Parliament and to the Council.					
14.5.	Member States shall ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group.			NP	Odnosi se samo na tela koja se osnuju na nivou EU.	
14.6.	The Cooperation Group may request from the CSIRTs network a technical report on selected topics.			NP	Odnosi se samo na tela koja se osnuju na nivou EU.	
14.7.	By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.			NP	Pravilo o primeni direktive.	

14.8.	The Commission may 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 39(2). The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4), point (e).			NP	Obaveza Komisije.	
14.9.	The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.			NP	Odnosi se samo na tela koja se osnuju na nivou EU.	
15.1.	***CSIRTs network*** In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.			NP	Odnosi se na CERTove država članica EU.	
15.2.	The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.			NP	Odnosi se na CERTove država članica EU.	
15.3.	The CSIRTs network shall have the following tasks: (a)to exchange information about the CSIRTs' capabilities; (b)to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;			NP	Odnosi se na CERTove država članica EU.	

	(c)to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities; (d)to exchange information with regard to cybersecurity publications and recommendations; (e)to ensure interoperability with regard to information-sharing specifications and protocols; (f)at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities; (g)at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State; (h)to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive; (i)to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State; (j)to discuss and identify further forms of operational cooperation, including in relation to: (i)categories of cyber threats and incidents; (ii)early warnings; (iii)mutual assistance; (iv)principles and arrangements for coordination in response to cross-border risks and incidents;					

	(v)contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State; (k)to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard; (l)to take stock of cybersecurity exercises, including those organised by ENISA; (m)at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT; (n)to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union; (o)where relevant, to discuss the peer-review reports referred to in Article 19(9); (p)to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.					
15.4.	By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report. The report shall, in particular, draw up conclusions and recommendations on the basis of the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.			NP	Pravilo primene odredbi direktive.	
15.5.	The CSIRTs network shall adopt its rules of procedure.			NP	Odnosi se na CERTove država članica EU.	

15.6.	The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.			NP	Odnosi se na CERTove država članica EU.	
16.1.	***European cyber crisis liaison organisation network (EU-CyCLONe)*** EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.			NP	Organizovana mreža za države članice EU.	
16.2.	EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer. ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information. Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.			NP	Organizovana mreža za države članice EU.	
16.3.	EU-CyCLONe shall have the following tasks: (a)to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises; (b)to develop a shared situational awareness for large-scale cybersecurity incidents and crises; (c)to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;			NP	Organizovana mreža za države članice EU.	

	(d)to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises; (e)to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).					
16.4-16.7.	EU-CyCLONe shall adopt its rules of procedure. EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6). By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.			NP	Organizovana mreža za države članice EU.	
17.1.	***International cooperation*** The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.			NP	Organizovana mreža za države članice EU.	
18.1.	***Report on the state of cybersecurity in the Union*** ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following:			NP	Obaveza ENISAe.	

	(a)a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape; (b)an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union; (c)an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises; (d)an aggregated assessment of the outcome of the peer reviews referred to in Article 19; (e)an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.					
18.2.	The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.			NP	Obaveza ENISAe	
18.3.	ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).			NP	Obaveza ENISAe	
19.1.	***Peer reviews*** The Cooperation Group shall, on 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual			NP	Obaveza ENISAe	

	trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed. The peer reviews shall cover at least one of the following: (a)the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23; (b)the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities; (c)the operational capabilities of the CSIRTs; (d)the level of implementation of mutual assistance referred to in Article 37; (e)the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29; (f)specific issues of cross-border or cross-sector nature.					
19.2-19.9.	The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews. Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review.			NP	Obaveza ENISAe	

	Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3. Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties. Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity					

	experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State. Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.					
20.1.	***Governance*** Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article. The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.	1.3.1.	Prilikom planiranja i primene mera zaštite IKT sistema treba se rukovoditi načelima: 1) načelo upravljanja rizikom – izbor i nivo primene mera se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanja posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti;	PU		
20.2.	Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	1.10.3.4.	Mere zaštite IKT sistema se odnose na: 4) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne	PU		

			obuke za zaposlene odgovorne za upravljanje informacionom bezbednošću, radi obezbeđivanja kontinuirane edukacije;			
21.1.	***Cybersecurity risk- management measures*** Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	1.10. 1.11. 1.12.	Mere zaštite IKT sistema od posebnog značaja Član 10. 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 smanjenje štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima. Mere zaštite primenjuju se u svim IKT sistemima operatora iz stava 1. ovog člana. Mere zaštite IKT sistema se odnose na: 1) uspostavljanje organizacione strukture, sa utvrđenim poslovima, znanjima, kompetencijama, iskustvom i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema; 2) prikupljanje podataka o pretnjama po informacionu bezbednost IKT sistema; 3) postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja; 4) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne obuke za zaposlene odgovorne za upravljanje informacionom bezbednošću, radi obezbeđivanja kontinuirane edukacije; 5) obezbeđivanje dovoljno resursa za adekvatno upravljanje informacionom bezbednošću; 6) zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema; 7) identifikovanje informacionih dobara i	PU		

			određivanje odgovornosti za njihovu zaštitu; 8) klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. ovog zakona; 9) zaštitu nosača podataka; 10) ograničenje pristupa podacima i sredstvima za obradu podataka; 11) odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža; 12) utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju; 13) predviđanje upotrebe kriptografskih kontrola i drugih tehnika za sakrivanje podataka radi zaštite poverljivosti, autentičnosti i integriteta podataka; 14) primena mera zaštite radi sprečavanja oticanja podataka; 15) fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu; 16) zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem; 17) obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka; 18) primenu odgovarajućih procedura i mera zaštite prilikom korišćenja usluge računarstva u klaudu; 19) praćenje IKT sistema u cilju otkrivanja ranjivosti i pretnji; 20) ograničenje pristupa internet stranicama koje mogu potencijalno da naruše bezbednost IKT sistema; 21) zaštitu podataka i sredstava za obradu podataka od zlonamernog softvera; 22) zaštitu od gubitka podataka redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za razmenu podataka; 23) čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema; 24) obezbeđivanje integriteta softvera i			

			operativnih sistema; 25) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema; 26) obezbeđivanje zaštite IKT sistema prilikom sprovođenja revizorskog testiranja; 27) zaštitu podataka u komunikacionim mrežama, uključujući uređaje i vodove; 28) bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema; 29) ispunjenje zahteva za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema; 30) zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema; 31) procedure za čuvanje i brisanje informacija u IKT sistemima, u skladu sa propisima; 32) zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga; 33) održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga; 34) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, kao i primenu mera sanacije posledica incidenta; 35) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje se definišu Planom kontinuiteta obavljanja posla; 36) usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite; 37) upotrebu multifaktorske autentikacije ili rešenja kontinuirane provere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije, te bezbednih komunikacionih sistema u hitnim slučajevima unutar operatora IKT sistema Podzakonski akt kojim se bliže uređuju mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada donosi Vlada, na predlog Ministarstva.			

			Akt o proceni rizika IKT sistema od posebnog značaja Član 11. Operator IKT sistema od posebnog značaja dužan je da donese akt o proceni rizika za IKT sisteme (u daljem tekstu: akt o proceni rizika) kojima upravlja. Aktom o proceni rizika vrši se procena rizika za IKT sistem od posebnog značaja s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj. Akt o proceni rizika revidira se najmanje jednom godišnje. Akt o proceni rizika izrađuje se u skladu sa opštom metodologijom za procenu rizika u IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a. Operator IKT sistema od posebnog značaja nije u obavezi da donese akt iz stava 1. ovog člana u slučaju kada ima definisanu procenu rizika u drugim postojećim internim aktima, koja obuhvata zahteve iz opšte metodologije iz stava 4. ovog člana. Akt o bezbednosti IKT sistema od posebnog značaja Član 12. Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema (u daljem tekstu: akt o bezbednosti). Aktom o bezbednosti određuju se mere zaštite, a naročito principi, 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. Akt o bezbednosti IKT sistema od posebnog značaja zasniva se na Aktu o proceni rizika iz člana 11. ovog zakona. Primena mera zaštite IKT sistema mora biti u skladu sa procenjenim rizicima, kako bi se obezbedila adekvatna zaštita sistema i minimizirao uticaj potencijalnih incidenata. Akt o bezbednosti mora da bude usklađen s promenama u okruženju i u samom IKT sistemu. Operator IKT sistema od posebnog značaja dužan je da, samostalno ili uz angažovanje spoljnih			

			eksperata, vrši proveru iz prethodnog stava najmanje jednom godišnje i da o tome sačini izveštaj. Podzakonski akt kojim se bliže uređuje sadržaj akta o bezbednosti, način provere IKT sistema od posebnog značaja i sadržaj izveštaja o proveri, kao i dostavljanje izveštaja nadležnom organu, donosi Vlada na predlog Ministarstva.			
21.2. (a)	The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: (a)policies on risk analysis and information system security;	1.11. 1.12.	Akt o proceni rizika IKT sistema od posebnog značaja Član 11. Operator IKT sistema od posebnog značaja dužan je da donese akt o proceni rizika za IKT sisteme (u daljem tekstu: akt o proceni rizika) kojima upravlja. Aktom o proceni rizika vrši se procena rizika za IKT sistem od posebnog značaja s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj. Akt o proceni rizika revidira se najmanje jednom godišnje. Akt o proceni rizika izrađuje se u skladu sa opštom metodologijom za procenu rizika u IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a. Operator IKT sistema od posebnog značaja nije u obavezi da donese akt iz stava 1. ovog člana u slučaju kada ima definisanu procenu rizika u drugim postojećim internim aktima, koja obuhvata zahteve iz opšte metodologije iz stava 4. ovog člana. Akt o bezbednosti IKT sistema od posebnog značaja Član 12. Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema (u daljem tekstu: akt o bezbednosti). Aktom o bezbednosti određuju se mere zaštite, a naročito principi, 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. Akt o bezbednosti IKT sistema od posebnog značaja zasniva se na Aktu o proceni rizika iz člana 11.	PU		

			ovog zakona. Primena mera zaštite IKT sistema mora biti u skladu sa procenjenim rizicima, kako bi se obezbedila adekvatna zaštita sistema i minimizirao uticaj potencijalnih incidenata. Akt o bezbednosti mora da bude usklađen s promenama u okruženju i u samom IKT sistemu. Operator IKT sistema od posebnog značaja dužan je da, samostalno ili uz angažovanje spoljnih eksperata, vrši proveru iz prethodnog stava najmanje jednom godišnje i da o tome sačini izveštaj. Podzakonski akt kojim se bliže uređuje sadržaj akta o bezbednosti, način provere IKT sistema od posebnog značaja i sadržaj izveštaja o proveri, kao i dostavljanje izveštaja nadležnom organu, donosi Vlada na predlog Ministarstva.			
21.2. (b)	(b)incident handling;	1.10.34. 1.10.35.	Mere zaštite IKT sistema se odnose na: 34) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, kao i primenu mera sanacije posledica incidenta; 35) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje se definišu Planom kontinuiteta obavljanja posla.			
21.2. (c)	(c)business continuity, such as backup management and disaster recovery, and crisis management;	1.10.22. 1.10.35.	Mere zaštite IKT sistema se odnose na: 22) zaštitu od gubitka podataka redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za razmenu podataka; 35) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje se definišu Planom kontinuiteta obavljanja posla.			
21.2. (d)	(d)supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	1.10.32. 1.10.33.	Mere zaštite IKT sistema se odnose na: 32) zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga; 33) održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;			

21.2. (e)	(e)security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	1.10.18. 1.10.24. 1.10.25. 1.10.26.	Mere zaštite IKT sistema se odnose na: 18) primenu odgovarajućih procedura i mera zaštite prilikom korišćenja usluge računarstva u klaudu; 24) obezbeđivanje integriteta softvera i operativnih sistema; 25) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema; 26) obezbeđivanje zaštite IKT sistema prilikom sprovođenja revizorskog testiranja;	PU		
21.2. (f)	(f)policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	1.10.36.	36) usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite.	PU		
21.2. (g)	(g)basic cyber hygiene practices and cybersecurity training;	1.10.4. 1.10.7.	Mere zaštite IKT sistema se odnose na: 4) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne obuke za zaposlene odgovorne za upravljanje informacionom bezbednošću, radi obezbeđivanja kontinuirane edukacije; 7) identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu;	PU		
21.2. (h)	(h)policies and procedures regarding the use of cryptography and, where appropriate, encryption;	1.10.13.	Mere zaštite IKT sistema se odnose na: 13) predviđanje upotrebe kriptografskih kontrola i drugih tehnika za sakrivanje podataka radi zaštite poverljivosti, autentičnosti i integriteta podataka;	PU		
21.2. (i)	(i)human resources security, access control policies and asset management;	1.10.1. 1.10.6. 1.10.7. 1.10.10.	Mere zaštite IKT sistema se odnose na: 1) uspostavljanje organizacione strukture, sa utvrđenim poslovima, znanjima, kompetencijama, iskustvom i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema; 6) zaštitu od rizika koji nastaju pri promenama	PU		

		1.10.12.	poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema; 7) identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu; 10) ograničenje pristupa podacima i sredstvima za obradu podataka; 12) utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju.			
21.2. (j)	(j)the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	1.10.37.	Mere zaštite IKT sistema se odnose na: 37) upotrebu multifaktorske autentikacije ili rešenja kontinuirane provere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije, te bezbednih komunikacionih sistema u hitnim slučajevima unutar operatora IKT sistema			
21.3.	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).	1.47. 1.48. 1.49.	Inspekcija za informacionu bezbednost Član 47. 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 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. Član 48. Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i	PU		

			penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Stručni nadzor Član 49. Stručni 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, vrši Kancelarija, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslove stručnog nadzora obavlja ovlašćeno lice zaposleno u Kancelariji (u daljem tekstu: ovlašćeno lice). U postupku stručnog nadzora ovlašćeno lice ima pravo i obavezu da kontroliše: 1) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj; 2) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite; 3) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema sa aktom o bezbednosti; 4) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost. Ako u vršenju stručnog nadzora Kancelarija utvrdi nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, o tome obaveštava nadziranog subjekta i određuje mu			

			rok u kome je dužan da ih otkloni. Rok iz stava 4. ovog člana ne može biti kraći od osam dana od dana prijema obaveštenja, osim u slučajevima koji zahtevaju hitno postupanje. Ako Kancelarija utvrdi da nadzirani subjekat nije, u ostavljenom roku, otklonio utvrđene nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, podnosi prijavu inspekciji. Kancelarija je dužna da po zahtevu inspektora za informacionu bezbednost obavi stručni nadzor i dostavi informaciju o utvrđenom činjeničnom stanju. Obrazac legitimacije i način izdavanja legitimacije ovlašćenog lica utvrđuje Kancelarija. Legitimacija ovlašćenog lica obavezno sadrži: grb Republike Srbije i naziv Kancelarije, ime i prezime ovlašćenog lica, fotografiju ovlašćenog lica, službeni broj legitimacije, datum izdavanja legitimacije, pečat Kancelarije, potpis direktora Kancelarije, kao i odštampani tekst sledeće sadržine: „Imalac ove legitimacije ima ovlašćenja u skladu sa odredbama člana 46. st. 3. i 4. Zakona o informacionoj bezbednosti.”			
21.4.	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	1.47. 1.48. 1.49.	Inspekcija za informacionu bezbednost Član 47. 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 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. Član 48. Ovlašćenja inspektora za informacionu bezbednost Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku	PU		

			vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Stručni nadzor Član 49. Stručni 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, vrši Kancelarija, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslove stručnog nadzora obavlja ovlašćeno lice zaposleno u Kancelariji (u daljem tekstu: ovlašćeno lice). U postupku stručnog nadzora ovlašćeno lice ima pravo i obavezu da kontroliše: 1) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj; 2) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite; 3) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema			

			sa aktom o bezbednosti; 4) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost. Ako u vršenju stručnog nadzora Kancelarija utvrdi nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, o tome obaveštava nadziranog subjekta i određuje mu rok u kome je dužan da ih otkloni. Rok iz stava 4. ovog člana ne može biti kraći od osam dana od dana prijema obaveštenja, osim u slučajevima koji zahtevaju hitno postupanje. Ako Kancelarija utvrdi da nadzirani subjekat nije, u ostavljenom roku, otklonio utvrđene nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, podnosi prijavu inspekciji. Kancelarija je dužna da po zahtevu inspektora za informacionu bezbednost obavi stručni nadzor i dostavi informaciju o utvrđenom činjeničnom stanju. Obrazac legitimacije i način izdavanja legitimacije ovlašćenog lica utvrđuje Kancelarija. Legitimacija ovlašćenog lica obavezno sadrži: grb Republike Srbije i naziv Kancelarije, ime i prezime ovlašćenog lica, fotografiju ovlašćenog lica, službeni broj legitimacije, datum izdavanja legitimacije, pečat Kancelarije, potpis direktora Kancelarije, kao i odštampani tekst sledeće sadržine: „Imalac ove legitimacije ima ovlašćenja u skladu sa odredbama člana 46. st. 3. i 4. Zakona o informacionoj bezbednosti.”			
21.5.	By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.	1.54.	Član 54. Rokovi za donošenje podzakonskih akata Podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona. Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti iz člana 18. ovog zakona donosi se u roku od 18 meseci od dana stupanja na snagu ovog zakona.	PU		

	The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).					
22.1.- 22.2.	***Union level coordinated security risk assessments of critical supply chains*** The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.			NP	Grupa koju osnivaju države članice EU	
23.1.	***Reporting obligations*** Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in	1.13.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident.	PU		

	paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.		Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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.			
23.2.	Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall	1.13.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od	PU		

	also inform those recipients of the significant cyber threat itself.		24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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.			
23.3.	An incident shall be considered to be significant if: (a)it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;	1.13.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione	PU		

	(b)it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.		bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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.			
23.4.	Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:	1.13. 1.14. 1.15.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da	PU		

	(a)without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (b)without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; (c)upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates; (d)a final report not later than one month after the submission of the incident notification under point (b), including the following: (i)a detailed description of the incident, including its severity and impact; (ii)the type of threat or root cause that is likely to have triggered the incident; (iii)applied and ongoing mitigation measures; (iv)where applicable, the cross-border impact of the incident; (e)in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard	1.24.	ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u			

	to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aaware of the significant incident.		jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno			

			obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi. Izveštavanje tokom i nakon incidenta Član 24. Operatori IKT sistema od posebnog značaja dužni su da: 1) dostavljaju izveštaj o incidentu, tokom trajanja incidenta, sa opisom mera koje su preduzete za rešavanje incidenta, u jedinstveni sistem za prijem obaveštenja o incidentima i to: (1) na svaka tri dana u slučaju incidenta srednjeg nivoa; (2) na svaka 24 sata u slučaju incidenata visokog i veoma visokog nivoa; 2) dostavljaju obaveštenja i dodatne izveštaje o bitnim događajima u vezi sa incidentom i			

			aktivnostima koje preduzimaju, na zahtev Kancelarije; 3) dostavljaju završni izveštaj o incidentu u roku od 15 dana od dana prestanka incidenta, koji sadrži sledeće podatke: (1) vrstu i detaljan opis incidenta, (2) vrstu pretnje i uzrok koji je doveo do incidenta; (3) vreme i trajanje incidenta, (4) ozbiljnost i uticaj incidenta, odnosno posledice koje je incident izazvao, (5) informaciju o eventualnom prekograničnom dejstvu incidenta, (6) preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge informacije od značaja za evidentiranje incidenta i statističku obradu. Nakon završenog incidenta Kancelarija priprema preporuke i savete za zaštitu od potencijalnih rizika, na osnovu analize izvršenog incidenta.			
23.5.	The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.	1.13 1.14. 1.15. 1.16.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i	PU		

			interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i			

			poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta;		

			6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi. Značaj incidenata prema nivou opasnosti Član 16. Incidenti u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti svrstavaju se prema nivou opasnosti, imajući u vidu posledice incidenta, u sledeće nivoe opasnosti: 1) nizak; 2) srednji; 3) visok; 4) veoma visok. Podzakonski akt kojim se uređuje postupak obaveštavanja o incidentima, obrasci za obaveštavanje, lista incidenata prema vrstama i klasifikacija incidenata prema nivou opasnosti donosi Vlada, na predlog Ministarstva.			
23.6.	Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	1.17. 1.18. 1.19. 1.20. 1.21. 1.22. 1.23.	Operativni tim za reagovanje na incidente Član 17. U cilju koordinisane reakcije na incidente visokog i veoma visokog nivoa Kancelarija za informacionu bezbednost obrazuje stalni operativni tim. Kancelarija za informacionu bezbednost utvrđuje kriterijume za imenovanje članova operativnog tima. Kancelarija za informacionu bezbednost može da, zavisno od prirode i posledica incidenta, zatraži uključivanje drugih organa u rad operativnog tima u okviru njihovih nadležnosti. Po potrebi, sastancima operativnog tima mogu prisustvovati i predstavnici posebnih CERT-ova,	PU		

			kao i druga lica. Lica koja učestvuju u radu stalnog operativnog tima dužna su da se sertifikuju za rad sa tajnim podacima. Plan za reagovanje u slučaju incidenta visokog nivoa i kriza informacione bezbednosti Član 18. Vlada donosi Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, na predlog Kancelarije za informacionu bezbednost. Plan iz stava 1. ovog člana obuhvata: 1) ciljeve mera i aktivnosti za reagovanje u slučaju incidenata visokog nivoa i kriza informacione bezbednosti; 2) delovanje nadležnih organa u cilju sprovođenja plana; 3) opis procedura u slučaju incidenata visokog nivoa i kriza informacione bezbednosti; 4) aktivnosti za unapređenje sposobnosti reagovanja na incidente, a pre svega planove odgovarajućih vežbi i obuka; 5) modele saradnje sa privatnim, nevladinim i akademskim sektorom; 6) međusobnu saradnju nadležnih organa. Prilikom izrade plana iz stava 1. ovog člana uspostavlja se saradnja sa organima i pravnim licima čije su nadležnosti, odnosno poslovi i delatnosti povezani sa planiranim aktivnostima. Plan iz stava 1. ovog člana se periodično menja i dopunjuje u skladu sa potrebama i novim okolnostima, a u celini se ponovo izrađuje i donosi svake treće godine, a ukoliko su se okolnosti u značajnoj meri promenile i ranije. Postupanje po prijemu obaveštenja o incidentu Član 19. Po prijemu obaveštenja o incidentu u IKT sistemu od posebnog značaja, Kancelarija za informacionu bezbednost postupa u skladu sa nadležnostima utvrđenim zakonom, odnosno prikuplja, analizira i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i incidentu, i u vezi sa tim obaveštava, pruža podršku, upozorava i savetuje operatora IKT sistema od posebnog značaja i vrši		

			druge poslove iz svoje nadležnosti. Kancelarija za informacionu bezbednost, nakon izvršene analize, utvrđuje nivo opasnosti incidenta. Kada je neophodno da javnost bude upoznata sa incidentom ili kada je incident takav da je od interesa za javnost, Kancelarija za informacionu bezbednost objavljuje informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio. Izuzetno od stava 3. ovog člana, Kancelarija za informacionu bezbednost može objaviti informaciju o incidentu koji se dogodio u operatoru prioritetnog IKT sistema od posebnog značaja koji obavlja delatnost u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3), uz prethodno pribavljenu saglasnost Narodne banke Srbije odnosno Komisije za hartije od vrednosti. Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da obaveštenja o incidentima proslede: 1) nadležnom javnom tužilaštvu, odnosno ministarstvu nadležnom za unutrašnje poslove, u slučaju da je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, 2) organu nadležnom za bezbednosne i kontraobaveštajne poslove od značaja za odbranu Republike Srbije ili organu nadležnom za poslove nacionalne bezbednosti, u slučaju da je incident povezan sa značajnim narušavanjem informacione bezbednosti koje ima ili može imati za posledicu ugrožavanje odbrane Republike Srbije ili nacionalne bezbednosti. Prilikom upravljanja incidentom Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge označavaju obaveštenje o incidentu, odnosno informacije o incidentu u skladu sa propisima i TLP (eng.„traffic light protocol”) protokolom. Postupanje u slučaju incidenta nivoa opasnosti „nizak” Član 20. U slučaju incidenata kojima je u skladu sa		

			klasifikacijom utvrđen nivo opasnosti „nizak” Kancelarija za informacionu bezbednost po potrebi daje preporuke za postupanje operatoru IKT sistema od posebnog značaja. Postupanje u slučaju incidenta nivoa opasnosti „srednji” Član 21. U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „srednji” Kancelarija za informacionu bezbednost daje preporuke za postupanje operatoru IKT sistema od posebnog značaja. Postupanje u slučaju incidenta nivoa opasnosti „visok” Član 22. U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „visok” Kancelarija za informacionu bezbednost je dužna da o tome obavesti Ministarstvo. Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, priprema preporuke i mere za rešavanje incidenta. Ministarstvo nakon prijema obaveštenja iz stava 1. ovog člana saziva sednicu Tela za koordinaciju poslova informacione bezbednosti. Nakon završetka incidenta Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, sačinjava završni izveštaj koji dostavlja Ministarstvu u roku od 30 dana nakon završenog incidenta. Postupanje u slučaju incidenta nivoa opasnosti „veoma visok” Član 23. U slučaju incidenta kojem je u skladu sa klasifikacijom utvrđen nivo opasnosti „veoma visok“ i koji predstavlja krizu informacione bezbednosti, rukovođenje i koordinaciju sprovođenja mera i zadataka preduzima Vlada. Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, izrađuje predlog za proglašavanje krize informacione bezbednosti, u skladu sa Planom za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, koji sadrži:			

			1) podatke o incidentu; 2) informacije o preduzetim merama; 3) razloge za proglašenje krize informacione bezbednosti; 4) zaduženje organa za postupanje u skladu sa svojim nadležnostima; 5) mere za rešavanje krize. Predlog za proglašenje krize informacione bezbednosti upućuje se Ministarstvu, koje po prijemu predloga bez odlaganja saziva sednicu Tela za koordinaciju poslova informacione bezbednosti. Vlada na predlog Ministarstva donosi odluku o proglašenju krize informacione bezbednosti i zadužuje organe da postupaju prema predloženim merama u skladu sa svojim nadležnostima. Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, koordinira rešavanjem krize informacione bezbednosti i najmanje jednom nedeljno izveštava Ministarstvo i Vladu o svim aktivnostima. Predlog za proglašenje završetka krize informacione bezbednosti upućuje se Ministarstvu. Odluku o proglašenju završetka krize informacione bezbednosti donosi Vlada na predlog Ministarstva. Nakon završetka krize informacione bezbednosti Kancelarija za informacionu bezbednost sačinjava završni izveštaj koji dostavlja Ministarstvu i Vladi u roku od 30 dana nakon završetka krize.			
23.7.	Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.	1.22.	Postupanje u slučaju incidenta nivoa opasnosti „visok" Član 22. U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti „visok" Kancelarija za informacionu bezbednost je dužna da o tome obavesti Ministarstvo. Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, priprema preporuke i mere za rešavanje incidenta. Ministarstvo nakon prijema obaveštenja iz stava 1. ovog člana saziva sednicu Tela za koordinaciju poslova informacione bezbednosti. Nakon završetka incidenta Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, sačinjava završni izveštaj koji dostavlja Ministarstvu u roku od 30 dana nakon završenog	PU		

			incidenta.			
23.8.	At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.	1.34.	Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država. Posebni centri za prevenciju bezbednosnih	PU		
23.9.	The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant			NP	Obaveza država članica prema	

	incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.				ENISAi	
23.10.	The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.	1.31.1.	Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema.	PU		
23.11.	The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article. By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities. The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 14(4), point (e). Those implementing acts shall be adopted in	1.54.	Član 54. Rokovi za donošenje podzakonskih akata Podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona. Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti iz člana 18. ovog zakona donosi se u roku od 18 meseci od dana stupanja na snagu ovog zakona.	PU		

	accordance with the examination procedure referred to in Article 39(2).					
24.1.	***Use of European cybersecurity certification schemes*** In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.			NP	Odredba se odnosi na korišćenje sertifikacionih šema u EU.	
24.2.	The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period. Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881.			NP	Ovlašćenja komisije.	
24.3.	Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.			NP	Ovlašćenja Komisije.	
25.1.	***Standardisation*** In order to promote the convergent implementation			PU	Osigurana implementacija primenom opštih propisa koji se	

	of Article 21(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 and international standards and technical specifications relevant to the security of network and information systems.				odnose na standardizaciju.	
25.2.	ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, 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 national standards, which would allow for those areas to be covered.			NP	Ovlašćenja ENISA.	
26.1.	***Jurisdiction and territoriality*** Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of: (a)providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services; (b)DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2; (c)public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.			NP	Reguliše međusobne nadležnosti država članica u slučaju sukoba jurisdikcija.	
26.2.	For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the					

	Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.					
26.3.	If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.			NP	Reguliše međusobne nadležnosti država članica u slučaju sukoba jurisdikcija.	
26.4.	The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.			NP	Reguliše međusobne nadležnosti država članica u slučaju sukoba jurisdikcija.	
26.5.	Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.			NP	Reguliše međusobne nadležnosti država članica u slučaju sukoba jurisdikcija.	
27.1.	***Registry of entities*** ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security			NP	Obaveza ENISA	

	service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.					
27.2.	Member States shall require entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025: (a)the name of the entity; (b)the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable; (c)the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3); (d)up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3); (e)the Member States where the entity provides services; and (f)the entity's IP ranges.	1.9.	Evidencija operatora IKT sistema od posebnog značaja Član 9. Ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Ministarstvo) uspostavlja i vodi evidenciju prioritetnih i važnih IKT sistema od posebnog značaja (u daljem tekstu: Evidencija) koja sadrži: 1) naziv, matični broj i sedište operatora IKT sistema od posebnog značaja; 2) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon administratora zaduženog za održavanje i upravljanje IKT sistemom 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, odnosno da li IKT sistem od posebnog značaja potpada pod prioritetan ili važan; 5) podatak o delatnosti operatora IKT sistema od posebnog značaja; 6) adresni opseg internet protokola (engl. „IP address range“) koji pripadaju IKT sistemu od posebnog značaja, a koji obuhvata podatke o javnim statičkim IP adresama; 7) veb stranice operatora IKT sistema od posebnog značaja; 8) broj lokacija na kojima se IKT sistem od posebnog značaja nalazi. Pored podataka iz stava 1. ovog člana, evidencija može da sadrži i druge dopunske podatke o IKT sistemu od posebnog značaja. Samostalni operatori IKT sistema izuzeti su od obaveze dostavljanja podataka iz stava 1. tač. 4), 5), 6) i 8) ovog člana.	PU		

			Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji donosi Ministarstvo. Operator IKT sistema od posebnog značaja dužan je da Ministarstvu dostavi podatke iz st. 1. i 2. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 4. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja. Operator IKT sistema od posebnog značaja dužan je da u slučaju promene podataka iz stava 1. ovog člana o tome obavesti Ministarstvo u roku od 15 dana od dana nastanka promene. Podaci iz stava 1. tač. 2) i 3) obrađuju se u svrhu izvršenja odredbi ovog zakona u pogledu dostavljanja obaveštenja i upozorenja značajnih za bezbednost IKT sistema od posebnog značaja, kao i radi uspostavljanja komunikacije i ostvarivanja saradnje u cilju otklanjanja štetnih posledica incidenata i preventivnog delovanja. Podaci iz stava 1. tač. 2) i 3) obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i čuvaju se do trenutka prestanka svrhe obrade ili do izvršene promene podataka u skladu sa stavom 5. ovog člana. Ministarstvo stavlja na raspolaganje ažurnu Evidenciju Kancelariji za informacionu bezbednost radi izvršenja odredbi ovog zakona u pogledu prikupljanja i razmene informacija o pretnjama, ranjivostima i incidentima i pružanja podrške, upozoravanja i savetovanja lica koja upravljaju IKT sistemima. Evidencija predstavlja tajni podatak u smislu zakona kojim se uređuje tajnost podataka.			
27.3.	Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.	1.9.	Evidencija operatora IKT sistema od posebnog značaja Član 9. Ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Ministarstvo) uspostavlja i vodi evidenciju prioritetnih i važnih IKT sistema od posebnog značaja (u daljem tekstu: Evidencija) koja sadrži: 1) naziv, matični broj i sedište operatora IKT sistema od posebnog značaja; 2) ime i prezime, službena adresa za prijem	PU		

			elektronske pošte i službeni kontakt telefon administratora zaduženog za održavanje i upravljanje IKT sistemom 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, odnosno da li IKT sistem od posebnog značaja potpada pod prioritetan ili važan; 5) podatak o delatnosti operatora IKT sistema od posebnog značaja; 6) adresni opseg internet protokola (engl. „IP address range“) koji pripadaju IKT sistemu od posebnog značaja, a koji obuhvata podatke o javnim statičkim IP adresama; 7) veb stranice operatora IKT sistema od posebnog značaja; 8) broj lokacija na kojima se IKT sistem od posebnog značaja nalazi. Pored podataka iz stava 1. ovog člana, evidencija može da sadrži i druge dopunske podatke o IKT sistemu od posebnog značaja. Samostalni operatori IKT sistema izuzeti su od obaveze dostavljanja podataka iz stava 1. tač. 4), 5), 6) i 8) ovog člana. Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji donosi Ministarstvo. Operator IKT sistema od posebnog značaja dužan je da Ministarstvu dostavi podatke iz st. 1. i 2. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 4. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja. Operator IKT sistema od posebnog značaja dužan je da u slučaju promene podataka iz stava 1. ovog člana o tome obavesti Ministarstvo u roku od 15 dana od dana nastanka promene. Podaci iz stava 1. tač. 2) i 3) obrađuju se u svrhu izvršenja odredbi ovog zakona u pogledu dostavljanja obaveštenja i upozorenja značajnih za bezbednost IKT sistema od posebnog značaja, kao i radi uspostavljanja komunikacije i ostvarivanja saradnje u cilju otklanjanja štetnih posledica incidenata i preventivnog delovanja.			

			Podaci iz stava 1. tač. 2) i 3) obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i čuvaju se do trenutka prestanka svrhe obrade ili do izvršene promene podataka u skladu sa stavom 5. ovog člana. Ministarstvo stavlja na raspolaganje ažurnu Evidenciju Kancelariji za informacionu bezbednost radi izvršenja odredbi ovog zakona u pogledu prikupljanja i razmene informacija o pretnjama, ranjivostima i incidentima i pružanja podrške, upozoravanja i savetovanja lica koja upravljaju IKT sistemima. Evidencija predstavlja tajni podatak u smislu zakona kojim se uređuje tajnost podataka.			
27.4.	Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.			NP	Obaveza prema ENISA	
27.5.	Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.			NP	Obaveza prema ENISA	
28.1.	***Database of domain name registration data*** For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.	1.35.1.	Organizacije koje su ovlašćene za upravljanje registrom domena najvišeg nivoa i pružanje usluga DNS-a obavezne su da prikupljaju, čuvaju i održavaju tačne i potpune podatke o registraciji domena u posebnoj bazi podataka, uz dužnu pažnju i u skladu sa propisima o zaštiti podataka o ličnosti.	PU		
28.2.	For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include: (a)the domain name;	1.37.2.	Baza podataka iz stava 1 ovog člana mora da sadrži najmanje sledeće podatke: 1) naziv domena; 2) datum registracije domena; 3) ime, kontakt adresu elektronske pošte i broj telefona registranta; 4) kontakt adresu elektronske pošte i broj telefona lica zaduženog za administraciju domena, ukoliko se razlikuju od podataka registranta.	PU		

	(b)the date of registration; (c)the registrant's name, contact email address and telephone number; (d)the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.					
28.3.	Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.	1.37.3.	Organizacije iz stava 1. ovog člana dužne su da usvoje i primene akte i procedure za verifikaciju tačnosti i potpunosti podataka u bazi podataka. Ove procedure moraju biti javno dostupne.	PU		
28.4.	Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.	1.37.4.	Organizacije iz stava 1. ovog člana dužne su da obezbede javnu dostupnost podataka koji nisu lični odmah po registraciji domena, a u skladu sa pravilima i uslovima registracije naziva nacionalnih internet domena.	PU		
28.5.	Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.	1.37.5. 1.37.6. 1.37.7.	Organizacije iz stava 1. ovog člana obavezne su da omoguće pristup specifičnim podacima o registraciji domena na osnovu zakonitih i obrazloženih zahteva ovlašćenih lica ili organa, u skladu sa ovlašćenjima dodeljenim propisima koji uređuju delokrug njihovog rada. Odgovor na zahtev iz stava 5. ovog člana mora biti dostavljen bez odlaganja, a najkasnije u roku od 72 sata od prijema zahteva. Akti i procedure za otkrivanje podataka na osnovu ovih zahteva moraju biti javno dostupni.	PU		
28.6.	Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.	1.37.8.	U skladu sa ovim članom, prikupljanje podataka o registraciji domena ne sme dovesti do dupliranja podataka. Organizacije iz stava 1. ovog člana dužne su da sarađuju radi izbegavanja dupliranja i osiguranja usklađenosti sa zakonom.	PU		

29.1.	***Cybersecurity information-sharing arrangements*** Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing: (a)aims to prevent, detect, respond to or recover from incidents or to mitigate their impact; (b)enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.	1.33. 1.34.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti. Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U	PU		

			slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
29.2.	Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.	1.33. 1.34.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol” (TLP), i poštujući propise o zaštiti podataka o ličnosti. Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija ostvaruje međunarodnu	PU		

			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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
29.3.	Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose	1.33. 1.34.	Saradnja na nacionalnom nivou Član 33. Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema. Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u	PU		

	conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).		organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Sastancima iz stava 2. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica. Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući „traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti. Međunarodna saradnja i poslovi jedinstvene tačke kontakta Član 34. Kancelarija 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. Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema. Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije. Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje			

			će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima. Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.			
29.4.	Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	1.47.	Inspekcija za informacionu bezbednost Član 47. 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 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.	PU		
29.5.	ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.			NP	Obaveza ENISA	
30.1.	***Voluntary notification of relevant information*** Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by: (a)essential and important entities with regard to incidents, cyber threats and near misses; (b)entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.			PU	Proističe iz odredbi članova 13-15 o obaveštavanju o incidentima.	

30.2.	Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.	1.13. 1.14. 1.15.	Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost Član 13. Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident. Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su: 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; 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; 4) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije; 5) incidenti koji dovode do neovlašćenog pristupa podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose; 6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 2. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture; 7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima. Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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	PU		

			tajnih podataka. Dostavljanje obaveštenja o incidentima Član 14. Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb stranice Ministarstva ili Kancelarije za informacionu bezbednost. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 2. tačka 1) podtačka (3) dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti. Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 2. tačka 1) podtačka (9) alineja treća i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 2. tačka 1) alineja prva, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge. Narodna banka Srbije i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da dobijena obaveštenja iz st. 2 i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima. Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz stava 2. i 3. ovog člana, dužni su da obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta. Operatori IKT sistema od posebnog značaja iz stava 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima. Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao			

			kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture. Organi iz st. 1–3. ovog zakona, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka. Sadržaj obaveštenja o incidentu Član 15. Obaveštenje o incidentu mora da sadrži sledeće podatke: 1) podatke o podnosiocu prijave; 2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela; 3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta; 4) posledice koje je incident izazvao; 5) preduzete aktivnosti radi ublažavanja posledica incidenta; 6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije; 7) informaciju o eventualnom prekograničnom dejstvu incidenta; 8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete; 9) druge relevantne informacije, po potrebi.			
31.1.	***General aspects concerning supervision and enforcement*** Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.	1.47. 1.49.	Inspekcija za informacionu bezbednost Član 47. 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 preko inspektora za	PU		

			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. Stručni nadzor Član 49. Stručni 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, vrši Kancelarija, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslove stručnog nadzora obavlja ovlašćeno lice zaposleno u Kancelariji (u daljem tekstu: ovlašćeno lice). U postupku stručnog nadzora ovlašćeno lice ima pravo i obavezu da kontroliše: 1) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj; 2) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite; 3) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema sa aktom o bezbednosti; 4) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost. Ako u vršenju stručnog nadzora Kancelarija utvrdi nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, o tome obaveštava nadziranog subjekta i određuje mu rok u kome je dužan da ih otkloni. Rok iz stava 4. ovog člana ne može biti kraći od osam dana od dana prijema obaveštenja, osim u slučajevima koji zahtevaju hitno postupanje. Ako Kancelarija utvrdi da nadzirani subjekat nije, u		

			ostavljenom roku, otklonio utvrđene nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, podnosi prijavu inspekciji. Kancelarija je dužna da po zahtevu inspektora za informacionu bezbednost obavi stručni nadzor i dostavi informaciju o utvrđenom činjeničnom stanju. Obrazac legitimacije i način izdavanja legitimacije ovlašćenog lica utvrđuje Kancelarija. Legitimacija ovlašćenog lica obavezno sadrži: grb Republike Srbije i naziv Kancelarije, ime i prezime ovlašćenog lica, fotografiju ovlašćenog lica, službeni broj legitimacije, datum izdavanja legitimacije, pečat Kancelarije, potpis direktora Kancelarije, kao i odštampani tekst sledeće sadržine: „Imalac ove legitimacije ima ovlašćenja u skladu sa odredbama člana 46. st. 3. i 4. Zakona o informacionoj bezbednosti.”			
31.2.	Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.	3.9.	Procena rizika Član 9. Inspekcijski nadzor zasniva se na proceni rizika i srazmeran je procenjenom riziku, tako da se rizikom delotvorno upravlja. Procena rizika je deo procesa analize rizika, koji obuhvata i upravljanje rizikom i obaveštavanje o riziku. Rizik, prema stepenu, može biti neznatan, nizak, srednji, visok i kritičan. Inspekcija nije dužna da vrši inspekcijski nadzor kada je procenjeni rizik neznatan. Rizik se procenjuje u toku pripreme plana inspekcijskog nadzora i pre i u toku inspekcijskog nadzora. Kada se u toku realizacije godišnjeg plana inspekcijskog nadzora promene okolnosti na osnovu kojih je procenjen rizik i sačinjen plan, inspekcija usklađuje procenu rizika i plan inspekcijskog nadzora sa novonastalim okolnostima. Procena rizika u toku pripreme plana inspekcijskog nadzora vrši se tako što inspekcija u praćenju i analizi stanja u oblasti inspekcijskog nadzora koja je u njenom delokrugu identifikuje rizike po zakonom i drugim propisom zaštićena dobra, prava i interese, koji mogu nastati iz poslovanja ili postupanja nadziranog subjekta i, prema odgovarajućim kriterijumima, procenjuje težinu štetnih posledica i	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			verovatnoću njihovog nastanka, tako da se dobije procenjeni stepen rizika. Težina štetnih posledica procenjuje se polazeći od: 1) prirode štetnih posledica, koja proizlazi iz vrste delatnosti ili aktivnosti nadziranog subjekta, odnosno karakteristika robe ili proizvoda koga nadzirani subjekat stavlja u promet ili usluga koje nadzirani subjekat pruža, ili radnji koje preduzima, odnosno ovlašćenja koja vrši u sklopu svog poslovanja ili postupanja, a u odnosu na zakonom i drugim propisom zaštićena dobra, prava i interese, i 2) obima štetnih posledica, pre svega kruga lica koji koriste robu, proizvod ili usluge, odnosno kruga lica koja ostvaruju određena prava u nadziranom subjektu ili u vezi sa nadziranim subjektom, odnosno opsega zakonom i drugim propisom zaštićenih dobara, prava i interesa na koje se odnosi delatnost ili aktivnost nadziranog subjekta ili na koje ona utiče. Verovatnoća nastanka štetnih posledica procenjuje se polazeći naročito od prethodnog poslovanja i postupanja nadziranog subjekta, uključujući poslednje utvrđeno stanje zakonitosti i bezbednosti njegovog poslovanja i postupanja. Verovatnoća nastanka štetnih posledica procenjuje se polazeći i od: srpskih standarda i pravila dobre prakse koje nadzirani subjekat primenjuje; sistema upravljanja i unutrašnjeg nadzora nad zakonitošću, pravilnošću i bezbednošću poslovanja i postupanja kod nadziranog subjekta, uzimajući u obzir politiku upravljanja rizicima i različite oblike unutrašnjeg nadzora kod nadziranog subjekta, kao i reviziju finansijskih izveštaja nadziranog subjekta; stanja u oblasti u kojoj se njegova delatnost ili aktivnost vrši i predviđanja budućih kretanja u njoj; unutrašnjih i spoljnih stručnih, tehničkih, tehnoloških i finansijskih kapaciteta nadziranog subjekta. Pored procene rizika za nadzirane subjekte, rizik se, prema posebno propisanim kriterijumima, može proceniti i za pojedina teritorijalna područja i druge teritorijalne i slične celine (npr. teritorijalne jedinice, oblasti i podoblasti, deonice i dr), objekte i grupe objekata, u skladu sa delokrugom inspekcije i potrebama vršenja inspekcijskog nadzora. Zajedničke elemente procene rizika u inspekcijskom		

			nadzoru propisuje Vlada. Posebne elemente procene rizika i učestalost vršenja inspekcijskog nadzora na osnovu procene rizika, kao i posebne kriterijume iz stava 8. ovog člana propisuje ministar nadležan za odgovarajuću oblast inspekcijskog nadzora, odnosno imalac javnog ovlašćenja koji vrši inspekcijski nadzor u određenoj oblasti. Posebne elemente procene rizika i učestalost vršenja inspekcijskog nadzora na osnovu procene rizika iz izvorne nadležnosti autonomne pokrajine i jedinice lokalne samouprave propisuje nadležni organ autonomne pokrajine i jedinice lokalne samouprave.			
31.3.	The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.	3.5.	Saradnja sa drugim organima, imaocima javnih ovlašćenja i pravnim i fizičkim licima Član 5. Saradnja nadležne inspekcije sa drugim organima državne uprave, organima autonomne pokrajine i jedinice lokalne samouprave, pravosudnim i drugim državnim organima i drugim zainteresovanim organima i organizacijama ostvaruje se u skladu sa nadležnostima inspekcije i oblicima saradnje utvrđenim propisima o državnoj upravi i posebnim zakonima. Saradnja, naročito, obuhvata međusobno obaveštavanje, razmenu podataka, pružanje pomoći i zajedničke mere i radnje od značaja za inspekcijski nadzor. Nadležna inspekcija u obavljanju poslova iz svog delokruga usklađuje planove inspekcijskog nadzora i svog rada, razmenjuje podatke, predlaže preduzimanje zajedničkih mera i aktivnosti od značaja za obavljanje poslova inspekcijskog nadzora i na drugi način sarađuje sa drugim inspekcijama i subjektima sa javnim ovlašćenjima koji vrše posebne oblike nadzora i kontrole – radi obavljanja obuhvatnijeg i delotvornijeg inspekcijskog nadzora i naročito radi suzbijanja delatnosti ili aktivnosti neregistrovanih subjekata. Državni organi, organi autonomne pokrajine i jedinice lokalne samouprave i imaoci javnih ovlašćenja dužni su, na zahtev inspektora, da mu u roku od 15 dana od prijema zahteva dostave tražene podatke i obaveštenja koji su značajni za inspekcijski nadzor.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			Nadležna inspekcija, u skladu sa zakonom, sarađuje sa fizičkim i pravnim licima, naročito u cilju preventivnog delovanja, kao i unapređenja uzajamne odgovornosti fizičkih i pravnih lica i inspekcija u procesu primene i nadzora nad primenom propisa. U tom cilju, inspekcija može održavati informativne i edukativne tribine i konsultativne sastanke sa predstavnicima privatnog sektora i drugim zainteresovanim stranama. Fizička i pravna lica mogu inspekciji podnositi predstavke i zahteve, i od nje tražiti podatke i obaveštenja, u skladu sa zakonom. Ako se u vezi sa vršenjem inspekcijskog nadzora osnovano očekuje da nadzirani subjekat pruži otpor ili se on pruži i inspektoru onemogućava ili bitno otežava vršenje inspekcijskog nadzora, inspektor može da zahteva pomoć policije i komunalne policije. Policija i komunalna policija pružaju pomoć prema zakonima kojima se uređuju policija i komunalna policija.			
31.4.	Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.	3.49.	Samostalnost u radu Član 49. Inspektor je samostalan u radu u granicama ovlašćenja utvrđenih zakonom i drugim propisom i za svoj rad lično je odgovoran. Niko ne sme iskorišćavanjem službenog položaja ili ovlašćenja, prekoračenjem granica svojih ovlašćenja, nevršenjem svoje dužnosti ili na drugi način onemogućavati ili ometati inspektora, odnosno službenika ovlašćenog za vršenje inspekcijskog nadzora u obavljanju inspekcijskog nadzora i preduzimanju mera i radnji na koje je ovlašćen.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	
	Supervisory and enforcement measures in relation to essential entities Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.		Ovlašćenja inspektora za informacionu bezbednost Član 48. Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok;			

	Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:		2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama.			

32.1. 32.2.	(a)on-site inspections and off-site supervision, including random checks conducted by trained professionals; (b)regular and targeted security audits carried out by an independent body or a competent authority; (c)ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity; (d)security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned; (e)requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27; (f)requests to access data, documents and information necessary to carry out their supervisory tasks; (g)requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.	1.48. 3.6. 3.7. 3.20. 3.21.	Vrste inspekcijskog nadzora Član 6. Inspekcijski nadzor, prema vrsti, može biti redovan, vanredan, mešoviti, kontrolni i dopunski. Redovan inspekcijski nadzor vrši se prema planu inspekcijskog nadzora. Inspekcijski nadzor na državnoj granici, koji se obavlja redovno, upodobljava se redovnom inspekcijskom nadzoru i na njega se shodno primenjuju odredbe ovog zakona, ako ovim ili posebnim zakonom nije drugačije određeno, odnosno kada to proističe iz potvrđenog međunarodnog ugovora ili pravnih tekovina Evropske unije. Vanredan inspekcijski nadzor vrši se: kada je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode, nesmetan rad organa i organizacija, komunalni red ili bezbednost; kada se posle donošenja godišnjeg	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	
	The results of any targeted security audit shall be made available to the competent authority. The		plana inspekcijskog nadzora proceni da je rizik visok ili kritičan ili promene okolnosti; kada takav			

	costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.		nadzor zahteva nadzirani subjekat; radi sprečavanja obavljanja delatnosti i vršenja aktivnosti neregistrovanih subjekata; po zahtevu javnog tužioca; kada se postupa po predstavci pravnog ili fizičkog lica; kada drugostepeni organ preko inspekcije dopunjava postupak ili ponavlja ceo postupak ili njegov deo, a nisu ispunjeni uslovi za dopunski inspekcijski nadzor. Vanredan inspekcijski nadzor po zahtevu nadziranog subjekta može biti utvrđujući, koji se vrši kada je potrebno utvrditi ispunjenost propisanih uslova nakon čijeg ispunjenja nadzirani subjekat stiče pravo za početak rada ili obavljanja delatnosti, vršenja aktivnosti ili ostvarivanje određenog prava, u skladu sa posebnim zakonom, ili potvrđujući, koji se vrši kada nadzirani subjekat podnese zahtev da se potvrdi zakonitost i bezbednost postupanja u vršenju određenog prava ili izvršenju određene obaveze, odnosno u njegovom poslovanju. Mešoviti inspekcijski nadzor vrši se istovremeno kao redovan i vanredan nadzor kod istog nadziranog subjekta, kada se predmet redovnog i vanrednog inspekcijskog nadzora delimično ili u celosti poklapaju ili su povezani. Kontrolni inspekcijski nadzor vrši se radi utvrđivanja izvršenja mera koje su predložene ili naložene nadziranom subjektu u okviru redovnog ili vanrednog inspekcijskog nadzora. Dopunski inspekcijski nadzor vrši se po službenoj dužnosti ili povodom zahteva nadziranog subjekta, radi utvrđivanja činjenica koje su od značaja za inspekcijski nadzor, a koje nisu utvrđene u redovnom, vanrednom, mešovitom ili kontrolnom inspekcijskom nadzoru, s tim da se može izvršiti samo jedan dopunski inspekcijski nadzor, u roku koji ne može biti duži od 30 dana od okončanja redovnog, vanrednog ili kontrolnog inspekcijskog nadzora. Oblici inspekcijskog nadzora Član 7. Inspekcijski nadzor, prema obliku, može biti terenski i kancelarijski. Terenski inspekcijski nadzor vrši se izvan službenih prostorija inspekcije, na licu mesta i sastoji se od			

			neposrednog uvida u zemljište, objekte, postrojenja, uređaje, prostorije, vozila i druga namenska prevozna sredstva, predmete, robu i druge predmete, akte i dokumentaciju nadziranog subjekta. Kancelarijski inspekcijski nadzor vrši se u službenim prostorijama inspekcije, uvidom u akte, podatke i dokumentaciju nadziranog subjekta. Prava i dužnosti nadziranog subjekta Član 20. Nadzirani subjekti imaju jednaka prava i obaveze u inspekcijskom nadzoru, što uključuje i pravo da inspekcija jednako postupa u istim ili bitno sličnim situacijama prema svim nadziranim subjektima. Nadzirani subjekat u postupku inspekcijskog nadzora ima pravo: da bude upoznat sa predmetom i trajanjem postupka, nalogom za inspekcijski nadzor i drugim aktima donetim u postupku; da bude upoznat sa pravima i dužnostima koje ima u vezi sa inspekcijskim nadzorom; da se izjasni o činjenicama bitnim za potpuno i pravilno utvrđivanje činjeničnog stanja i ponuđenim dokazima; da učestvuje u izvođenju dokaza, postavlja pitanja svedocima i veštacima, iznosi činjenice koje su od značaja za inspekcijski nadzor; da predlaže dokaze i iznosi pravne tvrdnje; da zahteva preventivno delovanje; da upozori inspektora na tajnost informacija koje mu čini dostupnim; da ukaže na nezakonitosti u postupku i da zahteva da se one otklone; da zahteva naknadu štete koja mu je prouzrokovana nezakonitim inspekcijskim nadzorom. Ako više inspekcija vrši zajednički nadzor, nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava koje je dao jednom od inspektora u tom nadzoru. Nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava o predmetu ranije izvršenog nadzora, osim ako su se ti podaci u međuvremenu promenili, kao i kada je davanje podataka neophodno radi preduzimanja hitnih mera radi sprečavanja ili otklanjanja opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Kada je uredno obavešten o predstojećem inspekcijskom nadzoru, nadzirani subjekat dužan je			

			da bude prisutan na mestu vršenja nadzora, osim ako postoje naročito opravdane okolnosti koje ga u tome sprečavaju, o čemu je dužan da blagovremeno na podesan način obavesti inspekciju. Ako nadzirani subjekat koji je uredno obavešten o predstojećem inspekcijskom nadzoru ne bude prisutan na mestu vršenja nadzora, a ne postoje okolnosti iz stava 5. ovog člana, inspekcijski nadzor se vrši u prisustvu službenog ili drugog lica koje se zatekne na mestu vršenja inspekcijskog nadzora. Nadzirani subjekat dužan je da inspektoru koji mu predoči službenu legitimaciju i uruči nalog za inspekcijski nadzor, kada je on izdat, odnosno koji postupi u skladu sa članom 18. st. 8. i 9. ovog zakona, omogući nesmetan inspekcijski nadzor, što podrazumeva naročito da: stavi na raspolaganje odgovarajući radni prostor za terenski nadzor; obezbedi uvid u poslovne knjige, opšte i pojedinačne akte, evidencije, izveštaje, ugovore, privatne isprave i drugu dokumentaciju nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih poseduje i čuva; omogući pristup lokaciji, zemljištu, objektima, poslovnom i drugom nestambenom prostoru, postrojenjima, uređajima, opremi, priboru, vozilima i drugim namenskim prevoznim sredstvima, drugim sredstvima rada, proizvodima, predmetima koji se stavljaju u promet, robi u prometu i drugim predmetima kojima obavlja delatnost ili vrši aktivnost, kao i drugim predmetima od značaja za inspekcijski nadzor; blagovremeno pruži potpune i tačne podatke koji su mu dostupni, a ako nešto od toga ne može – da razloge za to pisano obrazloži inspektoru. Nadzirani subjekat dužan je da se na zahtev inspektora usmeno ili pisano izjasni o predmetu nadzora. Nadzirani subjekat dužan je da poštuje integritet i službeno svojstvo inspektora. Nadzirani subjekat ima i druga prava i obaveze utvrđene ovim i drugim zakonom. Ovlašćenja inspektora radi utvrđivanja činjenica Član 21. Inspektor je ovlašćen da radi utvrđivanja činjenica: 1) izvrši uvid u javne isprave i podatke iz registara i		

			evidencija koje vode nadležni državni organi, organi autonomne pokrajine i organi jedinice lokalne samouprave i drugi imaoci javnih ovlašćenja ako su neophodni za inspekcijski nadzor, a nije mogao da ih pribavi po službenoj dužnosti, i da ih kopira, u skladu sa zakonom; 2) izvrši uvid u ličnu ili drugu javnu ispravu sa fotografijom koja je podobna da se identifikuju ovlašćena lica u nadziranom subjektu, druga zaposlena ili radno angažovana lica, fizička lica koja su nadzirani subjekti, svedoci, službena lica i zainteresovana lica, kao i fizička lica zatečena na mestu nadzora; 3) uzima pisane i usmene izjave nadziranih subjekata – fizičkih lica i zastupnika, odnosno ovlašćenih lica u nadziranom subjektu – pravnom licu i drugih zaposlenih ili radno angažovanih lica, svedoka, službenih lica i zainteresovanih lica, i da ih poziva da daju izjave o pitanjima od značaja za inspekcijski nadzor; 4) naloži da mu se u određenom roku stave na uvid poslovne knjige, opšti i pojedinačni akti, evidencije, ugovori i druga dokumentacija nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih nadzirani subjekat poseduje i čuva; 5) vrši uviđaj, odnosno pregleda i proverava lokaciju, zemljište, objekte, poslovni i drugi nestambeni prostor, postrojenja, uređaje, opremu, pribor, vozila i druga namenska prevozna sredstva, druga sredstva rada, proizvode, predmete koji se stavljaju u promet, robu u prometu i druge predmete kojima obavlja delatnost ili vrši aktivnost, kao i druge predmete od značaja za inspekcijski nadzor; 6) uzme potrebne uzorke radi njihovog ispitivanja i utvrđivanja činjeničnog stanja, u skladu sa posebnim zakonom i propisima donetim na osnovu zakona; 7) fotografiše i snimi prostor u kome se vrši inspekcijski nadzor i druge stvari koje su predmet nadzora; 7a) obezbedi dokaze; 8) preduzme druge radnje radi utvrđivanja činjeničnog stanja prema ovom i posebnom zakonu. Ako nadzirani subjekat obavlja delatnost preko organizacionih jedinica u svom sastavu koje se		

			nalaze na različitim adresama, inspekcijski nadzor u pogledu zajedničkih elemenata poslovanja ili postupanja i unutrašnjih pravila, opštih akata i procesa nadziranog subjekta vrši inspekcija nadležna prema mestu sedišta tog nadziranog subjekta. U vršenju inspekcijskog nadzora prema organizacionoj jedinici nadziranog subjekta iz stava 2. ovog člana, inspekcija nadležna za inspekcijski nadzor nad poslovanjem organizacione jedinice dužna je da pribavi podatke i informacije o zajedničkim elementima poslovanja ili postupanja, unutrašnjim pravilima, opštim aktima i procesima ovog subjekta od inspekcije nadležne prema mestu sedišta tog nadziranog subjekta. U slučaju neujednačenog postupanja inspekcije ili više inspekcija u vršenju inspekcijskog nadzora prema organizacionim jedinicima nadziranog subjekta iz stava 2. ovog člana, ovaj subjekat, odnosno inspekcija može da zatraži akt o primeni propisa od nadležnog organa ili organizacije. Inspektor se stara o tome da vršenjem svojih ovlašćenja ne ometa redovan proces rada, odnosno obavljanja delatnosti i vršenja aktivnosti nadziranog subjekta. Istovetnost kopija i originala dokumentacije nadziranog subjekta potvrđuje nadzirani subjekat svojim pečatom i potpisom. Ministar nadležan za odgovarajuću oblast inspekcijskog nadzora, odnosno imalac javnih ovlašćenja koji vrši inspekcijski nadzor u određenoj oblasti, ovlašćen je da bliže uredi uslove i način uzimanja i ispitivanja uzoraka.			
32.3.	When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.	3.16.1. 3.16.2.	Nalog za inspekcijski nadzor Član 16. Rukovodilac inspekcije ili lice koje on ovlasti izdaje pisani nalog za inspekcijski nadzor. Nalog za inspekcijski nadzor sadrži: podatke o inspekciji; podatke o inspektoru ili inspektorima koji vrše inspekcijski nadzor sa brojevima službenih legitimacija; podatke o nadziranom subjektu ili subjektima ako su poznati, a ako ti podaci nisu poznati, odnosno ako nije moguće utvrditi nadzirane subjekte ili je njihov broj prevelik – odgovarajuće	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			poznate informacije od značaja za određenje subjekta, odnosno subjekata kod kojih će se vršiti nadzor (npr.: vrsta delatnosti ili aktivnosti, teritorijalno područje, lokacija objekta, vrsta robe ili proizvoda, odnosno usluga itd.); pravni osnov inspekcijskog nadzora; navođenje i kratko objašnjenje vrste i oblika inspekcijskog nadzora; procenjeni rizik; precizan i jasan opis predmeta inspekcijskog nadzora; planirano trajanje inspekcijskog nadzora (dan početka i okončanja nadzora); razloge za izostavljanje obaveštenja, ako postoje; broj, vreme i mesto izdavanja; potpis izdavaoca naloga; pečat, kada je to potrebno prema obeležjima predmeta inspekcijskog nadzora.			
32.4.	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: (a)issue warnings about infringements of this Directive by the entities concerned; (b)adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive; (c)order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct; (d)order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period; (e)order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective	1.48. 3.25. 3.26. 3.27. 3.28.	Član 48. Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Mere upravljene prema nadziranom subjektu i njihova srazmernost Član 25. Nadziranom subjektu inspektor može izreći upravnu meru, i to preventivnu meru, meru za otklanjanje nezakonitosti, posebnu meru naredbe, zabrane ili	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

	or remedial measures which can be taken by those natural or legal persons in response to that threat; (f)order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline; (g)designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23; (h)order the entities concerned to make public aspects of infringements of this Directive in a specified manner; (i)impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.		zaplene ili meru za zaštitu prava trećih lica. Inspektor izriče one mere koje su srazmerne procenjenom riziku i otkrivenim, odnosno verovatnim nezakonitostima i štetnim posledicama, tako da se rizikom delotvorno upravlja, i kojima se najpovoljnije po nadziranog subjekta postižu cilj i svrha zakona i drugog propisa. Inspektor se obavezno stara o tome da mere iz stava 2. ovog člana budu srazmerne ekonomskoj snazi nadziranog subjekta, da se njihove štetne posledice svedu na najmanju meru i nastavi održivo poslovanje i razvoj nadziranog subjekta. Preventivne mere Član 26. Inspektor u zapisniku određuje odgovarajuće preventivne mere, ako je to potrebno da bi se sprečio nastanak nezakonitosti i štetnih posledica. Ako nadzirani subjekat ne postupi po preventivnim merama određenim u zapisniku, inspektor izriče te mere rešenjem. Preventivne mere jesu: 1) upozoravanje nadziranog subjekta o njegovim obavezama iz zakona i drugih propisa, kao i o propisanim radnjama i merama upravljenim prema nadziranom subjektu i sankcijama za postupanja suprotna tim obavezama; 2) ukazivanje nadziranom subjektu na mogućnost nastupanja štetnih posledica njegovog poslovanja ili postupanja; 3) nalaganje nadziranom subjektu preduzimanja ili uzdržavanja od određenih radnji radi otklanjanja uzroka verovatnih štetnih posledica, kao i odgovarajućih mera predostrožnosti u cilju sprečavanja nastanka mogućih štetnih posledica; 4) druge mere kojima se postiže preventivna uloga inspekcijskog nadzora. Preventivne mere mogu se izreći i nepoznatom subjektu inspekcijskog nadzora. Neregistrovanom subjektu se ne može izreći preventivna mera. Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju			

			nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti. Posebne mere naredbe, zabrane i zaplene Član 28. Ako nadzirani subjekat ne otkloni nezakonitost u		

			ostavljenom roku, inspektor je ovlašćen da donese rešenje i izrekne meru kojom, do otklanjanja nezakonitosti, nadziranom subjektu zabranjuje obavljanje delatnosti ili vršenje aktivnosti ili zaplenjuje dokumentaciju, robu i druge predmete koji su nadziranom subjektu poslužili za povredu propisa ili su time nastali. Inspektor je ovlašćen da, bez ostavljanja roka za otklanjanje nezakonitosti, izrekne meru zabrane obavljanja delatnosti ili vršenja aktivnosti ili zaplene predmeta ili dokumentacije ako je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu veće vrednosti, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode veće vrednosti, nesmetan rad organa i organizacija, komunalni red ili bezbednost. Inspektor koji zabrani obavljanje delatnosti ili vršenje aktivnosti ima pravo da naredi da se nadziranom subjektu zapečate poslovne i proizvodne prostorije, objekti i drugi prostor u kome obavlja delatnost ili vrši aktivnost ili koji tome služi, postrojenja, uređaji, oprema, pribor, sredstva rada i drugi predmeti kojima obavlja delatnost ili vrši aktivnost. Inspektor može izreći i drugu posebnu meru naredbe, zabrane ili zaplene (npr. mera povlačenja ili opozivanja proizvoda, mere ograničenja, mera uništavanja predmeta, mera uklanjanja objekta i dr), kad je to određeno posebnim zakonom.			
32.5.	Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to: (a)suspend temporarily, or request a certification or	1.48. 3.27.	Član 48. Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

	authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity; (b)request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity. Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such enforcement measures were applied. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence. The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Directive.		penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim			

			izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti.			
32.6.	Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive. As regards public administration entities, this paragraph shall be without prejudice to national law as regards the liability of public servants and elected or appointed officials.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno	PU		

			lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog		

			značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
32.7.	When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of: (a)the seriousness of the infringement and the	3.27. 4.42. 4.43.	Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

	importance of the provisions breached, the following, inter alia, constituting serious infringement in any event: (i)repeated violations; (ii)a failure to notify or remedy significant incidents; (iii)a failure to remedy deficiencies following binding instructions from competent authorities; (iv)the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement; (v)providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23; (b)the duration of the infringement; (c)any relevant previous infringements by the entity concerned; (d)any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected; (e)any intent or negligence on the part of the perpetrator of the infringement; (f)any measures taken by the entity to prevent or mitigate the material or non-material damage; (g)any adherence to approved codes of conduct or approved certification mechanisms; (h)the level of cooperation of the natural or legal persons held responsible with the competent authorities.		ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti. Odmeravanje kazne Član 42. Kazna za prekršaje odmerava se u granicama koje su za taj prekršaj propisane, a pri tome se uzimaju u obzir sve okolnosti koje utiču da kazna bude veća ili manja, a naročito: težina i posledice prekršaja, okolnosti pod kojima je prekršaj učinjen, stepen odgovornosti učinioca, ranija osuđivanost, lične			

			prilike učinioca i držanje učinioca posle učinjenog prekršaja. Ne može se uzeti u obzir kao otežavajuća okolnost ranije izrečena prekršajna sankcija učiniocu ako je od dana pravnosnažnosti odluke do dana donošenja nove proteklo više od četiri godine. Pri odmeravanju visine novčane kazne uzeće se u obzir i imovno stanje učinioca. Ublažavanje kazne Član 43. Ako se prilikom odmeravanja kazne utvrdi da prekršajem nisu prouzrokovane teže posledice, a postoje olakšavajuće okolnosti koje ukazuju da se i blažom kaznom može postići svrha kažnjavanja, propisana kazna se može ublažiti tako što se može: 1) izreći kazna ispod najmanje mere kazne koja je propisana za taj prekršaj ali ne ispod najmanje zakonske mere te vrste kazne; 2) umesto propisane kazne zatvora izreći novčana kazna ili rad u javnom interesu, ali ne ispod najmanje zakonske mere te vrste kazne; 3) umesto propisane kazne zatvora i novčane kazne izreći samo jedna od tih kazni.			
32.8.	The competent authorities shall set out a detailed reasoning for their enforcement measures. Before adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.	3.35. 3.36.	Zapisnik o inspekcijskom nadzoru Član 35. Inspektor sačinjava zapisnik o inspekcijskom nadzoru. U zapisnik se unose: podaci iz naloga za inspekcijski nadzor ako je izdat; vreme i mesto inspekcijskog nadzora, a naročito navođenje osnova i obrazloženje razloga koji su uslovili da se inspekcijski nadzor vrši van radnog vremena nadziranog subjekta u smislu člana 19. stav 2. ovog zakona; opis preduzetih radnji i popis preuzetih dokumenata; podaci o broju uzetih uzoraka i predlozima koje u vezi sa uzimanjem uzoraka daje ovlašćeno lice nadziranog subjekta; izjave koje su date; opis drugih izvedenih dokaza; zahtevi za izuzeće koji su podneti; utvrđeno činjenično stanje; konstatacija zakonitog poslovanja i postupanja nadziranog subjekta; opis otkrivenih nezakonitosti, sa navođenjem dokaza na osnovu kojeg je određena	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			činjenica utvrđena i pravnog osnova za utvrđivanje nezakonitosti; mere koje se izriču sa navođenjem pravnog osnova na kome su zasnovane i rokom za postupanje po njima; odgovarajuća obrazloženja; obaveza nadziranog subjekta da obaveštava inspektora o postupanju po merama i rok za to obaveštavanje; podaci o podnetim krivičnim prijavama, prijavama za privredni prestup i zahtevima za pokretanje prekršajnog postupka, ako su podnete, odnosno izdatim prekršajnim nalozima, ako su izdati, odnosno, u skladu sa članom 42. stav 3. ovog zakona, nepodnošenje zahteva za pokretanje prekršajnog postupka, odnosno neizdavanje prekršajnog naloga; podaci o drugim merama i radnjama na koje je inspektor ovlašćen, ako su preduzete; rok za davanje primedaba na zapisnik; navođenje da je zapisnik sa ili bez primedaba pročitan licu koje prisustvuje nadzoru; drugi podaci i navodi od značaja za inspekcijski nadzor. Kontrolna lista i analiza odgovarajuće stručne institucije, odnosno akreditovanog tela čine sastavni deo zapisnika. Ovlašćeno lice nadziranog subjekta može da odbije da primi zapisnik, što inspektor konstatuje u pisanom obliku i u zapisniku navodi razloge zbog kojih je prijem zapisnika odbijen. Zapisnik se dostavlja nadziranom subjektu u roku od osam dana od završetka inspekcijskog nadzora. Opšti obrazac zapisnika o inspekcijskom nadzoru propisuje ministar nadležan za poslove državne uprave. Opšti obrazac zapisnika o inspekcijskom nadzoru za inspekcijski nadzor iz izvorne nadležnosti autonomne pokrajine i jedinice lokalne samouprave propisuje nadležni organ autonomne pokrajine ili jedinice lokalne samouprave. Primedbe na zapisnik Član 36. Nadzirani subjekat ima pravo da u pisanom obliku stavi primedbe na zapisnik o inspekcijskom nadzoru, u roku od pet radnih dana od njegovog prijema. Inspektor ocenjuje primedbe, sve zajedno i svaku zasebno, i u međusobnoj vezi.		

			Inspektor može posle toga da izvrši dopunski inspekcijski nadzor, da bi utvrdio činjenice na koje se primedbe odnose. Ako su u primedbama na zapisnik iznete nove činjenice i novi dokazi, zbog kojih treba izmeniti činjenično stanje koje je utvrđeno u zapisniku ili drukčije pravne i druge ocene, inspektor o tome sastavlja dopunu zapisnika, na koju se ne može staviti primedba. Postupajući po primedbama na zapisnik, inspektor može da izmeni predloženu ili naloženu, odnosno izrečenu meru ili da odustane od nje.			
32.9.	Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive. Where appropriate, the competent authorities under Directive (EU) 2022/2557 may request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557.	3.5.	Saradnja sa drugim organima, imaocima javnih ovlašćenja i pravnim i fizičkim licima Član 5. Saradnja nadležne inspekcije sa drugim organima državne uprave, organima autonomne pokrajine i jedinice lokalne samouprave, pravosudnim i drugim državnim organima i drugim zainteresovanim organima i organizacijama ostvaruje se u skladu sa nadležnostima inspekcije i oblicima saradnje utvrđenim propisima o državnoj upravi i posebnim zakonima. Saradnja, naročito, obuhvata međusobno obaveštavanje, razmenu podataka, pružanje pomoći i zajedničke mere i radnje od značaja za inspekcijski nadzor. Nadležna inspekcija u obavljanju poslova iz svog delokruga usklađuje planove inspekcijskog nadzora i svog rada, razmenjuje podatke, predlaže preduzimanje zajedničkih mera i aktivnosti od značaja za obavljanje poslova inspekcijskog nadzora i na drugi način sarađuje sa drugim inspekcijama i subjektima sa javnim ovlašćenjima koji vrše posebne oblike nadzora i kontrole – radi obavljanja obuhvatnijeg i delotvornijeg inspekcijskog nadzora i naročito radi suzbijanja delatnosti ili aktivnosti neregistrovanih subjekata. Državni organi, organi autonomne pokrajine i jedinice lokalne samouprave i imaoci javnih ovlašćenja dužni su, na zahtev inspektora, da mu u roku od 15 dana od prijema zahteva dostave tražene podatke i obaveštenja koji su značajni za inspekcijski nadzor.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			Nadležna inspekcija, u skladu sa zakonom, sarađuje sa fizičkim i pravnim licima, naročito u cilju preventivnog delovanja, kao i unapređenja uzajamne odgovornosti fizičkih i pravnih lica i inspekcija u procesu primene i nadzora nad primenom propisa. U tom cilju, inspekcija može održavati informativne i edukativne tribine i konsultativne sastanke sa predstavnicima privatnog sektora i drugim zainteresovanim stranama. Fizička i pravna lica mogu inspekciji podnositi predstavke i zahteve, i od nje tražiti podatke i obaveštenja, u skladu sa zakonom. Ako se u vezi sa vršenjem inspekcijskog nadzora osnovano očekuje da nadzirani subjekat pruži otpor ili se on pruži i inspektoru onemogućava ili bitno otežava vršenje inspekcijskog nadzora, inspektor može da zahteva pomoć policije i komunalne policije. Policija i komunalna policija pružaju pomoć prema zakonima kojima se uređuju policija i komunalna policija.			
32.10.	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.	3.5.	Saradnja sa drugim organima, imaocima javnih ovlašćenja i pravnim i fizičkim licima Član 5. Saradnja nadležne inspekcije sa drugim organima državne uprave, organima autonomne pokrajine i jedinice lokalne samouprave, pravosudnim i drugim državnim organima i drugim zainteresovanim organima i organizacijama ostvaruje se u skladu sa nadležnostima inspekcije i oblicima saradnje utvrđenim propisima o državnoj upravi i posebnim zakonima. Saradnja, naročito, obuhvata međusobno obaveštavanje, razmenu podataka, pružanje pomoći i zajedničke mere i radnje od značaja za inspekcijski nadzor. Nadležna inspekcija u obavljanju poslova iz svog delokruga usklađuje planove inspekcijskog nadzora i svog rada, razmenjuje podatke, predlaže preduzimanje zajedničkih mera i aktivnosti od značaja za obavljanje poslova inspekcijskog nadzora i na drugi način sarađuje sa drugim inspekcijama i subjektima sa javnim ovlašćenjima koji vrše posebne oblike nadzora i kontrole – radi obavljanja obuhvatnijeg i delotvornijeg inspekcijskog nadzora i	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			naročito radi suzbijanja delatnosti ili aktivnosti neregistrovanih subjekata. Državni organi, organi autonomne pokrajine i jedinice lokalne samouprave i imaoci javnih ovlašćenja dužni su, na zahtev inspektora, da mu u roku od 15 dana od prijema zahteva dostave tražene podatke i obaveštenja koji su značajni za inspekcijski nadzor. Nadležna inspekcija, u skladu sa zakonom, sarađuje sa fizičkim i pravnim licima, naročito u cilju preventivnog delovanja, kao i unapređenja uzajamne odgovornosti fizičkih i pravnih lica i inspekcija u procesu primene i nadzora nad primenom propisa. U tom cilju, inspekcija može održavati informativne i edukativne tribine i konsultativne sastanke sa predstavnicima privatnog sektora i drugim zainteresovanim stranama. Fizička i pravna lica mogu inspekciji podnositi predstavke i zahteve, i od nje tražiti podatke i obaveštenja, u skladu sa zakonom. Ako se u vezi sa vršenjem inspekcijskog nadzora osnovano očekuje da nadzirani subjekat pruži otpor ili se on pruži i inspektoru onemogućava ili bitno otežava vršenje inspekcijskog nadzora, inspektor može da zahteva pomoć policije i komunalne policije. Policija i komunalna policija pružaju pomoć prema zakonima kojima se uređuju policija i komunalna policija.			
33.1.	***Supervisory and enforcement measures in relation to important entities*** When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1.48. 3.6. 3.7. 3.20. 3.21.	Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Vrste inspekcijskog nadzora Član 6. Inspekcijski nadzor, prema vrsti, može biti redovan, vanredan, mešoviti, kontrolni i dopunski. Redovan inspekcijski nadzor vrši se prema planu inspekcijskog nadzora. Inspekcijski nadzor na državnoj granici, koji se obavlja redovno, upodobljava se redovnom inspekcijskom nadzoru i na njega se shodno primenjuju odredbe ovog zakona, ako ovim ili posebnim zakonom nije drugačije određeno, odnosno kada to proističe iz potvrđenog međunarodnog ugovora ili pravnih tekovina Evropske unije. Vanredan inspekcijski nadzor vrši se: kada je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode, nesmetan rad organa i organizacija, komunalni red ili bezbednost; kada se posle donošenja godišnjeg plana inspekcijskog nadzora proceni da je rizik visok ili kritičan ili promene okolnosti; kada takav nadzor zahteva nadzirani subjekat; radi sprečavanja obavljanja delatnosti i vršenja aktivnosti neregistrovanih subjekata; po zahtevu javnog tužioca; kada se postupa po predstavci pravnog ili fizičkog lica; kada drugostepeni organ preko inspekcije dopunjava postupak ili ponavlja ceo postupak ili njegov deo, a nisu ispunjeni uslovi za dopunski inspekcijski nadzor. Vanredan inspekcijski nadzor po zahtevu nadziranog subjekta može biti utvrđujući, koji se vrši kada je potrebno utvrditi ispunjenost propisanih uslova nakon čijeg ispunjenja nadzirani subjekat			

			stiče pravo za početak rada ili obavljanja delatnosti, vršenja aktivnosti ili ostvarivanje određenog prava, u skladu sa posebnim zakonom, ili potvrđujući, koji se vrši kada nadzirani subjekat podnese zahtev da se potvrdi zakonitost i bezbednost postupanja u vršenju određenog prava ili izvršenju određene obaveze, odnosno u njegovom poslovanju. Mešoviti inspekcijski nadzor vrši se istovremeno kao redovan i vanredan nadzor kod istog nadziranog subjekta, kada se predmet redovnog i vanrednog inspekcijskog nadzora delimično ili u celosti poklapaju ili su povezani. Kontrolni inspekcijski nadzor vrši se radi utvrđivanja izvršenja mera koje su predložene ili naložene nadziranom subjektu u okviru redovnog ili vanrednog inspekcijskog nadzora. Dopunski inspekcijski nadzor vrši se po službenoj dužnosti ili povodom zahteva nadziranog subjekta, radi utvrđivanja činjenica koje su od značaja za inspekcijski nadzor, a koje nisu utvrđene u redovnom, vanrednom, mešovitom ili kontrolnom inspekcijskom nadzoru, s tim da se može izvršiti samo jedan dopunski inspekcijski nadzor, u roku koji ne može biti duži od 30 dana od okončanja redovnog, vanrednog ili kontrolnog inspekcijskog nadzora. Oblici inspekcijskog nadzora Član 7. Inspekcijski nadzor, prema obliku, može biti terenski i kancelarijski. Terenski inspekcijski nadzor vrši se izvan službenih prostorija inspekcije, na licu mesta i sastoji se od neposrednog uvida u zemljište, objekte, postrojenja, uređaje, prostorije, vozila i druga namenska prevozna sredstva, predmete, robu i druge predmete, akte i dokumentaciju nadziranog subjekta. Kancelarijski inspekcijski nadzor vrši se u službenim prostorijama inspekcije, uvidom u akte, podatke i dokumentaciju nadziranog subjekta. Prava i dužnosti nadziranog subjekta Član 20. Nadzirani subjekti imaju jednaka prava i obaveze u inspekcijskom nadzoru, što uključuje i pravo da		

			inspekcija jednako postupa u istim ili bitno sličnim situacijama prema svim nadziranim subjektima. Nadzirani subjekat u postupku inspekcijskog nadzora ima pravo: da bude upoznat sa predmetom i trajanjem postupka, nalogom za inspekcijski nadzor i drugim aktima donetim u postupku; da bude upoznat sa pravima i dužnostima koje ima u vezi sa inspekcijskim nadzorom; da se izjasni o činjenicama bitnim za potpuno i pravilno utvrđivanje činjeničnog stanja i ponuđenim dokazima; da učestvuje u izvođenju dokaza, postavlja pitanja svedocima i veštacima, iznosi činjenice koje su od značaja za inspekcijski nadzor; da predlaže dokaze i iznosi pravne tvrdnje; da zahteva preventivno delovanje; da upozori inspektora na tajnost informacija koje mu čini dostupnim; da ukaže na nezakonitosti u postupku i da zahteva da se one otklone; da zahteva naknadu štete koja mu je prouzrokovana nezakonitim inspekcijskim nadzorom. Ako više inspekcija vrši zajednički nadzor, nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava koje je dao jednom od inspektora u tom nadzoru. Nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava o predmetu ranije izvršenog nadzora, osim ako su se ti podaci u međuvremenu promenili, kao i kada je davanje podataka neophodno radi preduzimanja hitnih mera radi sprečavanja ili otklanjanja opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Kada je uredno obavešten o predstojećem inspekcijskom nadzoru, nadzirani subjekat dužan je da bude prisutan na mestu vršenja nadzora, osim ako postoje naročito opravdane okolnosti koje ga u tome sprečavaju, o čemu je dužan da blagovremeno na podesan način obavesti inspekciju. Ako nadzirani subjekat koji je uredno obavešten o predstojećem inspekcijskom nadzoru ne bude prisutan na mestu vršenja nadzora, a ne postoje okolnosti iz stava 5. ovog člana, inspekcijski nadzor se vrši u prisustvu službenog ili drugog lica koje se zatekne na mestu vršenja inspekcijskog nadzora. Nadzirani subjekat dužan je da inspektoru koji mu predoči službenu legitimaciju i uruči nalog za			

			inspekcijski nadzor, kada je on izdat, odnosno koji postupi u skladu sa članom 18. st. 8. i 9. ovog zakona, omogući nesmetan inspekcijski nadzor, što podrazumeva naročito da: stavi na raspolaganje odgovarajući radni prostor za terenski nadzor; obezbedi uvid u poslovne knjige, opšte i pojedinačne akte, evidencije, izveštaje, ugovore, privatne isprave i drugu dokumentaciju nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih poseduje i čuva; omogući pristup lokaciji, zemljištu, objektima, poslovnom i drugom nestambenom prostoru, postrojenjima, uređajima, opremi, priboru, vozilima i drugim namenskim prevoznim sredstvima, drugim sredstvima rada, proizvodima, predmetima koji se stavljaju u promet, robi u prometu i drugim predmetima kojima obavlja delatnost ili vrši aktivnost, kao i drugim predmetima od značaja za inspekcijski nadzor; blagovremeno pruži potpune i tačne podatke koji su mu dostupni, a ako nešto od toga ne može – da razloge za to pisano obrazloži inspektoru. Nadzirani subjekat dužan je da se na zahtev inspektora usmeno ili pisano izjasni o predmetu nadzora. Nadzirani subjekat dužan je da poštuje integritet i službeno svojstvo inspektora. Nadzirani subjekat ima i druga prava i obaveze utvrđene ovim i drugim zakonom. Ovlašćenja inspektora radi utvrđivanja činjenica Član 21. Inspektor je ovlašćen da radi utvrđivanja činjenica: 1) izvrši uvid u javne isprave i podatke iz registara i evidencija koje vode nadležni državni organi, organi autonomne pokrajine i organi jedinice lokalne samouprave i drugi imaoci javnih ovlašćenja ako su neophodni za inspekcijski nadzor, a nije mogao da ih pribavi po službenoj dužnosti, i da ih kopira, u skladu sa zakonom; 2) izvrši uvid u ličnu ili drugu javnu ispravu sa fotografijom koja je podobna da se identifikuju ovlašćena lica u nadziranom subjektu, druga zaposlena ili radno angažovana lica, fizička lica koja su nadzirani subjekti, svedoci, službena lica i zainteresovana lica, kao i fizička lica zatečena na			

			mestu nadzora; 3) uzima pisane i usmene izjave nadziranih subjekata – fizičkih lica i zastupnika, odnosno ovlašćenih lica u nadziranom subjektu – pravnom licu i drugih zaposlenih ili radno angažovanih lica, svedoka, službenih lica i zainteresovanih lica, i da ih poziva da daju izjave o pitanjima od značaja za inspekcijski nadzor; 4) naloži da mu se u određenom roku stave na uvid poslovne knjige, opšti i pojedinačni akti, evidencije, ugovori i druga dokumentacija nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih nadzirani subjekat poseduje i čuva; 5) vrši uviđaj, odnosno pregleda i proverava lokaciju, zemljište, objekte, poslovni i drugi nestambeni prostor, postrojenja, uređaje, opremu, pribor, vozila i druga namenska prevozna sredstva, druga sredstva rada, proizvode, predmete koji se stavljaju u promet, robu u prometu i druge predmete kojima obavlja delatnost ili vrši aktivnost, kao i druge predmete od značaja za inspekcijski nadzor; 6) uzme potrebne uzorke radi njihovog ispitivanja i utvrđivanja činjeničnog stanja, u skladu sa posebnim zakonom i propisima donetim na osnovu zakona; 7) fotografiše i snimi prostor u kome se vrši inspekcijski nadzor i druge stvari koje su predmet nadzora; 7a) obezbedi dokaze; 8) preduzme druge radnje radi utvrđivanja činjeničnog stanja prema ovom i posebnom zakonu. Ako nadzirani subjekat obavlja delatnost preko organizacionih jedinica u svom sastavu koje se nalaze na različitim adresama, inspekcijski nadzor u pogledu zajedničkih elemenata poslovanja ili postupanja i unutrašnjih pravila, opštih akata i procesa nadziranog subjekta vrši inspekcija nadležna prema mestu sedišta tog nadziranog subjekta. U vršenju inspekcijskog nadzora prema organizacionoj jedinici nadziranog subjekta iz stava 2. ovog člana, inspekcija nadležna za inspekcijski nadzor nad poslovanjem organizacione jedinice dužna je da pribavi podatke i informacije o zajedničkim elementima poslovanja ili postupanja,			

			unutrašnjim pravilima, opštim aktima i procesima ovog subjekta od inspekcije nadležne prema mestu sedišta tog nadziranog subjekta. U slučaju neujednačenog postupanja inspekcije ili više inspekcija u vršenju inspekcijskog nadzora prema organizacionim jedinicima nadziranog subjekta iz stava 2. ovog člana, ovaj subjekat, odnosno inspekcija može da zatraži akt o primeni propisa od nadležnog organa ili organizacije. Inspektor se stara o tome da vršenjem svojih ovlašćenja ne ometa redovan proces rada, odnosno obavljanja delatnosti i vršenja aktivnosti nadziranog subjekta. Istovetnost kopija i originala dokumentacije nadziranog subjekta potvrđuje nadzirani subjekat svojim pečatom i potpisom. Ministar nadležan za odgovarajuću oblast inspekcijskog nadzora, odnosno imalac javnih ovlašćenja koji vrši inspekcijski nadzor u određenoj oblasti, ovlašćen je da bliže uredi uslove i način uzimanja i ispitivanja uzoraka.			
33.2.	Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to: (a)on-site inspections and off-site ex post supervision conducted by trained professionals; (b)targeted security audits carried out by an independent body or a competent authority; (c)security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned; (d)requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;	1.48. 3.6. 3.7. 3.20. 3.21.	Ovlašćenja inspektora za informacionu bezbednost 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 utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

	(e)requests to access data, documents and information necessary to carry out their supervisory tasks; (f)requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information. The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.		Vrste inspekcijskog nadzora Član 6. Inspekcijski nadzor, prema vrsti, može biti redovan, vanredan, mešoviti, kontrolni i dopunski. Redovan inspekcijski nadzor vrši se prema planu inspekcijskog nadzora. Inspekcijski nadzor na državnoj granici, koji se obavlja redovno, upodobljava se redovnom inspekcijskom nadzoru i na njega se shodno primenjuju odredbe ovog zakona, ako ovim ili posebnim zakonom nije drugačije određeno, odnosno kada to proističe iz potvrđenog međunarodnog ugovora ili pravnih tekovina Evropske unije. Vanredan inspekcijski nadzor vrši se: kada je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode, nesmetan rad organa i organizacija, komunalni red ili bezbednost; kada se posle donošenja godišnjeg plana inspekcijskog nadzora proceni da je rizik visok ili kritičan ili promene okolnosti; kada takav nadzor zahteva nadzirani subjekat; radi sprečavanja obavljanja delatnosti i vršenja aktivnosti neregistrovanih subjekata; po zahtevu javnog tužioca; kada se postupa po predstavci pravnog ili fizičkog lica; kada drugostepeni organ preko inspekcije dopunjava postupak ili ponavlja ceo postupak ili njegov deo, a nisu ispunjeni uslovi za dopunski inspekcijski nadzor. Vanredan inspekcijski nadzor po zahtevu nadziranog subjekta može biti utvrđujući, koji se vrši kada je potrebno utvrditi ispunjenost propisanih uslova nakon čijeg ispunjenja nadzirani subjekat stiče pravo za početak rada ili obavljanja delatnosti, vršenja aktivnosti ili ostvarivanje određenog prava, u skladu sa posebnim zakonom, ili potvrđujući, koji se vrši kada nadzirani subjekat podnese zahtev da se potvrdi zakonitost i bezbednost postupanja u vršenju određenog prava ili izvršenju određene obaveze, odnosno u njegovom poslovanju.			

			Mešoviti inspekcijski nadzor vrši se istovremeno kao redovan i vanredan nadzor kod istog nadziranog subjekta, kada se predmet redovnog i vanrednog inspekcijskog nadzora delimično ili u celosti poklapaju ili su povezani. Kontrolni inspekcijski nadzor vrši se radi utvrđivanja izvršenja mera koje su predložene ili naložene nadziranom subjektu u okviru redovnog ili vanrednog inspekcijskog nadzora. Dopunski inspekcijski nadzor vrši se po službenoj dužnosti ili povodom zahteva nadziranog subjekta, radi utvrđivanja činjenica koje su od značaja za inspekcijski nadzor, a koje nisu utvrđene u redovnom, vanrednom, mešovitom ili kontrolnom inspekcijskom nadzoru, s tim da se može izvršiti samo jedan dopunski inspekcijski nadzor, u roku koji ne može biti duži od 30 dana od okončanja redovnog, vanrednog ili kontrolnog inspekcijskog nadzora. Oblici inspekcijskog nadzora Član 7. Inspekcijski nadzor, prema obliku, može biti terenski i kancelarijski. Terenski inspekcijski nadzor vrši se izvan službenih prostorija inspekcije, na licu mesta i sastoji se od neposrednog uvida u zemljište, objekte, postrojenja, uređaje, prostorije, vozila i druga namenska prevozna sredstva, predmete, robu i druge predmete, akte i dokumentaciju nadziranog subjekta. Kancelarijski inspekcijski nadzor vrši se u službenim prostorijama inspekcije, uvidom u akte, podatke i dokumentaciju nadziranog subjekta. Prava i dužnosti nadziranog subjekta Član 20. Nadzirani subjekti imaju jednaka prava i obaveze u inspekcijskom nadzoru, što uključuje i pravo da inspekcija jednako postupa u istim ili bitno sličnim situacijama prema svim nadziranim subjektima. Nadzirani subjekat u postupku inspekcijskog nadzora ima pravo: da bude upoznat sa predmetom i trajanjem postupka, nalogom za inspekcijski nadzor i drugim aktima donetim u postupku; da bude upoznat sa pravima i dužnostima koje ima u vezi sa			

			inspekcijskim nadzorom; da se izjasni o činjenicama bitnim za potpuno i pravilno utvrđivanje činjeničnog stanja i ponuđenim dokazima; da učestvuje u izvođenju dokaza, postavlja pitanja svedocima i veštacima, iznosi činjenice koje su od značaja za inspekcijski nadzor; da predlaže dokaze i iznosi pravne tvrdnje; da zahteva preventivno delovanje; da upozori inspektora na tajnost informacija koje mu čini dostupnim; da ukaže na nezakonitosti u postupku i da zahteva da se one otklone; da zahteva naknadu štete koja mu je prouzrokovana nezakonitim inspekcijskim nadzorom. Ako više inspekcija vrši zajednički nadzor, nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava koje je dao jednom od inspektora u tom nadzoru. Nadzirani subjekat ima pravo da inspektoru uskrati davanje podataka i izjava o predmetu ranije izvršenog nadzora, osim ako su se ti podaci u međuvremenu promenili, kao i kada je davanje podataka neophodno radi preduzimanja hitnih mera radi sprečavanja ili otklanjanja opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Kada je uredno obavešten o predstojećem inspekcijskom nadzoru, nadzirani subjekat dužan je da bude prisutan na mestu vršenja nadzora, osim ako postoje naročito opravdane okolnosti koje ga u tome sprečavaju, o čemu je dužan da blagovremeno na podesan način obavesti inspekciju. Ako nadzirani subjekat koji je uredno obavešten o predstojećem inspekcijskom nadzoru ne bude prisutan na mestu vršenja nadzora, a ne postoje okolnosti iz stava 5. ovog člana, inspekcijski nadzor se vrši u prisustvu službenog ili drugog lica koje se zatekne na mestu vršenja inspekcijskog nadzora. Nadzirani subjekat dužan je da inspektoru koji mu predoči službenu legitimaciju i uruči nalog za inspekcijski nadzor, kada je on izdat, odnosno koji postupi u skladu sa članom 18. st. 8. i 9. ovog zakona, omogući nesmetan inspekcijski nadzor, što podrazumeva naročito da: stavi na raspolaganje odgovarajući radni prostor za terenski nadzor; obezbedi uvid u poslovne knjige, opšte i pojedinačne akte, evidencije, izveštaje, ugovore,			

			privatne isprave i drugu dokumentaciju nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih poseduje i čuva; omogući pristup lokaciji, zemljištu, objektima, poslovnom i drugom nestambenom prostoru, postrojenjima, uređajima, opremi, priboru, vozilima i drugim namenskim prevoznim sredstvima, drugim sredstvima rada, proizvodima, predmetima koji se stavljaju u promet, robi u prometu i drugim predmetima kojima obavlja delatnost ili vrši aktivnost, kao i drugim predmetima od značaja za inspekcijski nadzor; blagovremeno pruži potpune i tačne podatke koji su mu dostupni, a ako nešto od toga ne može – da razloge za to pisano obrazloži inspektoru. Nadzirani subjekat dužan je da se na zahtev inspektora usmeno ili pisano izjasni o predmetu nadzora. Nadzirani subjekat dužan je da poštuje integritet i službeno svojstvo inspektora. Nadzirani subjekat ima i druga prava i obaveze utvrđene ovim i drugim zakonom. Ovlašćenja inspektora radi utvrđivanja činjenica Član 21. Inspektor je ovlašćen da radi utvrđivanja činjenica: 1) izvrši uvid u javne isprave i podatke iz registara i evidencija koje vode nadležni državni organi, organi autonomne pokrajine i organi jedinice lokalne samouprave i drugi imaoci javnih ovlašćenja ako su neophodni za inspekcijski nadzor, a nije mogao da ih pribavi po službenoj dužnosti, i da ih kopira, u skladu sa zakonom; 2) izvrši uvid u ličnu ili drugu javnu ispravu sa fotografijom koja je podobna da se identifikuju ovlašćena lica u nadziranom subjektu, druga zaposlena ili radno angažovana lica, fizička lica koja su nadzirani subjekti, svedoci, službena lica i zainteresovana lica, kao i fizička lica zatečena na mestu nadzora; 3) uzima pisane i usmene izjave nadziranih subjekata – fizičkih lica i zastupnika, odnosno ovlašćenih lica u nadziranom subjektu – pravnom licu i drugih zaposlenih ili radno angažovanih lica, svedoka, službenih lica i zainteresovanih lica, i da ih poziva da daju izjave o pitanjima od značaja za			

			inspekcijski nadzor; 4) naloži da mu se u određenom roku stave na uvid poslovne knjige, opšti i pojedinačni akti, evidencije, ugovori i druga dokumentacija nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih nadzirani subjekat poseduje i čuva; 5) vrši uviđaj, odnosno pregleda i proverava lokaciju, zemljište, objekte, poslovni i drugi nestambeni prostor, postrojenja, uređaje, opremu, pribor, vozila i druga namenska prevozna sredstva, druga sredstva rada, proizvode, predmete koji se stavljaju u promet, robu u prometu i druge predmete kojima obavlja delatnost ili vrši aktivnost, kao i druge predmete od značaja za inspekcijski nadzor; 6) uzme potrebne uzorke radi njihovog ispitivanja i utvrđivanja činjeničnog stanja, u skladu sa posebnim zakonom i propisima donetim na osnovu zakona; 7) fotografiše i snimi prostor u kome se vrši inspekcijski nadzor i druge stvari koje su predmet nadzora; 7a) obezbedi dokaze; 8) preduzme druge radnje radi utvrđivanja činjeničnog stanja prema ovom i posebnom zakonu. Ako nadzirani subjekat obavlja delatnost preko organizacionih jedinica u svom sastavu koje se nalaze na različitim adresama, inspekcijski nadzor u pogledu zajedničkih elemenata poslovanja ili postupanja i unutrašnjih pravila, opštih akata i procesa nadziranog subjekta vrši inspekcija nadležna prema mestu sedišta tog nadziranog subjekta. U vršenju inspekcijskog nadzora prema organizacionoj jedinici nadziranog subjekta iz stava 2. ovog člana, inspekcija nadležna za inspekcijski nadzor nad poslovanjem organizacione jedinice dužna je da pribavi podatke i informacije o zajedničkim elementima poslovanja ili postupanja, unutrašnjim pravilima, opštim aktima i procesima ovog subjekta od inspekcije nadležne prema mestu sedišta tog nadziranog subjekta. U slučaju neujednačenog postupanja inspekcije ili više inspekcija u vršenju inspekcijskog nadzora prema organizacionim jedinicima nadziranog subjekta iz stava 2. ovog člana, ovaj subjekat,			

			odnosno inspekcija može da zatraži akt o primeni propisa od nadležnog organa ili organizacije. Inspektor se stara o tome da vršenjem svojih ovlašćenja ne ometa redovan proces rada, odnosno obavljanja delatnosti i vršenja aktivnosti nadziranog subjekta. Istovetnost kopija i originala dokumentacije nadziranog subjekta potvrđuje nadzirani subjekat svojim pečatom i potpisom. Ministar nadležan za odgovarajuću oblast inspekcijskog nadzora, odnosno imalac javnih ovlašćenja koji vrši inspekcijski nadzor u određenoj oblasti, ovlašćen je da bliže uredi uslove i način uzimanja i ispitivanja uzoraka.			
33.3.	When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.	3.16.1. 3.16.2.	Nalog za inspekcijski nadzor Član 16. Rukovodilac inspekcije ili lice koje on ovlasti izdaje pisani nalog za inspekcijski nadzor. Nalog za inspekcijski nadzor sadrži: podatke o inspekciji; podatke o inspektoru ili inspektorima koji vrše inspekcijski nadzor sa brojevima službenih legitimacija; podatke o nadziranom subjektu ili subjektima ako su poznati, a ako ti podaci nisu poznati, odnosno ako nije moguće utvrditi nadzirane subjekte ili je njihov broj prevelik – odgovarajuće poznate informacije od značaja za određenje subjekta, odnosno subjekata kod kojih će se vršiti nadzor (npr.: vrsta delatnosti ili aktivnosti, teritorijalno područje, lokacija objekta, vrsta robe ili proizvoda, odnosno usluga itd.); pravni osnov inspekcijskog nadzora; navođenje i kratko objašnjenje vrste i oblika inspekcijskog nadzora; procenjeni rizik; precizan i jasan opis predmeta inspekcijskog nadzora; planirano trajanje inspekcijskog nadzora (dan početka i okončanja nadzora); razloge za izostavljanje obaveštenja, ako postoje; broj, vreme i mesto izdavanja; potpis izdavaoca naloga; pečat, kada je to potrebno prema obeležjima predmeta inspekcijskog nadzora.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	
33.4.	Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to:	1.48. 3.25.	Ovlašćenja inspektora za informacionu bezbednost Član 48. Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na	

	(a)issue warnings about infringements of this Directive by the entities concerned; (b)adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive; (c)order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct; (d)order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period; (e)order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat; (f)order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline; (g)order the entities concerned to make public aspects of infringements of this Directive in a specified manner; (h)impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.	3.26. 3.27. 3.28.	mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom: 1) naloži otklanjanje utvrđenih nepravilnosti i za to utvrdi razuman rok; 2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok; 3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika; 4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način; 5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama. Mere upravljene prema nadziranom subjektu i njihova srazmernost Član 25. Nadziranom subjektu inspektor može izreći upravnu meru, i to preventivnu meru, meru za otklanjanje nezakonitosti, posebnu meru naredbe, zabrane ili zaplene ili meru za zaštitu prava trećih lica. Inspektor izriče one mere koje su srazmerne procenjenom riziku i otkrivenim, odnosno verovatnim nezakonitostima i štetnim posledicama, tako da se rizikom delotvorno upravlja, i kojima se najpovoljnije po nadziranog subjekta postižu cilj i svrha zakona i drugog propisa. Inspektor se obavezno stara o tome da mere iz stava 2. ovog člana budu srazmerne ekonomskoj snazi nadziranog subjekta, da se njihove štetne posledice svedu na najmanju meru i nastavi održivo poslovanje i razvoj nadziranog subjekta. Preventivne mere Član 26. Inspektor u zapisniku određuje odgovarajuće preventivne mere, ako je to potrebno da bi se sprečio nastanak nezakonitosti i štetnih posledica.		osnovu Zakona o inspekcijskom nadzoru.	

			Ako nadzirani subjekat ne postupi po preventivnim merama određenim u zapisniku, inspektor izriče te mere rešenjem. Preventivne mere jesu: 1) upozoravanje nadziranog subjekta o njegovim obavezama iz zakona i drugih propisa, kao i o propisanim radnjama i merama upravljenim prema nadziranom subjektu i sankcijama za postupanja suprotna tim obavezama; 2) ukazivanje nadziranom subjektu na mogućnost nastupanja štetnih posledica njegovog poslovanja ili postupanja; 3) nalaganje nadziranom subjektu preduzimanja ili uzdržavanja od određenih radnji radi otklanjanja uzroka verovatnih štetnih posledica, kao i odgovarajućih mera predostrožnosti u cilju sprečavanja nastanka mogućih štetnih posledica; 4) druge mere kojima se postiže preventivna uloga inspekcijskog nadzora. Preventivne mere mogu se izreći i nepoznatom subjektu inspekcijskog nadzora. Neregistrovanom subjektu se ne može izreći preventivna mera. Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog		

			subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti. Posebne mere naredbe, zabrane i zaplene Član 28. Ako nadzirani subjekat ne otkloni nezakonitost u ostavljenom roku, inspektor je ovlašćen da donese rešenje i izrekne meru kojom, do otklanjanja nezakonitosti, nadziranom subjektu zabranjuje obavljanje delatnosti ili vršenje aktivnosti ili zaplenjuje dokumentaciju, robu i druge predmete koji su nadziranom subjektu poslužili za povredu propisa ili su time nastali. Inspektor je ovlašćen da, bez ostavljanja roka za otklanjanje nezakonitosti, izrekne meru zabrane obavljanja delatnosti ili vršenja aktivnosti ili zaplene predmeta ili dokumentacije ako je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu veće vrednosti, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode veće vrednosti, nesmetan rad organa i organizacija, komunalni red			

			ili bezbednost. Inspektor koji zabrani obavljanje delatnosti ili vršenje aktivnosti ima pravo da naredi da se nadziranom subjektu zapečate poslovne i proizvodne prostorije, objekti i drugi prostor u kome obavlja delatnost ili vrši aktivnost ili koji tome služi, postrojenja, uređaji, oprema, pribor, sredstva rada i drugi predmeti kojima obavlja delatnost ili vrši aktivnost. Inspektor može izreći i drugu posebnu meru naredbe, zabrane ili zaplene (npr. mera povlačenja ili opozivanja proizvoda, mere ograničenja, mera uništavanja predmeta, mera uklanjanja objekta i dr), kad je to određeno posebnim zakonom.			
33.5.	Article 32(6), (7) and (8) shall apply mutatis mutandis to the supervisory and enforcement measures provided for in this Article for important entities.	1.50. 1.51. 1.52. 1.53. 3.27. 3.35 3.36. 4.42. 4.43.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona;		

			Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa		

			ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti. Zapisnik o inspekcijskom nadzoru Član 35. Inspektor sačinjava zapisnik o inspekcijskom nadzoru. U zapisnik se unose: podaci iz naloga za			

			inspekcijski nadzor ako je izdat; vreme i mesto inspekcijskog nadzora, a naročito navođenje osnova i obrazloženje razloga koji su uslovili da se inspekcijski nadzor vrši van radnog vremena nadziranog subjekta u smislu člana 19. stav 2. ovog zakona; opis preduzetih radnji i popis preuzetih dokumenata; podaci o broju uzetih uzoraka i predlozima koje u vezi sa uzimanjem uzoraka daje ovlašćeno lice nadziranog subjekta; izjave koje su date; opis drugih izvedenih dokaza; zahtevi za izuzeće koji su podneti; utvrđeno činjenično stanje; konstatacija zakonitog poslovanja i postupanja nadziranog subjekta; opis otkrivenih nezakonitosti, sa navođenjem dokaza na osnovu kojeg je određena činjenica utvrđena i pravnog osnova za utvrđivanje nezakonitosti; mere koje se izriču sa navođenjem pravnog osnova na kome su zasnovane i rokom za postupanje po njima; odgovarajuća obrazloženja; obaveza nadziranog subjekta da obaveštava inspektora o postupanju po merama i rok za to obaveštavanje; podaci o podnetim krivičnim prijavama, prijavama za privredni prestup i zahtevima za pokretanje prekršajnog postupka, ako su podnete, odnosno izdatim prekršajnim nalozima, ako su izdati, odnosno, u skladu sa članom 42. stav 3. ovog zakona, nepodnošenje zahteva za pokretanje prekršajnog postupka, odnosno neizdavanje prekršajnog naloga; podaci o drugim merama i radnjama na koje je inspektor ovlašćen, ako su preduzete; rok za davanje primedaba na zapisnik; navođenje da je zapisnik sa ili bez primedaba pročitan licu koje prisustvuje nadzoru; drugi podaci i navodi od značaja za inspekcijski nadzor. Kontrolna lista i analiza odgovarajuće stručne institucije, odnosno akreditovanog tela čine sastavni deo zapisnika. Ovlašćeno lice nadziranog subjekta može da odbije da primi zapisnik, što inspektor konstatuje u pisanom obliku i u zapisniku navodi razloge zbog kojih je prijem zapisnika odbijen. Zapisnik se dostavlja nadziranom subjektu u roku od osam dana od završetka inspekcijskog nadzora. Opšti obrazac zapisnika o inspekcijskom nadzoru propisuje ministar nadležan za poslove državne uprave.			

			Opšti obrazac zapisnika o inspekcijskom nadzoru za inspekcijski nadzor iz izvorne nadležnosti autonomne pokrajine i jedinice lokalne samouprave propisuje nadležni organ autonomne pokrajine ili jedinice lokalne samouprave. Primedbe na zapisnik Član 36. Nadzirani subjekat ima pravo da u pisanom obliku stavi primedbe na zapisnik o inspekcijskom nadzoru, u roku od pet radnih dana od njegovog prijema. Inspektor ocenjuje primedbe, sve zajedno i svaku zasebno, i u međusobnoj vezi. Inspektor može posle toga da izvrši dopunski inspekcijski nadzor, da bi utvrdio činjenice na koje se primedbe odnose. Ako su u primedbama na zapisnik iznete nove činjenice i novi dokazi, zbog kojih treba izmeniti činjenično stanje koje je utvrđeno u zapisniku ili drukčije pravne i druge ocene, inspektor o tome sastavlja dopunu zapisnika, na koju se ne može staviti primedba. Postupajući po primedbama na zapisnik, inspektor može da izmeni predloženu ili naloženu, odnosno izrečenu meru ili da odustane od nje. Odmeravanje kazne Član 42. Kazna za prekršaje odmerava se u granicama koje su za taj prekršaj propisane, a pri tome se uzimaju u obzir sve okolnosti koje utiču da kazna bude veća ili manja, a naročito: težina i posledice prekršaja, okolnosti pod kojima je prekršaj učinjen, stepen odgovornosti učinioca, ranija osuđivanost, lične prilike učinioca i držanje učinioca posle učinjenog prekršaja. Ne može se uzeti u obzir kao otežavajuća okolnost ranije izrečena prekršajna sankcija učiniocu ako je od dana pravnosnažnosti odluke do dana donošenja nove proteklo više od četiri godine. Pri odmeravanju visine novčane kazne uzeće se u obzir i imovno stanje učinioca.			

			Ublažavanje kazne Član 43. Ako se prilikom odmeravanja kazne utvrdi da prekršajem nisu prouzrokovane teže posledice, a postoje olakšavajuće okolnosti koje ukazuju da se i blažom kaznom može postići svrha kažnjavanja, propisana kazna se može ublažiti tako što se može: 1) izreći kazna ispod najmanje mere kazne koja je propisana za taj prekršaj ali ne ispod najmanje zakonske mere te vrste kazne; 2) umesto propisane kazne zatvora izreći novčana kazna ili rad u javnom interesu, ali ne ispod najmanje zakonske mere te vrste kazne; 3) umesto propisane kazne zatvora i novčane kazne izreći samo jedna od tih kazni.			
33.6.	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.	3.5.	Saradnja sa drugim organima, imaocima javnih ovlašćenja i pravnim i fizičkim licima Član 5. Saradnja nadležne inspekcije sa drugim organima državne uprave, organima autonomne pokrajine i jedinice lokalne samouprave, pravosudnim i drugim državnim organima i drugim zainteresovanim organima i organizacijama ostvaruje se u skladu sa nadležnostima inspekcije i oblicima saradnje utvrđenim propisima o državnoj upravi i posebnim zakonima. Saradnja, naročito, obuhvata međusobno obaveštavanje, razmenu podataka, pružanje pomoći i zajedničke mere i radnje od značaja za inspekcijski nadzor. Nadležna inspekcija u obavljanju poslova iz svog delokruga usklađuje planove inspekcijskog nadzora i svog rada, razmenjuje podatke, predlaže preduzimanje zajedničkih mera i aktivnosti od značaja za obavljanje poslova inspekcijskog nadzora i na drugi način sarađuje sa drugim inspekcijama i subjektima sa javnim ovlašćenjima koji vrše posebne oblike nadzora i kontrole – radi obavljanja obuhvatnijeg i delotvornijeg inspekcijskog nadzora i naročito radi suzbijanja delatnosti ili aktivnosti neregistrovanih subjekata. Državni organi, organi autonomne pokrajine i jedinice lokalne samouprave i imaoci javnih ovlašćenja dužni su, na zahtev inspektora, da mu u roku od 15 dana od prijema zahteva dostave tražene	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			podatke i obaveštenja koji su značajni za inspekcijski nadzor. Nadležna inspekcija, u skladu sa zakonom, sarađuje sa fizičkim i pravnim licima, naročito u cilju preventivnog delovanja, kao i unapređenja uzajamne odgovornosti fizičkih i pravnih lica i inspekcija u procesu primene i nadzora nad primenom propisa. U tom cilju, inspekcija može održavati informativne i edukativne tribine i konsultativne sastanke sa predstavnicima privatnog sektora i drugim zainteresovanim stranama. Fizička i pravna lica mogu inspekciji podnositi predstavke i zahteve, i od nje tražiti podatke i obaveštenja, u skladu sa zakonom. Ako se u vezi sa vršenjem inspekcijskog nadzora osnovano očekuje da nadzirani subjekat pruži otpor ili se on pruži i inspektoru onemogućava ili bitno otežava vršenje inspekcijskog nadzora, inspektor može da zahteva pomoć policije i komunalne policije. Policija i komunalna policija pružaju pomoć prema zakonima kojima se uređuju policija i komunalna policija.			
34.1.	***General conditions for imposing administrative fines on essential and important entities*** Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	3.27.	Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			člana priloži dokumentaciju, odnosno drugi materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti.			
34.2.	Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).	3.27. 3.28.	Mere za otklanjanje nezakonitosti Član 27. Ako otkrije nezakonitost u poslovanju ili postupanju nadziranog subjekta, inspektor mu ukazuje na nezakonitost i opominje ga zbog toga, u skladu sa ovlašćenjima propisanim u posebnom zakonu nalaže ili predlaže mere i ostavlja primeren rok za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, i to unosi u zapisnik o inspekcijskom nadzoru. Nadzirani subjekat dužan je da pisano obavesti inspektora o tome da li je u ostavljenom roku preduzeo mere koje su mu naložene, odnosno predložene, otklonio nezakonitost i štetne posledice i ispunio propisane obaveze, i ako jeste – inspektor okončava postupak u skladu sa članom 37. stav 2. ovog zakona. Radi utvrđivanja da li su blagovremeno preduzete naložene, odnosno predložene mere, nezakonitost i štetne posledice otklonjene i propisane obaveze ispunjene, inspektor je ovlašćen da od nadziranog subjekta traži da uz obaveštenje iz stava 2. ovog člana priloži dokumentaciju, odnosno drugi	PU	Implementacija ovih odredbi je osigurana primenom inspektorskih ovlašćenja na osnovu Zakona o inspekcijskom nadzoru.	

			materijal (fotografije i dr) iz koga je vidljivo da su utvrđena nezakonitost i njene štetne posledice otklonjene, a propisane obaveze ispunjene. Ako nadzirani subjekat u ostavljenom roku ne preduzme mere koje su mu naložene, odnosno predložene, ne otkloni nezakonitost i štetne posledice i ne ispuni propisane obaveze, inspektor donosi rešenje kojim izriče mere za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza. Inspektor može bez odlaganja doneti rešenje kojim izriče mere za otklanjanje nezakonitosti, bez prethodnog ukazivanja na nezakonitost i ostavljanja roka za otklanjanje nezakonitosti i štetnih posledica i ispunjavanje propisanih obaveza, ako to nalaže neophodnost preduzimanja hitnih mera radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, životnu sredinu ili biljni ili životinjski svet. Inspektor može istovremeno izreći više mera za otklanjanje nezakonitosti. Posebne mere naredbe, zabrane i zaplene Član 28. Ako nadzirani subjekat ne otkloni nezakonitost u ostavljenom roku, inspektor je ovlašćen da donese rešenje i izrekne meru kojom, do otklanjanja nezakonitosti, nadziranom subjektu zabranjuje obavljanje delatnosti ili vršenje aktivnosti ili zaplenjuje dokumentaciju, robu i druge predmete koji su nadziranom subjektu poslužili za povredu propisa ili su time nastali. Inspektor je ovlašćen da, bez ostavljanja roka za otklanjanje nezakonitosti, izrekne meru zabrane obavljanja delatnosti ili vršenja aktivnosti ili zaplene predmeta ili dokumentacije ako je neophodno da se, saglasno delokrugu inspekcije, preduzmu hitne mere radi sprečavanja ili otklanjanja neposredne opasnosti po život ili zdravlje ljudi, imovinu veće vrednosti, prava i interese zaposlenih i radno angažovanih lica, privredu, životnu sredinu, biljni ili životinjski svet, javne prihode veće vrednosti, nesmetan rad organa i organizacija, komunalni red ili bezbednost. Inspektor koji zabrani obavljanje delatnosti ili		

			vršenje aktivnosti ima pravo da naredi da se nadziranom subjektu zapečate poslovne i proizvodne prostorije, objekti i drugi prostor u kome obavlja delatnost ili vrši aktivnost ili koji tome služi, postrojenja, uređaji, oprema, pribor, sredstva rada i drugi predmeti kojima obavlja delatnost ili vrši aktivnost. Inspektor može izreći i drugu posebnu meru naredbe, zabrane ili zaplene (npr. mera povlačenja ili opozivanja proizvoda, mere ograničenja, mera uništavanja predmeta, mera uklanjanja objekta i dr), kad je to određeno posebnim zakonom.			
34.3.	When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).	4.42. 4.43.	Odmeravanje kazne Član 42. Kazna za prekršaje odmerava se u granicama koje su za taj prekršaj propisane, a pri tome se uzimaju u obzir sve okolnosti koje utiču da kazna bude veća ili manja, a naročito: težina i posledice prekršaja, okolnosti pod kojima je prekršaj učinjen, stepen odgovornosti učinioca, ranija osuđivanost, lične prilike učinioca i držanje učinioca posle učinjenog prekršaja. Ne može se uzeti u obzir kao otežavajuća okolnost ranije izrečena prekršajna sankcija učiniocu ako je od dana pravnosnažnosti odluke do dana donošenja nove proteklo više od četiri godine. Pri odmeravanju visine novčane kazne uzeće se u obzir i imovno stanje učinioca. Ublažavanje kazne Član 43. Ako se prilikom odmeravanja kazne utvrdi da prekršajem nisu prouzrokovane teže posledice, a postoje olakšavajuće okolnosti koje ukazuju da se i blažom kaznom može postići svrha kažnjavanja, propisana kazna se može ublažiti tako što se može: 1) izreći kazna ispod najmanje mere kazne koja je propisana za taj prekršaj ali ne ispod najmanje zakonske mere te vrste kazne; 2) umesto propisane kazne zatvora izreći novčana kazna ili rad u javnom interesu, ali ne ispod najmanje zakonske mere te vrste kazne; 3) umesto propisane kazne zatvora i novčane kazne izreći samo jedna od tih kazni.	PU		

34.4.	Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona	DU	Ovakav način obračuna nije moguć prema opštim propisima o prekršajima, uključujući i maksimalne kazne koje se smeju propisati pravnim i fizičkim licima posebnim zakonima.	

			5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
34.5.	Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu	DU	Ovakav način obračuna nije moguć prema opštim propisima o prekršajima, uključujući i maksimalne kazne koje se smeju propisati pravnim i fizičkim licima posebnim zakonima.	

			bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do		

			500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog		

			značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
34.6.	Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona;	PU		

			2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je			

			operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
34.7.	Without prejudice to the powers of the competent authorities pursuant to Articles 32 and 33, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o	PU		

			bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara.			

			Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva			

			štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
34.8.	Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. The Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024 and, without delay, any subsequent amendment law or amendment affecting them.	1.50. 1.51. 1.52. 1.53.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.	PU		

			Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona;		

			Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
35.1.	***Infringements entailing a personal data breach*** Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of	5.52. 5.53.	Obaveštavanje Poverenika o povredi podataka o ličnosti Član 52. Rukovalac je dužan da o povredi podataka o ličnosti koja može da proizvede rizik po prava i slobode	PU	Primenom režima zaštite podataka o ličnosti i propisivanjm načina i svrhe obrade podataka o ličnosti ovim	

	the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.		fizičkih lica obavesti Poverenika bez nepotrebnog odlaganja, ili, ako je to moguće, u roku od 72 časa od saznanja za povredu. Ako rukovalac ne postupi u roku od 72 časa od saznanja za povredu, dužan je da obrazloži razloge zbog kojih nije postupio u tom roku. Obrađivač je dužan da, posle saznanja za povredu podataka o ličnosti, bez nepotrebnog odlaganja obavesti rukovaoca o toj povredi. Obaveštenje iz stava 1. ovog člana mora da sadrži najmanje sledeće informacije: 1) opis prirode povrede podataka o ličnosti, uključujući vrste podataka i približan broj lica na koja se podaci te vrste odnose, kao i približan broj podataka o ličnosti čija je bezbednost povređena; 2) ime i kontakt podatke lica za zaštitu podataka o ličnosti ili informacije o drugom načinu na koji se mogu dobiti podaci o povredi; 3) opis mogućih posledica povrede; 4) opis mera koje je rukovalac preduzeo ili čije je preduzimanje predloženo u vezi sa povredom, uključujući i mere koje su preduzete u cilju umanjenja štetnih posledica. Ako se sve informacije iz stava 4. ovog člana ne mogu dostaviti istovremeno, rukovalac bez nepotrebnog odlaganja postupno dostavlja dostupne informacije. Rukovalac je dužan da dokumentuje svaku povredu podataka o ličnosti, uključujući i činjenice o povredi, njenim posledicama i preduzetim merama za njihovo otklanjanje. Dokumentacija iz stava 6. ovog člana mora omogućiti Povereniku da utvrdi da li je rukovalac postupio u skladu sa odredbama ovog člana. Ako se radi o povredi podataka o ličnosti koje obrađuju nadležni organi u posebne svrhe, a koji su preneti rukovaocu u drugoj državi ili međunarodnoj organizaciji, rukovalac je dužan da bez nepotrebnog odlaganja dostavi informacije iz stava 4. ovog člana rukovaocu u toj drugoj državi ili međunarodnoj organizaciji, u skladu sa međunarodnim sporazumom. Poverenik propisuje obrazac obaveštenja iz stava 1. ovog člana i bliže uređuje način obaveštavanja.		zakonom.	

			Obaveštavanje lica o povredi podataka o ličnosti Član 53. Ako povreda podataka o ličnosti može da proizvede visok rizik po prava i slobode fizičkih lica, rukovalac je dužan da bez nepotrebnog odlaganja o povredi obavesti lice na koje se podaci odnose. U obaveštenju iz stava 1. ovog člana rukovalac je dužan da na jasan i razumljiv način opiše prirodu povrede podataka i navede najmanje informacije iz člana 52. stav 4. tač. 2) do 4) ovog zakona. Rukovalac nije dužan da obavesti lice iz stava 1. ovog člana ako: 1) je preduzeo odgovarajuće tehničke, organizacione i kadrovske mere zaštite u odnosu na podatke o ličnosti čija je bezbednost povređena, a posebno ako je kriptozaštitom ili drugim merama onemogućio razumljivost podataka svim licima koja nisu ovlašćena za pristup ovim podacima; 2) je naknadno preduzeo mere kojima je obezbedio da povreda podataka o ličnosti sa visokim rizikom za prava i slobode lica na koje se podaci odnose više ne može da proizvede posledice za to lice; 3) bi obaveštavanje lica na koje se podaci odnose predstavljalo nesrazmeran utrošak vremena i sredstava. U tom slučaju, rukovalac je dužan da putem javnog obaveštavanja ili na drugi delotvoran način obezbedi pružanje obaveštenja licu na koje se podaci odnose. Ako rukovalac nije obavestio lice na koje se podaci odnose o povredi podataka o ličnosti, Poverenik može, uzimajući u obzir mogućnost da povreda podataka proizvede visok rizik, da naloži rukovaocu da to učini ili može da utvrdi da su ispunjeni uslovi iz stava 3. ovog člana. Ako se radi o povredi podataka o ličnosti koje obrađuju nadležni organi u posebne svrhe, rukovalac može odložiti ili ograničiti obaveštavanje lica na koje se podaci odnose, u skladu sa uslovima i na osnovu razloga iz člana 25. stav 3. ovog zakona.			
35.2.	Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an administrative fine	4.8.	Zabrana ponovnog suđenja u istoj stvari Član 8. Nikome se ne može ponovo suditi niti mu može ponovo biti izrečena prekršajna sankcija za prekršaj o kome je pravnosnažno odlučeno u skladu sa	PU		

	pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive.		zakonom. Zabrana iz stava 1. ovog člana ne sprečava ponavljanje prekršajnog postupka u skladu sa ovim zakonom. Protiv učinioca prekršaja koji je u krivičnom postupku pravnosnažno oglašen krivim za krivično delo koje obuhvata i obeležja prekršaja ne može se za taj prekršaj pokrenuti postupak, a ako je pokrenut ili je u toku, ne može se nastaviti i dovršiti. Protiv učinioca prekršaja koji je u postupku po privrednom prestupu pravnosnažno oglašen odgovornim za privredni prestup koji obuhvata i obeležja prekršaja ne može se za taj prekršaj pokrenuti postupak, a ako je pokrenut ili je u toku, ne može se nastaviti i dovršiti.			
35.3.	Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.	5.72.	Međunarodna saradnja u vezi sa zaštitom podataka o ličnosti Član 72. Poverenik preduzima odgovarajuće mere u odnosima sa organima nadležnim za zaštitu podataka o ličnosti u drugim državama i međunarodnim organizacijama u cilju: 1) razvoja mehanizama međunarodne saradnje za olakšavanje delotvorne primene zakona koji se odnose na zaštitu podataka o ličnosti; 2) obezbeđivanja međunarodne uzajamne pomoći u primeni zakona koji se odnose na zaštitu podataka o ličnosti, uključujući i obaveštavanje, upućivanje na postupke zaštite i pravne pomoći u vršenju nadzora, kao i razmenu informacija, pod uslovom da su preduzete odgovarajuće mere zaštite podataka o ličnosti i osnovnih prava i sloboda; 3) angažovanja zainteresovanih strana u raspravama i aktivnostima koje su usmerene na razvoj međunarodne saradnje u primeni zakona koji se odnose na zaštitu podataka o ličnosti; 4) podsticanja i unapređivanja razmene informacija o zakonodavstvu koje se odnosi na zaštitu podataka o ličnosti i njegovoj primeni, uključujući i pitanja sukoba nadležnosti sa drugim državama u ovoj oblasti.	PU		
36.1.	***Penalties*** Member States shall lay down rules on penalties	1.50.	Član 50. Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno	DU	Kazne su propisane u skladu sa ograničenjima koja su	

	applicable to infringements of national measures 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 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay of any subsequent amendment affecting them.	1.51. 1.52. 1.53.	lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona; 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 51. Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona; 2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona; 3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona; 4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona 5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona; 6) ne dostavi statističke podatke iz člana 25. stav 1.		uspostavljena opštim propisima o prekršajima.	

			ovog zakona; 7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Član 52. Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona; Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara. Izuzetno od st. 1 - 3. 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 53.			

			Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema od posebnog značaja ako: 1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona; 2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona; 3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24 ovog zakona. Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara. Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.			
37.1.- 37.2.	***Mutual assistance*** Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that: (a)the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken; (b)a competent authority may request another competent authority to take supervisory or enforcement measures;			NP	Obaveze država članica	

	(c)a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner. The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.					
38.1.- 38.6.	***Exercise of the delegation*** The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. The power to adopt delegated acts referred to in Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023. The delegation of power referred to in Article 24(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke			NP	Prelazne i završne odredbe	

	shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. A delegated act adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.					
39.1.-39.3.	***Committee procedure*** The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.			NP	Prelazne i završne odredbe	

40.1.	***Review*** By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end 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. The report shall be accompanied, where necessary, by a legislative proposal.			NP	Prelazne i završne odredbe	
41.1- 41.2.	***Transposition*** By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 18 October 2024. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.			NP	Prelazne i završne odredbe	
42.-46.	***Amendment of Regulation (EU) No 910/2014*** In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024. ***Amendment of Directive (EU) 2018/1972*** In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024. ***Repeal***			NP	Prelazne i završne odredbe	

	Directive (EU) 2016/1148 is repealed with effect from 18 October 2024. References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III. ***Entry into force*** This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. ***Addressees*** This Directive is addressed to the Member States.					
ANNEX I	SECTORS OF HIGH CRITICALITY	1.5.	Operatori prioritetnih IKT sistema od posebnog značaja Član 5. Operatori prioritetnih IKT sistema od posebnog značaja su operatori IKT sistema od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori prioritetnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: (1) Energetika - proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - kombinovana proizvodnja električne i toplotne energije; - snabdevanje električnom energijom; - prenos električne energije i upravljanje prenosnim sistemom; - distribucija električne energije i	PU		

			upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom; - skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika; - upravljanje organizovanim tržištem električne energije; - proizvodnja, distribucija i snabdevanje toplotnom energijom; - transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta; - istraživanje i proizvodnja nafte i prirodnog gasa; - proizvodnja derivata nafte; - skladištenje nafte i derivata nafte; - transport i upravljanje transportnim sistemom za prirodni gas; - skladištenje i upravljanje skladištem prirodnog gasa; - distribucija i upravljanje distributivnim sistemom za prirodni gas; - snabdevanje i javno snabdevanje prirodnim gasom; - proizvodnja i prerada uglja; - proizvodnja, skladištenje i prenos vodonika. (2) Saobraćaj - obavljanje javnog avio-prevoza uz važeću operativnu dozvolu; - upravljanje aerodromom; - usluge kontrole letenja; - upravljanje javnom železničkom infrastrukturom; - poslovi železničkih preduzeća; - obavljanje prevoza putnika i tereta unutrašnjim vodama; - upravljanje lukama; - servis za upravljanje brodskim saobraćajem (VTS); - rečni informacioni servisi (RIS); - upravljanje putnom infrastrukturom;			

			- upravljanje inteligentnim transportnim sistemima (ITS). (3) Bankarstvo i finansijska tržišta - poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti; - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama; - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta; - poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala; - poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina. (4) Zdravstvo - pružanje zdravstvene zaštite; - rad nacionalnih referentnih laboratorija; - istraživanje i razvoj lekova; - proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu; - proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja. (5) Voda za piće - snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (6) Otpadne vode - sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti. (7) Digitalna infrastruktura - pružanje usluga računarstva u klaudu; - pružanje usluge centra za čuvanje i skladištenje podataka. (8) Upravljanje IKT uslugama koje se pružaju			

			operatorima prioritetnih IKT sistema od posebnog značaja - pružanje upravljanih usluga; - pružanje upravljanih bezbednosnih usluga. (9) Ostale oblasti - upravljanje nuklearnim objektima; - pružanje kvalifikovanih usluga od poverenja, pružanje usluga DNS-a i upravljanje registrom domena najvišeg nivoa, sa izuzetkom operatora korenskih servera imena; - pružanje usluga mreže za isporuku sadržaja; - obavljanje delatnosti elektronskih komunikacija; - tačka za razmenu internet saobraćaja; - izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije; - oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti. 2) organi; 3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura.			
ANNEX II	OTHER CRITICAL SECTORS	1.6.	Operatori važnih IKT sistema od posebnog značaja Član 6. Operatori važnih IKT sistema od posebnog značaja su operatori IKT sistemi čiji bi prekid ili poremećaj u pružanju usluga mogao da ima značajan uticaj na javni interes, funkcionisanje drugih sektora ili bi stvorio značajan sistemski rizik. Operatori važnih IKT sistema od posebnog značaja su: 1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima: - poštanske usluge u smislu zakona kojim se uređuje oblast poštanskih usluga; - upravljanje otpadom, u smislu zakona kojim se uređuje upravljanje otpadom, izuzev privrednih subjekata kojima navedeni posao nije pretežni deo njihove delatnosti; - upravljanje ambalažnim otpadom, u	PU		

			smislu zakona kojim se uređuje upravljanje ambalažnim otpadom; - proizvodnja i snabdevanje hemikalijama, u skladu sa zakonom kojim se uređuju hemikalije; - proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade; - proizvodnja računara, elektronskih i optičkih proizvoda; - proizvodnja električne opreme; - proizvodnja mašina i uređaja; - proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz; - proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava; - usluge informacionog društva u smislu zakona o elektronskoj trgovini; - proizvodnja, promet i prevoz naoružanja i vojne opreme. 2) naučnoistraživačke institucije; 3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne spadaju u operatore prioritetnih IKT sistema od posebnog značaja prema kriterijumima za određivanje operatora. Podzakonski akt kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi za određivanje operatora prioritetnih i važnih IKT sistema od posebnog značaja donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti. Ministarstva u čijim nadležnostima su oblasti u kojima operatori prioritetnih i važnih IKT sistema od posebnog značaja obavljaju delatnosti, dužni su da u postupku izrade podzakonskog akta iz stava 3. ovog člana, dostave ministarstvu nadležnom za poslove informacione bezbednosti predloge sektorskih kriterijuma radi određivanja operatora IKT sistema od posebnog značaja.			
ANNEX III	CORRELATION TABLE			NP		