Zadeva: OBVESTILO: Zakon o informacijski varnosti
Od: Info ZKOS <info@zdruzenje-kos.si>
Datum: 19. 5. 2026, 08:49
Za: Info ZKOS <info@zdruzenje-kos.si>

Zadeva: OBVESTILO ČLANICAM ZKOS V ZVEZI Z NOVIMI PRAVILI O INFORMACIJSKI VARNOSTI

Ljubljana, 18.5.2026

Spoštovani,

od 19. junija lani je v veljavi novi **Zakon o informacijski varnosti (ZInfV-1)**, ki v slovenski pravni red med drugim prenaša določbe **direktive NIS 2** (Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148).

O tem in o določenih obvezah smo poročali že v lanskem letu na skupščini, letnem posvetu in na letošnji skupščini po koncu v okviru splošne razprave.

Ker smo bili na združenju neformalno obveščeni, da nekateri operaterji še ne izpolnjujete svojih obveznosti iz navedenega zakona (npr. obveznosti glede samoregistracije), v nadaljevanju podajamo podrobnejša pojasnila v zvezi z obveznostmi operaterjev kot ponudnikov javnih elektronskih komunikacijskih omrežij in storitev.

Kot **zavezance** Zakon o informacijski varnosti (v 1. alineji 1. točke 2. odstavka 6. člena zakona) med drugim opredeljuje vse subjekte, ki opravljajo storitev kot ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, in sicer ne glede na število zaposlenih ali letni promet/letno bilančno vsoto. Navedeno pomeni, **da vsi operaterji telekomunikacijskih storitev izpolnjujejo zakonski kriterij za uvrstitev med zavezance po ZInfV-1**.

Zakon zavezance nadalje razdeljuje na **bistvene** in **pomembne** subjekte. Med ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev se za bistvene subjekte štejejo tisti, ki imajo:

- vsaj 50 zaposlenih in
- letni promet ali letno bilančno vsoto vsaj 10 milijonov eurov (3. točka 2. odstavka 7. člena ZInfV-1).

Operater, ki te »velikostne« kriterije izpolnjuje, šteje za bistven subjekt. Če teh kriterijev ne izpolnjuje, pa je operaterja elektronskih komunikacijskih omrežij mogoče šteti za pomembni subjekt v smislu 7. člena ZInfV-1.

Kot zavezanec po ZInfV-1 mora ponudnik javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev **opraviti samoregistracijo** pri pristojnem organu, to je Uradu Vlade RS za informacijsko varnost (URSIV).

V skladu z drugim odstavkom 60. člena ZInfV-1 so morali zavezanci prvo registracijo po mehanizmu za samoregistracijo opraviti v šestih mesecih po uveljavitvi zakona, torej do 19. decembra 2025. **V primeru, da samoregistracije še niste izvedli, jo čim prej opravite!**

Samoregistracija se izvede prek spletnega obrazca, ki je dostopen na portalu Republike Slovenije: https://ursiv.si/. Več informacij ter navodila za izpolnjevanje spletnega obrazca so dostopni na naslednjih povezavah:

- https://www.gov.si/novice/2025-08-21-na-voljo-je-spletni-obrazec-za-samoregistracijo-zavezancev-po-zakonu-o-informacijski-varnosti/
- https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Navodila/Navodila-za-izpolnjevanje-obrazca_v1.2.november25.pdf.

Zavezanci z uporabo mehanizma za samoregistracijo sporočijo tudi morebitne spremembe podatkov, ki so jih podali ob registraciji, najpozneje v desetih delovnih dneh od datuma spremembe.

Poleg registracije pa morajo bistveni in pomembni subjekti izvajati tudi druge obveznosti glede zagotavljanja informacijske varnosti, ki jih nalaga ta zakon. Ne gre za popolno novost, saj so imeli operaterji že pred uveljavitvijo ZInfV-1 po določbah Zakona o elektronskih komunikacijah (ZEKom-2) vsebinsko podobne obveznosti na področju informacijske varnosti. ZInfV-1 smiselno enake obveznosti opredeljuje na nekoliko bolj splošen način, da se lahko enotno nanašajo na različne zavezance na različnih vsebinskih področjih. Med temi obveznostmi so bistvene naslednje:

- Zavezanci morajo imeti odgovorne osebe za izvajanje ukrepov po tem zakonu. Odgovorne osebe se najmanj vsaka štiri leta izobražujejo oziroma usposabljajo na področju obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti ali storitve, ki jih izvaja subjekt. Odgovorne osebe zagotavljajo redno usposabljanje zaposlenih, da pridobijo dovolj znanj in spretnosti, s katerimi se usposobijo za prepoznavanje tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja subjekt. Odgovorne osebe zagotavljajo, da vsi skrbniki informacijsko-komunikacijskih sistemov zavezanca opravijo redno letno usposabljanje, da pridobijo in ohranijo raven znanj in spretnosti ter so usposobljeni za prepoznavanje in ocenjevanje tveganj ter za oceno praks obvladovanja tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja subjekt.

- Bistveni in pomembni subjekti za zagotavljanje visoke ravni informacijske in kibernetske varnosti ter odpornosti svojih omrežnih in informacijskih sistemov

  V skladu z ZInfV-1 morata SUVI in SUNP obsegati najmanj:

  1. politiko ali področne politike o varnosti omrežnih in informacijskih sistemov,
  2. natančen in posodobljen popis informacijskih in drugih sredstev in podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter njihove upravljavce;
  3. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije;
  4. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij ter določitvijo vlog in odgovornosti;
  5. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
  6. načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente ter opisom vlog in odgovornosti za odzivanje na incidente;
  7. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in

razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost, pri čemer ta načrt upošteva tveganja in področne posebnosti bistvenega ali pomembnega subjekta in

8. politiko s postopki za presojo učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

- Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, pri čemer mora ta sistem obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke in procese, ki so potrebni za njihovo delovanje ali opravljanje storitev.
- Vzorčni primeri teh politik so dostopni
- Bistveni in pomembni subjekti morajo sprejeti tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve. Podrobne zahteve glede
- Bistveni ali pomembni subjekt lahko ob upoštevanju ocene tveganja preveri preteklost zaposlenih in kandidatov za zaposlitev na delovnih mestih, pomembnih za opravljanje storitev subjekta, ki imajo ali bodo imeli pooblastilo za neposredni ali oddaljeni dostop do njegovih ključnih informacijskih sistemov. V skladu z oceno tveganja lahko preveri preteklost tudi za zaposlene pri pogodbenih izvajalcih. Preverjanje preteklosti se opravi za zadnjih pet let. Preverjanje se opravi na podlagi soglasja osebe. Če oseba ne da soglasja za preverjanje preteklosti, se ji delo na delovnih mestih in v prostorih iz prvega odstavka tega člena ne dovoli oziroma se pogodba ne sklene. Za ta namen lahko subjekt vodi tudi evidence s podatki o osebah.
- Bistveni in pomembni subjekti določijo postopke in ustrezna orodja za spremljanje in beleženje dogodkov v svojih omrežjih in informacijskih sistemih oziroma zagotovijo zbiranje in ohranjanje dnevniških zapisov, da bi zaznali ali odkrili dogodke, ki bi se lahko šteli za incidente ali skorajšnje incidente, in se ustrezno odzvali za ublažitev njihovega negativnega učinka. Dnevniški zapisi morajo biti zbrani in ohranjeni v obsegu in na način, ki omogoča rekonstrukcijo in analizo incidentov ali skorajšnjih incidentov.
- Pomembni subjekti izvedejo samooceno skladnosti najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Samoocena skladnosti se izvede na način, da se dokumentirano preverita skladnost pomembnega subjekta z njegovo varnostno dokumentacijo in izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost. Samoocena skladnosti se lahko izvede tudi v okviru notranje revizije. Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt izpolnjuje zahteve, predpisane s tem zakonom, ta sestavi izjavo o skladnosti, pri čemer ta vsebuje potrebne elemente samoocenjevanja skladnosti, ki omogočajo izvedbo ponovljivosti opravljene ocene. Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt ne izpolnjuje predpisanih zahtev, ta sestavi izjavo o ugotavljanju neskladnosti, v kateri navede ugotovljene neskladnosti in način njihove odprave z roki za izvedbo.

Bistveni subjekti izvedejo oceno skladnosti najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Ocena skladnosti se izvaja kot revizija skladnosti s predpisi s področja informacijske varnosti ali v okviru notranje revizije, ki se izvaja na podlagi drugih predpisov in vključuje področje informacijske varnosti iz ZInfV-2 in na podlagi tega zakona izdanih podzakonskih predpisov ali izvedbenih aktov Evropske komisije. Oceno skladnosti lahko v okviru notranje revizije poleg revizorjev informacijskih sistemov izvajajo tudi notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo, ki je posameznik oziroma posameznica ali organizacija, ki ima izkazano poglobljeno strokovno znanje na področju

informacijsko-komunikacijskih tehnologij, katerega ali katere delo revizor uporabi kot strokovno pomoč pri pridobivanju zadostnih in ustreznih revizijskih dokazov. Revizor informacijskih sistemov ali notranji revizor pripravi poročilo o izvedeni oceni skladnosti. Če poročilo o izvedeni oceni skladnosti iz prejšnjega odstavka vsebuje ugotovitve neskladnosti in priporočila revizorja informacijskih sistemov za njihovo odpravo, bistveni subjekt pripravi načrt za odpravo ugotovljenih neskladnosti, določi način njihove odprave in roke za izvedbo.

- Bistveni in pomembni subjekti morajo pristojnemu nacionalnemu organu na podlagi pisne zahteve predložiti podatke in informacije, ki jih ta potrebuje za izvajanje svojih pristojnosti po tem zakonu, in sicer v roku, ki ga določi v svoji pisni zahtevi. Zahtevani podatki in informacije morajo biti sorazmerni namenu, za katerega bodo uporabljeni. Pristojni nacionalni organ mora v zahtevi navesti namen uporabe zahtevanih podatkov in informacij.

- Za obvladovanje tveganj za varnost omrežij in informacijskih sistemov bistveni in pomembni subjekti pri izvajanju ukrepov za obvladovanje tveganj prednostno uporabljajo kvalificirane storitve zaupanja in tiste proizvode, storitve ali postopke IKT, ki so jih razvili bistveni ali pomembni subjekti ali so bili kupljeni pri drugih subjektih in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi 49. člena Uredbe 2019/881/EU.

- Bistveni in pomembni subjekti za zagotovitev skladnega izvajanja ukrepov za obvladovanje tveganj in varnostno dokumentacijo v največji možni meri in skladno z najboljšimi razpoložljivimi praksami ter tudi priporočili in smernicami agencije ENISA uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. Pristojni nacionalni organ na osrednjem spletnem mestu državne uprave objavlja ustrezne informacije o evropskih in mednarodnih standardih in tehničnih specifikacijah, ki obravnavajo varnost omrežnih in informacijskih sistemov, ter ozavešča zavezance glede njihove uporabe. Za nadgradnjo ravni kibernetske varnosti bistvenih in pomembnih subjektov regulativni organi ali nadzorniki, ki so pristojni za posamezne sektorje, na osrednjem spletnem mestu državne uprave objavljajo tehnično specifične industrijske standarde in tehnične specifikacije, ki se štejejo kot priporočila. Za primer, da bodo za operaterje potrebni posebni sektorsko specifični ukrepi, lahko AKOS izda splošni akt, kjer za operaterje predpiše posebne tehnične usmeritve ter tehnične in informacijske ukrepe.

- Bistveni in pomembni subjekti pristojni skupini CSIRT nemudoma (tj. načeloma v roku 24 ur) in v skladu z nacionalnim načrtom odzivanja priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega, če:

  1. je zadevnemu subjektu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube ali

  2. je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

Zakon v 29. in 30. členu odloča podrobnejše postopke in zahteve glede poročanja incidentov.

Kot lahko ugotovite, gre za obveznosti, ki so jim bili operaterji večinoma podvrženi že pred uveljavitvijo ZInfV-1, zakon pa vsebinsko enake obveznosti določa za širši krog zavezancev. Za operaterje, ki so že doslej izvajali predpisane ukrepe s področja informacijske varnosti po dosedanjih predpisih, se zdi verjetno, da v zvezi z uresničevanjem teh obveznosti po novi zakonodaji ne bodo potrebne korenite spremembe, pač pa sprotna prilagoditev sistema upravljanja varnosti (SUVI in SUNP) v skladu z vsebinskimi zahtevami ZInfV-1, ob

upoštevanju priporočil ENISA na tem področju ter morebitnega splošnega akta AKOS (če bo ta sprejet).

Če kateri telekomunikacijski operater poleg ponujanja javnih elektronskih komunikacijskih omrežij in/ali storitev opravlja tudi druge storitve iz seznama kritičnih sektorjev iz Priloge 1 in Priloge 2 navedenega zakona, ima lahko še druge (specifične ali področne) obveznosti, ki pritičejo tem drugim/dodatnim storitvam.

S spoštovanjem

--

Simon Stegel



ZDRUŽENJE KABELSKIH OPERATERJEV SLOVENIJE
"GOSPODARSKO INTERESNO ZDRUŽENJE"
Celovška cesta 150 1000 LJUBLJANA

tel: +386 41 412 234
E-mail: simon.stegel@zdruzenje-kos.si
Web: http://www.zdruzenje-kos.si