



Savska c. 41/VII, 10000 ZAGREB  
poštanski pretinac 93

e-mail: [info@upuz.hr](mailto:info@upuz.hr)

IBAN: HR2523600001101235488

Matični broj: 3279855

OIB: 32787730056

CENTRALA	6311-550
FAX	6176-659
Direktor	6311-551
Pravna služba	6311-570
Ekonomska služba	6311-558
Računovodstvo, narudžbe i pretplata	6311-556

ZAGREB  
SAVSKA 41/7

REPUBLIKA HRVATSKA  
MINISTARSTVO ZDRAVSTVA  
Ksaver 200a, 10000 Zagreb  
n/p ministrice  
doc.dr.sc. Irena Hrštić, dr.med. spec.

Broj: 89/I-9/25  
Zagreb, 18.03.2025.

**Predmet:** Osiguranje potrebnih resursa za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima u zdravstvenom sustavu  
- zamolba za izdavanje upute zdravstvenim ustanovama, dostavlja se

Poštovana ministrice doc.dr.sc. Irena Hrštić, dr.med. spec.,

budući da je **Europska komisija u siječnju ove godine predstavila Akcijski plan usmjeren na jačanje kibernetičke sigurnosti bolnica i pružatelja zdravstvene zaštite koji se planira provesti tijekom 2025. i 2026. godine**, a koji uključuje i uspostavu Europskog centra za podršku kibernetičkoj sigurnosti u zdravstvu koji će bolnicama i zdravstvenim ustanovama pružati prilagođene smjernice, alate, usluge i obuku, ravnatelji zdravstvenih ustanova obraćaju se Udruzi poslodavaca u zdravstvu Hrvatske i traže informacije o tome na koji način će se zdravstvenim ustanovama **osigurati financijska sredstva za nabavu opreme i računalnih programa, certificirane u skladu s programima/normama u području kibersigurnosti i osposobljavanje osoba odgovornih za upravljanje mjerama i zaposlenika zdravstvenih ustanova, s ciljem učinkovite provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima u zdravstvenom sustavu.**

Naime, Akcijski plan nadovezuje se na postojeći zakonodavni okvir EU-a u području kibernetičke sigurnosti, uključujući Direktivu (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 (SL L 330/80, 27.12.2022.) (dalje u tekstu: **NIS2 direktiva**) na snazi od 16. siječnja 2023. godine, koja **postavlja zdravstveni sektor kao kritično područje**, i preuzeta je u hrvatsko zakonodavstvo Zakonom o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24., dalje u tekstu: Zakon) na snazi od 15. veljače 2024. godine. **Pod točkom 5. Priloga I. Zakona, u sektore visoke kritičnosti kategorizirano je zdravstvo te obuhvaća pružatelje zdravstvene zaštite, odnosno svaku fizičku ili pravnu osobu ili bilo koji subjekt koji obavlja zdravstvenu djelatnost u Republici Hrvatskoj u skladu sa zakonom kojim se uređuje zdravstvena zaštita, referentne laboratorije EU-a iz članka 15. Uredbe (EU) 2022/2371 Europskog parlamenta i Vijeća, subjekte koji obavljaju djelatnosti istraživanja i razvoja lijekova, subjekte koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. (»Narodne novine«, br. 58/07. i 72/07.). Ujedno, sukladno članku 9. podstavku 1. i članku 11. podstavku 2. Zakona, zdravstvo je**

razvrstano u kategoriju ključnih subjekata. Člankom 28. Zakona izrijekom je utvrđeno da su ključni i važni subjekti dužni prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima koristiti se određenim IKT (*informacijsko-komunikacijska tehnologija, dalje: IKT*) proizvodima, IKT uslugama i IKT procesima te upravljanim sigurnosnim uslugama koje su certificirane na temelju europskih programa kibernetičke sigurnosne certifikacije ili nacionalnih shema kibernetičke sigurnosne certifikacije, ako je takva obveza propisana: mjerodavnim propisima Europske unije, posebnim propisima kojima se uređuje područje pružanja određenih usluga odnosno obavljanja određenih djelatnosti, ovim Zakonom ili Uredbom o kibernetičkoj sigurnosti („Narodne novine“ br. 135/24., dalje u tekstu: Uredba) koju je na temelju članka 24. Zakona, Vlada Republike Hrvatske donijela na sjednici održanoj 21. studenoga 2024. i koja je snazi od 30. studenoga 2024. godine.

U bitnom, Zakonodavac je člankom 29. izrijekom utvrdio da su za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima sukladno ovom Zakonu odgovorni članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršna tijela jedinica lokalne i područne (regionalne) samouprave (u daljnjem tekstu: osobe odgovorne za upravljanje mjerama). Osobe odgovorne za upravljanje mjerama dužne su odobravati mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati radi usklađivanja s obvezama utvrđenim ovim Zakonom i provedbenim propisom o zahtjevima kibernetičke sigurnosti te kontrolirati njihovu provedbu. U svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja, osobe odgovorne za upravljanje mjerama dužne su: pohađati odgovarajuća osposobljavanja, zaposlenicima subjekta omogućiti pohađanje odgovarajućih osposobljavanja. Nadalje, Zakonodavac izrijekom utvrđuje i prekršajnu odgovornost ključnog subjekta i člankom 101. stavkom 1. Zakona propisuje da će se novčanom kaznom u iznosu od 10.000,00 eura do 10.000.000,00 eura ili u iznosu od 0,5 % do najviše 2 % ukupnog godišnjeg prometa dotičnog subjekta na svjetskoj razini ostvarenog u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći, kazniti za prekršaj prekršajno odgovoran ključan subjekt, koji ne poduzima, djelomično poduzima ili ne poduzima u roku propisane mjere upravljanja kibernetičkim sigurnosnim rizicima (članak 26. ovoga Zakona), koji se prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima ne koristi certificiranim IKT proizvodima, IKT uslugama i IKT procesima, ako je takva obveza propisana za subjekta (članak 28. ovoga Zakona), čije osobe odgovorne za upravljanje mjerama ne odobravaju mjere upravljanja kibernetičkim sigurnosnim rizicima i/ili ne kontroliraju njihovu provedbu odnosno ne osiguravaju provedbu odgovarajućih osposobljavanja u svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja (članak 29. ovoga Zakona), kao i u svim drugim taksativno navedenim slučajevima iz članka 101. stavka 1. Zakona. Stavkom 2. istog članka Zakona utvrđeno je da će se za prekršaj iz stavka 1. kazniti i fizičke osobe koje su sukladno članku 29. ovoga Zakona odgovorne za upravljanje mjerama prekršajno odgovornog ključnog subjekta, novčanom kaznom u iznosu od 1000,00 do 6000,00 eura.

Prilogom II. Uredbe, utvrđena je predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima te je s tim u vezi utvrđeno, da će subjekt u okviru provedbe ove mjere provoditi i podskupove mjera, među inim, definirati i usvojiti na

upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga, odgovornosti i obveza, te koji opisuje procese upravljanja kibernetičkom sigurnošću u subjektu, osigurati upoznavanje svih zaposlenika subjekta i relevantnih pravnih osoba, s kojima subjekt ima poslovni odnos, poput njegovih dobavljača ili pružatelja usluga, s glavnim strateškim odrednicama kibernetičke sigurnosne politike koji se na njih odnose, osigurati potrebne resurse za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima, što uključuje financijska sredstva, tehničke alate i ljudske potencijale s potrebnim stručnim znanjima.

Sukladno članku 56. stavku 2. Zakona, na prijedlog SOA-e (*Sigurnosno-obavještajna agencija*), kao tijela odgovornog za upravljanje kibernetičkim krizama, **Vlada Republike Hrvatske 9. siječnja 2025. godine donijela je Nacionalni program upravljanja kibernetičkim krizama**, o čemu je SOA zadužena izvijestiti sva tijela uključena u rad Međuresorne radne skupine za pripremu prijedloga podzakonskih akata Zakona o kibernetičkoj sigurnosti i **druga tijela državne uprave kojima su posebnim zakonima dodijeljene sektorske nadležnosti u sektorima iz Priloga I. i Priloga II. Zakona o kibernetičkoj sigurnosti**. Također, u obrazloženju Odluke o njegovom donošenju navedeno je da su sredstva za provedbu Nacionalnog programa upravljanja kibernetičkim krizama osigurana u državnom proračunu Republike Hrvatske te provedba istog neće iziskivati dodatni fiskalni učinak.

Iz gore navedenih razloga predlaže se nabavu opreme za kibersigurnost, isplanirati i provesti „na vrijeme“ te s tim u vezi molimo resorno Ministarstvo da izda uputu zdravstvenim ustanovama i iste obavijesti o tome na koji način su za zdravstvo planirana odnosno osigurana financijska sredstva za nabavu opreme certificirane u skladu s programima/normama u području kibersigurnosti (državni proračun, EU sufinanciranje ili dr.) i kada se financijska sredstva planiraju dodijeliti te na koji način je planirano u zdravstvenim ustanovama organizirati i provesti osposobljavanje osoba odgovornih za upravljanje i zaposlenika za učinkovitu provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima.

Unaprijed zahvaljujemo, uz srdačan pozdrav.

S poštovanjem,

Dostaviti:

1. Naslovu
2. Arhiva, ovdje

Obavijest o tome:

1. Hrvatski zavod za zdravstveno osiguranje, Margaretska 3, 10000 Zagreb, n/p ravnatelja Lucian Vukelić, dr. med. spec.



Direktor:

Mr. Dražen Jurković, dr. med. spec.