nis2.hr

NIS 2 vodič za hrvatske tvrtke

Sektori, rokovi, mjere upravljanja rizicima i kontrolna lista za reviziju.

Izdanje: 3. listopada 2026. · www.nis2.hr

> **Napomena:** Ovaj vodič ima informativni karakter i nije pravni savjet. Rokovi i pojedinosti podzakonskih akata mijenjaju se, stoga prije donošenja odluka provjerite aktualni tekst propisa u Narodnim novinama (nn.hr) i na stranicama nadležnih tijela.

1. Što je NIS 2?

NIS 2 je Direktiva (EU) 2022/2555 o mjerama za visoku zajedničku razinu kibernetičke sigurnosti u Uniji. Zamjenjuje prvu NIS direktivu iz 2016. i znatno proširuje krug obveznika, pooštrava sigurnosne zahtjeve te uvodi stroge sankcije i osobnu odgovornost uprave.

U Hrvatskoj je direktiva prenesena:

- **Zakonom o kibernetičkoj sigurnosti** (NN 14/2024), na snazi od 15. veljače 2024.
- **Uredbom o kibernetičkoj sigurnosti** (NN 135/2024), koja razrađuje mjere, kategorizaciju i postupke.

Nadležna tijela (sažetak)

Tijelo	Uloga
Nacionalno vijeće za kibernetičku sigurnost	Strateško usmjeravanje i koordinacija
SOA (Sigurnosno-obavještajna agencija)	Središnje državno tijelo za kibernetičku sigurnost, nadzor
ZSIS	Tehnička i CSIRT funkcija za državna tijela
CARNET (Nacionalni CERT)	CSIRT za ostale subjekte, zaprimanje prijava incidenata
Sektorska tijela (npr. HNB, HANFA, HAKOM)	Nadzor u pojedinim sektorima

---

2. Tko je obuhvaćen?

2.1. Kriterij veličine

Opće pravilo: obveza vrijedi za **srednja i velika poduzeća** koja djeluju u obuhvaćenim sektorima.

Veličina	Kriterij
Srednje poduzeće	50 ili više zaposlenih **ili** godišnji prihod/bilanca veća od 10 mil. EUR
Veliko poduzeće	250 ili više zaposlenih **ili** godišnji prihod veći od 50 mil. EUR i bilanca veća od 43 mil. EUR

Određene subjekte zakon obuhvaća **bez obzira na veličinu** (npr. pružatelji javnih elektroničkih komunikacijskih mreža, pružatelji usluga povjerenja, registri naziva domena, jedini pružatelji kritične usluge u državi).

2.2. Ključni i važni subjekti

Kategorija	Tko	Nadzor
Ključni subjekti	Veliki subjekti iz sektora visoke kritičnosti (Prilog I.)	Proaktivni (redoviti nadzor i revizije)
Važni subjekti	Srednji subjekti iz Priloga I. te srednji i veliki iz Priloga II.	Reaktivni (nakon incidenta ili sumnje)

2.3. Sektori visoke kritičnosti (Prilog I.)

1. **Energetika** – električna energija, centralno grijanje i hlađenje, nafta, plin, vodik
2. **Promet** – zračni, željeznički, vodni i cestovni
3. **Bankarstvo**
4. **Infrastruktura financijskog tržišta** – burze, središnje druge ugovorne strane
5. **Zdravstvo** – pružatelji zdravstvene zaštite, laboratoriji, proizvođači lijekova i ključnih medicinskih proizvoda
6. **Pitka voda**
7. **Otpadne vode**
8. **Digitalna infrastruktura** – IXP, DNS, registri .hr domena, računalstvo u oblaku, podatkovni centri, CDN, pružatelji elektroničkih komunikacija i usluga povjerenja
9. **Upravljanje IKT uslugama (B2B)** – upravljani pružatelji usluga (MSP) i upravljani pružatelji sigurnosnih usluga (MSSP)
10. **Javna uprava**
11. **Svemir**

2.4. Ostali kritični sektori (Prilog II.)

1. **Poštanske i kurirske usluge**
2. **Gospodarenje otpadom**
3. **Proizvodnja, izrada i distribucija kemikalija**
4. **Proizvodnja, prerada i distribucija hrane**
5. **Proizvodnja** – medicinski proizvodi, računala i elektronika, električna oprema, strojevi, motorna vozila, ostala prijevozna sredstva
6. **Digitalni pružatelji** – internetska tržnica, tražilice, platforme društvenih mreža
7. **Istraživanje**

2.5. Brza provjera: jeste li obuhvaćeni?

1. Djelujete li u nekom od sektora iz Priloga I. ili II.?
2. Imate li 50+ zaposlenih ili godišnji prihod/bilancu iznad 10 mil. EUR?
3. Pružate li uslugu koju zakon obuhvaća neovisno o veličini?
4. Jeste li dobavljač obuhvaćenom subjektu? (Neizravno ste pogođeni kroz ugovorne zahtjeve lanca opskrbe.)

Ako je odgovor na 1. i 2. (ili 3.) **da**, vjerojatno ste obveznik i trebate provesti **samoprocjenu**.

---

3. Ključni rokovi i obveze u vremenu

> Točne datume uvijek provjerite u Zakonu i Uredbi te na stranicama SOA-e i CARNET-a. Dolje je pregled **vrsta rokova** i njihova redoslijeda.

Korak	Opis
Stupanje Zakona na snagu	15. veljače 2024.
Uredba o kibernetičkoj sigurnosti	Objavljena u NN 135/2024 – razrađuje mjere i postupke
Samoprocjena i prijava	Subjekti utvrđuju spadaju li u obuhvat i dostavljaju podatke nadležnom tijelu u roku propisanom Zakonom/Uredbom
Provedba mjera upravljanja rizicima	Prijelazno razdoblje za usklađivanje propisano Zakonom/Uredbom
Prva revizija / samoprocjena zrelosti	Periodički, prema kategoriji subjekta

Rokovi za prijavu incidenata (stalna obveza)

Za **značajne incidente** vrijedi trostupanjska prijava:

Rok	Obveza
24 sata od saznanja	**Rano upozorenje** – sumnja na nezakonitu/zlonamjernu radnju, mogući prekogranični učinak
72 sata od saznanja	**Obavijest o incidentu** – početna procjena, ozbiljnost, učinak, pokazatelji kompromitacije
1 mjesec od obavijesti	**Završno izvješće** – opis, uzrok, mjere ublažavanja, prekogranični učinak

---

4. Zahtjevi za upravljanje rizicima

Subjekti moraju provesti **primjerene i razmjerne tehničke, operativne i organizacijske mjere** temeljene na pristupu koji obuhvaća sve opasnosti (*all-hazards*). Minimalni skup mjera:

1. **Politike analize rizika i sigurnosti informacijskih sustava**
2. **Postupanje s incidentima** – otkrivanje, odgovor, oporavak
3. **Kontinuitet poslovanja** – sigurnosne kopije, oporavak od katastrofe, upravljanje krizom
4. **Sigurnost lanca opskrbe** – odnosi s izravnim dobavljačima i pružateljima usluga
5. **Sigurnost pri nabavi, razvoju i održavanju sustava** – uključujući upravljanje i objavu ranjivosti
6. **Politike i postupci za procjenu učinkovitosti mjera**
7. **Osnovna kiberhigijena i izobrazba** o kibernetičkoj sigurnosti
8. **Politike i postupci kriptografije i, prema potrebi, enkripcije**
9. **Sigurnost ljudskih resursa, kontrola pristupa i upravljanje imovinom**
10. **Višefaktorska autentifikacija** (MFA), sigurna glasovna, video i tekstualna komunikacija te sigurni komunikacijski sustavi za hitne slučajeve

Odgovornost uprave

- Uprava **odobrava** mjere upravljanja rizicima i **nadzire** njihovu provedbu.
- Članovi uprave **moraju proći izobrazbu** iz područja kibernetičke sigurnosti.
- Uprava može **osobno odgovarati** za propuste, uključujući privremenu zabranu obavljanja dužnosti u slučaju ključnih subjekata.

Lanac opskrbe

Obveznici moraju procjenjivati ranjivosti i sigurnosne prakse **svojih dobavljača** i ugraditi sigurnosne zahtjeve u ugovore. Praktična posljedica: i **manje tvrtke koje nisu izravni obveznici** sve češće dobivaju upitnike i ugovorne klauzule od svojih klijenata.

---

5. Nadzor i sankcije

Kategorija	Najviša novčana kazna (prema direktivi)
Ključni subjekti	do **10 mil. EUR** ili **2 %** ukupnog svjetskog godišnjeg prihoda (što je više)
Važni subjekti	do **7 mil. EUR** ili **1,4 %** ukupnog svjetskog godišnjeg prihoda (što je više)

Nadležna tijela mogu provoditi inspekcije na licu mjesta, sigurnosne revizije, skenirati ranjivosti, tražiti informacije i dokaze te izdavati obvezujuće upute. Točni iznosi prekršajnih kazni u Hrvatskoj propisani su Zakonom.

---

6. Kontrolna lista za reviziju (audit checklist)

Označite svaku stavku statusom: ✅ ispunjeno · 🟡 djelomično · ❌ nije ispunjeno · ➖ nije primjenjivo.

A. Obuhvat i organizacija

- ☐ Provedena samoprocjena obuhvata (sektor, veličina, kategorija ključni/važni)
- ☐ Podaci dostavljeni nadležnom tijelu i redovito ažurirani
- ☐ Imenovana odgovorna osoba za kibernetičku sigurnost
- ☐ Definirane uloge i odgovornosti (RACI) za sigurnost informacija
- ☐ Odobrena i objavljena politika sigurnosti informacija

B. Upravljanje i uprava

- ☐ Uprava je formalno odobrila mjere upravljanja rizicima
- ☐ Uprava je prošla izobrazbu iz kibernetičke sigurnosti (dokaz o izobrazbi)
- ☐ Uprava se redovito izvješćuje o stanju sigurnosti i rizicima
- ☐ Osiguran proračun i resursi za provedbu mjera

C. Upravljanje rizicima

- ☐ Registar imovine (sustavi, podaci, usluge, dobavljači)
- ☐ Dokumentirana metodologija procjene rizika
- ☐ Provedena procjena rizika u posljednjih 12 mjeseci
- ☐ Plan postupanja s rizicima s vlasnicima i rokovima
- ☐ Redovita revizija i ažuriranje procjene

D. Tehničke i operativne mjere

- ☐ **MFA** za administrativni, udaljeni i kritični pristup
- ☐ Upravljanje pristupom (načelo najmanjih ovlasti, periodični pregled prava)
- ☐ Upravljanje zakrpama i ranjivostima s definiranim rokovima

- □ Zaštita krajnjih točaka (EDR/antivirus), segmentacija mreže, vatrozid
- □ Centralno prikupljanje i nadzor zapisa (logging, SIEM ili ekvivalent)
- □ Kriptografija: politika, zaštita podataka u mirovanju i prijenosu
- □ Sigurni razvoj i nabava (ako se razvija softver)
- □ Redovito testiranje (skeniranje ranjivosti, penetracijski testovi)

E. Postupanje s incidentima

- □ Dokumentiran plan odgovora na incidente
- □ Definirani kriteriji za **značajan incident**
- □ Postupak prijave: **24 h / 72 h / 1 mjesec** s kontaktima i predlošcima
- □ Imenovan tim i kanali komunikacije za incidente
- □ Provedene vježbe (tabletop) i evidentirani zaključci
- □ Evidencija incidenata i naučenih lekcija

F. Kontinuitet poslovanja

- □ Plan kontinuiteta poslovanja (BCP) i oporavka od katastrofe (DRP)
- □ Sigurnosne kopije: pravilo 3-2-1, **izolirana/nepromjenjiva** kopija
- □ Redovito testirano **vraćanje** podataka (ne samo izrada kopija)
- □ Definirani RTO i RPO za kritične usluge
- □ Plan upravljanja krizom i komunikacije

G. Lanac opskrbe

- □ Popis ključnih dobavljača i pružatelja usluga (uključujući oblak i MSP)
- □ Procjena sigurnosnog rizika dobavljača
- □ Sigurnosne klauzule u ugovorima (prijava incidenata, pravo na reviziju)
- □ Praćenje usklađenosti dobavljača i plan izlaza

H. Ljudi i svijest

- □ Program podizanja svijesti za sve zaposlenike (najmanje godišnje)
- □ Simulacije phishinga
- □ Sigurnosne provjere i postupci pri zapošljavanju i odlasku
- □ Specijalistička izobrazba tima za IT i sigurnost

I. Dokaz usklađenosti

- □ Središnji repozitorij dokumentacije i dokaza (politike, zapisnici, izvješća)
- □ Interna ili vanjska revizija prema planu
- □ Plan korektivnih mjera s rokovima i odgovornim osobama
- □ Mjerenje i izvještavanje o pokazateljima (KPI/KRI)

---

7. Praktičan plan provedbe (90 dana)

Razdoblje	Aktivnosti
Dani 1–15	Samoprocjena obuhvata, imenovanje odgovorne osobe, uključivanje uprave
Dani 16–45	Registar imovine, procjena rizika, gap analiza prema kontrolnoj listi
Dani 46–75	Politike i postupci, MFA, sigurnosne kopije, plan odgovora na incidente
Dani 76–90	Izobrazba uprave i zaposlenika, vježba incidenta, pregled dobavljača, dokumentiranje dokaza

---

8. Povezani standardi

Usklađenost s NIS 2 značajno olakšava primjena priznatih okvira:

- **ISO/IEC 27001** – sustav upravljanja sigurnošću informacija
- **ISO/IEC 27002** – kontrole
- **ISO 22301** – kontinuitet poslovanja
- **NIST CSF** – okvir upravljanja kibernetičkim rizikom
- **CIS Controls** – prioritizirane tehničke kontrole

---

9. Najčešća pitanja

Je li NIS 2 obvezan i za male tvrtke? Općenito ne, osim ako pružaju uslugu koju zakon obuhvaća neovisno o veličini. Međutim, kao dobavljači obveznika mogu biti ugovorno obvezni na usklađenost.

Što ako ne znam spadam li u obuhvat? Provedite samoprocjenu prema sektorima i kriterijima veličine, a za granične slučajeve zatražite mišljenje nadležnog tijela ili stručnjaka.

Zamjenjuje li ISO 27001 NIS 2? Ne, ali pokriva velik dio zahtjeva. NIS 2 dodaje obveze prijave incidenata, odgovornost uprave i nadzor nadležnih tijela.

Tko prima prijave incidenata? Nacionalni CSIRT (CARNET/ZSIS, ovisno o subjektu). Provjerite aktualni postupak prijave.

---

10. Korisni izvori

- Narodne novine: Zakon o kibernetičkoj sigurnosti (NN 14/2024) i Uredba (NN 135/2024) – nn.hr
- Direktiva (EU) 2022/2555 – eur-lex.europa.eu
- ENISA – enisa.europa.eu
- Nacionalni CERT / CARNET – cert.hr

Zadnje ažuriranje: listopad 2026. Dokument je informativan; za pravno obvezujuće tumačenje obratite se odvjetniku ili nadležnom tijelu.

Provjerite svoj status

Besplatni kalkulator spremnosti: www.nis2.hr

Pitanja i stručna podrška: info@nis2.hr