

## [Nova stroža pravila počinju se primjenjivati na kiberotpornost i fizičku otpornost kritičnih subjekata i mreža](https://digital-strategy.ec.europa.eu/hr/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks)

<https://digital-strategy.ec.europa.eu/hr/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks>

Dvije ključne direktive o kritičnoj i digitalnoj infrastrukturi upravo su stupile na snagu i njima će se ojačati otpornost EU-a na prijetnje na internetu i izvan njega, od kibernetičkih napada do kriminala, rizika za javno zdravlje ili prirodnih katastrofa.



iStock photo Getty images plus

Nedavne prijetnje ključnoj infrastrukturi EU-a pokušale su ugroziti našu kolektivnu sigurnost. Komisija je već 2020. predložila znatno poboljšanje pravila EU-a o otpornosti kritičnih subjekata i sigurnosti mrežnih i informacijskih sustava.

Dvije su direktive koje stupaju na snagu:

- **[Direktiva o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije \(Direktiva NIS 2\)](https://eur-lex.europa.eu/eli/dir/2022/2555)** (<https://eur-lex.europa.eu/eli/dir/2022/2555>)
- **[Direktiva o otpornosti kritičnih subjekata \(Direktiva o otpornosti kritičnih subjekata\)](https://eur-lex.europa.eu/eli/dir/2022/2557/oj)** (<https://eur-lex.europa.eu/eli/dir/2022/2557/oj>)

**Direktivom NIS 2 osigurat će se sigurnija i snažnija Europaznatnim proširenjem sektora i vrste kritičnih subjekata obuhvaćenih njezinim područjem primjene.** To uključuje pružatelje javnih elektroničkih komunikacijskih mreža i usluga, usluge podatkovnih centara, gospodarenje otpadnim vodama i otpadom, proizvodnju ključnih proizvoda, poštanske i kurirske usluge te tijela javne uprave, kao i zdravstveni sektor u širem smislu. Nadalje, **postrožit će se zahtjevi za**

**upravljanje kibersigurnosnim rizicima koje su poduzeća obvezna poštovati**, a obveze izvješćivanja o incidentima pojednostavnit će se **preciznijim odredbama o izvješćivanju, sadržaju i vremenskom okviru**. Direktivom NIS2 zamjenjuju se [pravila o sigurnosti mrežnih i informacijskih sustava](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC) ([https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC)), prvo zakonodavstvo na razini EU-a o kibersigurnosti.

S obzirom na sve složenije rizično okruženje, novom Direktivom o **otpornosti kritičnih subjekata zamjenjuje se Direktiva** o europskoj kritičnoj infrastrukturi iz 2008. Novim će se pravilima ojačati otpornost kritične infrastrukture na niz prijetnji, uključujući prirodne opasnosti, terorističke napade, unutarnje prijetnje ili sabotazu. Obuhvatit će se 11 **sektora**: energetika, promet, bankarstvo, infrastruktura financijskog tržišta, zdravstvo, pitka voda, otpadne vode, digitalna infrastruktura, javna uprava, svemir i hrana. Države članice morat će donijeti **nacionalnu strategiju** i provoditi **redovite procjene rizika** kako bi utvrdile subjekte koji se smatraju ključnima ili ključnima za društvo i gospodarstvo.

Države članice imaju rok od 21 mjeseca za prenošenje obiju direktiva u nacionalno zakonodavstvo. Tijekom tog razdoblja države članice donose i objavljuju mjere potrebne za usklađivanje s njima.

Vijeće je u prosincu 2022. donijelo **preporuku** ([https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_6238](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238)) o **koordinacijskom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture**, u kojoj se države članice pozivaju da ubrzaju pripreme za prenošenje i primjenu Direktive NIS 2 i Direktive o otpornosti kritičnih subjekata (CER).

## Više podataka

- [Direktiva NIS 2](https://digital-strategy.ec.europa.eu/en/news/new-stronger-cybersecurity-rules-kicking-safer-eu-digital-landscape) (<https://digital-strategy.ec.europa.eu/en/news/new-stronger-cybersecurity-rules-kicking-safer-eu-digital-landscape>)
- [Pitanja i odgovori za NIS](https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers) (<https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers>)
- [Informativni članak o NIS-u](https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2) (<https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2>)
- [Direktiva o otpornosti kritičnih subjekata](https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en) ([https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16\\_en](https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en))

---

### Source URL:

<https://digital-strategy.ec.europa.eu/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks>