NN br. 109/12, 33/13-ispravak, 126/13, 67/16 i 66/19

PRAVILNIK
O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA

- neslužbeni pročišćeni tekst -

I. OPĆE ODREDBE

SADRŽAJ PRAVILNIKA

Članak 1.

Ovim Pravilnikom propisuju se način i rokovi u kojima operatori javnih komunikacijskih mreža moraju poduzimati sve odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža, u svrhu osiguravanja neprekinutog obavljanja usluga koje se pružaju putem tih mreža, te uređuje način izvješćivanja Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: Agencija) od strane operatora javnih komunikacijskih mreža i elektroničkih komunikacijskih usluga o povredi sigurnosti ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga.

Ovaj Pravilnik usklađen je s odredbom članka 13.a Direktive 2002/21/EC Europskog parlamenta i Vijeća o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge koja je izmijenjena i dopunjena Direktivom 2009/140/EC.

POJMOVI I ZNAČENJA

Članak 2.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *informacijski sustav*: komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike,
2. *integritet (cjelovitost) mreže*: skup tehničkih zahtjeva za procese, rad i izmjene u elektroničkoj komunikacijskoj mreži, u svrhu osiguravanja nesmetane uporabe međusobno povezanih elektroničkih komunikacijskih mreža, kao i pristupa tim

mrežama te cjelovitosti podataka pohranjenih u elektroničkoj komunikacijskoj mreži,

3. *sigurnosni incident*: događaj koji može uzrokovati narušavanje sigurnosti i/ili gubitak integriteta mreže koji može utjecati na rad elektroničkih komunikacijskih mreža i/ili usluga.
4. *računalno-sigurnosni incident:* jedan ili više računalnih sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava ili računalne mreže, te ugrožavaju povjerljivost, cjelovitost i dostupnost informacija koji se korištenjem informacijskog sustava ili računalne mreže kreiraju, obrađuju, pohranjuju ili prenose.

(NN br. 66/19, dodana nova točka 4.)

MJERE ZA ZAŠTITU SIGURNOSTI I INTEGRITETA MREŽA I USLUGA

Članak 3.

(1) Operatori su obvezni provesti odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svojih javnih komunikacijskih mreža i/ili usluga. Te mjere moraju osigurati neprekidno pružanje javnih komunikacijskih usluga putem mreža, kao i stupanj sigurnosti, odgovarajući na prijetnje i sprječavajući sigurnosne incidente ili ublažavajući njihov utjecaj na rad javne komunikacijske mreže, mrežno povezivanje kao i/ili na javne komunikacijske usluge korisnika. Poduzete mjere osobito se provode kako bi se spriječio i umanjio utjecaj sigurnosnih incidenata na korisnike usluga i međusobno povezane elektroničke komunikacijske mreže.

(2) U mjere pod stavkom 1. moraju biti uključene i procedure za upravljanje rizicima, sigurnosni zahtjevi za osoblje, sigurnost sustava i prostora, upravljanje postupcima, upravljanje sigurnosnim incidentima, upravljanje kontinuitetom poslovanja te nadzor i testiranje sigurnosti.

(3) Popis minimalnih mjera iz stavka 1. i 2. ovog članka i referentnih normi za njihovo provođenje prikazan je u Dodatku 1.

(4) Osim navedenih referentnih normi iz Dodatka 1. operatori mogu primijeniti i druge odgovarajuće norme u svrhu ostvarivanja mjera iz ovog članka.

(5) Operatori su obvezni elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja dostaviti Agenciji dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme.

Članak 3.a.

(1) Operator mora najmanje jednom godišnje provesti reviziju informacijskog sustava kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti iz Dodatka 1 ovog Pravilnika.

(2) Nalaz revizije iz stavka 1. ovog članka, zajedno s planom uklanjanja uočenih nedostataka, potrebno je dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu.

(3) Postupak revizije treba provoditi tako da se u obzir uzme značaj pojedinih dijelova informacijskog sustava za funkcioniranje cijelog sustava te rezultate prethodnih revizija. Reviziju mogu obavljati zaposlenici operatora koji nisu vezani za područje revizije i koji imaju odgovarajuće znanje i iskustvo ili vanjsko revizorsko tijelo.

OBAVJEŠTAVANJE AGENCIJE O SIGURNOSNIM INCIDENTIMA

Članak 4.

(1) Operatori su obvezni obavijestiti Agenciju u slučaju neovlaštenog povezivanja s javnom komunikacijskom mrežom ili dijelom mreže te u slučaju kršenja sigurnosti ili integriteta javnih komunikacijskih usluga, koji su značajnije utjecali na obavljanje djelatnosti javnih komunikacijskih mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2.

(2) O sigurnosnim incidentima iz stavka 1. operatori moraju obavijestiti Agenciju bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. ovog Pravilnika:

1. u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2,
2. u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta,
3. u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta.

(3) Operatori moraju osigurati Agenciji podatke za kontakt sukladno Dodatku 3 u svrhu brze razmjene informacija o sigurnosnim incidentima između operatora i Agencije, te pružiti potrebne tehničke informacije Agenciji radi praćenja sigurnosti i integriteta javnih komunikacijskih mreža.

(4) Sve obavijesti o sigurnosnim incidentima moraju se dostavljati Agenciji upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način sukladno obrascu iz Dodatka 3.

(5) Agencija može zatražiti dopunu izvješća iz stavka 2. u svrhu praćenja određenog sigurnosnog incidenta te boljeg razumijevanja prirode nastalog sigurnosnog incidenta.

(6) Operator može obavijestiti Agenciju i o drugim, po mišljenju operatora, važnim sigurnosnim incidentima koji se odnose na sigurnost i integritet javnih komunikacijskih mreža i/ili usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavka 1.

Članak 5.

(1) Operatori su obvezni obavijestiti Agenciju o svakom značajnom računalno-sigurnosnom incidentu koji je značajnije utjecao na dostupnost, cjelovitost ili povjerljivost informacijskog sustava ili računalne mreže, sukladno kriterijima za izvješćivanje iz Dodatka 2. ovog Pravilnika. Prilikom podnošenja prijava sukladno ovom članku, u cijelosti se primjenjuje Nacionalna taksonomija računalno-sigurnosnih incidenata.

(2) O računalno-sigurnosnim incidentima iz stavka 1. operatori moraju obavijestiti Agenciju bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. ovog Pravilnika:
   1. u roku od najviše 24 sata nakon otkrivanja računalno-sigurnosnog incidenta
   2. u roku od najviše 20 dana od dana otklanjanja računalno-sigurnosnog incidenta.

(3) Sve obavijesti o računalno-sigurnosnim incidentima moraju se dostavljati Agenciji upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte racunalni.incidenti@hakom.hr ili na drugi prikladan način, sukladno obrascu iz Dodatka 3.

(4) Nakon pribavljanja potpunih informacija sukladno ovom članku, Agencija će informacije o prijavljenim računalno-sigurnosnim incidentima dostaviti CERT-u kao nacionalnom tijelu za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

(5) Nakon razmatranja prijavljenih incidenata, Agencija će u suradnji s Nacionalnim CERT-om, naložiti eventualnu dopunu izvješća te poduzimanje drugih mjera propisanih Zakonom, uključujući i davanje određenih preporuka, smjernica i upozorenja o sigurnosnim ugrozama.

(6) U slučaju potrebe pokretanja odgovarajućeg postupka iz nadležnosti Agencije u odnosu na prijavljene incidente, Agencija će aktivno surađivati sa CERT-om, te u slučaju potrebe zatražiti stručnu pomoć i koordinaciju pri definiraju konkretnih aktivnosti i korektivnih mjera u vezi s nastalim ili potencijalnim računalno-sigurnosnim incidentima.

(7) Nacionalni CERT će temeljem prikupljenih prijava dobivenih putem adrese elektroničke pošte navedene u stavku 3. ovog članka, dostaviti Agenciji najmanje jednom mjesečno izvješće o značajnim incidentima iz prethodnog razdoblja.

(8) U slučaju osiguravanja alternativnog načina podnošenja prijava pri CERT-u putem odgovarajuće platforme, Agencija će obavijestiti operatore o promijeni načina prijavljivanja značajnih računalno-sigurnosnih incidenata.

(NN br. 66/19, dodan novi članak 5.)

OBAVJEŠTAVANJE DRUGIH SUBJEKATA O SIGURNOSNIM INCIDENTIMA

Članak 6.

Operatori su obvezni bez odgode:

1. na odgovarajući način obavijestiti korisnike javnih komunikacijskih usluga o značajnijem prekidu pružanja javnih komunikacijskih mreža i/ili usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2. Ako su ugrožene osnovne usluge kao što su glasovna usluga, SMS usluga ili usluga pristupa internetu, operatori moraju bez odgode objaviti informacije o nastalom značajnom incidentu na službenoj stranici. Informacije o značajnom incidentu moraju sadržavati opis područja obuhvaćenog incidentom, koji može biti prikazan i u kartografskom obliku
2. obavijestiti druge operatore o mjerama koje mogu biti poduzete od strane korisnika javnih komunikacijskih usluga kako bi se uklonila prijetnja sigurnosnog incidenta, koje se odnose na terminalnu opremu korisnika, navodeći moguće troškove vezane uz provođenje takvih mjera.

ZAVRŠNE ODREDBE

Članak 7.

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga stupa na snagu šest (6) mjeseci od dana objave u „Narodnim novinama“.

PRIJELAZNE I ZAVRŠNE ODREDBE PRAVILNIKA O IZMJENAMA PRAVILNIKA O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA (NN br. 126/13)

Ovaj Pravilnik stupa na snagu osmog (8) dana od dana objave u „Narodnim novinama“.

PRIJELAZNE I ZAVRŠNE ODREDBE PRAVILNIKA O IZMJENAMA I DOPUNAMA PRAVILNIKA O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA (NN br. 67/16)

Ovaj Pravilnik stupa na snagu 1. siječnja 2017.

PRIJELAZNE I ZAVRŠNE ODREDBE PRAVILNIKA O IZMJENAMA I DOPUNAMA PRAVILNIKA O NAČINU I ROKOVIMA

PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA
(NN br. 66/19)

Ovaj Pravilnik o izmjenama i dopunama Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga stupa na snagu u roku od 3 mjeseca od dana objave u „Narodnim novinama“.

DODATAK 1

MINIMALNE MJERE SIGURNOSTI

Minimalne mjere sigurnosti	Referentne norme
Procedure za upravljanje rizicima	ISO 27001:2013 ISO 27002:2015 ISO 27005:2011
Sigurnosni zahtjevi za osoblje	ISO 27001:2013 ISO 27002:2015
Sigurnost sustava i prostora	ISO 27001:2013 ISO 27002:2015
Upravljanje postupcima	ISO 27001:2013 ISO 27002:2015
Upravljanje sigurnosnim incidentima	ISO 27001:2013 ISO 27002:2015
Upravljanje kontinuitetom poslovanja	ISO 22301:2012
Nadzor i testiranje sigurnosti	ISO 27001:2013 ISO 27002:2015

DODATAK 2

KRITERIJI ZA IZVJEŠĆIVANJE

Sigurnosni incidenti	**Minimum krajnjih korisnika obuhvaćenih sigurnosnim incidentom**	**Minimalno trajanje sigurnosnog incidenta**
Mrežno onemogućavanje, primanja, ostvarivanja ili točnog usmjeravanja poziva prema hitnim službama	10 000 korisnika	neovisno o trajanju
Onemogućena govorna usluga u nepokretnoj mreži	12 670 korisnika	8 sati
Onemogućena govorna usluga u nepokretnoj mreži	25 340 korisnika	6 sati
Onemogućena govorna usluga u nepokretnoj mreži	63 350 korisnika	4 sata
Onemogućena govorna usluga u nepokretnoj mreži	126 700 korisnika	2 sata
Onemogućena govorna usluga u nepokretnoj mreži	190 000 korisnika	1 sat
Onemogućena govorna usluga u pokretnoj mreži	45 465 korisnika	8 sati
Onemogućena govorna usluga u pokretnoj mreži	90 930 korisnika	6 sati

Onemogućena govorna usluga u pokretnoj mreži	227 326 korisnika	4 sata
Onemogućena govorna usluga u	454 652 korisnika	2 sata
pokretnoj mreži		
Onemogućena govorna usluga u pokretnoj mreži	681 979 korisnika	1 sat
Onemogućena usluga pristupa internetu u nepokretnoj mreži	11 133 korisnika	8 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	22 266 korisnika	6 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	55 666 korisnika	4 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	111 333 korisnika	2 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	167 000 korisnika	1 sat
Onemogućena usluga pristupa internetu u pokretnoj mreži	35 814 korisnika	8 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	71 628 korisnika	6 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	179 070 korisnika	4 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	358 140 korisnika	2 sata

Onemogućena usluga pristupa internetu u pokretnoj mreži	537 211 korisnika	1 sat

Računalno-sigurnosni incident		Uvjeti prijave računalno-sigurnosnog incidenta
Kategorija	**Potkategorija**	
Uspješno ostvarena kompromitacija	Malware URL	Zlonamjerna funkcionalnost aktivna je duže od 12 sati.
	Phishing URL	
	Spam URL	
	Web Defacement	
	Sustav zaražen zlonamjernim kodom	
	C&C	
	Korisnički račun	
Pokušaj neovlaštenog pristupa	Pogađanje zaporki	Potrebno je prijaviti svaki slučaj detektiranog pokušaja neovlaštenog pristupa.
	Pokušaj iskorištavanja ranjivosti	
Dostupnost	DoS -Volumetrički napad	Potrebno je prijaviti napade na infrastrukturu operatora koji pruža uslugu pristupa internetu.
	DoS - Napad na aplikacijskom sloju	
Prijevare	Phishing	Potrebno je prijaviti svaki detektirani slučaj ciljanog phishing napada (kampanje) prema davatelju usluge pristupa internetu koji za cilj ima stjecanje financijske koristi, krađu osjetljivih podataka ili pokretanje zlonamjernog programa.
Ciljani napad – APT (eng. Advanced persistent threat)		Potrebno je prijaviti svaki slučaj ovakvog oblika napada.
Ostalo		Prijava po procjeni operatora davatelja usluga

(NN br. 66/19, izmjena Dodatka 2)

DODATAK 3

PREDLOŽAK ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA

Potrebni podaci	Popunjava operator
Opis sigurnosnog incidenta	
Naziv operatora	
Datum i vrijeme nastanka/otkrivanja sigurnosnog incidenta	
Izvorni uzrok	☐ Sistemske greške ☐ Ljudska greška ☐ Zlonamjerne radnje ☐ Prirodni fenomen ☐ Greška treće strane
Početni uzrok	☐ Palež ☐ Presjek kabela ☐ Krađa kabela ☐ Prekid hlađenja ☐ DoS napad ☐ Zemljotres ☐ Elektromagnetska interferencija ☐ Pogrešna zamjena/nadogradnja hardvera ☐ Pogrešna zamjena/nadogradnja softvera ☐ Vatra ☐ Poplava ☐ Iscrpljene zalihe goriva ☐ Kvar na hardveru ☐ Krađa hardvera ☐ Obilan snijeg/led ☐ Oluja ☐ Zlonamjerni softveri i virusi ☐ Preotimanje mrežnog prometa ☐ Nema informacije ☐ Ništa ☐ Preopterećenje ☐ Proceduralna mana ☐ Prekid napajanja ☐ Strujni udari ☐ Sigurnosno isključivanje ☐ Softverska greška ☐ Teroristički napad ☐ Požar ☐ Drugo
Naknadni uzrok	☐ Palež ☐ Presjek kabela ☐ Krađa kabela ☐ Prekid hlađenja ☐ DoS napad ☐ Zemljotres ☐ Elektromagnetska interferencija ☐ Pogrešna zamjena/nadogradnja hardvera ☐ Pogrešna zamjena/nadogradnja softvera ☐ Vatra ☐ Poplava ☐ Iscrpljene zalihe goriva ☐ Kvar na hardveru ☐ Krađa hardvera ☐ Obilan snijeg/led ☐ Oluja ☐ Zlonamjerni softveri i virusi ☐ Preotimanje mrežnog prometa ☐ Nema informacije ☐ Ništa ☐ Preopterećenje ☐ Proceduralna mana ☐ Prekid napajanja ☐ Strujni udari ☐ Sigurnosno isključivanje ☐ Softverska greška ☐ Teroristički napad ☐ Požar ☐ Drugo
Imovina obuhvaćena incidentom	☐ Adresni poslužitelji ☐ Rezervno napajanje ☐ Sustavi naplate i posredovanja ☐ Zgrade i fizički sigurnosni sustavi ☐ Sustav hlađenja ☐ Inteligentni mrežni uređaji ☐ Međukonekcijske točke ☐ Logički sigurnosni sustavi ☐ Bazne stanice i upravljački sklopovi ☐ Centar za razmjenu poruka ☐ Nema infomacije ☐ Operativni sustav potpore ☐ Nadzemni kabeli ☐ PSTN prospojnici ☐ Sustav napajanja ☐ Ulični kabineti ☐ Podmorski kabeli ☐ Pretplatnička oprema ☐ Prospojnici i usmjerivači ☐ Prijenosni čvorovi

Vrsta usluge koju obuhvaća sigurnosni incident	☐ Nepokretna telefonija Trajanje _____ Broj korisnika_____ Tehnologije: ☐ PSTN ☐ VoIP ☐ DSL ☐ Vlakno ☐ Kabel ☐ Nepokretni internet Trajanje _____ Broj korisnika_____ Tehnologije: ☐ DSL ☐ Vlakno ☐ Kabel ☐ Pokretna telefonija Trajanje _____ Broj korisnika_____ Tehnologije: ☐ GSM ☐ UMTS ☐ LTE ☐ Pokretni internet Trajanje _____ Broj korisnika_____ Tehnologije: ☐ GPRS/EDGE ☐ UMTS ☐ LTE ☐ SMS Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ MMS Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Satelitska TV Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Međunarodni roming Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Radijsko emitirnje Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ TV emitiranje Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Kabelska TV Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ IPTV Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Video na zahtjev Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Javni WIFI Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Glasovne web usluge Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Usluge web poruka Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Javni email Trajanje _____ Broj korisnika_____ Tehnologije: _____ ☐ Ostale obuhvaćene usluge Trajanje _____ Broj korisnika_____ Ime usluge: _____
Mreža	☐ Zračni kabel ☐ Podzemni kabel ☐ Sustav električnih kabela ☐ Optička vlakna ☐ Radio (zemaljska) mreža ☐ Satelitska mreža ☐ Podmorski kabel

Utjecaj na hitne službe	☐ DA ☐ NE
Utjecaj na međupovezivanje	☐ DA ☐ NE
Rješavanje sigurnosnog incidenta i opis poduzetih mjera (opis aktivnosti koje su poduzete nakon otkrića incidenta za rješavanje incidenta)	
Mjere poduzete nakon otklanjanja sigurnosnog incidenta (opis poduzetih aktivnosti od strane operatora za smanjivanje vjerojatnosti ponavljanja incidenta ili utjecaja incidenta)	
Dugoročne mjere	
Kontakt podaci za praćenje procesa	
Ostale važne informacije	

PREDLOŽAK ZA IZVJEŠĆIVANJE RAČUNALNO-SIGURNOSNIH INCIDENATA

Potrebni podaci	Popunjava operator	
Opis sigurnosnog incidenta		
Naziv operatora		
Datum i vrijeme nastanka/otkrivanja sigurnosnog incidenta		
Klasifikacija incidenta (prema Nacionalnoj taksonomiji)		
Podklasifikacija incidenta (prema Nacionalnoj taksonomiji)		
UČINAK INCIDENTA		
Usluge/procesi zahvaćeni incidentom (zaustavljene, ugrožene, usporene)		
Vrijeme trajanja sigurnosnog incidenta		
Broj obuhvaćenih korisnika		
Utjecaj na hitne službe	☐ DA	☐ NE
Utjecaj na međupovezivanje	☐ DA	☐ NE

RJEŠAVANJE INCIDENTA	
IP adresa izvora incidenta	
URL (npr. phishing URL, malware URL,...)	
Tekst poruke koja upućuje na incident (npr. tekst phishing poruke)	
Rješavanje sigurnosnog incidenta i opis poduzetih mjera (opis aktivnosti koje su poduzete nakon otkrića incidenta za rješavanje incidenta)	
Mjere poduzete nakon otklanjanja sigurnosnog incidenta (opis poduzetih aktivnosti od strane operatora za smanjivanje vjerojatnosti ponavljanja incidenta ili utjecaja incidenta)	
Dugoročne mjere	
Kontakt podaci za praćenje procesa	
Ostale važne informacije	

(NN br. 66/19, izmjena Dodatka 3)