**Prijedlog**

Na temelju članka 24. Zakona o kibernetičkoj sigurnosti („Narodne novine“, br. 14/24.), Vlada Republike Hrvatske je na sjednici održanoj \_\_\_ \_\_\_\_\_\_\_ 2024. donijela

 **UREDBU**

**o kibernetičkoj sigurnosti**

**DIO I.**

**OPĆE ODREDBE**

Članak 1.

Ovom se Uredbom uređuju mjerila za razvrstavanje subjekata temeljem posebnih kriterija za provedbu kategorizacije subjekata, kriteriji za provođenje procjena u svrhu kategorizacije subjekata javnog sektora i subjekata iz sustava obrazovanja, prikupljanje podataka u svrhu provođenja kategorizacije subjekata i vođenja posebnog registra subjekata, vođenje popisa ključnih i važnih subjekata, vođenje posebnog registra subjekata, mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe, provođenje samoprocjena kibernetičke sigurnosti, kriteriji za utvrđivanje značajnih incidenata, obavještavanje o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima, prava pristupa i druga pitanja bitna za korištenje nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, podnošenje zahtjeva i prijedloga, prikupljanje podataka potrebnih za provođenje procjene kritičnosti subjekata, kao i druga pitanja bitna za provedbu pristupanja subjekata nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora.

Članak 2.

Sastavni su dio ove Uredbe:

* Prilog I. - Popis sektora djelatnosti (u daljnjem tekstu: Prilog I. ove Uredbe)
* Prilog II. - Mjere upravljanja kibernetičkim sigurnosnim rizicima (u daljnjem tekstu: Prilog II. ove Uredbe) i
* Prilog III. - Posebne mjere fizičke sigurnosti za subjekte iz sektora digitalne infrastrukture (u daljnjem tekstu: Prilog III. ove Uredbe).

Članak 3.

Ovom se Uredbom u hrvatsko zakonodavstvo preuzima Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS2) (SL L 333/80, 27. 12. 2022.).

Članak 4.

(1) U smislu ove Uredbe pojedini pojmovi imaju sljedeće značenje:

1. *djelatnost* je svaka djelatnost izrijekom navedena u Prilogu I. i Prilogu II. Zakona o kibernetičkoj sigurnosti („Narodne novine“, broj: 14/24., u daljnjem tekstu: Zakon)

2. *haktivizam* podrazumijeva korištenje kibernetičkih napada u svrhu promoviranja i poticanja određenih političkih stavova ili društvenih promjena, kao i s ciljem izražavanja neke vrste građanskog neposluha, a provode ga organizirane kibernetičke grupe čiji članovi se nazivaju haktivisti

3. *indikatori kompromitacije* (*Indicators of Compromise – IoCs*) su podaci koji predstavljaju indikatore moguće kompromitacije mrežnog i informacijskog sustava, koji se koriste u svrhu otkrivanja i sprečavanja kibernetičkih napada, odnosno u cilju smanjenja potencijalne štete zaustavljanjem kibernetičkog napada u njegovim ranijim fazama, a tipični indikatori kompromitacije su IP adrese, imena datoteka, kriptografski sažeci datoteka, maliciozne domene i domene upravljanja i kontrole kibernetičkih napadača

4. *javni pružatelj medijske usluge* je pružatelj medijske usluge kako je definiran Uredbom (EU) 2024/1083 Europskog parlamenta i Vijeća od 11. travnja 2024. o uspostavi zajedničkog okvira za medijske usluge na unutarnjem tržištu i izmjeni Direktive 2010/13/EU (Europski akt o slobodi medija) (Tekst značajan za EGP) (SL L, 17.4.2024.)

5. *nadležna tijela za provedbu kategorizacije subjekata* su nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona, prema podjeli nadležnosti iz Priloga III. Zakona

6. *nadležno tijelo za vođenje posebnog registra subjekata* je Sigurnosno-obavještajna agencija

7. *obveznici dostave podataka za kategorizaciju subjekata* su subjekti iz Priloga I. i II. Zakona

8. *obveznici dostave podataka za vođenje posebnog registra subjekata* su pružatelji usluga DNS-a, registar naziva vršne nacionalne internetske domene, registrari, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica i pružatelji platformi za usluge društvenih mreža

9. *operativna tehnologija (OT)* predstavlja širok raspon programibilnih sustava i uređaja koji su u određenoj interakciji s fizičkim okruženjem ili upravljaju drugim uređajima koji su u interakciji s fizičkim okruženjem te otkrivaju ili uzrokuju izravnu promjenu fizičkog okruženja putem nadzora i/ili upravljanja uređajima, procesima i događajima

10. *osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima* su članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršnih tijela jedinica lokalne i područne (regionalne) samouprave

11. *primatelj usluge* je svaka fizička i pravna osoba kojoj ključni ili važni subjekt pruža uslugu temeljem zakona ili ugovora o pružanju usluge. Ugovor o pružanju usluge je ugovor kojim se uređuje pružanje i korištenje usluge ili drugi pravno obvezujući dokument koji uređuje pravni odnos između primatelja usluge i ključnog ili važnog subjekta kao pružatelja usluge, uključujući opće uvjete poslovanja subjekta i druga unaprijed sastavljena pisana pravila kojima subjekt unaprijed regulira pravne odnose s primateljima svojih usluga

12. *primijenjeno znanstveno istraživanje* je industrijsko istraživanje, eksperimentalni razvoj ili njihova kombinacija. Industrijsko istraživanje je planirano istraživanje ili kritički pregled radi stjecanja novih znanja i vještina za razvoj novih proizvoda, procesa ili usluga odnosno za postizanje znatnog poboljšanja postojećih proizvoda, procesa ili usluga. Eksperimentalni razvoj je stjecanje, kombiniranje, oblikovanje i uporaba postojećih znanstvenih, tehnoloških, poslovnih i ostalih mjerodavnih znanja i vještina radi razvoja novih ili poboljšanih proizvoda, procesa ili usluga. Eksperimentalni razvoj može uključivati aktivnosti kojima je cilj konceptualno definiranje, planiranje i dokumentiranje novih proizvoda, procesa ili usluga

13. *smanjena razina kvalitete usluge* je razina kvalitete usluge koja je manja od propisane ili ugovorene razine kvalitete usluge

14. *učinak na autentičnost* je utjecaj na svojstvo da je entitet ono za što tvrdi da jest (npr. kompromitiranje korisničkog identiteta)

15. *učinak na cjelovitost* je utjecaj na svojstvo točnosti i potpunosti (npr. namjerno ili slučajno neovlašteno mijenjanje ili uništavanje komunikacijskih podataka ili metapodataka)

16. *učinak na dostupnost* je utjecaj na kontinuitet pružanja usluge, smanjenje razine kvalitete usluge te djelomični ili potpuni prekid pružanja usluge

17. *učinak na povjerljivost* je utjecaj na svojstvo dostupnosti na način da je informacija dostupna neovlaštenim osobama, pojedincima, entitetima ili procesima (npr. kompromitiranje povjerljivosti komunikacije, komunikacijskih podataka ili metapodataka)

18. *usluga* je svaka usluga izrijekom navedena u Prilogu I. i Prilogu II. Zakona, kao i svaka druga usluga koju ključni ili važni subjekt pruža temeljem zakona ili drugih propisa u okviru obavljanja djelatnosti iz Priloga I. i Priloga II. Zakona.

(2) Ostali pojmovi koji se koriste u ovoj Uredbi imaju jednako značenje kao pojmovi koji se koriste u Zakonu.

(3) Izrazi koji se koriste u ovoj Uredbi, a imaju rodno značenje odnose se jednako na muški i ženski rod.

Članak 5.

 Odredbe ove Uredbe koje se odnose na nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti odnose se i na nadležna tijela za provedbu posebnih zakona kada se tim odredbama uređuju pitanja vezana uz zahtjeve kibernetičke sigurnosti i njihovu provedbu, a koja nisu uređena posebnim zakonima u smislu članka 8. Zakona.

Članak 6.

Nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka dužna su u skladu s pravom Europske unije i relevantnim nacionalnim pravom čuvati sigurnost i komercijalne interese ključnih i važnih subjekta te povjerljivost dostavljenih informacija u provedbi njihovih obveza sukladno ovoj Uredbi.

**DIO II.**

**KATEGORIZACIJA SUBJEKATA TEMELJEM POSEBNIH KRITERIJA, KATEGORIZACIJA SUBJEKATA JAVNOG SEKTORA I SUBJEKATA IZ SUSTAVA OBRAZOVANJA**

**POGLAVLJE I.**

**MJERILA ZA KATEGORIZACIJU SUBJEKATA TEMELJEM POSEBNIH KRITERIJA**

Članak 7.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 1. Zakona provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona za koje se u postupku kategorizacije subjekata utvrdi da su na području najmanje jedne županije, neovisno o broju stanovnika gradova i općina u njezinom sastavu, jedini pružatelj usluge zbog koje je subjekt predmet postupka kategorizacije subjekata.

(2) Temeljem mjerila iz stavka 1. ovog članka:

- privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se u kategoriju ključnih subjekata

- privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

Članak 8.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju obavlja, mogao imati na javnu sigurnost, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona od kojih se izravno dobavljaju proizvodi ili naručuju usluge obuhvaćene Prilogom I. ili Prilogom II. Zakona za:

* policijske namjene
* zaštitu državne granice ili
* zaštitu i spašavanje u slučaju velikih nesreća, katastrofa i kriza.

(2) Temeljem mjerila iz stavka 1. ovog članka:

- privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se u kategoriju ključnih subjekata

- privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

(3) Postupci kategorizacije subjekata iz stavka 1. ovog članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za unutarnje poslove.

Članak 9.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju obavlja, mogao imati na javnu zaštitu, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona:

- koji su odlukama nadležnog tijela državne uprave određeni kao operativne snage sustava civilne zaštite od posebnog interesa na državnoj razini ili su

- odlukama izvršnih tijela jedinica lokalne i područne (regionalne) samouprave određeni pravnom osobom od interesa za sustav civilne zaštite.

(2) Temeljem mjerila iz stavka 1. podstavka 1. ovog članka privatni i javni subjekti iz Priloga I. i Priloga II. Zakona razvrstavaju se u kategoriju ključnih subjekata.

(3) Temeljem mjerila iz stavka 1. podstavka 2. ovog članka privatni i javni subjekti iz Priloga I. i Priloga II. Zakona razvrstavaju se u kategoriju važnih subjekata.

(4) Postupci kategorizacije subjekata iz stavka 1. ovog članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za uspostavu sustava civilne zaštite.

Članak 10.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 2. Zakona, prema kriteriju značajnosti učinka koji bi poremećaj u funkcioniranju usluge koju subjekt pruža, odnosno djelatnosti koju subjekt obavlja, mogao imati na javno zdravlje, provodi se za pružatelje zdravstvene zaštite iz Priloga I. Zakona koji pružaju jednu od slijedećih zdravstvenih djelatnosti:

* suzbijanje zaraznih bolesti
* opskrbu lijekovima i medicinskim proizvodima za zdravstvenu zaštitu
* prikupljanje i pripremu medicinskih pripravaka i presadaka ljudskog podrijetla ili
* hitnu medicinu.

(2) Pružatelji zdravstvene zaštite iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovog članka u kategoriju ključnih subjekata, neovisno o tome pružaju li zdravstvene djelatnosti iz stavka 1. ovog članka na primarnoj, sekundarnoj ili tercijarnoj razini.

(3) Postupci kategorizacije subjekata iz stavka 1. ovog članka provode se u povodu obrazloženog zahtjeva tijela državne uprave nadležnog za zdravstvo.

Članak 11.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 3. Zakona provodi se za privatne i javne subjekte iz sektora energetike, sektora prometa, sektora digitalne infrastrukture te pružatelje upravljanih usluga i pružatelje upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona, za koje se u postupku kategorizacije subjekata utvrdi da tržišni udio subjekta u pružanju usluga, odnosno obavljanju djelatnosti zbog koje je subjekt predmet postupka kategorizacije subjekata, na području Republike Hrvatske iznosi 25% ili više.

(2) Razvrstavanje subjekata temeljem članka 11. podstavka 3. Zakona provodi se i za pružatelje upravljanih usluga i pružatelje upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona koji upravljanje usluge i upravljane sigurnosne usluge pružaju ključnim i važnim subjektima.

(3) Privatni i javni subjekti iz sektora energetike, sektora prometa, sektora digitalne infrastrukture i pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovog članka u kategoriju ključnih subjekata.

(4) Pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga iz sektora upravljanje uslugama IKT-a (B2B) iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 2. ovog članka u kategoriju važnih subjekata.

 Članak 12.

(1) Razvrstavanje subjekata temeljem članka 11. podstavka 4. Zakona, prema kriteriju posebne važnosti subjekta na nacionalnoj razini, provodi se za privatne i javne subjekte iz Priloga I. i Priloga II. Zakona koji su odlukom Vlade Republike Hrvatske određeni pravnom osobom od posebnog interesa za Republiku Hrvatsku.

(2) Privatni i javni subjekti iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovog članka u kategoriju ključnih subjekata.

(3) Privatni i javni subjekti iz Priloga II. Zakona razvrstavaju se temeljem mjerila iz stavka 1. ovog članka u kategoriju važnih subjekata.

(4) Razvrstavanje subjekata temeljem članka 11. podstavka 4. Zakona, prema kriteriju posebne važnosti subjekta na regionalnoj i lokalnoj razini, provodi se za:

- privatne i javne subjekte iz sektora energetike, podsektora električna energija, podsektora centralizirano grijanje i hlađenje i podsektora plin, sektora voda za ljudsku potrošnju i sektora otpadne vode iz Priloga I. Zakona i

- privatne i javne subjekte iz sektora poštanske i kurirske usluge iz Priloga II. Zakona,

za koje se u postupku kategorizacije subjekata utvrdi da tržišni udio subjekta u pružanju usluga, odnosno obavljanju djelatnosti zbog koje je subjekt predmet postupka kategorizacije subjekata, na području jedne županije, neovisno o broju stanovnika gradova i općina u njezinom sastavu, iznosi 40% ili više.

(5) Privatni i javni subjekti iz sektora energetike, podsektora električna energija, podsektora centralizirano grijanje i hlađenje i podsektora plin, sektora voda za ljudsku potrošnju i sektora otpadne vode iz Priloga I. Zakona razvrstavaju se temeljem mjerila iz stavka 4. ovog članka u kategoriju ključnih subjekata.

(6) Privatni i javni subjekti iz sektora poštanske i kurirske usluge iz Priloga II. Zakona razvrstavaju se temeljem mjerila iz stavka 4. ovog članka u kategoriju važnih subjekata.

Članak 13.

Mjerila za kategorizaciju temeljem posebnih kriterija iz članaka 7. do 12. ove Uredbe primjenjuju se na privatne i javne subjekte iz Priloga I. i II. Zakona koji nisu kategorizirani temeljem općih kriterija za kategorizaciju subjekata iz članaka 9. i 10. Zakona.

**POGLAVLJE II.**

**PROVOĐENJE KATEGORIZACIJE SUBJEKATA JAVNOG SEKTORA I SUBJEKATA IZ SUSTAVA OBRAZOVANJA**

Članak 14.

(1) Državna tijela i pravne osobe s javnim ovlastima razvrstavaju se u kategoriju ključnih subjekata ako ispunjavaju sljedeće kriterije:

- osnivač subjekta je Republika Hrvatska, a ustanovljava se za područje Republike Hrvatske i djelatnost obavlja na nacionalnoj razini i pritom nije kategoriziran niti u jednom drugom sektoru visoke kritičnosti ili drugom kritičnom sektoru iz Priloga I. i Priloga II. Zakona i

- utjecaj značajnog kibernetičkog incidenta i ozbiljne kibernetičke prijetnje na mrežni i informacijski sustav tog subjekta može izazvati značajne:

1. posljedice za život i zdravlje ljudi ili na okoliš

2. materijalne i nematerijalne štete tom subjektu ili drugim pravnim i fizičkim osobama

3. poremećaje kod subjekta u obavljanju redovnih djelatnosti (normativne, regulatorne, pružanje usluga)

4. međuresorne posljedice (utjecaj na druge sektore društvenih ili gospodarskih djelatnosti) ili

5. negativne javne utjecaje (remećenje svakodnevnog života, gubitak povjerenja, gubitak javnih i ostalih usluga).

(2) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti prilikom kategorizacije subjekata javnog sektora provodi procjenu kriterija iz stavka 1. podstavka 2. ovog članka na način da procjenjuje svaku od posljedica utjecaja značajnog kibernetičkog incidenta i ozbiljne kibernetičke prijetnje zasebno i u odnosu s drugim posljedicama.

Članak 15.

Jedinice lokalne i područne (regionalne) samouprave razvrstavaju se u kategoriju važnih subjekata ako ispunjavaju najmanje jedan od slijedećih kriterija:

* + obavljaju poslove od područnog (regionalnog) značaja
	+ predstavljaju gospodarska, financijska, kulturna, zdravstvena, prometna i znanstvena središta razvitka šireg okruženja
	+ ovlaštene su provoditi poslove u području gospodarskog razvoja te planiranja i razvoja mreže obrazovnih, zdravstvenih, socijalnih i kulturnih ustanova ili
	+ su im povjereni poslovi državne uprave.

 Članak 16.

Subjekti iz sustava obrazovanja razvrstavaju se temeljem članka 13. Zakona u kategoriju važnih subjekata po osnovi procjene njihove posebne važnosti za obavljanje odgojnog odnosno obrazovnog rada ako ispunjavaju najmanje jedan od sljedećih kriterija:

* + predstavljaju visoko učilište koje provodi primijenjena znanstvena istraživanja u svrhu inovacija i razvoja tehnologija, neovisno o osnivaču ustanove
	+ pružaju e-usluge nacionalnih informacijskih sustava značajnih za sustav odgoja i obrazovanja u Republici Hrvatskoj
	+ predstavlja visoko učilište koje pruža usluge informacijskih sustava značajnih za sustav obrazovanja u Republici Hrvatskoj ili
	+ predstavljaju javnu ustanovu koja provodi vanjsko vrednovanje u odgojno-obrazovnom sustavu Republike Hrvatske i ispite temeljene na nacionalnim standardima.

**DIO III.**

**POPISI KLJUČNIH I VAŽNIH SUBJEKATA I POSEBAN REGISTAR SUBJEKATA**

**POGLAVLJE I.**

**OBVEZE SUBJEKATA IZ PRILOGA I. I PRILOGA II. ZAKONA**

Članak 17.

(1) Obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su imenovati kontakt osobu odgovornu za dostavu podataka.

(2) Kontakt osoba odgovorna za dostavu podataka mora biti imenovana iz reda:

* + članova upravljačkog tijela subjekta
	+ državnih dužnosnika u tijelima državne uprave i drugim državnim tijelima ili
	+ izvršnih čelnika jedinica lokalne i područne (regionalne) samouprave.

Članak 18.

(1) Kontakt osoba odgovorna za dostavu podataka odgovorna je za pravodobnu dostavu točnih i potpunih podataka i obavijesti o promjenama podataka sukladno članku 20. i članku 23. Zakona te odredbama ove Uredbe.

(2) Kontakt osoba odgovorna za dostavu podataka dužna je imenovati najmanje dvije osobe ovlaštene za operacionalizaciju dostave podataka i obavijesti o promjenama podataka iz članka 20. i članka 23. Zakona.

Članak 19.

(1) Obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su nadležnom tijelu za provedbu kategorizacije subjekata odnosno nadležnom tijelu za vođenje posebnog registra subjekata, bez odgode, a najkasnije u roku osam dana od dana zaprimanja zahtjeva iz članka 20. stavka 1. i članka 23. stavka 2. Zakona, dostaviti podatke o imenovanoj kontakt osobi odgovornoj za dostavu podataka i osobama ovlaštenima za operacionalizaciju dostave, i to:

* + ime i prezime imenovanih osoba
	+ podatke o njihovom radnom mjestu odnosno dužnosti u subjektu
	+ adresu elektroničke pošte kontakt osobe odgovorne za dostavu podataka i
	+ adrese elektroničke pošte koje će osobe ovlaštene za operacionalizaciju dostave koristiti u svrhe dostave podataka i obavijesti o promjenama podataka.

(2) U slučaju promjene osoba iz stavka 1. ovog članka ili pojedinih podataka dostavljenih sukladno stavku 1. ovog članka, obveznici dostave podataka za kategorizaciju subjekata i obveznici dostave podataka za vođenje posebnog registra subjekata dužni su o promjeni obavijestiti nadležno tijelo za provedbu kategorizacije subjekata odnosno nadležno tijelo za vođenje posebnog registra subjekata, bez odgode, a najkasnije u roku 15 dana od dana imenovanja nove osobe odnosno promjene pojedinih podataka dostavljenih sukladno stavku 1. ovog članka.

(3) Obavijesti iz stavaka 1. i 2. ovog članka dostavljaju se nadležnom tijelu za provedbu kategorizacije subjekata odnosno nadležnom tijelu za vođenje posebnog registra subjekata prema uputama iz članka 22. ove Uredbe.

Članak 20.

(1) Obveznici dostave podataka za kategorizaciju subjekata dužni su nadležnom tijelu za provedbu kategorizacije subjekata dostavljati podatke i obavijesti o promjenama podataka iz članka 20. Zakona kako slijedi:

* + „*naziv subjekta*“ naziv odnosno ime pod kojim subjekt posluje odnosno obavlja djelatnost u Republici Hrvatskoj, s naznakom i skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu, te osobni identifikacijski broj subjekta (u daljnjem tekstu: OIB)
	+ „*adresa*“ adresa sjedišta subjekta, te adresa kontakt osobe odgovorne za dostavu podataka, ako je različita od adrese sjedišta subjekta
	+ „*ažurirane podatke za kontakt, uključujući adrese e-pošte*“ adresa mrežne stranice subjekta, ime i prezime kontakt osobe odgovorne za dostavu podataka i osoba ovlaštenih za operacionalizaciju dostave, brojeve telefona, brojeve mobitela i adrese elektroničke pošte kontakt osobe odgovorne za dostavu podataka i osoba ovlaštenih za operacionalizaciju dostave
	+ „*IP adresne raspone*“ IP adresne raspone koje subjekt koristi u Republici Hrvatskoj
	+ „*relevantni sektor, podsektor i vrstu subjekta iz Priloga I. i Priloga II. Zakona*“ nazive sektora, podsektora i vrste subjekta, prema nazivima iz Priloga I. ove Uredbe
	+ „*popis država članica u kojima subjekt pruža usluge obuhvaćene područjem primjene Zakona*“ popis država članica Europske unije (u daljnjem tekstu: država članica) u kojima subjekt pruža usluge odnosno obavlja djelatnosti iz Priloga I. odnosno Priloga II. Zakona i pravni oblik pružanja odnosno obavljanja tih djelatnosti u drugim državama članicama
	+ „*druge podatke o pružanju svojih usluga ili obavljanju svojih djelatnosti bitne za provedbu kategorizacije subjekta ili utvrđivanje nadležnosti nad subjektom*“ podatke o veličini subjekta i druge podatke koje je od subjekta zatražilo nadležno tijelo za provedbu kategorizacije subjekata, u svrhu provedbe kategorizacije subjekta ili utvrđivanja nadležnosti nad subjektom.

Članak 21.

(1) Obveznici dostave podataka za vođenje posebnog registra subjekata dužni su nadležnom tijelu za vođenje posebnog registra subjekata dostavljati podatke i obavijesti o promjenama podataka iz članka 23. Zakona kako slijedi:

* + „*naziv subjekta*“ naziv odnosno ime pod kojim subjekt posluje odnosno obavlja djelatnost u Republici Hrvatskoj, s naznakom i skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu, te OIB
	+ „*adresa glavnog poslovnog nastana subjekta*“ adresa glavnog poslovnog nastana subjekta u smislu članka 14. stavaka 3. i 4. Zakona
	+ „*popis usluga iz članka 22. Zakona*“ popis usluga iz članka 22. Zakona koje subjekt pruža u Republici Hrvatskoj
	+ „*adrese poslovnih jedinica u Republici Hrvatskoj*“ adrese svih poslovnih jedinica subjekta koje se nalaze u Republici Hrvatskoj
	+ „*IP adresne raspone*“ IP adresne raspone koje subjekt koristi u Republici Hrvatskoj
	+ „*popis drugih država članica u kojima subjekt posluje*“ popis drugih država članica u kojima subjekt pruža usluge iz članka 22. Zakona
	+ „*adrese drugih poslovnih jedinica*“ adrese poslovnih jedinica subjekta u kojima subjekt pruža usluge iz članka 22. Zakona koje se nalaze u drugim državama članicama i
	+ „*ažurirane podatke za kontakt, uključujući adrese e-pošte i telefonske brojeve subjekta*“ adresa mrežne stranice subjekta, ime i prezime kontakt osobe odgovorne za dostavu podataka, broj telefona, broj mobitela i adresa elektroničke pošte kontakt osobe odgovorne za dostavu podataka, ako subjekt ima glavni poslovni nastan u Republici Hrvatskoj u smislu članka 14. stavaka 3. i 4. Zakona ili
	+ „*naziv i adresa predstavnika, ažurirani podaci za kontakt, uključujući adrese e-pošte i telefonske brojeve predstavnika*“ naziv odnosno ime, adresa, broj telefona, broj mobitela i adresa elektroničke pošte fizičke ili pravne osobe koja ima poslovni nastan u Republici Hrvatskoj ili drugoj državi članici, a koju je obveznik dostave podataka za vođenje posebnog registra subjekata koji nema poslovni nastan u Europskoj uniji izričito imenovao da djeluje u njegovo ime te kojoj se nadležno tijelo može obratiti umjesto samom subjektu vezano uz obveze tog subjekta na temelju ove Uredbe.

Članak 22.

(1) Podaci iz članaka 20. i 21. ove Uredbe i obavijesti o njihovoj promjeni dostavljaju se u elektroničkom obliku, prema uputama koje nadležna tijela za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata objavljuju na svojim mrežnim stranicama.

(2) Nadležna tijela za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata dužni su u uputama iz stavka 1. ovog članka definirati način dostave u iznimnim slučajevima kada dostava u elektroničkom obliku iz opravdanih razloga nije moguća.

(3) Nadležno tijelo za vođenje posebnog registra subjekata dužno je u uputama iz stavka 1. ovog članka definirati način sastavljanja i dostave podataka i obavijesti o promjenama podataka u slučaju kada su mu isti subjekti dužni dostavljati podatke i obavijesti o promjenama podataka po osnovi obveza koje za te subjekte proizlaze kao obveznika dostave podataka za vođenje posebnog registra subjekata i obveznika dostave podataka za kategorizaciju subjekata.

Članak 23.

(1) Upute iz članka 22. ove Uredbe sadržavaju i upute za dobrovoljnu dostavu podataka u svrhu provedbe postupka kategorizacije subjekta.

(2) Dostava podataka o subjektu sukladno uputama za dobrovoljnu dostavu podataka iz stavka 1. ovog članka smatra se jednakovrijednoj dostavi podataka na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti iz članka 20. stavka 1. Zakona.

(3) Dostava podataka o subjektu sukladno stavcima 1. i 2. ovog članka ne utječe na obvezu obavještavanja subjekta o provedenoj kategorizaciji sukladno članku 19. Zakona.

(4) Dostava podataka o subjektu sukladno stavcima 1. i 2. ovog članka ne utječe na obveze subjekta iz članaka 17. do 19. ove Uredbe.

Članak 24.

(1) Ukoliko podaci ili obavijesti o promjenama podataka nisu dostavljeni u skladu s člancima 19. do 23. ove Uredbe, nadležno tijelo za provedbu kategorizacije subjekata i nadležno tijelo za vođenje posebnog registra subjekata će o tome obavijestiti subjekta i odrediti rok u kojem je subjekt dužan otkloniti nedostatke i dostaviti podatke odnosno izmjenu, dopunu ili ispravak podataka, uz upozorenje na pravne posljedice sukladno Zakonu ako to ne učini u ostavljenom roku.

(2) Obavijest iz stavka 1. ovog članka dostavlja se na adresu elektroničke pošte kontakt osobe odgovorne za dostavu podataka odnosno adresu elektroničke pošte predstavnika obveznika dostave podataka za vođenje posebnog registra subjekata koji nema poslovni nastan u Europskoj uniji.

**POGLAVLJE II.**

**PRIKUPLJANJE PODATAKA IZ DRUGIH IZVORA**

Članak 25.

(1) U svrhu provedbe obveza iz članka 21. stavka 1. podstavka 1. Zakona, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti dužni su voditi popis subjekata iz Priloga I. i Priloga II. Zakona za koje u okviru svog djelokruga prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka.

(2) Popis subjekata iz stavka 1. ovog članka sadrži sljedeće podatke:

* sektore, podsektore i vrste subjekata iz Priloga I. i Priloga II. Zakona za koje prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka, prema nazivima iz Priloga I. ove Uredbe
* za svaki sektor, podsektor i vrstu subjekta iz podstavka 1. ovog stavka, nazive subjekata odnosno nazive ili imena pod kojima subjekti posluju odnosno obavljaju djelatnosti iz Priloga I. i Priloga II. Zakona u Republici Hrvatskoj, s naznakom i skraćenog naziva odnosno imena, ako ga subjekt upotrebljava u pravnom prometu
* pravnu osnovu temeljem koje prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka o subjektima iz podstavka 2. ovog stavka
* naznaku o tome vode li registre, evidencije i zbirke podataka koji se odnose na veličinu subjekata u smislu članka 15. Zakona i koje podatke prikupljaju te
* podatak o tome vode li registre, evidencije i zbirke podataka za subjekte iz podstavka 2. ovog stavka u elektroničkom obliku, uz očitovanje o mogućnostima pristupa podacima u tim registrima, evidencijama i zbirkama podataka elektroničkim putem.

(3) Popisi subjekata iz stavka 1. ovog članka dostavljaju se prema uputama koje nadležna tijela za provedbu kategorizacije subjekata objavljuju na svojim mrežnim stranicama.

(4) Popisi subjekata iz stavka 1. ovog članka dostavljaju se nadležnim tijelima za provedbu kategorizacije subjekata jednom godišnje, najkasnije do 1. ožujka tekuće godine za prethodnu godinu.

(5) Iznimno od stavka 4. ovog članka, ako u odnosu na prethodno dostavljeni popis subjekata nije bilo promjena, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti o tome obavještavaju nadležno tijelo za provedbu kategorizacije subjekata, bez obveze dostave novog popisa subjekata.

(6) Iznimno od stavaka 1. i 4. ovog članka, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti nisu u obvezi voditi i redovito dostavljati popise subjekata iz stavka 1. ovog članka, ako su nadležnim tijelima za provedbu kategorizacije subjekata omogućili elektroničkim putem pristup odgovarajućim podacima o subjektima u registrima, evidencijama i zbirkama podataka.

Članak 26.

Članak 25. ove Uredbe ne primjenjuje se na:

* sektor bankarstva
* sektor infrastruktura financijskog tržišta te
* podsektor zračnog prometa.

**POGLAVLJE III.**

**NAČIN VOĐENJA I SADRŽAJ POPISA KLJUČNIH I VAŽNIH SUBJEKATA**

Članak 27.

(1) Popisi ključnih i važnih subjekata vode se u elektroničkom obliku.

(2) U Popise ključnih i važnih subjekata upisuju se podaci propisani ovom Uredbom i sve promjene tih podataka, na način da su iz istih vidljivi izvorno upisani podaci i naknadno unesene promjene tih podataka.

Članak 28.

(1) Popisi ključnih i važnih subjekata vode se po sektorima, podsektorima i vrstama subjekata iz Priloga I. i Priloga II. Zakona, prema nazivima iz Priloga I. ove Uredbe.

(2) Popisi ključnih i važnih subjekata sadrže opće podatke o subjektu i podatke o provedenoj kategorizaciji subjekta.

(3) U Popise ključnih i važnih subjekata pod „*opći podaci o subjektu*“ upisuju se sljedeći podaci:

* naziv subjekta
* OIB subjekta
* adresa subjekta
* broj telefona, broj mobitela i adresa elektroničke pošte kontakt osobe odgovorne za dostavu podataka
* IP adresni rasponi koje subjekt koristi u Republici Hrvatskoj
* popis država članica u kojima subjekt pruža usluge odnosno obavlja djelatnosti iz Priloga I. odnosno Priloga II. Zakona i
* datum upisa subjekta u Popis ključnih i važnih subjekata.

 (4) U Popise ključnih i važnih subjekata pod „*podaci o provedenoj kategorizaciji subjekta*“ upisuju se sljedeći podaci:

* podatak o kategoriji subjekta odnosno naznaku je li subjekt razvrstan kao ključni i/ili važni subjekt
* podatak temeljem koje odredbe Zakona je provedena kategorizacija subjekta
* naziv sektora, podsektora i vrste subjekta u koju je subjekt razvrstan, prema nazivima iz Priloga I. ove Uredbe
* datum provedene kategorizacije subjekta
* za subjekt utvrđenu obvezujuću razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe
* datum obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 2. Zakona, kada je primjenjivo
* napomenu je li za subjekt izrađen protokol o postupanju nadležnih tijela iz članka 59. stavka 3. Zakona, kada je primjenjivo i
* datum provedene provjere Popisa iz članka 17. stavka 2. Zakona.

(5) Opći podaci o subjektu upisuju se u Popis ključnih i važnih subjekata temeljem podataka dostavljenih sukladno člancima 19., 20., 22. i 23. ove Uredbe.

(6) Podaci o provedenoj kategorizaciji subjekta i obvezujućoj razini mjera upravljanja kibernetičkim sigurnosnim rizicima upisuju se temeljem podataka utvrđenih u postupku kategorizacije subjekta ili provedenih provjera Popisa ključnih i važnih subjekata iz članka 17. stavka 2. Zakona.

Članak 29.

(1) Nadležna tijela za provedbu kategorizacije subjekata dužna su subjekt upisati u Popis ključnih i važnih subjekata najkasnije u roku osam dana od dana provedene kategorizacije subjekta.

(2) Nadležna tijela za provedbu kategorizacije subjekata dužna su upisati promjenu kategorije subjekta i drugih povezanih podataka u Popis ključnih i važnih subjekata najkasnije u roku osam dana od dana dostave obavijesti iz članka 19. stavka 2. Zakona.

(3) Nadležna tijela za provedbu kategorizacije subjekata dužna su upisati promjene općih podataka o subjektu u roku osam dana od dana primitka obavijesti o promjenama podataka iz članaka 19. i 20. ove Uredbe.

Članak 30.

(1) Nadležna tijela za provedbu kategorizacije subjekata dužna su subjekte koji se nakon ažuriranja Popisa ključnih i važnih subjekata više ne smatraju ni ključnim subjektima ni važnim subjektima voditi u Popisu ključnih i važnih subjekata s naznakom „neaktivan“.

(2) Nadležna tijela za provedbu kategorizacije subjekata dužna su provjerama Popisa ključnih i važnih subjekata iz članka 17. stavka 2. Zakona obuhvatiti i subjekte iz stavka 1. ovog članka, osim ako je za subjekta u prethodnom postupku provjere utvrđeno da je prestao s radom.

Članak 31.

(1) U svrhu provedbe obveza iz članka 18. stavka 2. Zakona, nadležna tijela za provedbu kategorizacije subjekata dužna su podatke o provedenim kategorizacijama subjekata dostavljati jedinstvenoj kontaktnoj točki sukladno smjernicama jedinstvene kontaktne točke o sadržaju, načinu dostave i rokovima dostave obavijesti o provedenim kategorizacijama subjekata.

(2) U svrhu provedbe članka 43. Zakona, nadležna tijela za provedbu kategorizacije subjekata dužna su Popise ključnih i važnih subjekata, uključujući sva naknadna ažuriranja Popisa, dostavljati pravovremeno i u odgovarajućem formatu Hrvatskoj akademskoj i istraživačkoj mreži – CARNET (u daljnjem tekstu: CARNET).

**POGLAVLJE IV.**

**NAČIN VOĐENJA I SADRŽAJ POSEBNOG REGISTRA SUBJEKATA**

Članak 32.

(1) Poseban registar subjekata vodi se u elektroničkom obliku.

(2) U Poseban registar subjekata upisuju se podaci propisani ovom Uredbom i sve promjene tih podataka, na način da su iz istog vidljivi izvorno upisani podaci i naknadno unesene promjene tih podataka.

Članak 33.

(1) U Posebnom registru subjekata vode se sljedeći podaci:

* naziv subjekta
* OIB subjekta
* popis usluga iz članka 22. Zakona koje subjekt pruža u Republici Hrvatskoj
* adresa glavnog poslovnog nastana subjekta
* adrese poslovnih jedinica subjekta u Republici Hrvatskoj
* IP adresni rasponi koje subjekt koristi u Republici Hrvatskoj
* popis drugih država članica u kojima subjekt pruža usluge iz članka 22. Zakona
* adrese poslovnih jedinica subjekta u kojima subjekt pruža usluge iz članka 22. Zakona koje se nalaze u drugim državama članicama
* broj telefona, broj mobitela i adresa elektroničke pošte kontakt osobe odgovorne za dostavu podataka ili predstavnika subjekta, ako subjekt nema poslovni nastan u Europskoj uniji i
* datum upisa subjekta u Poseban registar subjekata.

(2) Podaci o subjektu upisuju se u Poseban registar subjekata temeljem podataka dostavljenih sukladno člancima 19., 21. i 22. ove Uredbe.

Članak 34.

U svrhu provedbe obveza iz članka 23. stavka 4. Zakona, nadležno tijelo za vođenje posebnog registra subjekata dužno je podatke o subjektima iz članka 22. Zakona dostavljati, putem jedinstvene kontaktne točke, Europskoj agenciji za kibernetičku sigurnost (u daljnjem tekstu: ENISA) u rokovima i na način kako je definirano njezinim smjernicama.

**DIO IV.**

**UPRAVLJANJE KIBERNETIČKIM SIGURNOSNIM RIZICIMA**

**POGLAVLJE I.**

**NACIONALNA PROCJENA KIBERNETIČKIH SIGURNOSNIH RIZIKA**

Članak 35.

(1) U okviru postupka kategorizacije subjekta provodi se nacionalna procjena kibernetičkih sigurnosnih rizika (u daljnjem tekstu: nacionalna procjena rizika) za svaki subjekt kategoriziran kao ključni odnosno važni subjekt.

(2) Cilj provođenja nacionalne procjene rizika je definirati razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koju je dužan provoditi subjekt koji je kategoriziran kao ključni odnosno važni subjekt.

Članak 36.

 Nacionalna procjena rizika provodi se temeljem sljedećih kriterija:

* veličine subjekta
* pripadnosti subjekta određenom sektoru iz Priloga I. i Priloga II. Zakona
* procjene tipičnih vrsta kibernetičkih napada, kao što su onemogućavanje usluge ili sabotaža, krađa podataka ili špijunaža, kibernetički kriminal, haktivizam ili dezinformacije, a koji su globalno prisutni u sektoru kojem subjekt pripada
* procjene jesu li pojedine vrste kibernetičkih napada općenito moguće ili su ciljane za pojedini sektor
* procjene ozbiljnosti poremećaja u funkcioniranju usluga odnosno obavljanju djelatnosti koje tipične vrste kibernetičkih napada mogu uzrokovati u pojedinom sektoru
* procjene tipičnih vrsta kibernetičkih napadača za pojedine sektore, kao što su konkurentski poslovni napadači, haktivisti, teroristi, kibernetički kriminalci ili državno-sponzorirani napadači, te procjena razine njihovih kibernetičkih vještina i
* procjene vjerojatnosti pojave pojedine vrste kibernetičkih napada koju uzrokuje određena vrsta kibernetičkih napadača za svaki pojedini sektor.

Članak 37.

Nacionalnu procjenu rizika provode nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti u okviru prvog postupka kategorizacije subjekta i nakon svakog ažuriranja popisa ključnih i važnih subjekata sukladno članku 17. stavku 2. Zakona.

 Članak 38.

(1) Rezultat nacionalne procjene rizika je utvrđivanje niske, srednje ili visoke razine kibernetičkih sigurnosnih rizika.

(2) Ovisno o utvrđenoj razini kibernetičkih sigurnosnih rizika za svaki subjekt kategoriziran kao ključni odnosno važni subjekt utvrđuje se obveza provedbe jedne od tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima na sljedeći način:

* niska razina kibernetičkih sigurnosnih rizika obvezuje subjekt na provedbu osnovne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe
* srednja razina kibernetičkih sigurnosnih rizika obvezuje subjekt na provedbu srednje razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe
* visoka razina kibernetičkih sigurnosnih rizika obvezuje subjekt na provedbu napredne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe.

Članak 39.

(1) Ukoliko subjekt pruža usluge ili obavlja djelatnosti koje pripadaju u više različitih sektora iz Priloga I. i Priloga II. Zakona, nacionalna procjena rizika se provodi za glavnu djelatnost subjekta.

(2) Ukoliko se glavna djelatnost subjekta ne može nedvojbeno utvrditi, nacionalna procjena rizika provodi se za sve usluge i djelatnosti zbog pružanja odnosno obavljanja kojih je subjekt kategoriziran kao ključni ili važni subjekt te se kao konačna nacionalna procjena rizika subjekta uzima najviša utvrđena razina kibernetičkih sigurnosnih rizika.

Članak 40.

(1) Nacionalna procjena rizika i utvrđivanje obvezujuće razine mjera upravljanja kibernetičkim sigurnosnim rizicima za ključne i važne subjekte iz članka 38. ove Uredbe, provodi se sukladno pravilima za provedbu nacionalne procjene kibernetičkih sigurnosnih rizika, čiji je sastavni dio pripadni kalkulator za izračun razine kibernetičkih sigurnosnih rizika.

(2) Pravila za provedbu nacionalne procjene kibernetičkih sigurnosnih rizika iz stavka 1. ovog članka donosi središnje državno tijelo za kibernetičku sigurnost.

(3) Središnje državno tijelo za kibernetičku sigurnost objavljuje pravila iz stavka 2. ovog članka na svojim mrežnim stranicama.

**POGLAVLJE II.**

**MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA**

Članak 41.

Popis mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđeni su Prilogom II. ove Uredbe za sve tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. ove Uredbe.

Članak 42.

(1) Osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 1. ove Uredbe predstavlja opći skup mjera kibernetičke sigurnosne prakse koji je moguće postići s lako dostupnim tehnologijama i dobro poznatim i dokumentiranim najboljim kibernetičkim sigurnosnim praksama, primjeren u slučaju subjekata čije djelatnosti pripadaju sektorima za koje nisu tipični ciljani kibernetički napadi koje provode napadači s višom razinom kibernetičkih vještina, a cilj primjene osnovne razine je zaštiti subjekt od većine globalno prisutnih kibernetičkih napada, odnosno od kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(2) Srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 2. ove Uredbe predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima, a cilj primjene srednje razine je dodatno umanjiti rizike od ciljanih kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(3) Napredna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 38. stavka 2. podstavka 3. ove Uredbe predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima, a cilj primjene napredne razine je smanjenje rizika od naprednih kibernetičkih napada koje provode kibernetički napadači s naprednim vještinama i resursima.

Članak 43.

(1) Popis mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. ove Uredbe, za svaku mjeru sadrži:

* naziv mjere
* cilj mjere
* razradu mjere na podskupove mjera upravljanja kibernetičkim sigurnosnim rizicima
* primjenjivost mjere u kontekstu IT i OT sustava
* tablični prikaz raspodjele podskupova mjera iz podstavka 3. ovog stavka po razinama mjera iz članka 38. ove Uredbe.

Članak 44.

(1) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz članka 38. ove Uredbe obvezujuća, označeni su u tabličnom prikazu iz članka 43. stavka 1. podstavka 5. ove Uredbe oznakom „A“.

(2) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz članka 38. ove Uredbe obvezujuća pod uvjetima opisanim u razradi mjere iz članka 43. podstavka 4. ove Uredbe pod „UVJET:“, označeni su u tabličnom prikazu iz članka 43. stavka 1. podstavka 5. ove Uredbe oznakom „B“.

(3) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima čija je provedba u okviru određene razine mjera iz članka 38. ove Uredbe dobrovoljna, označeni su u tabličnom prikazu iz članka 43. stavka 1. podstavka 5. ove Uredbe oznakom „C“.

Članak 45.

(1) Podskupovi mjera upravljanja kibernetičkim sigurnosnim rizicima koji su u tabličnom prikazu iz članka 43. stavka 1. podstavka 5. ove Uredbe označeni oznakom „C“, preporučuju se za provedbu ovisno o rezultatima procjene rizika koju subjekt provodi u okviru provedbe mjere naziva „Upravljanje rizicima“ iz točke 3. Priloga II. ove Uredbe.

(2) Provedba podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima koji su u tabličnom prikazu iz članka 43. stavka 1. podstavka 5. ove Uredbe označeni oznakom „C“ dodatno se boduje kroz postupak samoprocjene kibernetičke sigurnosti i revizije kibernetičke sigurnosti.

(3) Za potrebe provedbe procjene rizika iz stavka 1. ovog članka, središnje državno tijelo za kibernetičku sigurnost donosi smjernice kojima se pojašnjava provedba mjere naziva „Upravljanje rizicima“ iz točke 3. Priloga II. ove Uredbe.

(4) Središnje državno tijelo za kibernetičku sigurnost objavljuje smjernice iz stavka 3. ovog članka na svojim mrežnim stranicama.

Članak 46.

(1) Usluge koje pružaju, odnosno djelatnosti koje obavljaju privatni i javni subjekti iz sektora digitalne infrastrukture iz Priloga I. Zakona, temelje se na mrežnim i informacijskim sustavima te se ovom Uredbom za te vrste subjekata utvrđuje posebni, prošireni skup mjera fizičke sigurnosti kao dio mjera upravljanja kibernetičkim sigurnosnim rizicima koje su ti subjekti dužni provoditi.

(2) Prošireni skup mjera fizičke sigurnosti iz stavka 1. ovog članka utvrđen je Prilogom III. ove Uredbe.

Članak 47.

(1) U svrhu provedbe dobrovoljnih mehanizama kibernetičke zaštite iz članka 50. Zakona, subjekti koji nisu kategorizirani kao ključni i važni subjekti provode najmanje osnovnu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima.

(2) U slučajevima iz članka 60. Zakona, nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su provoditi naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima.

Članak 48.

(1) Sve provedene mjere upravljanja kibernetičkim sigurnosnim rizicima, ključni i važni subjekti i subjekti iz članka 47. ove Uredbe moraju ažurirati:

* u planiranim vremenskim razdobljima, a najmanje jednom godišnje u okviru redovite godišnje procjene rizika subjekta
* kada dođe do značajnog incidenta
* kada provode značajne promjene u okviru mrežnog i informacijskog sustava
* u okviru većih poslovno-organizacijskih promjena, spajanja ili promjene vlasničke strukture subjekta koja može imati utjecaja na upravljanje subjektom
* kada se utvrdi neusklađenost subjekta u postupku revizije kibernetičke sigurnosti ili samoprocjene kibernetičke sigurnosti ili
* kada se subjektu izreknu korektivne mjere u postupku stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti.

Članak 49.

(1) Kako bi se olakšala provedba mjera upravljanja kibernetičkim sigurnosnim rizicima, središnje državno tijelo za kibernetičku sigurnost izrađuje korelacijski pregled mjera iz Priloga II. ove Uredbe, kao i svih podskupova ovih mjera, na najvažnije europske i međunarodne norme i najbolje prakse iz otvorenih izvora (mapiranje mjera).

(2) Središnje državno tijelo za kibernetičku sigurnost objavljuje korelacijski pregled iz stavka 1. ovog članka na svojim mrežnim stranicama.

Članak 50.

U svrhu podizanja razine kibernetičke sigurnosti subjekata koji nisu kategorizirani kao ključni ili važni subjekti i ne provode dobrovoljne mehanizme kibernetičke zaštite iz članka 50. Zakona, subjekata koji tek započinju s uvođenjem mjera upravljanja kibernetičkim sigurnosnim rizicima ili predstavljaju mikro ili mali subjekt malog gospodarstva s ograničenim resursima i znanjem u pitanjima upravljanja kibernetičkim sigurnosnim rizicima, središnje državno tijelo za kibernetičku sigurnost priprema i na svojim mrežnim stranicama objavljuje preporuke za provođenje dobre prakse kibernetičke sigurnosti.

**POGLAVLJE III.**

**SAMOPROCJENA KIBERNETIČKE SIGURNOSTI**

Članak 51.

(1) Samoprocjenom kibernetičke sigurnosti utvrđuje se stupanj usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trend podizanja razine zrelosti kibernetičke sigurnosti subjekta.

(2) Samoprocjena kibernetičke sigurnosti u važnim subjektima i subjektima iz članka 47. ove Uredbe se provodi najmanje jednom u dvije godine.

(3) Samoprocjena kibernetičke sigurnosti u ključnim subjektima se može provoditi kao priprema za provedbu revizije kibernetičke sigurnosti ili stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti iz članka 75. stavka 1. Zakona.

Članak 52.

(1) Samoprocjena kibernetičke sigurnosti se temelji na procjeni stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima u subjektu.

(2) Procjenom stupnja usklađenosti dokumentiranih mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se postoje li dokumentirane sigurnosne politike o provedbi mjera i u kojoj mjeri su u skladu sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima Prilogom II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe koju je subjekt sukladno ovoj Uredbi dužan provoditi.

(3) Procjenom usklađenosti implementacije mjera upravljanja kibernetičkim sigurnosnim rizicima utvrđuje se u kojoj mjeri su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima usklađene sa zahtjevima utvrđenim za mjere upravljanja kibernetičkim sigurnosnim rizicima Prilogom II. ove Uredbe, za onu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe koju je subjekt sukladno ovoj Uredbi dužan provoditi.

(4) Procjene stupnja usklađenosti iz stavaka 2. i 3. ovog članka se provode za sve:

* podskupove mjera koje subjekt provodi kao obvezujuće sukladno članku 44. stavku 1. i 2. ove Uredbe
* podskupove mjera koje subjekt provodi kao dobrovoljne sukladno članku 44. stavku 3. ove Uredbe.

Članak 53.

(1) Osim procjene stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima sukladno članku 52. ove Uredbe, samoprocjenom kibernetičke sigurnosti se utvrđuje i trend podizanja razine zrelosti kibernetičke sigurnosti subjekta.

(2) Trend podizanja razine zrelosti kibernetičke sigurnosti subjekta mjeri se utvrđivanjem postignute razine zrelosti i ima za cilj postići da subjekt svakom sljedećom samoprocjenom kibernetičke sigurnosti podigne razinu zrelosti napredujući na višu razinu..

(3) Razine zrelosti kibernetičke sigurnosti iz stavka 2. ovog članka su početna, ponovljiva, definirana, upravljana i optimizirana.

Članak 54.

(1) Utvrđivanje stupnja usklađenosti dokumentiranih i implementiranih mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 52. ove Uredbe i trend podizanja razine zrelosti kibernetičke sigurnosti iz članka 53. ove Uredbe provodi se temeljem bodovanja.

(2) U svrhu provedbe bodovanja iz stavka 1. ovog članka, za svaku razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. ove Uredbe utvrđuje se potreban broj bodova za potvrđivanje sukladnosti subjekta s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za subjekt sukladno članku 38. ove Uredbe.

(3) Dodatnim bodovanjem mjera i podskupova mjera koje je subjekt proveo kao dobrovoljne mjere upravljanja kibernetičkim sigurnosnim rizicima, utvrđuje se ispunjava li subjekt uvjete za trend podizanja razine zrelosti kibernetičke sigurnosti subjekta na višu razinu zrelosti u okviru pet razina zrelosti iz članka 53. stavka 3. ove Uredbe.

Članak 55.

(1) Izjava o sukladnosti iz članka 35. stavka 3. Zakona mora sadržavati sljedeće podatke:

* naziv i adresu subjekta
* naziv sektora, podsektora i vrstu subjekta, prema nazivima iz Priloga I. Uredbe, za ključne i važne subjekte, odnosno naziv sektora i glavne poslovne djelatnosti subjekta iz članka 47. ove Uredbe
* utvrđenu razinu kibernetičkih sigurnosnih rizika za subjekt, kada je primjenjivo
* utvrđenu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima za subjekt
* ostvareni broj bodova u postupku samoprocjene kibernetičke sigurnosti kojim se potvrđuje sukladnost subjekta sa za subjekt utvrđenom razinom mjera upravljanja kibernetičkim sigurnosnim rizicima
* ostvareni broj bodova u postupku samoprocjene kibernetičke sigurnosti kojim se potvrđuje potreban broj bodova koji predstavlja ispunjavanje uvjeta trenda podizanja zrelosti kibernetičke sigurnosti subjekta
* izjavu osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima da rezultati provedene samoprocjene kibernetičke sigurnosti za subjekt pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom i ovom Uredbom
* potpis osobe odgovorne za upravljanje mjerama upravljanja kibernetičkim sigurnosnim rizicima.

(2) Subjekt je dužan izjave o sukladnosti iz članka 35. stavka 3. Zakona i drugu dokumentaciju nastalu u postupku samoprocjene kibernetičke sigurnosti čuvati 10 godina od sastavljanja takve izjave.

Članak 56.

 Subjekti za provedbu samoprocjene kibernetičke sigurnosti moraju odrediti svoje zaposlenike ili vanjske suradnike koji posjeduju:

* relevantna znanja iz implementacije međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti
* završen tečaj za internog revizora po nekoj od relevantnih međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti i
* najmanje 3 godine radnog iskustva u okviru provođenja sličnih vrsta interne revizije u području mrežnih i informacijskih sustava odnosno kibernetičke sigurnosti.

Članak 57.

(1) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti donosi pravila za provedbu samoprocjena kibernetičke sigurnosti, čiji su sastavni dio opisi razina zrelosti kibernetičke sigurnosti iz članka 53. stavka 3. ove Uredbe, pripadni kalkulator za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta te obrazac izjave o sukladnosti.

(2) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti objavljuje pravila iz stavka 1. ovog članka na svojim mrežnim stranicama.

**DIO V.**

**PRAVILA OBAVJEŠTAVANJA O KIBERNETIČKIM PRIJETNJAMA I INCIDENTIMA ZA KLJUČNE I VAŽNE SUBJEKTE**

**POGLAVLJE I.**

**OBAVJEŠTAVANJE O ZNAČAJNIM INCIDENTIMA**

Članak 58.

Značajan incident je svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 59. do 62. ove Uredbe, uzimajući u obzir kriterijske pragove, kada su propisani.

**ODJELJAK I.**

**KRITERIJI ZA UTVRĐIVANJE ZNAČAJNIH INCIDENATA**

Članak 59.

(1) Incidenti koji uzrokuju ili mogu uzrokovati ozbiljne poremećaje u funkcioniranju usluga su incidenti:

* koji negativno utječu na dostupnost usluge ili narušavaju kvalitetu usluge ili
* imaju ili mogu imati negativan učinak na autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga.

(2) Smatra se da incident negativno utječe na dostupnost usluge ili narušava kvalitetu usluge, ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

* najmanje 20% primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje 1 sat
* najmanje 1% primatelja usluge nije moglo pristupiti usluzi u trajanju od najmanje 8 sati, pod uvjetom da 1% primatelja usluge čini najmanje 100 primatelja usluge
* pristup usluzi nije bio moguć u trajanju od 1 sata ili više, a subjekt nije u mogućnosti utvrditi koliko primatelja usluge nije moglo pristupiti usluzi tijekom vremenskog perioda u kojem usluga nije bila dostupna
* najmanje 30 % primatelja usluge povremeno nije moglo pristupiti usluzi ili nije moglo uslugu funkcionalno koristiti zbog smanjene razine kvalitete usluge, ako su povremeni prekidi pristupa usluzi, odnosno nemogućnost funkcionalnog korištenja usluge, trajali ukupno najmanje 1 sat tijekom vremenskog perioda od 4 sata
* pristup usluzi u bolnici, zračnoj luci, zračnom prijevozniku, objektu banke s podatkovnim centrima, objektu policijskog sustava, aktivnom vodocrpilištu i centru upravljanja, objektu operatora elektroničkih komunikacija, objektu tijela sigurnosno-obavještajnog sustava, objektu profesionalne vatrogasne postrojbe ili subjektu koji su utvrđeni kao kritični subjekti na temelju zakona kojim se uređuje područje kritične infrastrukture nije bio moguć u trajanju od najmanje 1 sat
* pristup usluzi kontrole zračnog prometa nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna
* pristup usluzi koja se koristi za potrebe Ministarstva obrane i Oružanih snaga Republike Hrvatske, civilnih nositelja obrambenog planiranja, odnosno za potrebe pravnih osoba posebno važnih za obranu nije bio moguć u trajanju od najmanje 1 sat
* pristup usluzi Centra 112 i drugih hitnih službi nije bio moguć, neovisno o trajanju prekida pristupa usluzi i broju primatelja kojima usluga nije bila dostupna
* pristup usluzi na području najmanje jedne županije ili jednog velikog grada ili grada koji predstavlja sjedište županije nije bio moguć u trajanju od najmanje 1 sat.

(3) Smatra se da incident ima ili može imati negativan učinak na autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

* kritičnim dijelovima mrežnog i informacijskog sustava subjekta ili kritičnim podacima ostvaren je pristup od strane neovlaštene osobe ili su stečeni preduvjeti za ostvarivanje pristupa neovlaštenoj osobi
* kritični mrežni i informacijski sustavi subjekta konfigurirani su od strane neovlaštene osobe ili su stečeni preduvjeti koji omogućavaju konfiguraciju kritičnog mrežnog i informacijskog sustava neovlaštenoj osobi
* zbog incidenta su nastupile okolnosti koje onemogućuju ovlaštenoj osobi konfiguriranje kritičnog mrežnog i informacijskog sustava
* konfiguracija kritičnog mrežnog i informacijskog sustava subjekta neovlašteno je mijenjana, dopunjavana ili je iz drugih razloga postala nepouzdana ili su kritični podaci neovlašteno uklonjeni, mijenjani, dopunjavani ili su iz drugih razloga postali nepouzdani
* kritični mrežni i informacijski sustavi subjekta i/ili drugi mrežni i informacijski sustavi subjekta koji mogu utjecati na kritične mrežne i informacijske sustave subjekta obavljaju zadaće koje odstupaju od uspostavljenih procedura obavljanja poslovnih aktivnosti na sustavu i/ili uspostavljenog okvira kontrola u kojem ti sustavi uobičajeno djeluju, a osobito ako obavljaju zadaće za koje nije predviđeno da ih ti sustavi obavljaju ili ne obavljaju osnovne zadaće za koje je predviđeno da ih ti sustavi obavljaju.

(4) U smislu stavka 3. ovog članka smatra se da su svi sustavi i podaci kritični, ako subjekt nije proveo klasifikaciju kritičnosti mrežnih i informacijskih sustava, nije utvrdio kritične podatke ili ne može utvrditi kritične mrežne i informacijske sustave ili kritične podatke na koje je incident negativno utjecao.

Članak 60.

(1) Smatra se da incident uzrokuje ili može uzrokovati financijske gubitke za subjekt ako je ispunjen najmanje jedan od sljedećih kriterijskih pragova:

* ako gubitak prihoda ili troškovi uzrokovani incidentom ili zbroj tih dvaju faktora iznosi 100.000,00 eura ili najmanje 5% ukupnog godišnjeg poslovnog prihoda subjekta, ovisno o tome koji iznos je niži
* ako pristup usluzi nije bio moguć najmanje 1 sat primateljima usluga od kojih je subjekt u prethodnoj godini ostvario prihode u iznosu od 100.000,00 eura ili najmanje 5% ukupnog godišnjeg poslovnog prihoda subjekta, ovisno o tome koji iznos je niži
* ako je incident uzrokovao reputacijsku štetu subjektu.

(2) Ukupnim godišnjim poslovnim prihodom subjekta u smislu stavka 1. ovog članka smatra se ukupan godišnji poslovni prihod subjekta prema financijskim izvještajima za prethodnu godinu, neovisno o tome pruža li subjekt i druge usluge odnosno obavlja li i druge djelatnosti koje nisu obuhvaćene Prilogom I. i Prilogom II. Zakona.

(3) Prihodom u smislu stavka 1. ovog članka smatraju se svi prihodi subjekta na godišnjoj razini, neovisno o tome ostvaruje li ih ili ih je planirao ostvariti redovnim poslovanjem subjekta ili radnjama koje izlaze izvan opsega redovnog poslovanja subjekta.

(4) Troškovima u smislu stavka 1. ovog članka smatraju se svi troškovi koji su za subjekt nastali zbog poduzimanja radnji i aktivnosti radi zaustavljanja incidenta, odgovora na incident ili oporavka od incidenta, uključujući sve radnje i aktivnosti poduzete radi uspostavljanja redovnog opsega poslovanja subjekta. Troškovima se ne smatraju ugovorne kazne ili druge vrste naknada koje je subjekt u obvezi namiriti zbog povrede ugovornih odnosa uzrokovanih incidentom, neovisno o tome radi li se o fizičkim i pravnim osobama, zaposlenicima subjekta ili njegovim vanjskim suradnicima.

(5) Smatra se da je incident uzrokovao štetu ugledu subjekta u smislu stavka 1. podstavka 4. ovog članka, ako je ispunjen jedan od sljedećih kriterijskih pragova:

* o incidentu je izvještavao javni pružatelj medijske usluge
* incident je rezultirao podizanjem prigovora, tužbi ili drugih pravnih lijekova najmanje 1% primatelja njegovih usluga protiv subjekta.

Članak 61.

(1) Smatra se da je incident utjecao ili bi mogao utjecati na druge fizičke i pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete, ako je zbog incidenta posljedično nastupilo jedno od sljedećeg:

* smrt ili tjelesna ozljeda koja je zahtijevala hospitalizaciju ili terapijske postupke
* potpuno uništenje ili znatno oštećenje materijalne imovine drugih fizičkih ili pravnih osoba ili
* obustava ili znatno smanjenje poslovanja drugih fizičkih i pravnih osoba.

 (2) Drugim fizičkim i pravnim osobama u smislu stavka 1. ovog članka smatraju se primatelji usluga ključnog i važnog subjekta, ali i svaka druga fizička i pravna osoba koja je zbog značajnog incidenta pretrpjela materijalnu ili nematerijalnu štetu iz stavka 1. ovog članka.

Članak 62.

Incidenti koji pojedinačno ne ispunjavaju kriterije za značajan incident iz članaka 59. do 61. ove Uredbe, smatrat će se značajnim incidentom ako su se:

- dogodili najmanje dva puta u razdoblju od 6 mjeseci

- imaju isti temeljni uzrok i

- zajedno ispunjavaju najmanje jedan kriterij za značajan incident iz članaka 59. do 61. ove Uredbe.

Članak 63.

Prekidi u pružanju usluge ili narušavanje kvalitete usluge uslijed planiranog redovnog održavanja mrežnog i informacijskog sustava ključnih i važnih subjekata ne smatraju se značajnim incidentom u smislu članaka 59. do 62. ove Uredbe.

**ODJELJAK II.**

**OBAVIJESTI O ZNAČAJNIM INCIDENTIMA**

Članak 64.

Ključni i važni subjekti dužni su nadležni CSIRT obavijestiti o svakom značajnom incidentu.

Članak 65.

Ključni i važni subjekti dužni su nadležnom CSIRT-u dostavljati sljedeće vrste obavijesti o značajnom incidentu:

* rano upozorenje o značajnom incidentu
* početnu obavijest o značajnom incidentu
* privremeno izvješće o značajnom incidentu
* izvješće o napretku
* završno izvješće o značajnom incidentu.

Članak 66.

 (1) Rano upozorenje o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u bez odgode, a najkasnije u roku 24 sata od trenutka saznanja za značajan incident.

(2) Rano upozorenje o značajnom incidentu mora sadržavati:

* datum i vrijeme saznanja za incident
* opis osnovnih značajki incidenta
* podatak o tome postoji li sumnja da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem
* procjenu subjekta može li incident imati prekogranični utjecaj i
* procjenu subjekta može li incident imati međusektorski utjecaj.

Članak 67.

 (1) Početna obavijest o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u bez odgode, a najkasnije u roku 72 sata od trenutka saznanja za značajan incident.

(2) Početna obavijest o značajnom incidentu mora sadržavati:

* ažurirani opis osnovnih značajki incidenta i drugih informacija dostavljenih sukladno članku 66. ove Uredbe
* početnu procjenu značajnog incidenta i
* indikatore kompromitacije, ako su dostupni.

(3) Početna procjena značajnog incidenta uključuje procjenu ključnog i važnog subjekta o:

* tome koji mrežni i informacijski sustav subjekta je pogođen incidentom i važnosti tog sustava za pružanje usluga odnosno obavljanje djelatnosti subjekta
* ozbiljnosti i učinku incidenta, uzimajući pri tome u obzir mjeru u kojoj je ugroženo pružanje usluga odnosno obavljanje djelatnosti subjekta, trajanje incidenta i broj primatelja usluga na koje je incident utjecao
* tehničkim značajkama incidenta
* ranjivostima koje se iskorištavaju i
* iskustvima subjekta sa sličnim incidentima.

Članak 68.

Iznimno od članka 66. stavka 1. ove Uredbe i članka 67. stavka 1. ove Uredbe, pružatelji usluga povjerenja dužni su nadležnom CSIRT-u bez odgode, a najkasnije u roku 24 sata od trenutka saznanja za značajan incident, dostaviti početnu obavijest o značajnom incidentu, uključujući podatak o datumu i vremenu saznanja za incident.

Članak 69.

 (1) Ključni i važni subjekti dužni su dostaviti privremeno izvješće o značajnom incidentu na zahtjev nadležnog CSIRT-a.

(2) U zahtjevu iz stavka 1. ovog članka, nadležni CSIRT dužan je odrediti:

* na koje podatke iz članka 67. ove Uredbe se zahtjev odnosi i
* rok za dostavu privremenog izvješća o značajnom incidentu.

(3) Rok za dostavu privremenog izvješća o značajnom incidentu određuje se ovisno o opsegu i složenosti podataka na koje se zahtjev iz stavka 1. ovog članka odnosi, s tim da ostavljeni rok ne može biti kraći od 48 sati niti duži od 7 dana od primitka zahtjeva za dostavu privremenog izvješća.

(4) Ako to ocijeni potrebnim, nadležni CSIRT može višekratno, sve do dostave završnog izvješće o značajnom incidentu, podnositi zahtjeve iz stavka 1. ovog članka.

Članak 70.

(1) Završno izvješće o značajnom incidentu ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u najkasnije u roku 30 dana od dana dostave početne obavijesti o značajnom incidentu.

(2) Završno izvješće o značajnom incidentu mora sadržavati:

* detaljan opis incidenta
* vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident
* potvrđene indikatore kompromitacije
* podatke o kibernetičkom napadaču na kojeg se sumnja ili je potvrđen
* podatke o ozbiljnosti i učinku incidenta, koji obvezno uključuju opis poremećaja koje je incident izazvao u pružanju usluga odnosno obavljanju djelatnosti subjekta, trajanju incidenta i broju primatelja usluga na koje je incident utjecao te o možebitnoj kompromitaciji osjetljivih podataka
* primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku
* mjere za postizanje više razine kibernetičke sigurnosti koje subjekt planira primijeniti kako bi se minimizirala mogućnost ponavljanja istog ili sličnog incidenta te kako bi se ublažio rizik
* podatke o prekograničnom učinku incidenta, ako je incident imao takav učinak i
* podatke o međusektorskom učinku incidenta, ako je incident imao takav učinak.

Članak 71.

(1) U slučaju da je incident još u tijeku, ključni i važni subjekti dužni su u roku iz članka 70. stavka 1. ove Uredbe nadležnom CSIRT-u, umjesto završnog izvješća o značajnom incidentu, dostaviti izvješće o napretku.

(2) Izvješće o napretku mora sadržavati:

* ažurirani opis osnovnih značajki incidenta, početne procjene značajnog incidenta i drugih informacija dostavljenih sukladno člancima 67. do 69. ove Uredbe
* vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident
* primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku i
* procjena i obrazloženje uzroka koji su doveli do produženog trajanja odgovora na incident.

(3) U slučaju trajanja značajnog incidenta duže od 60 dana od dana podnošenja početne obavijesti o značajnom incidentu, ključni i važni subjekti dužni su dostavljati nadležnom CSIRT-u izvješće o napretku svakih 30 dana.

(4) U slučajevima iz stavaka 1. i 3. ovog članka, ključni i važni subjekti dužni su dostaviti nadležnom CSIRT-u završno izvješće o značajnom incidentu najkasnije u roku 30 dana od posljednje dostavljenog izvješća o napretku.

Članak 72.

(1) Obavijesti o značajnim incidentima dostavljaju se na obrascima koji se utvrđuju općim smjernicama za provedbu obveze obavještavanja o značajnim incidentima.

(2) Opće smjernice iz stavka 1. ovog članka donose zajedno nadležni CSIRT-ovi, uz suglasnost središnjeg državnog tijela za kibernetičku sigurnost.

(3) Obrasci i opće smjernice iz stavka 1. ovog članka izrađuju se vodeći računa o ENISA-inim tehničkim smjernicama o parametrima za informacije u svrhu obavještavanja ENISA-e temeljem članka 42. stavka 2. Zakona.

(4) Nadležni CSIRT-ovi objavljuju opće smjernice iz stavka 1. ovog članka na svojim mrežnim stranicama.

Članak 73.

(1) Nadležni CSIRT-ovi mogu donositi sektorske smjernice za provedbu obveze obavještavanja o značajnim incidentima, ako postoje sektorske specifičnosti koje nisu obuhvaćene općim smjernicama iz članka 72. ove Uredbe.

(2) Nadležni CSIRT-ovi objavljuju sektorske smjernice iz stavka 1. ovog članka na svojim mrežnim stranicama.

Članak 74.

(1) O provedbi obveze ključnih i važnih subjekata vezano uz dostavu obavijesti o značajnim incidentima tijelima kaznenog progona u slučajevima iz članka 37. stavka 3. Zakona, donose se posebne smjernice.

(2) Smjernice iz stavka 1. ovog članka donose zajedno nadležni CSIRT-ovi, u suradnji s tijelima kaznenog progona.

(3) Nadležni CSIRT-ovi objavljuju smjernice iz stavka 1. ovog članka na svojim mrežnim stranicama.

**ODJELJAK III.**

**POSTUPANJA NADLEŽNOG CSIRT-a POVODOM ZAPRIMLJENIH OBAVIJESTI O ZNAČAJNIM INCIDENTIMA**

Članak 75.

Ako obavijest o značajnom incidentu nije dostavljena u skladu s člancima 66. do 72. ove Uredbe, nadležni CSIRT će o tome obavijestiti subjekta i odrediti rok u kojem je subjekt dužan otkloniti nedostatke, uz upozorenje na pravne posljedice sukladno Zakonu ako to ne učini u ostavljenom roku.

Članak 76.

(1) Nadležni CSIRT dužan je bez odgode, a najkasnije u roku 24 sata od primitka ranog upozorenja o značajnom incidentu, dostaviti subjektu početne povratne podatke o incidentu.

(2) Uz početne povratne podatke o incidentu, nadležni CSIRT dostavit će ključnom i važnom subjektu smjernice i operativne savjete o provedbi mogućih mjera ublažavanja incidenta, ako je subjekt to zatražio u ranom upozorenju o značajnom incidentu odnosno početnoj obavijesti o značajnom incidentu u slučajevima iz članka 68. ove Uredbe.

(3) U slučaju da je subjekt sukladno članku 75. ove Uredbe pozvan na otklanjanje nedostataka u dostavljenom ranom upozorenju o značajnom incidentu, rok iz stavka 1. ovog članka računa se od dostave ispravljenog ranog upozorenja o značajnom incidentu.

(4) Rokovi iz stavaka 1. i 3 ovog članka u slučajevima iz članka 68. ove Uredbe računaju se od primitka početne obavijesti o značajnom incidentu.

Članak 77.

Nadležni CSIRT po zaprimanju obavijesti iz članaka 67. do 71. ove Uredbe provodi analizu i klasifikaciju incidenta prema nacionalnoj taksonomiji incidenata te, ako to dopuštaju okolnosti, nakon primitka takve obavijesti, dostavlja ključnim i važnim subjektima informacije relevantne za daljnje postupanje sa značajnim incidentom, a osobito informacije koje bi mogle pridonijeti djelotvornom rješavanju značajnog incidenta.

Članak 78.

Nacionalnu taksonomiju incidenata iz članka 77. ove Uredbe donosi središnje državno tijelo za kibernetičku sigurnost, na prijedlog nadležnih CSIRT-ova.

Članak 79.

(1) Nadležni CSIRT uključuje se u postupak rješavanja značajnog incidenta na zahtjev ključnog i važnog subjekta.

(2) Zahtjev iz stavka 1. ovog članka ključni i važni subjekt može podnijeti u okviru bilo koje od faza izvještavanja o značajnom incidentu iz članka 65. ove Uredbe, koristeći obrasce za izvještavanje iz članka 72. ove Uredbe.

(3) U slučaju iz stavka 1. ovog članka, ključni i važni subjekti dužni su nadležnom CSIRT-u, na njegov zahtjev, dostaviti sve podatke potrebne za djelotvorno rješavanje značajnog incidenta.

(4) Dostava podataka sukladno stavku 3. ovog članka ne utječe na provedbu obveza ključnih i važnih subjekata iz članaka 65. do 72. ove Uredbe.

Članak 80.

(1) Nadležni CSIRT po zaprimanju obavijesti iz članaka 66. do 72. ove Uredbe o značajnim incidentima koji imaju prekogranični ili međusektorski učinak, dužan je bez odgode, a najkasnije u roku tri dana od primitka takve obavijesti, dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti izvješće o mogućem prekograničnom i međusektorskom učinku značajnog incidenta, s procjenom potencijalnog učinka incidenta.

(2) Prilikom izrade izvješća iz stavka 1. ovog članka nadležni CSIRT je dužan uzeti u obzir i podatke koje su mu o značajnom incidentu dostavili jedinstvena kontaktna točka i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

Članak 81.

Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je bez odgode, a najkasnije u roku tri dana od primitka izvješća iz članka 80. stavka 1. ove Uredbe, očitovati se nadležnom CSIRT-u o procjeni prekograničnog i međusektorskog učinka incidenta.

Članak 82.

(1) Ako zaprimi nove podatke o značajnom incidentu koji su od utjecaja na prethodno danu procjenu učinka incidenta ili kada to od njega zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, nadležni CSIRT dužan je izraditi novo izvješće o prekograničnom i međusektorskom učinku značajnog incidenta, s novom procjenom učinka incidenta.

(2) U slučaju iz stavka 1. ovog članka na odgovarajući način se primjenjuju članci 80. i 81. ove Uredbe.

Članak 83.

Izvješća nadležnog CSIRT-a iz članaka 80. i 82. ove Uredbe i očitovanje nadležnog tijela iz članka 81. ove Uredbe dostavljaju se jedinstvenoj kontaktnoj točki bez odgode.

Članak 84.

U obavljanju zadaća iz članaka 75. do 83. ove Uredbe, nadležni CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika.

**POGLAVLJE II.**

**OBAVJEŠTAVANJE PRIMATELJA USLUGA O ZNAČAJNIM INCIDENTIMA I OZBILJNIM KIBERNETIČKIM PRIJETNJAMA**

Članak 85.

(1) Ključni i važni subjekti su dužni, bez odgode, a najkasnije 72 sata od saznanja za značajan incident, na jasan i lako dokaziv način, o značajnom incidentu obavijestiti primatelje svojih usluga na koje bi takav incident mogao utjecati.

 (2) Obavijest iz stavka 1. ovoga članka mora sadržavati sljedeće podatke o značajnom incidentu:

* vrstu i kratki opis incidenta
* uzrok incidenta
* mogući utjecaj incidenta na uslugu
* kontakt podatke subjekta i
* upute o postupanju primatelja usluga u svrhu ublažavanja učinka nastalog incidenta i naknade uzrokovane štete.

(3) U slučaju da u trenutku slanja obavijesti iz stavka 1. ovog članka ključnom i važnom subjektu nisu poznati neki od podataka iz stavka 2. ovog članka, subjekt je dužan bez odgode, odnosno odmah po saznanju, dostaviti i te preostale podatke primateljima usluga na koje bi takav incident mogao utjecati.

Članak 86.

(1) U slučaju pojave ozbiljne kibernetičke prijetnje, ključni i važni subjekti dužni su primatelje svojih usluga, na koje bi takva prijetnja mogla utjecati, obavijestiti o svim mogućim mjerama zaštite ili pravnim sredstvima koje mogu uporabiti u svrhu sprečavanja ili naknade uzrokovane štete te, po potrebi, obavijestiti primatelje usluga i o samoj ozbiljnoj kibernetičkoj prijetnji.

(2) Na obavještavanje primatelja usluga o ozbiljnim kibernetičkim prijetnjama na odgovarajući način se primjenjuje članak 85. ove Uredbe.

**POGLAVLJE III.**

**OBAVIJESTI KLJUČNIH I VAŽNIH SUBJEKATA NA DOBROVOLJNOJ OSNOVI**

Članak 87.

(1) Kada dobrovoljno obavještavaju o ostalim incidentima na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o incidentu koja mora sadržavati:

* datum i vrijeme saznanja za incident
* opis tehničkih značajki incidenta, uključujući trajanje incidenta i vrstu prijetnje ili temeljnog uzroka koji je vjerojatno uzrokovao incident
* indikatore kompromitacije, ako su dostupni
* podatke o ranjivostima koje se iskorištavaju
* podatke o tome koji mrežni i informacijski sustav subjekta je pogođen incidentom
* opis poremećaja koje je incident izazvao u pružanju usluga odnosno obavljanju djelatnosti subjekta te broj primatelja usluga subjekta i/ili korisnika mrežnog i informacijskog sustava subjekta na koje je incident utjecao
* primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku
* iskustva subjekta sa sličnim incidentima u prošlosti i
* podatak o tome postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovog članka odmah po saznanju za incident, a najkasnije u roku 30 dana od trenutka saznanja za incident, vodeći pri tome računa o ozbiljnosti incidenta i opsegu podataka o izbjegnutom incidentu kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o incidentu do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovog članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovog članka.

Članak 88.

(1) Kada dobrovoljno obavještavaju o kibernetičkim prijetnjama na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o kibernetičkoj prijetnji koja mora sadržavati:

* datum i vrijeme saznanja za kibernetičku prijetnju
* opis kibernetičke prijetnje i njezin trenutni status
* podatke o potencijalnom učinku kibernetičke prijetnje na mrežne i informacijske sustave subjekta i njegove korisnike, uključujući opis poremećaja koje bi kibernetička prijetnja mogla izazvati u pružanju usluga odnosno obavljanju djelatnosti subjekta i
* opis mjera primijenjenih u svrhu sprječavanja učinka kibernetičke prijetnje na mrežne i informacijske sustave subjekta.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovog članka odmah po saznanju za kibernetičku prijetnju, a najkasnije u roku 30 dana od trenutka saznanja za kibernetičku prijetnju, vodeći pri tome računa o ozbiljnosti kibernetičke prijetnje i opsegu podataka o kibernetičkoj prijetnji kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o kibernetičkoj prijetnji do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovog članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovog članka.

Članak 89.

(1) Kada dobrovoljno obavještavaju o izbjegnutim incidentima na temelju članka 39. Zakona, ključni i važni subjekti nadležnom CSIRT-u dostavljaju obavijest o izbjegnutom incidentu koja mora sadržavati:

* datum i vrijeme saznanja za izbjegnuti incident
* opis tehničkih značajki izbjegnutog incidenta, uključujući vrstu prijetnje ili temeljnog uzroka koji je mogao uzrokovati incident
* indikatore kompromitacije, ako su dostupni
* podatke o ranjivostima koje se pokušalo iskoristiti
* podatke o tome koji mrežni i informacijski sustav subjekta je bio izložen izbjegnutom incidentu
* podatke o potencijalnom učinku izbjegnutog incidenta na mrežne i informacijske sustave subjekta i njegove korisnike, uključujući opis poremećaja koje je izbjegnuti incident mogao izazvati u pružanju usluga odnosno obavljanju djelatnosti subjekta
* iskustva subjekta sa sličnim izbjegnutim incidentima u prošlosti i
* podatak o tome postoji li sumnja da je izbjegnuti incident uzrokovan nezakonitim ili zlonamjernim djelovanjem.

(2) Ključni i važni subjekti mogu nadležnom CSIRT-u dostaviti obavijest iz stavka 1. ovog članka odmah po saznanju za izbjegnuti incident, a najkasnije u roku 30 dana od trenutka saznanja za izbjegnuti incident, vodeći pri tome računa o ozbiljnosti izbjegnutog incidenta i opsegu podataka o izbjegnutom incidentu kojima subjekt raspolaže.

(3) Od trenutka dostave obavijesti o izbjegnutom incidentu do isteka krajnjeg roka za njezinu dostavu iz stavka 2. ovog članka, ključni i važni subjekti mogu nadležnom CSIRT-u dostavljati ažurirane podatke iz stavka 1. ovog članka.

Članak 90.

(1) Obavijesti o incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima dostavljaju se na obrascima koji se utvrđuju smjernicama za provedbu dobrovoljnog obavještavanja.

(2) Smjernice iz stavka 1. ovog članka zajednički donose nadležni CSIRT-ovi, uz suglasnost središnjeg državnog tijela za kibernetičku sigurnost.

(3) Obrasci i smjernice iz stavka 1. ovog članka izrađuju se vodeći računa o ENISA-inim tehničkim smjernicama o parametrima za informacije u svrhu obavještavanja ENISA-e temeljem članka 42. stavka 2. Zakona.

(4) Nadležni CSIRT-ovi objavljuju smjernice iz stavka 1. ovog članka na svojim mrežnim stranicama.

Članak 91.

(1) U povodu obavijesti iz članaka 87. do 89. ove Uredbe, nadležni CSIRT dostavit će ključnom i važnom subjektu preporuke i operativne savjete o provedbi mogućih mjera ublažavanja i djelotvornog rješavanja incidenta, sprečavanja nastanka potencijalnog učinka kibernetičke prijetnje i izbjegnutog incidenta, ako je subjekt to zatražio u dostavljenoj obavijesti o incidentu, obavijesti o kibernetičkoj prijetnji odnosno izbjegnutom incidentu.

(2) Kada iz dostavljenih podataka proizlazi da prijavljeni događaj ima obilježja značajnog incidenta iz članaka 59. do 62. ove Uredbe, nadležni CSIRT dostavit će ključnom i važnom subjektu obavijest o obvezi obavještavanja o značajnom incidentu sukladno člancima 64. do 74. ove Uredbe.

Članak 92.

(1) Nadležni CSIRT uključuje se u postupak rješavanja incidenta o kojem je obavješten temeljem članka 87. ove Uredbe, ako je subjekt to zatražio u dostavljenoj obavijesti o incidentu.

(2) U slučaju iz stavka 1. ovog članka na odgovarajući način se primjenjuje članak 79. stavak 3. ove Uredbe.

Članak 93.

U obavljanju zadaća iz članaka 91. i 92. ove Uredbe, nadležni CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika, a prilikom obrade zaprimljenih obavijesti ključnih i važnih subjekata na temelju članaka 37. i 39. Zakona, daje prednost obradi obavijesti o značajnim incidentima.

**POGLAVLJE IV.**

**NACIONALNA PLATFORMA ZA PRIKUPLJANJE, ANALIZU I RAZMJENU PODATAKA O KIBERNETIČKIM PRIJETNJAMA I INCIDENTIMA**

Članak 94.

(1) Ključni i važni subjekti dužni su koristiti nacionalnu platformu za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima (u daljnjem tekstu: nacionalna platforma) kao primarni način dostave obavijesti o:

* značajnim incidentima sukladno članku 37. Zakona i člancima 58. do 73. ove Uredbe
* ostalim incidentima, izbjegnutim incidentima i kibernetičkim prijetnjama sukladno članku 39. Zakona i člancima 87. do 90. ove Uredbe.

(2) U iznimnim slučajevima kada dostava obavijesti sukladno stavku 1. ovog članka iz opravdanih razloga nije moguća, ključni i važni subjekti dužni su obavijesti iz stavka 1. ovog članka dostavljati komunikacijskim kanalima definiranim u smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

Članak 95.

(1) Ključni i važni subjekti stječu status subjekta korisnika nacionalne platforme na dan upisa subjekta u Popis ključnih i važnih subjekata.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su u obavijesti o provedenoj kategorizaciji subjekata iz članka 19. stavka 1. Zakona obavijestiti ključnog i važnog subjekta o stjecanju statusa subjekta korisnika nacionalne platforme i obvezama koje za njega proizlaze iz članaka 96. i 97. ove Uredbe.

Članak 96.

(1) Ključni i važni subjekti dužni su u roku osam dana od primitka obavijesti iz članka 95. stavka 2. ove Uredbe imenovati osobu odgovornu za administriranje računa subjekta na nacionalnoj platformi (u daljnjem tekstu: administrator).

(2) Ključni i važni subjekti dužni su administratora imenovati iz reda svojih zaposlenika.

(3) Ključni i važni subjekt može imenovati do dva administratora.

(4) Podatke o imenovanim administratorima, uključujući promjene osoba administratora ili pojedinih podataka o imenovanim administratorima, ključni i važni subjekti unose u nacionalnu platformu sukladno uputi koja čini sastavni dio obavijesti iz članka 19. stavka 1. Zakona.

Članak 97.

(1) Ključni i važni subjekti dužni su u roku osam dana od primitka obavijesti iz članka 95. stavka 2. ove Uredbe imenovati osobe ovlaštene za provedbu obavještavanja iz članaka 37. i 39. Zakona (u daljnjem tekstu: korisnici nacionalne platforme).

(2) Ključni i važni subjekti mogu korisnike nacionalne platforme imenovati iz reda svojih zaposlenika ili zaposlenika vanjskog davatelja povezanih usluga u subjektu, pri čemu odgovornost za provedbu obavještavanja iz članaka 37. i 39. Zakona ostaje na ključnom i važnom subjektu.

(3) Ključni i važni subjekti dužni su u odluci o imenovanju korisnika nacionalne platforme odrediti opseg njihovih korisničkih prava na način da određuje:

* zadužuje li se osoba za obavještavanje iz članka 37. Zakona i/ili za obavještavanje iz članka 39. Zakona i
* vrstu usluga odnosno djelatnosti subjekta iz Priloga I. i II. Zakona na koje se zaduženje iz prethodne alineje odnosi.

(3) Prilikom određivanja ukupnog broja korisnika nacionalne platforme ključni i važni subjekti dužni su uzeti u obzir veličinu subjekta, njegovu strukturu, stupanj izloženosti subjekta rizicima i vjerojatnost pojave incidenata.

(4) Administrator može biti imenovan i korisnikom nacionalne platforme.

Članak 98.

U nacionalnoj platformi administrator ima sljedeće ovlasti za subjekt za koji je imenovan:

* unošenja korisnika nacionalne platforme i njihovih korisničkih prava,
* ažuriranja podataka o korisnicima nacionalne platforme i
* deaktiviranja korisnika nacionalne platforme i
* deaktiviranja korisničkih prava.

Članak 99.

Temeljem odluke o imenovanju korisnika nacionalne platforme iz članka 97. ove Uredbe, u okvirima njihovih korisničkih prava, administrator u nacionalnoj platformi dodjeljuje korisnicima nacionalne platforme subjekta za koji je imenovan sljedeće ovlasti:

* unošenja obavijesti o značajnim incidentima iz članka 37. Zakona i/ili
* unošenja obavijesti o ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima iz članka 37. Zakona.

Članak 100.

 (1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su u obavijesti iz članka 19. stavka 3. Zakona obavijestiti subjekta o prestanku statusa subjekta korisnika nacionalne platforme.

(2) Obavijest iz stavka 1. ovog članka nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dostavlja i CARNET-u, radi provedbe deaktivacije korisničkih računa administratora i korisnika nacionalne platforme za subjekta na kojeg se obavijest odnosi.

(3) CARNET je dužan provesti deaktivaciju korisničkih računa iz stavka 2. ovog članka bez odgode.

Članak 101.

(1) Ključni i važni subjekti dužni su koristiti nacionalnu platformu sukladno uvjetima korištenja nacionalne platforme.

(2) Uvjete korištenja nacionalne platforme utvrđuje ravnatelj CARNET-a, po prethodno pribavljenom mišljenju nadležnih CSIRT-ova i nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti.

(3) Prilikom utvrđivanja i ažuriranja uvjeta korištenja nacionalne platforme ravnatelj CARNET-a dužan je voditi računa o smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

(4) Uvjetima korištenja nacionalne platforme utvrđuju se, između ostalog, uvjeti korištenja nacionalne platforme u slučajevima iz članka 59. stavka 3. Zakona, a sukladno protokolu o postupanju nadležnih tijela koji je sklopljen za subjekt.

Članak 102.

(1) Nadležnim tijelima iz Priloga III. Zakona i jedinstvenoj kontaktnoj točki, CARNET dodjeljuje prava pristupa nacionalnoj platformi i omogućava njezino korištenje u opsegu koji je tim tijelima potreban za provedbu njihovih zadaća propisanih Zakonom i to:

* nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti za provedbu zadaća iz članka 59. stavaka 1. do 5., članka 64. i članka 65. Zakona
* nadležnim CSIRT-ovima za provedbu zadaća iz članka 66. Zakona i
* jedinstvenoj kontaktnoj točki za provedbu zadaća iz članaka 40. do 42. Zakona.

(2) Nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka dužna su CARNET obavijestiti o:

* zaposlenicima odgovornim za administriranje računima nadležnog tijela odnosno jedinstvene kontaktne točke na nacionalnoj platformi
* ostalim zaposlenicima nadležnog tijela odnosno jedinstvene kontaktne točke ovlaštenim za korištenje nacionalne platforme i
* opsegu korisničkih prava za osobe iz podstavka 1. i 2. ovog stavka.

 (3) U slučajevima iz članka 94. stavka 2. ove Uredbe nadležna tijela iz Priloga III. Zakona i jedinstvena kontaktna točka ostvaruju pristup dostavljenim obavijestima ključnih i važnih subjekata sukladno smjernicama nadležnih CSIRT-ova iz članka 72. stavka 1. i članka 90. stavka 1. ove Uredbe.

 Članak 103.

(1) Podaci o pojedinom značajnom incidentu čuvaju se u nacionalnoj platformi 25 godina od dana dostave završnog izvješća o značajnom incidentu iz članka 70. ove Uredbe.

(2) Podaci o pojedinim ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima čuvaju se u nacionalnoj platformi 15 godina od dana dostave obavijesti iz članaka 87. do 89. ove Uredbe.

(3) Podaci o subjektima korisnicima nacionalne platforme, njihovim administratorima i korisnicima nacionalne platforme čuvaju se 15 godina od dana deaktivacije korisničkog računa subjekta sukladno članku 100. ove Uredbe, pod uvjetom da su u tom roku istekli rokovi čuvanja za sve značajne incidente o kojima je dotični subjekt obavijestio nadležni CSIRT.

(4) Nadležni CSIRT-ovi dužni su, prema podjeli nadležnosti iz Priloga III. Zakona, nakon isteka rokova čuvanja iz stavaka 1. i 2. ovoga članka, brisati u nacionalnoj platformi podatke o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima.

(5) CARNET je dužan nakon isteka roka čuvanja iz stavka 3. ovoga članka brisati u nacionalnoj platformi podatke o subjektima korisnicima nacionalne platforme, njihovim administratorima i korisnicima nacionalne platforme.

**DIO VI.**

**PROVEDBA OBAVJEŠTAVANJA O INCIDENTIMA I KIBERNETIČKIM PRIJETNJAMA KAO DOBROVOLJNI MEHANIZAM KIBERNETIČKE ZAŠTITE**

Članak 104.

(1) Subjekti iz članka 47. stavka 1. ove Uredbe koji namjeravaju koristiti mogućnost obavještavanja o incidentima i kibernetičkim prijetnjama temeljem članka 50. stavka 2. Zakona, dužni su o takvoj namjeri obavijestiti nadležni CSIRT.

(2) U prilogu obavijesti iz stavka 1. ovog članka, subjekt je dužan dostaviti izjavu o sukladnosti iz članka 35. stavka 3. Zakona, koja nije starija od godine dana od dana sastavljanja obavijesti iz stavka 1. ovog članka.

Članak 105.

(1) Subjekti iz članka 47. stavka 1. ove Uredbe dužni su najmanje jednom u dvije godine provoditi samoprocjene kibernetičke sigurnosti sve dok koriste mogućnost obavještavanja o incidentima i kibernetičkim prijetnjama temeljem članka 50. stavka 2. Zakona, a sastavljene izjave o sukladnosti iz članka 35. stavka 3. Zakona dostaviti nadležnom CSIRT-u bez odgode, a najkasnije u roku osam dana od dana njihova sastavljanja.

(2) Rok iz stavka 1. ovog članka računa se od dana sastavljanja izjave o sukladnosti dostavljene nadležnom CSIRT-u sukladno članku 104. stavku 2. ove Uredbe odnosno od dana sastavljanja dostavljene izjave o sukladnosti iz članka 35. stavka 3. Zakona nadležnom CSIRT-u.

Članak 106.

Značajan incident u smislu članka 50. stavka 2. Zakona, o kojem subjekti iz članka 47. stavka 1. ove Uredbe dobrovoljno obavještavaju nadležni CSIRT, je svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 58. do 62. ove Uredbe, uzimajući u obzir kriterijske pragove, kada su propisani.

Članak 107.

(1) Na provedbu obavještavanja o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima temeljenog na članku 50. stavku 2. Zakona na odgovarajući način se primjenjuju članci 87. do 92. ove Uredbe.

(2) Subjekti iz članka 47. stavka 1. ove Uredbe dužni su obavijesti o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima dostavljati isključivo komunikacijskim kanalima definiranim u smjernicama nadležnih CSIRT-ova iz članka 90. stavka 1. ove Uredbe.

 Članak 108.

Prilikom obrade obavijesti o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima zaprimljenih temeljem članaka 37., 39. i 50. stavka 2. Zakona, nadležni CSIRT daje prednost obradi obavijesti zaprimljenih temeljem članaka 37. i 39. Zakona.

**DIO VII.**

**NACIONALNI SUSTAV ZA OTKRIVANJE KIBERNETIČKIH PRIJETNJI I ZAŠTITU KIBERNETIČKOG PROSTORA**

Članak 109.

(1) Ključni subjekti, važni subjekti i drugi subjekti koji nisu kategorizirani kao ključni ili važni subjekti mogu dobrovoljno provesti mjeru kibernetičke zaštite pristupom nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora (u daljnjem tekstu: nacionalni sustav), ako je središnje državno tijelo za kibernetičku sigurnost procijenilo subjekta kritičnim u smislu članka 52. stavka 1. Zakona.

(2) U svrhu provedbe procjena kritičnosti subjekata u smislu članka 52. stavka 1. Zakona i odlučivanja o prioritetima u provedbi dobrovoljne mjere kibernetičke zaštite pristupa nacionalnom sustavu, središnje državno tijelo za kibernetičku sigurnost razvrstava subjekte prema kategorijama rizičnosti.

Članak 110.

(1) Procjena kritičnosti subjekta u smislu članka 52. stavka 1. Zakona provodi se na temelju zahtjeva za pristupanje nacionalnom sustavu kojeg podnosi subjekt, odnosno na temelju prijedloga za pristupanje nacionalnom sustavu kojeg podnosi tijelo državne uprave ili regulatorno tijelo nadležno za sektor kojem pravna osoba pripada.

(2) Zahtjevi i prijedlozi za pristupanje nacionalnom sustavu moraju sadržavati podatke o:

* uslugama koje subjekt pruža ili djelatnostima koje subjekt obavlja u odnosu na druge pružatelje istih ili istovrsnih usluga i djelatnosti u Republici Hrvatskoj
* mrežnim i informacijskim sustavima kojima se subjekt koristi u pružanju usluga ili obavljanju djelatnosti te njihovoj izloženosti rizicima, opasnostima i prijetnjama u kibernetičkom prostoru i
* načinu projektiranja, upravljanja i održavanja mrežnih i informacijskih sustava subjekta, kao i primijenjenim relevantnim europskim i međunarodnim normama i najboljim sigurnosnim praksama.

(3) Osim podataka iz stavka 2. ovog članka, prijedlozi za pristupanje nacionalnom sustavu moraju sadržavati i očitovanje podnositelja prijedloga o razlozima zbog kojih se za subjekta predlaže provesti mjeru kibernetičke zaštite pristupanja nacionalnom sustavu.

(4) Zahtjevi i prijedlozi za pristupanje nacionalnom sustavu podnose se središnjem državnom tijelu za kibernetičku sigurnost prema uputama koje središnje državno tijelo za kibernetičku sigurnost objavljuje na svojim mrežnim stranicama.

(5) O podnesenom prijedlogu za pristupanje nacionalnom sustavu, podnositelj prijedloga je dužan obavijestiti i subjekta za kojeg je takav prijedlog podnio.

Članak 111.

(1) Središnje državno tijelo za kibernetičku sigurnost može, po potrebi, od subjekta za kojeg se provodi procjena u svrhu kritičnosti subjekta za pristupanjem nacionalnom sustavu, zatražiti dostavljanje dodatnih podataka o mrežnim i informacijskim sustavima subjekta.

(2) Zatražene podatke subjekt dostavlja središnjem državnom tijelu za kibernetičku sigurnost sukladno uputama iz članka 110. stavka 4. ove Uredbe.

Članak 112.

(1) Iznimno od članka 109. ove Uredbe, ministarstva su dužna provesti mjeru kibernetičke zaštite obveznog pristupa nacionalnom sustavu.

(2) Iznimno od članka 109. ove Uredbe, druga tijela državne uprave, državna tijela i pravne osobe s javnim ovlastima su dužna provesti mjeru kibernetičke zaštite obveznog pristupa nacionalnom sustavu kada su ispunjeni sljedeći kriteriji:

* subjekt je kategoriziran kao ključni subjekt ili
* je središnje državno tijelo za kibernetičku sigurnost procijenilo subjekta kritičnim u smislu članka 52. stavka 1. Zakona.

(3) Procjena kritičnosti subjekata iz stavka 2. podstavka 2. ovog članka provodi se u povodu prijedloga nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti za javni sektor.

(4) Središnje državno tijelo za kibernetičku sigurnost dužno je obavijestiti subjekta o ispunjavanju kriterija iz stavka 2. podstavka 2. ovog članka i o obvezi pristupanja nacionalnom sustavu.

 Članak 113.

(1) Neovisno o tome provodi li se kao obvezujuća ili dobrovoljna mjera kibernetičke zaštite, pristupanje nacionalnom sustavu provodi se na temelju sporazuma koji sklapaju središnje državno tijelo za kibernetičku sigurnost i subjekt koji pristupa nacionalnom sustavu.

(2) Sporazumom iz stavka 1. ovog članka uređuju se:

* međusobna prava i obveze središnjeg državnog tijela i subjekta koji pristupa nacionalnom sustavu
* obostrani uvjeti zaštite podataka i povjerljivosti
* održavanje i zaštita programske opreme i alata nacionalnog sustava i
* tehnički i drugi uvjeti za pristupanje i korištenje nacionalnog sustava.

(3) Sporazumi iz stavka 2. ovog članka klasificiraju se odgovarajućim stupnjem tajnosti.

**DIO VIII.**

**PRIJELAZNE I ZAVRŠNE ODREDBE**

Članak 114.

(1) Jedinstvena kontaktna točka donijet će smjernice iz članka 31. stavka 1. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(2) Središnje državno tijelo za kibernetičku sigurnost donijet će pravila iz članka 40. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

(3) Središnje državno tijelo za kibernetičku sigurnost donijet će smjernice iz članka 45. stavka 3. ove Uredbe u roku od 6 mjeseci od dana stupanja na snagu ove Uredbe.

(4) Središnje državno tijelo za kibernetičku sigurnost izradit će korelacijski pregled mjera iz članka 49. ove Uredbe u roku od 6 mjeseci od dana stupanja na snagu ove Uredbe.

(5) Središnje državno tijelo za kibernetičku sigurnost donijet će nacionalnu taksonomiju incidenata iz članka 77. ove Uredbe u roku 90 dana od dana stupanja na snagu ove Uredbe.

(6) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti donijet će pravila iz članka 57. ove Uredbe u roku od 6 mjeseci od dana stupanja na snagu ove Uredbe.

(7) Nadležni CSIRT-ovi donijet će smjernice iz članaka 72., 74. i 90. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

Članak 115.

Danom stupanja na snagu ove Uredbe prestaje važiti Odluka o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza, KLASA: 022-03/21-04/91, URBROJ: 50301-29/09-21-2, od 1. travnja 2021.

Članak 116.

Ova Uredba stupa na snagu osmoga dana od dana objave u „Narodnim novinama“, osim odredaba članaka 104. i 105. ove Uredbe koje stupaju na snagu 1. siječnja 2026. godine.