PRIROČNIK

za slovenska podjetja o skladnosti z Direktivo NIS2 in Zakonom ZInfV-1

Verzija 1.0 - junij 2025

Avtor: Albin Duraković, Cyber Security Engineer, Comtrade SI d.o.o.

www.comtradeintegration.com | **cyops.si@comtrade.com**

Kazalo vsebine

1. Uvod: Premik v novo obdobje kibernetske varnosti v Sloveniji

1.1. Namen tega priročnika

Ta priročnik je pripravljen z namenom zagotoviti jasno, celovito in praktično razumevanje obveznosti, ki jih imajo slovenska podjetja v skladu z Direktivo Evropske unije o ukrepih za visoko skupno raven kibernetske varnosti (Direktiva NIS2) ter novim slovenskim Zakonom o informacijski varnosti (ZInfV-1).

Namenjen je pomoči podjetjem pri ugotavljanju, ali sodijo v področje uporabe omenjenih predpisov, ter pri določanju potrebnih korakov za dosego in ohranjanje skladnosti. Poleg tega dokument poudarja ključni pomen proaktivnega pristopa k upravljanju kibernetskih tveganj v okolju, kjer se grožnje nenehno razvijajo, regulativne zahteve pa postajajo vse strožje.

1.2. Zakaj sta Direktiva NIS2 in Zakon ZInfV-1 pomembna za slovenska podjetja

Digitalna preobrazba je podjetjem prinesla številne priložnosti, hkrati pa jih izpostavila tudi vse večjemu številu sofisticiranih kibernetskih groženj. Kot odgovor so Evropska unija in njene države članice, vključno s Slovenijo, okrepile pravne okvire za izboljšanje odpornosti na področju kibernetske varnosti. Direktiva NIS2 in njen slovenski prenos v obliki Zakona ZInfV-1 predstavljata pomemben korak naprej od prejšnje Direktive NIS1, saj uvajata višjo raven usklajenosti in varnosti v celotni EU.

Skladnost z obema predpisoma ni zgolj pravna formalnost, temveč predstavlja ključen steber poslovne odpornosti. Bistvena je za zagotavljanje neprekinjenega poslovanja, zaščito občutljivih podatkov ter ohranjanje zaupanja strank in ugleda organizacije.

Zakon ZInfV-1 uvaja sistemski pristop k upravljanju informacijskih in kibernetskih tveganj ter vzpostavlja celovit nacionalni okvir, ki naj bi znatno okrepil odpornost tako javnega kot zasebnega sektorja na kibernetske grožnje. Novi zakon nadomešča predhodni ZInfV ter vključuje tudi prenos Direktive EU o odpornosti kritičnih subjektov (Direktiva CER), s čimer odraža celostni pristop k nacionalni varnosti in odpornosti.

Jezikovne določbe zakona, kot je zahteva po „pristopu vseh nevarnosti“ (ang. *all-hazards approach*) pri upravljanju tveganj, opredeljene v 21. in 22. členu zakona, skupaj z bistveno razširjenim obsegom zavezancev, jasno kažejo, da reaktiven pristop ni več sprejemljiv. Organizacije morajo proaktivno vključiti vidike kibernetske varnosti v svojo poslovno strategijo in operativno načrtovanje.

Zakon predpisuje podrobne zahteve glede priprave celovite varnostne dokumentacije ter uvedbe učinkovitih ukrepov za obvladovanje tveganj, ki vključujejo načrtovanje vnaprej ter izvajanje stalnih izboljšav – in ne le odzivanja po varnostnem incidentu.

Ob tem velja poudariti, da združen prenos Direktive NIS2 (osredotočene na digitalno odpornost) in Direktive CER (ki obravnava širšo odpornost kritičnih subjektov) v enoten nacionalni zakon ZInfV-1 predstavlja strateško odločitev slovenskega zakonodajalca.

Ta integracija odraža razumevanje, da sta kibernetska in fizična varnost vse bolj prepleteni.

Za slovenska podjetja to pomeni, da bodo morali ukrepi na področju kibernetske varnosti postati sestavni del širšega okvira operativne odpornosti – zlasti v primeru, da organizacija spada med kritične subjekte po Direktivi CER. Takšen celosten pristop predstavlja pomemben premik od tradicionalnega razumevanja informacijske varnosti.

2. Razumevanje regulativnega okvira: Direktiva NIS2 in ZInfV-1

2.1. Evropska Direktiva NIS2: Temelj za okrepljeno kibernetsko varnost

2.1.1. Ključni cilji in razširjeno področje uporabe

Direktiva NIS2 (Direktiva (EU) 2022/2555) si prizadeva vzpostaviti visoko skupno raven kibernetske varnosti v vseh državah članicah EU ter odpraviti pomanjkljivosti, ugotovljene pri njeni predhodnici - Direktivi NIS1. Njena ključna usmeritev je razširitev obveznosti na širši nabor sektorjev in zavezancev.

Nova direktiva zdaj zajema **18 kritičnih sektorjev** in se nanaša tako na srednje velika kot velika podjetja, ki delujejo v teh sektorjih. Znatno zaostruje varnostne zahteve, izrecno obravnava tveganja v dobavnih verigah, poenostavlja obveznosti poročanja o incidentih ter uvaja strožje nadzorne mehanizme in postopke izvrševanja. Poleg tega zahteva, da države članice vzpostavijo celovite nacionalne strategije kibernetske varnosti in okrepijo svoje institucionalne zmogljivosti na tem področju.

2.1.2. Temeljna načela

Direktiva NIS2 temelji na več ključnih načelih:

- **Pristop, ki temelji na tveganju**: Subjekti morajo izvajati ukrepe kibernetske varnosti, sorazmerne s tveganji, ki jih sami zaznajo in ocenijo.
- **Odgovornost vodstva**: Vodstveni organi zavezancev so izrecno odgovorni za odobritev in nadzor izvajanja ukrepov za obvladovanje tveganj na področju kibernetske varnosti.
- **Obvezno poročanje o incidentih**: Pomembne kibernetske incidente je treba prijaviti pristojnim nacionalnim organom v večstopenjskem postopku.
- **Varnost dobavne verige**: Subjekti morajo obvladovati tudi tveganja kibernetske varnosti, povezana z njihovimi dobavitelji in ponudniki storitev znotraj celotne dobavne verige.
- **Okrepljeno sodelovanje**: Direktiva spodbuja poglobljeno sodelovanje in izmenjavo informacij med državami članicami prek struktur, kot sta Evropska mreža organizacij za zvezo v kibernetskih krizah (**EU-CyCLONe**) in mreža nacionalnih enot za odzivanje na računalniške varnostne incidente (**CSIRT**).

2.2. Zakon o informacijski varnosti (ZInfV-1): Nacionalna implementacija v Sloveniji

2.2.1. Prenos Direktive NIS2 in nacionalne posebnosti

Zakon o informacijski varnosti (ZInfV-1) predstavlja glavni zakonodajni okvir za implementacijo Direktive NIS2 v Sloveniji. ZInfV-1 presega zgolj neposredni prenos Direktive NI2, temveč vključuje tudi vrsto nacionalnih prilagoditev, usmerjenih v nadaljnjo krepitev kibernetske odpornosti slovenskih organizacij.

Zakon širi področje uporabe tudi na sektorje, ki niso zajeti v direktivi – med drugim vključuje raziskovalne in visokošolske ustanove, kar odraža prilagojen pristop slovenskega zakonodajalca k prepoznavanju domačih tveganj. ZInfV-1 ob tem razveljavlja prejšnji zakon (ZInfV) in vzpostavlja nov, celovitejši okvir za obvladovanje kibernetskih tveganj.

Dodajanje nacionalno pomembnih sektorjev kaže na odločitev Slovenije, da preseže minimalne zahteve EU in razvije proaktivno, tveganjsko utemeljeno strategijo. Ta pristop temelji na nacionalni oceni tveganj, ki je izpostavila dodatna področja kot posebej ranljiva ali sistemsko pomembna za varnost družbe in gospodarstva.

2.2.2. Uradna objava in začetek veljavnosti

Državni zbor Republike Slovenije je ZInfV-1 sprejel **23. maja 2025**. Po ustaljenem zakonodajnem postopku začne zakon veljati 15 dni po objavi v Uradnem listu Republike Slovenije. V Uradnem listu Republike Slovenije št. 40/25 je bil dne **4. junija 2025** objavljen Zakon o informacijski varnosti (ZInfV-1). Zakon začne veljati **19. junija 2025.**

Za primerjavo: Direktiva NIS2 (Direktiva (EU) 2022/2555) je bila objavljena v Uradnem listu EU 27. decembra 2022 (UL L 333, str. 80) in je uradno začela veljati januarja 2023. Države članice EU so morale direktivo prenesti v svojo nacionalno zakonodajo do 17. oktobra 2024.

2.3. Tabela: Ključni mejniki in roki za dosego skladnosti

Pot do polne skladnosti z ZInfV-1 je večstopenjski proces, ne zgolj enkratno dejanje. Zakon predvideva ločene roke za registracijo, organizacijsko uskladitev in tehnično skladnost, kar organizacijam omogoča postopno uvajanje potrebnih ukrepov. Takšen postopni pristop priznava kompleksnost in obseg sprememb, ki jih morajo zavezanci uvesti, hkrati pa ohranja poudarek na pravočasnem in odgovornem ukrepanju. Podjetja morajo zato strateško načrtovati svojo pot do skladnosti, z jasno določenimi koraki v skladu s predpisanimi roki.

Mejnik	**Datum**
Začetek veljavnosti Direktive NIS2 (EU) 2022/2555	Januar 2023

Rok za prenos Direktive NIS2 za države članice EU	17. oktober 2024
Sprejetje ZInfV-1 v Državnem zboru RS	23. maj 2025
Objava ZInfV-1 v Uradnem listu RS	4. junij 2025
Začetek veljavnosti ZInfV-1	19. junij 2025
Rok za samoregistracijo zavezancev po ZInfV-1	September 2025 (približno 3 mesece po začetku veljavnosti zakona oz. 6 mesecev za obstoječe zavezance)
Rok za organizacijsko skladnost po ZInfV-1	Približno junij 2026 (1 leto po začetku veljavnosti ZInfV-1)
Rok za tehnično skladnost po ZInfV-1	Približno junij 2027 (2 leti po začetku veljavnosti ZInfV-1)

3. Ugotavljanje veljavnosti: Ali ZInfV-1 vpliva na vaše podjetje?

Ugotavljanje, ali se vaša organizacija uvršča med zavezance v skladu z ZInfV-1, je ključno izhodišče. Ta postopek je večplasten, saj vključuje oceno sektorja, vrste storitve, velikost podjetja, nacionalnega pomena in potencialnega sistemskega vpliva. Podjetja se ne smejo zanašati zgolj na število zaposlenih ali podatke o prihodkih, temveč morajo natančno analizirati svoje poslovanje glede na merila, določena v zakonu.

3.1. Opredelitev zavezancev (ZInfV-1, 6. člen)

ZInfV-1 določa, kdo je zavezanec na podlagi več kriterijev. Splošno pravilo, določeno v 6. členu (1), navaja, da se zakon uporablja za subjekte, ki:

1. opravljajo storitve, navedene po sektorjih, podsektorjih in vrstah subjekt**ov v Prilogi 1 (visoko kritični sektorji) ali Prilogi 2 (drugi kritični sektorji) zakona;**

in

2. izpolnjujejo določene **velikostne pragove**: zaposlujejo vsaj 50 oseb in imajo letni promet ali letno bilančno vsoto najmanj 10 milijonov EUR.

Vendar pa 6. člen (2) določa nekatere vrste subjektov, ki so zavezanci **ne glede na njihovo velikost**:

- Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev.
- Ponudniki storitev zaupanja.
- Registri za imena vrhnje domene (TLD) in ponudniki storitev sistema domenskih imen (DNS).
- Subjekti, ki so edini ponudnik storitve ali dejavnosti v Republiki Sloveniji, ki jih uvršča v Prilogo 1 ali Prilogo 2.

- Subjekti, katerih prekinitev storitve bi lahko pomembno vplivala na javni red, javno varnost ali javno zdravje.
- Subjekti, katerih prekinitev storitve bi lahko povzročila sistemsko tveganje, zlasti za sektorje, navedene v Prilogi 1 ali Prilogi 2, kjer bi takšna prekinitev lahko imela čezmejni vpliv.
- Subjekti, za katere se šteje, da imajo poseben pomen na nacionalni ali lokalni ravni za določen sektor iz Priloge 1 ali Priloge 2, za zagotavljanje določene storitve ali zaradi soodvisnosti z drugimi sektorji v Sloveniji.
- Organi državne uprave na nacionalni ravni.

Poleg tega 6. člen (3) opredeljuje dodatne subjekte, ki so zavezanci po ZInfV-1, ne glede na merila v prejšnjih odstavkih:

- Subjekti, določeni kot kritični po zakonu, ki ureja kritično infrastrukturo.
- Subjekti, ki opravljajo storitve registracije domenskih imen (ti so zavezanci, vendar se po 7. členu ne razvrščajo naprej kot bistveni ali pomembni).
- Subjekti, opredeljeni kot storitve državnega pomena v nacionalnih načrtih zaščite in reševanja, če bi okvara njihovih omrežnih in informacijskih sistemov ogrozila izvajanje nalog zaščite in reševanja iz teh načrtov.
- Mestne občine kot organi javne uprave na lokalni ravni.

Obseg ZInfV-1 predstavlja znatno razširitev v primerjavi s prejšnjo zakonodajo - ocenjuje se, da se bo število zajetih subjektov povečalo s približno 1.000 na med 6.000 in 8.000. Kvalitativna merila, povezana z vplivom na javni red, varnost, zdravje, sistemsko tveganje in nacionalni/lokalni pomen (točke 3, 4, 5 drugega odstavka 6. člena), delujejo kot pomembna "vseobsegajoča" določila. Ta organom omogočajo, da vključijo subjekte, ki se morda ne ujemajo povsem z vnaprej določenimi kategorijami velikosti ali sektorja, vendar so njihove storitve kljub temu ključne, kar odraža perspektivo "vseh nevarnosti" in sistemskega tveganja v uredbi.

3.2. Kategorije zavezancev: "Bistveni" in "pomembni" subjekti

Zavezanci (razen ponudnikov storitev registracije domenskih imen in nekaterih drugih) se po 7. členu ZInfV-1 nadalje delijo na "bistvene subjekte" ali "pomembne subjekte".

3.2.1. "Bistveni subjekti" (ZInfV-1, 7. člen)

Bistveni subjekti običajno vključujejo:

- Subjekte, ki delujejo v sektorjih, navedenih v **Prilogi 1 (visoko kritični sektorji)**, in izpolnjujejo višje velikostne pragove:
  - zaposlujejo vsaj 250 oseb; ALI
  - imajo letni promet vsaj 50 milijonov EUR; ALI
  - imajo letno bilančno vsoto vsaj 43 milijonov EUR (7. člen (2), točka 1).
- Ponudniki kvalificiranih storitev zaupanja, registri za imena vrhnje domene (TLD) in ponudniki storitev DNS, ne glede na njihovo velikost (7. člen (2), točka 2).
- Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki zaposlujejo vsaj 50 oseb IN imajo letni promet ali letno bilančno vsoto vsaj 10 milijonov EUR (7. člen (2), točka 3).

- Organi državne uprave na nacionalni ravni (7. člen (2), točka 4).
- Druge vrste subjektov iz Priloge 1, ki so s sklepom vlade določeni kot bistveni na podlagi meril iz 2. do 5. točke drugega odstavka 6. člena, na predlog pristojnega nacionalnega organa (URSIV) (7. člen (2), točka 5).
- Subjekti, določeni kot kritični po zakonu, ki ureja kritično infrastrukturo (7. člen (2), točka 6).
- Posebni subjekti iz sektorja 9 (upravljanje storitev IKT) Priloge 1, ki niso drugače zajeti in so določeni s sklepom vlade na predlog URSIV (7. člen (2), točka 7).

3.2.2. "Pomembni subjekti" (ZInfV-1, 7. člen)

Pomembni subjekti na splošno vključujejo:

- Subjekte, ki delujejo v sektorjih, navedenih v **Prilogi 2 (drugi kritični sektorji)**, in izpolnjujejo splošna velikostna merila za zavezance (≥50 zaposlenih IN promet/bilančna vsota ≥ 10 milijonov EUR), vključno s tistimi, ki so s sklepom vlade določeni kot pomembni na podlagi 2. do 5. točke drugega odstavka 6. člena, na predlog URSIV (7. člen (3), prva alinea).
- Subjekte iz 3. točke tretjega odstavka 6. člena (ključni za nacionalne načrte zaščite/reševanja), določene kot pomembne s sklepom vlade na predlog URSIV (7. člen (3), druga alinea).
- Druge zavezance, opredeljene v 6. členu, ki ne izpolnjujejo meril za bistvene subjekte (7. člen (3), tretja alinea).

Določba, ki vladi omogoča, da s sklepom določi dodatne subjekte kot bistvene ali pomembne, pomeni, da seznam zavezancev ni statičen. Podjetja, ki delujejo blizu pragov ali v kritičnih dobavnih verigah, bi morala aktivno spremljati sporočila URSIV in biti na tekočem z razvojem nacionalne strategije za kibernetsko varnost, saj se lahko njihova klasifikacija sčasoma spremeni.

3.3. Tabela: Bistveni vs. pomembni subjekti - ključne razlike in pragovi (ZInfV-1, 6., 7. člen)

Ta tabela povzema glavna merila za razlikovanje med bistvenimi in pomembnimi subjekti po ZInfV-1. To razlikovanje je temeljno, saj lahko vpliva na strogost določenih obveznosti, nadzorni pregled in višino morebitnih kazni.

Značilnost	Bistveni subjekti	Pomembni subjekti
Primarna priloga sektorja	Priloga 1 (visoko kritični sektorji)	Priloga 2 (drugi kritični sektorji) ali Priloga 1, če ne izpolnjujejo meril za bistvene.
Splošni velikostni pragovi	≥250 zaposlenih ALI promet ≥ 50 mio. EUR ALI bilančna vsota ≥ 43 mio. EUR (če so v Prilogi 1).	≥50 zaposlenih IN promet ≥ 10 mio. EUR ALI bilančna vsota ≥ 10 mio. EUR.

Posebne vrste ponudnikov	Ponudniki kvalificiranih storitev zaupanja, registri TLD, ponudniki DNS (vseh velikosti). Ponudniki javnih e-komunikacijskih omrežij/storitev (≥50 zaposlenih IN 10 mio. EUR prometa/bilance). Državna uprava. Kritični subjekti.	Subjekti, ključni za nacionalno zaščito/reševanje. Mestne občine. Drugi zavezanci, ki niso razvrščeni kot bistveni.
Imenovanje	Lahko so imenovani s sklepom vlade na podlagi posebnih meril (npr. sistemsko tveganje, nacionalni pomen za subjekte iz Priloge 1 ali določene upravljavce storitev IKT).	Lahko so imenovani s sklepom vlade na podlagi posebnih meril (npr. sistemsko tveganje, nacionalni pomen za subjekte iz Priloge 2 ali tiste, ki so ključni za zaščito/reševanje).
Intenzivnost nadzora	Potencialno višja/pogostejša.	Podvrženi nadzoru, vendar potencialno manj intenzivnemu kot bistveni subjekti.
Najvišje globe (pravna oseba)	Do 10 milijonov EUR ali 2 % svetovnega prometa.	Do 7 milijonov EUR ali 1,4 % svetovnega prometa.

Vir: ZInfV-1, členi 52-58; za višine glob.

3.4. Sektorji, zajeti v ZInfV-1 (Priloga 1, Priloga 2)

ZInfV-1 v svojih prilogah vsebuje podrobne sezname sektorjev, podsektorjev in vrst subjektov. Podjetja morajo neposredno preveriti te priloge, da ugotovijo, ali njihove specifične dejavnosti spadajo na področje uporabe.

3.4.1. Priloga 1 ZInfV-1 (Visoko kritični sektorji)

Ta priloga vključuje sektorje, kot so:

1. **Energija**: Električna energija (proizvodnja, prenos, distribucija, dobava, delovanje trga, agregacija, odziv na povpraševanje, shranjevanje energije, delovanje polnilnih mest za električna vozila); daljinsko ogrevanje in hlajenje; nafta (naftovodi, proizvodnja, rafiniranje, skladiščenje, transport, centralne skladiščne agencije); plin (dobava, distribucija, prenos, skladiščenje, UZP, rafiniranje, predelava); vodik (proizvodnja, skladiščenje, prenos).
2. **Promet**: Zračni (prevozniki, letališča, kontrola zračnega prometa); železniški (upravljavci infrastrukture, železniški prevozniki); vodni (družbe za prevoz po celinskih, morskih in obalnih vodah; pristaniške uprave; službe za nadzor plovbe); cestni (upravljavci cest za upravljanje prometa, operaterji inteligentnih transportnih sistemov).
3. **Bančništvo**: Kreditne institucije.
4. **Infrastruktura finančnega trga**: Upravljavci mest trgovanja; centralne nasprotne stranke.

5. **Zdravstvo**: Izvajalci zdravstvene dejavnosti; referenčni laboratoriji EU; raziskave in razvoj zdravil; subjekti, ki proizvajajo farmacevtske surovine/pripravke; subjekti, ki proizvajajo kritične medicinske pripomočke za izredne razmere na področju javnega zdravja; subjekti z dovoljenjem za promet z zdravili na debelo.
6. **Pitna voda**: Dobavitelji in distributerji.
7. **Odpadne vode**: Podjetja, ki zbirajo, odvajajo ali čistijo komunalne odpadne vode.
8. **Digitalna infrastruktura**: Ponudniki medomrežnih povezovalnih točk; ponudniki storitev DNS (razen operaterjev korenskih strežnikov); registri za imena vrhnje domene (TLD); ponudniki storitev računalništva v oblaku; ponudniki storitev podatkovnih centrov; ponudniki omrežij za dostavo vsebin; ponudniki storitev zaupanja; ponudniki javnih elektronskih komunikacijskih omrežij; ponudniki javno dostopnih elektronskih komunikacijskih storitev.
9. **Upravljanje storitev IKT (medpodjetniško)**: Ponudniki upravljanih storitev; ponudniki upravljanih varnostnih storitev.
10. **Javna uprava**: Organi državne uprave.
11. **Vesolje**: Upravljavci zemeljske infrastrukture, ki podpira vesoljske storitve.

3.4.2. Priloga 2 ZInfV-1 (Drugi kritični sektorji)

Ta priloga vključuje sektorje, kot so:

1. **Poštne in kurirske storitve**: Ponudniki poštnih storitev, vključno z dostavo paketov.
2. **Ravnanje z odpadki**: Podjetja, ki izvajajo postopke ravnanja z odpadki.
3. **Proizvodnja, izdelava in distribucija kemikalij**: Podjetja, ki proizvajajo in distribuirajo snovi/zmesi in izdelke iz njih.
4. **Proizvodnja, predelava in distribucija hrane**: Živilska podjetja v veleprodaji, industrijski proizvodnji in predelavi.
5. **Proizvodnja**: Medicinski pripomočki (ki niso v Prilogi 1); računalniki, elektronski in optični izdelki; električna oprema; drugi stroji in naprave; motorna vozila, priklopniki in polpriklopniki; druga transportna oprema.
6. **Digitalni ponudniki**: Ponudniki spletnih tržnic; ponudniki spletnih iskalnikov; ponudniki platform družbenih omrežij.
7. **Raziskave**: Raziskovalne organizacije (kot so opredeljene v zakonu, osredotočene na uporabne raziskave/eksperimentalni razvoj za komercialno uporabo, razen splošnih akademskih/izobraževalnih institucij, če ni drugače določeno).
8. **Javna uprava (lokalna samouprava)**: Mestne občine.

3.5. Izjeme in posebni primeri

ZInfV-1 vključuje posebne izjeme in primere:

- **Finančni sektor**: Subjekti v bančništvu in na področju infrastrukture finančnega trga, navedeni v Prilogi 1, so primarno urejeni s specifično zakonodajo finančnega sektorja glede digitalne operativne odpornosti (npr. DORA). Zato se poglavji IV (Ukrepi za obvladovanje tveganj in obveščanje o incidentih) in IX (Nadzor) ZInfV-1 zanje ne uporabljata za vidike, ki jih pokriva takšna *lex specialis* (3. člen (1)).

- **Sistemi s tajnimi podatki**: Informacijski in komunikacijski sistemi, ki varujejo tajne podatke in so prestali varnostno preverjanje ter prejeli varnostno dovoljenje nacionalnega varnostnega organa, so na splošno izvzeti. Vendar pa je treba o incidentih v teh sistemih še vedno poročati pristojnemu nacionalnemu organu po ZInfV-1 (3. člen (2)).
- **Banka Slovenije**: Banka Slovenije je izrecno izključena iz obveznosti po ZInfV-1 (6. člen (5)).
- **Ponudniki storitev registracije domenskih imen**: Čeprav so zavezanci po 2. točki tretjega odstavka 6. člena, se ti subjekti ne razvrščajo naprej kot bistveni ali pomembni po 7. členu (1).
- **Izvrševanje v javnem sektorju**: Subjekti javnega sektorja so sicer zavezanci, vendar se za neskladnost običajno soočajo z odreditvijo ukrepov za odpravo nepravilnosti namesto z denarnimi kaznimi, kar predstavlja drugačen pristop k izvrševanju za to kategorijo.

4. Osnovne zahteve za skladnost po ZInfV-1

Doseganje skladnosti z ZInfV-1 zahteva celosten pristop, ki obravnava upravljanje, obvladovanje tveganj, obravnavanje incidentov ter različne operativne in tehnične varnostne ukrepe. Zakon je na mnogih področjih izrazito preskriptiven in vsebuje podrobne sezname zahtev, ki puščajo manj prostora za interpretacijo v primerjavi z nekaterimi starejšimi, bolj načelnimi predpisi.

4.1. Upravljanje in odgovornost vodstva (ZInfV-1, 20. člen)

Temeljni kamen ZInfV-1 je izrecna dodelitev odgovornosti za kibernetsko varnost najvišjim ravnem organizacije.

- **Vloga in odgovornosti vodstva**: 20. člen (1) določa, da so predstojniki organov javne uprave in odgovorne osebe pravnih oseb (opredeljene kot fizične osebe, ki vodijo, nadzorujejo ali upravljajo poslovanje subjekta ali so zakonsko pooblaščene za zagotavljanje njegovega zakonitega delovanja) neposredno odgovorne za izvajanje ukrepov za obvladovanje tveganj na področju kibernetske varnosti, opredeljenih v 21. in 22. členu. Te ukrepe morajo formalno odobriti in nenehno nadzorovati njihovo izvajanje (20. člen (2)). To predstavlja pomemben dvig kibernetske varnosti na raven uprave ali najvišjega vodstva. Vztrajna malomarnost pri izpolnjevanju teh dolžnosti lahko v hudih primerih privede do odpoklica vodstvenega osebja po Zakonu o gospodarskih družbah. Ta neposredna odgovornost, skupaj z morebitno osebno odgovornostjo, temeljito spreminja pogovor o kibernetski varnosti znotraj organizacij in ga sili, da se obravnava kot strateško poslovno tveganje, ne zgolj kot problem oddelka za IT.
- **Obvezno usposabljanje za odgovorne osebe**: Da bi zagotovili, da je vodstvo usposobljeno za opravljanje teh odgovornosti, 20. člen (3) določa, da se morajo odgovorne osebe vsaj enkrat na štiri leta udeležiti usposabljanja ali izobraževanja o obvladovanju informacijskih in kibernetskih varnostnih tveganj ter o njihovem vplivu na dejavnosti ali storitve subjekta. Poseben program in način tega usposabljanja bo določila vlada na predlog URSIV (20. člen (6)).

4.2. Ukrepi za obvladovanje tveganj na področju kibernetske varnosti (ZInfV-1, 22. člen)

ZInfV-1 nalaga proaktiven in celovit pristop k obvladovanju tveganj na področju kibernetske varnosti:

- **Sprejetje pristopa "vseh nevarnosti"**: Subjekti morajo izvajati ukrepe, namenjene zaščiti svojih omrežnih in informacijskih sistemov ter njihovega fizičnega okolja pred širokim spektrom morebitnih incidentov (22. člen (2)).
- **Minimalni zahtevani ukrepi**: 22. člen (2) navaja minimalni nabor tehničnih, operativnih in organizacijskih ukrepov. Ta seznam je obsežen in vključuje, vendar ni omejen na:
  - Podporo vodstva informacijski in kibernetski varnosti ter njeno vključitev v letne poslovne/delovne načrte.
  - Zagotavljanje integritete osebja v zvezi z informacijsko in kibernetsko varnostjo (pred zaposlitvijo, med njo in po njej).
  - Osnovne prakse kibernetske higiene in usposabljanje o kibernetski varnosti za vse zaposlene.
  - Varnost človeških virov, preverjanje identitete uporabnikov, upravljanje ravni dostopnosti informacij in avtorizacija dostopa.
  - Vzpostavitev in upravljanje varnostnih kopij podatkov.
  - Zagotavljanje in vzdrževanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov (podrobneje v 24. členu).
  - Upravljanje omrežnih in informacijskih sistemov, ki se uporabljajo za delovanje/storitve, z jasno odgovornostjo za zaščito.
  - Politike in postopki glede uporabe kriptografije in, kjer je to potrebno, šifriranja.
  - Upravljanje prometa in komunikacij.
  - Varnost dobavne verige, vključno z določitvijo minimalnih zahtev kibernetske varnosti za ključne dobavitelje/ponudnike.
  - Fizična in tehnična zaščita prostorov in dostopa do območij, kjer so ključni omrežni in informacijski sistemi.
  - Varnostni mehanizmi v aplikativni programski opremi, vključno z varnostjo pri nabavi, razvoju in vzdrževanju ter postopki za obravnavo in razkrivanje ranljivosti.
  - Upravljanje in preprečevanje izkoriščanja tehničnih ranljivosti.
  - Zaščita pred zlonamerno programsko opremo in metode za odkrivanje poskusov vdorov ter preprečevanje incidentov.
  - Uporaba večfaktorske avtentikacije (MFA) ali rešitev za stalno avtentikacijo, kjer ocena tveganja to zahteva.
  - Uporaba varnih glasovnih, video in besedilnih komunikacij ter varnih sistemov za nujno komuniciranje znotraj subjekta, kot je ustrezno.
  - Politike in postopki glede uporabe storitev v oblaku za delovanje ali zagotavljanje storitev. (22. člen (2)).

4.2.1. Tabela: Kontrolni seznam obveznih ukrepov za obvladovanje tveganj (ZInfV-1, 22. člen (2))

Naslednja tabela ponuja kontrolni seznam, ki temelji na teh obveznih ukrepih:

Kategorija	Specifično področje ukrepa
Upravljanje in politike	Podpora vodstva in vključitev v načrte; Politike za kriptografijo/šifriranje; Politike za uporabo storitev v oblaku.
Varnost človeških virov	Preverjanje integritete osebja; Varnost človeških virov, preverjanje identitete, ravni dostopa; Usposabljanje zaposlenih in kibernetska higiena.
Upravljanje sredstev in sistemov	Upravljanje omrežnih/informacijskih sistemov in odgovornost; Upravljanje varnostnih kopij; Upravljanje dnevniških zapisov.
Tehnični varnostni nadzor	Upravljanje prometa in komunikacij; Fizična in tehnična zaščita prostorov; Zaščita pred zlonamerno programsko opremo in odkrivanje vdorov; Večfaktorska/stalna avtentikacija; Varne komunikacije (glas, video, besedilo, nujne).
Razvoj in vzdrževanje	Varnost pri nabavi, razvoju, vzdrževanju sistemov; Obravnava in razkrivanje ranljivosti.
Varnost dobavne verige	Obravnavanje tveganj z neposrednimi dobavitelji/ponudniki storitev; Določanje minimalnih zahtev.
Upravljanje ranljivosti	Upravljanje in preprečevanje izkoriščanja tehničnih ranljivosti.

Ta kontrolni seznam prevaja pravne zahteve v praktično orodje za analizo vrzeli in načrtovanje izvajanja, s čimer zagotavlja, da so obravnavana vsa obvezna področja nadzora.

- **Ocena tveganja**: Izvedeni ukrepi morajo biti sorazmerni z ugotovljenimi tveganji. Ta ocena mora upoštevati najnovejše stanje tehnike, ustrezne evropske in mednarodne standarde (URSIV načrtuje preslikavo obveznosti ZInfV-1 v standard ISO/IEC 27001 v prihodnjem podzakonskem aktu), stroške izvajanja, stopnjo izpostavljenosti subjekta tveganjem, njegovo velikost, verjetnost nastanka incidentov in morebitno resnost takšnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom (22. člen (3)). Metodologije, kot so tiste, opisane v standardu ISO 27005 (opredelitev konteksta, identifikacija, analiza, vrednotenje in obravnava tveganj), lahko zagotovijo strukturiran pristop. Vzdrževanje celovitega registra tveganj je ključna komponenta tega procesa.

4.3. Varnostna dokumentacija (ZInfV-1, 21. člen)

ZInfV-1 nalaga vzpostavitev in vzdrževanje celovite varnostne dokumentacije.

- **Sistem upravljanja informacijske varnosti (SUIV)**: Zahteva se dokumentiran SUIV.
- **Sistem upravljanja neprekinjenega poslovanja (SUNP)**: Zahteva se tudi dokumentiran SUNP, ki temelji na pristopu vseh nevarnosti.
- **Zahtevane politike in načrti (21. člen (1))**: Ta dokumentacija mora vključevati vsaj:
  - Politiko ali sektorske politike o varnosti omrežnih in informacijskih sistemov.
  - Natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za neprekinjeno delovanje omrežnih in informacijskih sistemov, skupaj z njihovimi skrbniki.
  - Analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije.
  - Politiko in načrt neprekinjenega poslovanja, ki zajema analizo vpliva na poslovanje (BIA), postopke za zagotavljanje neprekinjenega poslovanja, določitev minimalne ravni delovanja, upravljanje varnostnih kopij ter opredeljene vloge in odgovornosti.
  - Načrt okrevanja in obnove omrežnih in informacijskih sistemov, potrebnih za njihovo delovanje ali zagotavljanje storitev, vključno z opisom odgovornosti in postopkov za obnovo teh sistemov po motečem dogodku.
  - Načrt odzivanja na incidente z jasnim protokolom obveščanja pristojne enote CSIRT, vključno z opisom sistema za odkrivanje in odzivanje ter vlogami in odgovornostmi za odzivanje na incidente.
  - Načrt varnostnih ukrepov, namenjen zagotavljanju celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov ali obvladovanju informacijskih in kibernetskih varnostnih tveganj, ob upoštevanju tveganj in sektorskih posebnosti subjekta.
  - Politiko s postopki za ocenjevanje učinkovitosti varnostnih ukrepov za obvladovanje informacijskih in kibernetskih varnostnih tveganj, vključno z določitvijo kazalnikov učinkovitosti in analizo zbranih podatkov.

4.4. Upravljanje in poročanje o incidentih (ZInfV-1, 29., 30. člen)

Učinkovito upravljanje incidentov in pravočasno poročanje sta ključni obveznosti.

- **Opredelitev "pomembnega incidenta" (29. člen)**: Incident se šteje za "pomemben", če:
  - je povzročil ali bi lahko povzročil resne motnje v delovanju ali finančne izgube za subjekt (29. člen (1)).
  - je prizadel ali bi lahko prizadel druge fizične ali pravne osebe s povzročitvijo znatne materialne ali nematerialne škode (29. člen (1)). Pri ugotavljanju pomembnosti incidenta morajo subjekti upoštevati dejavnike, kot so število uporabnikov, ki jih je prizadela prekinitev storitve, trajanje incidenta, prizadeto geografsko območje, stopnja motenj storitve, obseg vpliva na gospodarske in družbene dejavnosti, resnost morebitne izgube ali kršitve podatkov ter vpliv na kritično infrastrukturo (29. člen (2)). Direktiva NIS2 se prav tako nanaša na incidente, ki *bi lahko* povzročili znatne motnje ali škodo.

- **Obveznosti poročanja: komu in kdaj (30. člen)**: O pomembnih incidentih je treba poročati pristojni enoti CSIRT brez nepotrebnega odlašanja (30. člen (1)). Postopek poročanja je večstopenjski in zahteva dobro uigrane notranje postopke, jasne vloge in potencialno vnaprej pripravljene komunikacijske predloge za izpolnjevanje kratkih rokov med krizo. Potreba po "začetni oceni resnosti in vpliva" v 72 urah pomeni hitre analitične zmožnosti.

    - **Časovni okviri**:
        - **Zgodnje opozorilo/začetno obvestilo**: V **24 urah** po seznanitvi z incidentom (30. člen (2)). To obvestilo mora navajati, ali obstaja sum, da je bil incident povzročen z nezakonitimi dejanji.
        - **Vmesno poročilo/posodobitev**: V **72 urah** po seznanitvi z incidentom (30. člen (3)). To poročilo mora vsebovati posodobitev stanja in začetno oceno resnosti in vpliva incidenta.
        - **Končno poročilo**: Najpozneje **en mesec** po predložitvi vmesnega (72-urnega) poročila (30. člen (5)). Če incident takrat še traja, je treba namesto tega predložiti poročilo o napredku, ki mu sledi končno poročilo en mesec po razrešitvi incidenta.
    - **Prostovoljno poročanje** o incidentih, ki (še) niso opredeljeni kot pomembni, ter o pomembnih kibernetskih grožnjah in skorajšnjih incidentih se spodbuja (30. člen (8), 35. člen).
    - Če obstaja sum, da incident predstavlja kaznivo dejanje, ga je treba prijaviti tudi pristojnim organom pregona (policiji v Sloveniji). URSIV in enote CSIRT naj bi zagotovili smernice glede tega.

4.4.1. Tabela: Časovni okviri za poročanje o incidentih in ključne informacije (ZInfV-1, 30. člen)

Ta tabela zagotavlja ključen hiter pregled obveznega, časovno občutljivega postopka poročanja o incidentih.

Faza poročanja	Rok od seznanitve	Prejemnik	Ključne zahtevane informacije (primeri)
Zgodnje opozorilo	V 24 urah	Pristojna enota CSIRT	Navedba incidenta, sum na nezakonito dejanje.
Vmesno poročilo	V 72 urah	Pristojna enota CSIRT	Posodobitev o incidentu, začetna ocena resnosti in vpliva.
Končno/vmesno poročilo o napredku	V 1 mesecu od 72-urnega poročila	Pristojna enota CSIRT	Celovite podrobnosti o incidentu, temeljni vzrok, sprejeti ukrepi, pridobljene izkušnje (končno); Posodobitev stanja, če še traja (o napredku).

4.5. Varnost dobavne verige (ZInfV-1, 22. člen (2) točka 10, 22. člen (4))

Subjekti so odgovorni za obvladovanje tveganj kibernetske varnosti, ki izvirajo iz njihovih dobavnih verig.

- Obveznosti se nanašajo na odnose z neposrednimi dobavitelji in ponudniki storitev (22. člen (4)).
- Subjekti morajo upoštevati specifične ranljivosti svojih neposrednih dobaviteljev in splošno kakovost izdelkov in praks kibernetske varnosti svojih dobaviteljev, vključno z njihovimi varnimi razvojnimi procesi (22. člen (4)).
- Določiti morajo ustrezne minimalne zahteve kibernetske varnosti za ključne dobavitelje in ponudnike storitev ter lahko preverjajo izvajanje teh zahtev (22. člen (4)).
- Upoštevati je treba rezultate usklajenih ocen tveganja kritičnih dobavnih verig na ravni EU, če so na voljo (22. člen (4)).

4.6. Neprekinjeno poslovanje in krizno upravljanje (ZInfV-1, 21. člen (1) točki 4, 5)

Zagotavljanje operativne odpornosti je ključno.

- Zahteva se dokumentirana politika in načrt neprekinjenega poslovanja, vključno z analizo vpliva na poslovanje (BIA), postopki za neprekinjenost in upravljanjem varnostnih kopij.
- Obvezen je tudi dokumentiran načrt okrevanja in obnove omrežnih in informacijskih sistemov. Direktiva NIS2 podobno poudarja potrebo po robustnih načrtih neprekinjenega poslovanja, vključno s postopki za varnostno kopiranje in obnovo po nesreči.

4.7. Varnost v omrežnih in informacijskih sistemih

- **Obravnava in razkrivanje ranljivosti (ZInfV-1, 17. člen, 22. člen (2) točka 12)**:
  Subjekti morajo vzpostaviti politike in postopke za varnost pri nabavi, razvoju in vzdrževanju omrežnih in informacijskih sistemov, kar vključuje obravnavo in razkrivanje ranljivosti (22. člen (2) točka 12). Slovenija določi enoto CSIRT kot nacionalnega koordinatorja za usklajeno razkrivanje ranljivosti (17. člen). Poleg tega ENISA vzdržuje Evropsko zbirko podatkov o ranljivostih (EUVD) kot vir.
- **Uporaba kriptografije in šifriranja (ZInfV-1, 22. člen (2) točka 8)**:
  Zahtevajo se politike in postopki glede uporabe kriptografije in, kjer je to ustrezno, šifriranja.
- **Večfaktorska avtentikacija (MFA) (ZInfV-1, 22. člen (2) točka 15)**:
  Uporaba MFA ali rešitev za stalno avtentikacijo je obvezna, kjer je to potrebno za obvladovanje tveganj.
- **Usposabljanje zaposlenih in kibernetska higiena (ZInfV-1, 20. člen (4), 22. člen (2) točka 3)**:
  Človeški dejavnik je ključen vidik kibernetske varnosti.
  - Vodstvo je odgovorno za zagotavljanje rednega usposabljanja zaposlenih, da pridobijo zadostno znanje in veščine za prepoznavanje informacijskih in kibernetskih varnostnih tveganj ter razumevanje njihovega potencialnega vpliva na storitve subjekta (20. člen (4)).

- Izvajanje osnovnih praks kibernetske higiene in zagotavljanje usposabljanja o kibernetski varnosti sta obvezna ukrepa za obvladovanje tveganj (22. člen (2) točka 3).
- Skrbniki informacijskih in komunikacijskih sistemov zavezanca se morajo redno letno usposabljati za ohranjanje znanja in veščin pri prepoznavanju in ocenjevanju tveganj ter vrednotenju praks obvladovanja tveganj (20. člen (5)).

4.8. Upravljanje dnevniških zapisov (ZInfV-1, 24. člen)

Celovito beleženje je bistveno za analizo incidentov in forenzično preiskavo. Podrobne zahteve za zbiranje in hrambo dnevniških zapisov poudarjajo njihov pomen za razumevanje incidentov, rekonstrukcijo dogodkov in potencialno dokazovanje skladnosti.

- **Obseg, hramba in varnost** - Subjekti morajo opredeliti postopke in uporabljati ustrezna orodja za spremljanje in beleženje dogodkov v svojih omrežjih in informacijskih sistemih. Zagotoviti morajo zbiranje in hrambo dnevniških zapisov v obsegu in na način, ki omogoča rekonstrukcijo in analizo incidentov ali skorajšnjih incidentov (24. člen (1)).
- **Minimalni obseg dnevniških zapisov** je podrobno opisan v 24. členu (2) in vključuje omrežni promet (odhodni in dohodni), ustvarjanje/spreminjanje/brisanje uporabnikov in spremembe dovoljenj, dostop do sistema/aplikacije/podatkovne baze, dogodke avtentikacije, ves privilegiran dostop in dejavnosti, dostop do ali spremembe kritičnih konfiguracijskih in varnostnih datotek, dnevnike dogodkov iz varnostnih orodij (npr. antivirus, IDS, požarni zidovi), uporabo sistemskih virov in dostop/uporabo omrežne opreme.
- **Dnevniški zapisi morajo biti shranjeni** na način, ki zagotavlja njihovo avtentičnost, celovitost, razpoložljivost in zaupnost. Subjekti morajo prav tako zagotoviti, da imajo vsi sistemi sinhronizirane časovne vire za omogočanje korelacije dnevniških zapisov (24. člen (3)).
- **Minimalna doba hrambe** dnevniških zapisov je **šest mesecev**, vendar se lahko podaljša, če analiza obvladovanja tveganj subjekta kaže, da je daljše obdobje ustrezno za obvladovanje ugotovljenih tveganj (24. člen (4)).
- Posebne **zahteve glede lokacije hrambe** dnevniških zapisov veljajo za bistvene subjekte, določene kot kritične po zakonu o kritični infrastrukturi (hraniti se morajo v Sloveniji, druga kopija je dovoljena v EU), in za subjekte v sektorjih digitalne infrastrukture, bančništva in infrastrukture finančnega trga (lahko se hranijo v EU ali zunaj EU pod določenimi pogoji) (24. člen (5)-(8)).

4.9. Uporaba certificiranih IKT izdelkov, storitev in procesov (ZInfV-1, 27. člen, 22. člen (6))

ZInfV-1 spodbuja uporabo certificiranih rešitev.

- Subjekti naj bi upoštevali uporabo IKT izdelkov, storitev in procesov, ki so bili certificirani v okviru evropskih shem kibernetske varnostne certifikacije (27. člen).
- ENISA je odgovorna za vodenje registra certificiranih IKT izdelkov, storitev in procesov.
- Pri sprejemanju varnostnih ukrepov naj bi subjekti upoštevali tudi vse relevantne izvedbene akte Evropske komisije, ki opredeljujejo tehnične, metodološke ali sektorske zahteve (22. člen (6)).

5. Praktični koraki do skladnosti z ZInfV-1

Doseganje skladnosti z ZInfV-1 zahteva strukturiran in proaktiven pristop. Naslednji koraki opisujejo ključne ukrepe za prizadeta slovenska podjetja.

5.1. Samoregistracija zavezancev (ZInfV-1, 8. člen)

Postopek samoregistracije je prva formalna interakcija, ki jo bo večina podjetij imela z ZInfV-1 in URSIV. Zagotavljanje natančnosti in pravočasnosti v tem koraku je ključnega pomena za vzpostavitev ustreznega odnosa s pristojnim organom.

- **Postopek in roki**:
  - Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je zadolžen za vzpostavitev mehanizma za samoregistracijo zavezancev v štirih mesecih po začetku veljavnosti ZInfV-1 (8. člen (1) in 60. člen).
  - Zavezanci se morajo registrirati prek tega mehanizma v 30 dneh od izpolnitve meril iz 6. in 7. člena (ali od datuma sklepa vlade, če so tako določeni) (8. člen (2)).
  - Za subjekte, ki že izpolnjujejo merila ob začetku veljavnosti ZInfV-1, mora biti prva registracija opravljena v šestih mesecih po začetku veljavnosti zakona (60. člen ZInfV-
  - Dokler uradni mehanizem za samoregistracijo ne bo deloval, je URSIV sporočil, da je treba informacije pošiljati digitalno na njihov določen elektronski naslov.
- **Informacije, ki jih je treba zagotoviti (8. člen (2))**: Registracija zahteva podrobne informacije o subjektu, vključno z:
  - Imenom, naslovom, kontaktnimi podatki, matično številko in elektronskim naslovom za uradno vročanje.
  - Ustreznim sektorjem in podsektorjem iz Priloge 1 ali Priloge 2 ali kategorijo zavezanca, če ni vključen v te priloge, vendar je zavezanec po 6. členu (3).
  - Navedbo, ali subjekt izpolnjuje velikostne pragove (število zaposlenih, letni promet/bilančna vsota).
  - Kontaktno osebo za informacijsko varnost in njenega namestnika, vključno z elektronskimi naslovi in telefonskimi številkami.
  - Dodeljenimi bloki javnih IP naslovov.
  - Seznamom držav članic EU, kjer se zagotavljajo storitve, ki spadajo pod ZInfV-1.
  - Registriranimi številkami avtonomnih sistemov (ASN) in vsemi domenskimi imeni, ki jih zavezanec uporablja pri svojem delovanju.

5.2. Izvedba analize vrzeli glede na zahteve ZInfV-1

Čeprav zakon tega izrecno ne zahteva, je izvedba analize vrzeli zelo priporočljiv temeljni korak za vsak program skladnosti.

- To vključuje sistematično primerjavo trenutne drže kibernetske varnosti podjetja, vključno z obstoječimi politikami, postopki, tehničnimi nadzori in dokumentacijo, z podrobnimi zahtevami, določenimi v ZInfV-1.

Ključni členi, na katere se je treba osredotočiti, vključujejo 20. člen (Upravljanje), 21. člen (Varnostna dokumentacija), 22. člen (Ukrepi za obvladovanje tveganj), 24. člen (Dnevniški zapisi) ter 29. in 30. člen (Upravljanje in poročanje o incidentih).
- Analiza bi morala biti usmerjena v identifikacijo manjkajočih nadzorov, neustrezne dokumentacije ali postopkovnih pomanjkljivosti.
- Ko so vrzeli identificirane, jih je treba prednostno razvrstiti glede na povezano raven tveganja in nujnost za doseganje skladnosti z določenimi določbami.

5.3. Razvoj in izvajanje varnostne dokumentacije in ukrepov

Na podlagi ugotovitev analize vrzeli morajo podjetja razviti novo ali posodobiti obstoječo varnostno dokumentacijo in izvesti zahtevane ukrepe.

- **Varnostna dokumentacija (21. člen)**: To vključuje vzpostavitev ali izpopolnitev dokumentiranega sistema upravljanja informacijske varnosti (SUIV) in sistema upravljanja neprekinjenega poslovanja (SUNP), skupaj z vsemi specifičnimi politikami in načrti, ki jih zahteva 21. člen (npr. analiza obvladovanja tveganj, načrt odzivanja na incidente, načrt okrevanja). Poudarek na dokumentiranih sistemih pomeni, da bo dokazovanje skladnosti močno odvisno od celovite in posodobljene dokumentacije. Inšpektorji bodo verjetno sprejeli pristop, kjer velja: "če ni zapisano, se ni zgodilo".
- **Ukrepi za obvladovanje tveganj (22. člen)**: Izvedite ali izboljšajte tehnične, operativne in organizacijske ukrepe, navedene v 22. členu (2). To bo vključevalo širok spekter dejavnosti, potencialno vključno z uvajanjem tehnologije (npr. za MFA, šifriranje, beleženje/SIEM), prenovo procesov (npr. za odzivanje na incidente, obvladovanje tveganj v dobavni verigi) in kulturnimi pobudami (npr. okrepljeni programi usposabljanja).

5.4. Ocenjevanje skladnosti (ZInfV-1, 25. člen)

ZInfV-1 nalaga redni cikel ocenjevanja skladnosti, s čimer zagotavlja, da se ukrepi in dokumentacija na področju kibernetske varnosti pregledujejo in posodabljajo. To v zakonodajo vgrajuje filozofijo nenehnega izboljševanja, s čimer se skladnost premika od enkratnega projekta k stalnemu procesu.

- **Revizije za bistvene subjekte**:
  - Bistveni subjekti morajo opraviti oceno skladnosti vsaj enkrat na dve leti ali v primeru pomembnega kibernetskovarnostnega incidenta (25. člen (1)).
  - Ta ocena se običajno izvede kot revizija skladnosti s predpisi o informacijski varnosti ali kot del notranje revizije, ki vključuje vidike informacijske varnosti po ZInfV-1. Revizijo lahko izvajajo notranji revizorji, po možnosti v sodelovanju s strokovnjakom za informacijsko tehnologijo, ali kvalificirani zunanji revizorji informacijskih sistemov.
  - Revizor(ji) pripravi(jo) poročilo z ugotovitvami. Če se ugotovijo neskladnosti, mora bistveni subjekt pripraviti načrt za odpravo pomanjkljivosti, v katerem opredeli korektivne ukrepe in roke za njihovo izvedbo (25. člen (1), (2)).
- **Samoocenjevanje za pomembne subjekte**:
  - Pomembni subjekti morajo opraviti samoocenjevanje svojega stanja skladnosti vsaj enkrat na dve leti ali po pomembnem incidentu (25. člen (3)).

- To samoocenjevanje vključuje dokumentirano preverjanje upoštevanja lastne varnostne dokumentacije subjekta in izvajanja ukrepov za obvladovanje tveganj na področju kibernetske varnosti, ki jih predpisuje ZInfV-1. To se lahko izvede tudi kot del notranje revizije.
- Če samoocenjevanje potrdi skladnost, pomembni subjekt izda uradno izjavo o skladnosti. Ta izjava mora vsebovati dovolj podrobnosti, da omogoča ponovljivost ocene (25. člen (4)).
- Če samoocenjevanje razkrije neskladnost, mora subjekt pripraviti izjavo o neskladnosti, v kateri mora podrobno navesti ugotovljene pomanjkljivosti in opredeliti načrt za njihovo odpravo, vključno s specifičnimi roki (25. člen (5)).
- To dokumentacijo o samoocenjevanju (izjavo o skladnosti ali neskladnosti in načrt za odpravo pomanjkljivosti) mora hraniti pomembni subjekt in je ni treba proaktivno predložiti URSIV. Vendar pa mora biti na voljo na zahtevo med inšpekcijskim pregledom.

6. Nadzor, izvrševanje in kazni (ZInfV-1, poglavje IX - Nadzor, čl. 42-51, poglavje X - Kazenske določbe, čl. 52-58)

ZInfV-1 vzpostavlja robusten okvir za nadzor in izvrševanje, podprt z znatnimi kaznimi za neskladnost. Cilj tega okvira je zagotoviti, da zavezanci resno jemljejo svoje obveznosti na področju kibernetske varnosti.

6.1. Pristojni organi za nadzor

- **Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)**: URSIV je določen kot primarni pristojni nacionalni organ po ZInfV-1 (10. člen). Njegova notranja organizacijska enota, Inšpektorat za informacijsko varnost, je odgovorna za izvajanje inšpekcijskih pregledov zavezancev (10. člen (2) točka 26, 42. člen).
- **Sektorsko specifični nadzorni organi**: ZInfV-1 omogoča sodelovanje in morebitne vloge sektorskih regulatorjev (18. člen (1) točka 2). Predvideva se, da se bo nadzor lahko izvajal skupaj z URSIV in ustreznimi sektorskimi regulatorji, pri čemer se bo izkoristilo njihovo področju specifično strokovno znanje. Ta večplasten nadzorni pristop lahko privede do bolj niansiranega in kontekstualno ozaveščenega nadzora, zlasti glede na raznolikost sektorjev, ki jih zakon zajema.

6.2. Inšpekcijski postopki in pooblastila inšpektorjev (ZInfV-1, čl. 46-51)

Inšpektorji URSIV (in potencialno sodelujočih sektorskih organov) imajo obsežna pooblastila za preverjanje skladnosti.

V skladu s 47. členom lahko inšpektorji:

- Zahtevajo dostop do in pregledajo vso relevantno varnostno dokumentacijo.
- Dostopajo do prostorov, poslovnih objektov in opreme.
- Opravljajo razgovore z odgovornimi osebami in drugimi relevantnimi zaposlenimi.
- Pregledujejo naprave, informacijske sisteme in omrežja.
- Odredijo izvedbo korektivnih ukrepov za odpravo ugotovljenih pomanjkljivosti.

Čeprav bodo inšpekcijski pregledi morda prednostno obravnavali bistvene subjekte, so tudi pomembni subjekti v celoti podvrženi nadzornim dejavnostim.

Inšpekcijski pregledi bodo običajno vključevali pregled varnostne dokumentacije (po 21. členu), preverjanje izvajanja predpisanih varnostnih ukrepov (po 22. členu) in potencialno bolj poglobljene varnostne revizije omrežij in fizičnih prostorov.

6.3. Kazni za neskladnost (ZInfV-1, čl. 52-58)

ZInfV-1 uvaja strog kazenski režim, ki vključuje znatne globe za pravne osebe in potencialno odgovornost njihovih odgovornih oseb. Okvir izvrševanja je zasnovan z lestvijo stopnjevanja, ki se pogosto začne z opozorili in odreditvami ukrepov, nato napreduje do prisilnih dnevnih kazni in na koncu do glob. V hudih primerih, ki vključujejo bistvene subjekte, lahko regulativni organi celo začasno odvzamejo certifikate podjetja ali si prizadevajo za odpoklic vodstva zaradi vztrajne malomarnosti. Ta strukturiran pristop organom omogoča, da subjekte najprej usmerijo k skladnosti, vendar z znatno kaznovalno močjo v rezervi.

- **Globe za pravne osebe**:
  - **Bistveni subjekti**: Se lahko soočijo z globami do **10 milijonov EUR** ali do **2 %** njihovega celotnega svetovnega letnega prometa za preteklo poslovno leto, kar je višje. 52. člen ZInfV-1 določa različne razpone glob za različne kršitve s strani bistvenih subjektov. Na primer, neizvajanje ukrepov za obvladovanje tveganj (22. člen) ali neporočanje o pomembnih incidentih (30. člen) lahko privede do glob za pravno osebo v razponu od 40.000 EUR do 200.000 EUR. Te se lahko znatno povečajo za hujše ali ponavljajoče se prekrške, potencialno do omenjenih maksimumov.
  - **Pomembni subjekti**: Se lahko soočijo z globami do **7 milijonov EUR** ali do **1,4 %** njihovega celotnega svetovnega letnega prometa za preteklo poslovno leto, kar je višje. 53. člen ZInfV-1 podrobno določa ustrezne razpone glob za pomembne subjekte, na primer od 20.000 EUR do 100.000 EUR za podobne kršitve kot zgoraj, ponovno z možnostjo stopnjevanja do maksimumov.
- **Odgovornost odgovornih oseb**: Odgovorne osebe v pravnih osebah (npr. direktorji ali člani uprav) so lahko tudi osebno odgovorne in se soočijo z globami. Na primer, 52. člen (2) in 53. člen (2) določata razpone glob za odgovorne osebe, običajno od 1.000 EUR do 10.000 EUR za določene kršitve, z možnostjo višjih glob za hujše napake. Kot je bilo že omenjeno, se lahko vodstvo sooči tudi z odpoklicem po Zakonu o gospodarskih družbah za vztrajno malomarnost.

ZInfV-1 podrobno določa tudi posebne globe za druge vrste neskladnosti, kot so neuspešna samoregistracija kot zavezanec (54. člen), nezagotavljanje zahtevanih informacij organom (55. člen) ali oviranje nadzornih dejavnosti (56. člen).

Znatne globe, primerjane s svetovnim prometom, ZInfV-1 usklajujejo z drugimi pomembnimi predpisi EU, kot je GDPR, v smislu finančnega odvračanja. To finančno tveganje je glavni dejavnik, ki organizacije spodbuja k dodeljevanju zadostnih sredstev za skladnost na področju kibernetske varnosti.

7. Slovenski ekosistem kibernetske varnosti: Podpora in sodelovanje

Premagovanje zapletenosti ZInfV-1 ni samotno prizadevanje. Slovenija je vzpostavila nacionalni ekosistem kibernetske varnosti s ključnimi organi in mehanizmi za podporo zavezancem in spodbujanje sodelovanja.

7.1. Nacionalni pristojni organ: URSIV (ZInfV-1, 10. člen)

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je osrednji steber slovenskega okvira kibernetske varnosti po ZInfV-1. Njegova večplastna vloga koordinatorja, nadzornika, nacionalnega koordinacijskega centra za kibernetsko varnost (NCC-SI), upravljavca kibernetskih kriz in nacionalnega organa za kibernetsko varnostno certificiranje ga postavlja kot primarno središče za vse nacionalne zadeve kibernetske varnosti, povezane z zakonom. Ta centralizacija si prizadeva ustvariti skladen in enoten nacionalni pristop. Za podjetja bo URSIV glavna kontaktna točka za uradna navodila, postopek samoregistracije in na koncu tudi za izvršilne ukrepe.

Ključne vloge URSIV vključujejo:

- Koordiniranje delovanja nacionalnega sistema informacijske varnosti.
- Razvijanje nacionalnih zmogljivosti za kibernetsko obrambo.
- Zagotavljanje strokovne podpore in analiz na področju informacijske varnosti zavezancem.
- Sodelovanje z drugimi relevantnimi organi in organizacijami (enote CSIRT, sektorski regulatorji, organi pregona).
- Ozaveščanje o kibernetski varnosti in pomenu poročanja o incidentih.
- Organiziranje in koordiniranje usposabljanj, vaj in izobraževanj na področju informacijske varnosti.
- Zagotavljanje priprave in izvajanja nacionalne strategije za kibernetsko varnost.
- Razvijanje in vzdrževanje nacionalnega načrta za odzivanje na kibernetske incidente, incidente velikega obsega in krize.
- Opravljanje nalog inšpekcijskega nadzora prek svojega Inšpektorata za informacijsko varnost.
- Delovanje kot Nacionalni koordinacijski center za kibernetsko varnost (NCC-SI) v skladu z Uredbo EU 2021/887.
- Služenje kot enotna kontaktna točka za čezmejno sodelovanje na področju kibernetske varnosti.

7.2. Enota za odzivanje na računalniške varnostne incidente (CSIRT) (ZInfV-1, čl. 13-16)

Enote CSIRT so operativna prva linija za odzivanje na incidente in obveščanje o grožnjah. Slovenska vlada določi posebne ekipe CSIRT in njihove pristojnosti za obravnavo incidentov, ki prizadenejo določene skupine zavezancev (13. člen (1)). Vzpostavitev odnosa z ustrezno enoto CSIRT in razumevanje, kako jo vključiti, je praktična nujnost za zavezance.

Ključne enote CSIRT v Sloveniji vključujejo:

- **SI-CERT**: Nacionalna slovenska ekipa za odzivanje na računalniške varnostne incidente, ki deluje v okviru ARNES (Akademska in raziskovalna mreža Slovenije). SI-CERT je odgovoren za obravnavo incidentov za širok krog subjektov v zasebnem in javnem sektorju ter za vrhnjo domeno .si. Prav tako ima pomembno vlogo v nacionalnih programih za ozaveščanje o kibernetski varnosti, kot je "Varni na internetu".
- **SIGOV-CERT**: Ta CSIRT primarno podpira organe javne uprave in zagotavlja varnost vladnih informacijskih sistemov. (Po ZInfV-1 njegove naloge verjetno opravlja ena od enot CSIRT, formalno določenih v 13. členu).

Enote CSIRT so zadolžene za spremljanje kibernetskih groženj in ranljivosti, zagotavljanje zgodnjih opozoril in alarmov, odzivanje na incidente in pomoč prizadetim subjektom, zbiranje in analizo forenzičnih podatkov, izvajanje dinamičnih analiz tveganj in incidentov, vzdrževanje situacijske zavednosti in na zahtevo izvajanje proaktivnih pregledov sistemov subjektov za odkrivanje ranljivosti. Prav tako mednarodno sodelujejo v mreži CSIRT (15. člen).

7.3. Mehanizmi za izmenjavo informacij (ZInfV-1, 18. člen, 34. člen)

Učinkovita izmenjava informacij je ključna za usklajen nacionalni odziv na kibernetske grožnje.

- URSIV je zadolžen za vzpostavitev namenske digitalne platforme za poročanje o pomembnih incidentih in za lajšanje medagencijskega sodelovanja ter izmenjave informacij o incidentih, kibernetskih grožnjah in skorajšnjih incidentih med pristojnim nacionalnim organom, enotno kontaktno točko, enotami CSIRT in drugimi relevantnimi organi (18. člen (2), 30. člen (10)). Medtem ko je ta platforma v razvoju, se vmesna komunikacija pogosto opira na e-pošto. Prihodnji uspeh teh platform bo odvisen od njihove zasnove, uporabnosti in zaupanja, ki jim ga bodo izkazali sodelujoči subjekti.
- Enote CSIRT morajo prav tako sodelovati in izmenjevati relevantne informacije s sektorskimi ali medsektorskimi skupnostmi zavezancev (13. člen (4), 34. člen).
- URSIV prispeva k preglednosti z objavo polletnih poročil o stanju informacijske in kibernetske varnosti v Sloveniji.

7.4. Nacionalna strategija in načrt odzivanja na področju kibernetske varnosti (ZInfV-1, 9. člen, 12. člen)

Slovenski pristop h kibernetski varnosti vodijo strateški nacionalni dokumenti.

- **Nacionalna strategija za kibernetsko varnost**, ki jo sprejme vlada, zagotavlja krovni okvir za vzpostavitev učinkovitega nacionalnega sistema informacijske in kibernetske varnosti. Opredeljuje cilje, prednostne naloge, strukture upravljanja, vloge in odgovornosti ključnih deležnikov, ukrepe pripravljenosti in politike o različnih vidikih, kot so varnost dobavne verige, upravljanje ranljivosti in ozaveščenost javnosti (9. člen).
- **Nacionalni načrt odzivanja** na kibernetske incidente, kibernetske incidente velikega obsega in krize razvije URSIV (v vlogi organa za upravljanje kibernetskih kriz) in ga sprejme vlada. Ta načrt opredeljuje cilje, postopke in vloge deležnikov za upravljanje takšnih dogodkov, zagotavlja usklajen odziv na nacionalni ravni in omogoča sodelovanje znotraj EU (12. člen).

8. Zaključek: Sprejemanje kibernetske odpornosti

Uvedba Direktive NIS2 in njen prenos v slovenski pravni red prek ZInfV-1 pomeni prelomni trenutek za področje kibernetske varnosti v Sloveniji. Za podjetja, ki spadajo na področje uporabe tega novega regulativnega okvira, to ne predstavlja le dodatnega skladnostnega bremena, temveč strateški imperativ, ki zahteva pozornost na najvišjih ravneh upravljanja. Cilj presega zgolj izpolnjevanje zahtev; njegov namen je spodbujanje globoko ukoreninjene kulture kibernetske odpornosti, ki organizacijam omogoča učinkovito predvidevanje, obvladovanje, odzivanje na ter okrevanje po kibernetskih grožnjah.

8.1. Ključna sporočila za slovenska podjetja

- **Strateški imperativ**: Kibernetska varnost po ZInfV-1 in NIS2 mora biti obravnavana kot sestavni del poslovne strategije in zagotavljanja neprekinjenega poslovanja, ne kot izolirana funkcija IT.
- **Odgovornost vodstva**: Izrecna dodelitev odgovornosti vodstvu, skupaj z obveznim usposabljanjem in morebitno osebno odgovornostjo, poudarja potrebo po vključenosti in nadzoru na ravni uprave.
- **Proaktiven pristop, ki temelji na tveganju**: Reaktiven odnos ni več zadosten. Podjetja morajo proaktivno identificirati, ocenjevati in obvladovati tveganja na področju kibernetske varnosti z uporabo pristopa "vseh nevarnosti" ter izvajati ukrepe, sorazmerne z njihovim specifičnim profilom tveganja.
- **Poznavanje obveznosti**: Temeljito razumevanje, ali je podjetje opredeljeno kot "bistveni" ali "pomembni" subjekt, je ključno, saj to določa specifične obveznosti in potencialno stopnjo nadzora.
- **Dokumentacija in ocenjevanje sta ključna**: Celovita in ažurna varnostna dokumentacija (SUIV, SUNP, politike, načrti) ter redne ocene skladnosti (revizije ali samoocenjevanja) so ključne za dokazovanje skrbnosti in upoštevanja zakona.
- **Sodelovanje z ekosistemom**: Izkoristite podporo in navodila nacionalnih organov, kot sta URSIV in enote CSIRT (zlasti SI-CERT). Pravočasno poročanje o incidentih in sodelovanje sta obvezna elementa skladnosti.

8.2. Proaktivni koraki za stalno skladnost

Doseganje in ohranjanje skladnosti na dinamičnem področju kibernetske varnosti je stalen proces, ne enkraten cilj. Podjetja bi morala:

- **Ostati informirana**: Redno spremljati navodila URSIV, posodobitve o razvijajočih se kibernetskih grožnjah in ranljivostih ter morebitne spremembe ali nadaljnje izvedbene akte v okviru ZInfV-1 in NIS2.
- **Spodbujati kulturo kibernetske varnosti**: Spodbujati ozaveščenost in odgovornost za kibernetsko varnost med vsemi zaposlenimi z rednim usposabljanjem in jasno komunikacijo.
- **Nenehno izboljševati**: Redno posodabljati varnostne ukrepe, načrte odzivanja na incidente in ureditve neprekinjenega poslovanja na podlagi preteklih izkušenj, aktualnih groženj in sprememb poslovnega okolja. Dvoletni cikel ocenjevanja, ki ga zahteva ZInfV-1, naj bo obravnavan kot minimalni standard.

- **Ustrezno vlagati**: Določite zadostna finančna, tehnična in kadrovska sredstva za kibernetsko varnost ter jo prepoznajte kot ključno naložbo v poslovno odpornost in zanesljivost.

S sprejetjem teh načel in proaktivnim pristopom k obveznostim iz ZInfV-1 lahko slovenska podjetja ne le zagotovijo regulativne zahteve, temveč tudi bistveno okrepijo svojo zaščito pred vse večjim spektrom kibernetskih groženj ter tako zaščitijo svoje poslovanje, ugled in zaupanje deležnikov v vse bolj digitalnem okolju.

9. Okrepite svojo skladnost s SOC partnerjem

Številne organizacije se danes soočajo z izzivi pri vzpostavitvi in vzdrževanju 24/7 nadzora, hitrem odzivanju na incidente, učinkovitem upravljanju dnevnikov ter pravočasnem zaznavanju groženj. Naš Security Operations Center (SOC) je zasnovan posebej za podjetja, ki želijo te zahteve izpolniti učinkovito in stroškovno optimizirano.

Podpiramo vas lahko pri:

- zbiranju, analizi in varni hrambi dnevnikov;
- zaznavanju incidentov, triaži ter 24/7 obveščanju;
- podpori pri skladnostnem poročanju in dokumentaciji;
- odkrivanju ranljivosti in vpogledu v tveganja v dobavni verigi.

Če želite preveriti, kako lahko naše SOC-storitve dopolnijo vaše skladnostne aktivnosti, nas kontaktirajte na ***cyops.si@comtrade.com***.

10. Priloge

Slovar ključnih izrazov

Ta slovar vsebuje opredelitve nekaterih ključnih izrazov, uporabljenih v ZInfV-1 in Direktivi NIS2. Opredelitve temeljijo predvsem na 5. členu ZInfV-1 ter splošnem razumevanju dokumentacije Direktive NIS2.

- **Bistveni subjekt (Essential Entity)**: Zavezanec, ki običajno deluje v visoko kritičnem sektorju (Priloga 1 ZInfV-1) in izpolnjuje posebne (pogosto višje) velikostne pragove ali merila ter je podvržen potencialno strožjemu nadzoru.

- **CSIRT (Enota za odzivanje na računalniške varnostne incidente)**: Ekipa, odgovorna za obravnavo varnostnih kršitev in incidentov, izvajanje analiz in pomoč pri upravljanju incidentov.

- **Kibernetska varnost (Cybersecurity)**: Dejavnosti, potrebne za zaščito omrežnih in informacijskih sistemov, njihovih uporabnikov in drugih oseb, ki jih prizadenejo kibernetske grožnje.

- **Digitalna infrastruktura (Digital Infrastructure)**: Sektor, ki zajema ponudnike medomrežnih povezovalnih točk, storitev DNS, registrov TLD, storitev računalništva v oblaku, storitev podatkovnih centrov, omrežij za dostavo vsebin, storitev zaupanja ter javnih elektronskih komunikacijskih omrežij/storitev.

- **Incident (Incident)**: Dogodek, ki je ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih zagotavljajo ali so dostopne prek omrežnih in informacijskih sistemov.

- **Informacijska varnost (Information Security)**: Varovanje in zaščita omrežnih in informacijskih sistemov ter povezanih podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, motnjo, spremembo ali uničenjem, da se zagotovijo zaupnost, avtentičnost, celovitost in razpoložljivost.

- **Omrežni in informacijski sistem (Network and Information System)**: Elektronsko komunikacijsko omrežje, katera koli naprava ali skupina medsebojno povezanih naprav, ki izvajajo samodejno obdelavo digitalnih podatkov, ali digitalni podatki, ki jih ti elementi shranjujejo, obdelujejo, pridobivajo ali prenašajo.

- **Pomembni subjekt (Important Entity)**: Zavezanec, ki pogosto deluje v drugih kritičnih sektorjih (Priloga 2 ZInfV-1) ali izpolnjuje splošne velikostne pragove in je podvržen posebnim obveznostim na področju kibernetske varnosti.

- **Pomemben incident (Significant Incident)**: Incident, ki je povzročil ali bi lahko povzročil resne motnje v delovanju ali finančne izgube za subjekt ali je prizadel ali bi lahko prizadel druge fizične ali pravne osebe s povzročitvijo znatne materialne ali nematerialne škode.

- **Tveganje (Risk)**: Možnost izgube ali motnje zaradi incidenta, izražena kot kombinacija velikosti izgube ali motnje in verjetnosti nastanka incidenta.

- **URSIV (Urad Vlade Republike Slovenije za informacijsko varnost)**: Pristojni nacionalni organ za kibernetsko varnost v Sloveniji po ZInfV-1.

- **Zavezanec (Obligated Entity)**: Javni ali zasebni subjekt, ki spada na področje uporabe ZInfV-1 zaradi svojega sektorja, zagotovljenih storitev in/ali velikosti ali drugih posebnih meril.