Gospodarska zbornica Slovenije

Vodstvo
Dimičeva 13, 1504 Ljubljana, 01 5898 413, www.gzs.si, kabinet@gzs.si

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
Vojkova cesta 55
1000 Ljubljana
glavna.pisarna@mors.si

DRŽAVNI ZBOR RS
Odbor za obrambo
Šubičeva ulica 4
1000 Ljubljana
gp@dz-rs.si

Ljubljana, 4. 11. 2024

Zadeva: predlogi in pripombe Gospodarske zbornice Slovenije k predlogu Zakona o kritični infrastrukturi

Ministrstvo za obrambo RS (v nadaljevanju: MORS) je v zakonodajni postopek poslalo predlog Zakona o kritični infrastrukturi (v nadaljevanju: predlog zakona). Gospodarska zbornica Slovenije (v nadaljevanju: GZS) je predlog zakona obravnavala v okviru svojih združenj, zbornic in strokovnih skupin. Pozdravljamo sprejem novega Zakona o kritični infrastrukturi, s katerim se v slovenski pravni red prenaša Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov (v nadaljnjem besedilu: Direktiva 2022/2557), vendar hkrati podajamo predloge in pripombe za njegovo izboljšavo.

Na GZS pričakujemo, da se nas, kot največjo asociacijo gospodarskih subjektov iz različnih panog, aktivno vključi v pripravo strategije za odpornost kritičnih subjektov, nacionalne ocene tveganja ter podzakonskih predpisov, ki bodo sprejeti na podlagi novega Zakona o kritični infrastrukturi.

Povzetek bistvenih pripomb in predlogov:

Gospodarska zbornica Slovenije (GZS) podaja ključne predloge in pripombe k predlogu Zakona o kritični infrastrukturi (ZKI-1), ki ga je pripravilo Ministrstvo za obrambo RS. GZS pozdravlja prenos evropske Direktive 2022/2557 v slovensko zakonodajo, a izpostavlja potrebo po jasnih smernicah za lokalizacijo kritične infrastrukture in izboljšani koordinacijo med državnimi institucijami ter nosilci sektorjev kritične infrastrukture. Poudarjeno je, da morajo biti opredeljeni mehanizmi financiranja, ki bodo kritičnim subjektom olajšali izvajanje zahtevanih ukrepov, saj bodo nova določila povečala finančne, kadrovske in administrativne obremenitve. GZS predlaga vzpostavitev enotne točke za poročanje in poziva k prilagoditvi rokov ter obrazcev, s čimer bi olajšali administrativna bremena podjetij. Dodatno se zavzema za izvedbo simulacije izrednih dogodkov, kar bi omogočilo boljše preverjanje odpornosti kritičnih subjektov.

I. Splošne pripombe

a) Lokalizacija kritične infrastrukture

Kritična infrastruktura je po definiciji potrebna za omogočanje opravljanja za Slovenijo bistvenih storitev. Takšna opredelitev in visoko vrednotenje njenega pomena pomeni, da v zvezi z njenim upravljanjem obstajajo nacionalno pogojene okoliščine na katere morajo biti pozorni kritični subjekti. Opozorili bi na trend, ki smo mu priča tudi pospešeno v EU - premikanje »storitev« v oblak, trend, ki se mu ni mogoče izogniti in mu bomo priča v prihajajočem obdobju, ki bo vendarle terjal odziv varuhov tudi s stališča nacionalnih varnosti. Z vse večjo povezljivostjo in digitalizacijo, tudi kritični subjekti sledijo razvojnim tehnološkim trendom, s katerim optimizirajo poslovanje, sem sodi vzpostavitev platform v (zasebnem ali javnem) oblaku (t.i. cloudifikacija). Jasno je, da IT okolje postaja bolj in bolj zapleteno, sicer je treba poudariti, da se s to kompleksnostjo dogaja tudi pospešen razvoj varnosti, s katerim se poskrbi, da so oblaki ustrezno zavarovani. S prehodom se zgodijo pozitivne poslovne, finančne in okoljske prednosti.

Kljub temu, da se ta trend pospešeno odvija in da se mu ni moč izogniti, menimo, da bi morala država sprejeti strokovne smernice oz. usmeritve, kaj naj kritični sektor upošteva, ko omrežje, njegove funkcije ali storitve seli v oblak, ki se nahaja tako rekoč lokacijsko povsod ter geografsko razpršeno in ni nujno lokaliziran na Slovenijo. Menimo, da je to potrebno in da je iluzorno pričakovati, da se bo »vse« nahajalo v Sloveniji. Zato je potrebno opredeliti pravila (da se nahaja znotraj EU, da morajo biti sklenjeni ustrezni porazumi, tveganja pa še dodatno pregledana in ovrednotena, ….). V predlogu zakona te specifike niso opredeljene.

b) Nejasnost relacije in koordinacije s Civilno zaščito RS

Opozarjamo, da iz predloga zakona ni jasen način obvladovanja izrednih razmer oz. relacija ter koordinacija s Civilno zaščito RS (Zakon o varstvu pred naravnimi in drugimi nesrečami) v primeru odpovedi odpornosti kritičnih subjektov (npr. kritični subjekti v elektroenergetskem sistemu vključno z jedrskimi kapacitetami).

c) Velik problem koordinacije in usklajevanja

Velik problem, ki je v praksi zaznan že pri obstoječem veljavnem Zakonu o kritični infrastrukturi, predstavlja koordinacija in usklajevanje med posameznimi državnimi organi. Sistem kritične infrastrukture je med sabo zelo povezan, kritični subjekti so med sabo zelo soodvisni.
Menimo, da je nujno potrebno določiti sodelovanje med Agencijo za komunikacijska omrežja in storitve Republike Slovenije (AKOS), Uradom Vlade Republike Slovenije za informacijsko varnost (URSIV) in Ministrstvom za obrambo (MORS) saj so nosilci zakonov (Zakon o elektronskih komunikacijah (ZEKom-2), Zakon o informacijski varnosti (ZInfV) in Zakon o kritični infrastrukturi (ZKI), ki za nekatere poslovne subjekte določajo obveznosti, ki se medsebojno prepletajo. Prav tako je nujno potrebno zagotoviti sodelovanje med posameznimi nosilci sektorjev kritične infrastrukture (ministrstva), saj gre, kot že omenjeno, za močno medsebojno soodvisnost kritičnih subjektov.

d) Simulacija izrednega dogodka na domačih tleh

Menimo, da je nujno potrebna izvedba simulacije izrednega dogodka na domačih tleh, saj do sedaj ni bila izvedena še nobena. Takšna simulacija bi pokazala morebitne pomanjkljivosti v načrtih za odpornost kritičnih subjektov.

II. Pripombe in predlogi k posameznim členom

- **k 5. členu predloga zakona (strategija za odpornost kritičnih subjektov)**

Opominjamo, da se podjetja v praksi srečujejo z nekaterimi konkretnimi dilemami (npr. grožnja pomanjkanja elektrike zaradi geopolitičnih razmer, ki smo jim bili priča v letu 2022). Ta problematike še vedno ni v celoti naslovljena, niti rešena, razprava je zastala. Menimo, da je potrebno razrešiti odprete dileme, ki so povezane z neprekinjenim delovanjem kritične infrastrukture, če ne drugače, vsaj v strategiji za odpornost kritičnih subjektov, ki je predvidena v 5. členu predloga zakona.

- **k 11. členu (podpora kritičnim subjektom)**

1. odst. 11. člena predloga zakona določa, da nosilci sektorjev in ministrstvo kritičnim subjektom pri krepitvi njihove odpornosti zagotavljajo podporo z različnimi ukrepi, kot sta zlasti strokovna pomoč ter organizacija usposabljanj in vaj za preverjanje njihove odpornosti. Nadalje so v 15. členu predloga zakona opredeljeni ukrepi za odpornost, ki so stalni in dodatni. Če morajo dodatne ukrepe za odpornost izvesti kritični subjekti, lahko vlada odloči o dodelitvi sredstev za izvedbo teh ukrepov za odpornost.

Predlog zakona kritičnim subjektom določa obveznost, da sprejmejo ukrepe za neprekinjeno opravljanje bistvenih storitev, ki so definirane kot storitve, ki so ključne za ohranitev življenjsko pomembnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja, s čimer se zasleduje širši javni interes. Zagotavljanje ukrepov bo pomenilo za podjetja, ki bodo identificirana kot kritični subjekti, dodatne finančne, kadrovske in administrativne obremenitve, kar bo vplivalo na konkurenčnost teh podjetij. Zato menimo, da je s strani države potrebno sofinanciranje tako stalnih kot tudi dodatnih ukrepov. Ne zagovarjamo prenosa nalog in pristojnosti na državo, temveč zagovarjamo rešitev, da del stroškov, ki nastanejo zaradi varstva javnega interesa, sofinancira tudi država.

Dodatno navajamo, da tudi člen 10/1 Direktive 2022/2557 določa, da države članice lahko brez poseganja v veljavna pravila o državni pomoči kritičnim subjektom zagotovijo finančna sredstva, kadar je potrebno in utemeljeno s cilji javnega interesa. Zato ocenjujemo, da mora biti sofinanciranje države urejeno tudi v predlogu zakona.

Menimo, da bi bilo po uveljavitvi zakona, določitvi kritičnih subjektov in kritične infrastrukture ter ko bodo znani tudi okvirni stroški izvajanja ukrepov za odpornost pri kritičnih subjektih, potrebno oblikovati finančni vir, ki bo kritičnim subjektom pomagal pri izvajanju načrta za odpornost in zahtevanih ukrepov ter zagotavljal njihov razvoj in posodobitve. Razumemo, da to v danem trenutku ni mogoče. Je pa izjemnega pomena za zagotavljanje konkurenčnosti teh podjetij na trgu (dodatni stroški varovanja, večje zaloge, investicije v posodobitve... vse to namreč vpliva na uspešnost in učinkovitost ter konkurenčen položaj podjetja na trgu) in njihov stabilen dolgoročni razvoj.

- **k 15. členu predloga zakona (ukrepi za odpornost)**

15. člen predloga zakona opredeljuje ukrepe za odpornost in v 7. odstavku določa možnost, da lahko vlada odloči o dodelitvi sredstev za izvedbo teh ukrepov za odpornost, če morajo dodatne ukrepe za odpornost izvesti kritični subjekti,

Ta dikcija je v primerjavi z EU direktivo, ki v členu 10 opredeljuje podporo držav članic kritičnim subjektom, precej širša (10/1 – Države članice podpirajo kritične subjekte pri krepitvi njihove odpornosti. Ta podpora lahko vključuje razvoj gradiva z vodili in metodologij, podporo pri organizaciji vaj za preizkušanje njihove odpornosti ter zagotavljanje svetovanja in usposabljanja za osebje kritičnih subjektov. Države članice lahko brez poseganja v veljavna pravila o državni pomoči kritičnim subjektom zagotovijo finančna sredstva, kadar je potrebno in utemeljeno s cilji javnega interesa.). Smiselno bi bilo dikcijo neposredno vnesti v predlog zakona.

- **k 16. členu predloga zakona (posodabljanje načrta za odpornost)**

16. člen predloga zakona določa posodabljanje načrta za odpornost najmanj enkrat na dve leti. Direktiva 2022/2557 predpisuje, da kritični subjekti vsaj vsaka 4 leta izvedejo oceno tveganja. Ocena tveganja je del načrta za odpornost, zato predlagamo, da se v Sloveniji načrt za odpornost posodablja na 4 leta. Gre za širše določene obveznosti v predlogu zakona kot jih določa Direktiva 2022/2557, kar posledično pomeni dodatne administrativne obremenitve slovenskim podjetjem.

Opozarjamo, da pri zdajšnji dikciji 1. odst. 16. člena predloga zakona, da morajo kritični subjekti načrt za odpornost redno posodabljati, najmanj pa enkrat na dve leti, ni jasno razvidno, ali šteje koledarsko leto ali datum sprejetja načrta za odpornost.

Menimo, da je enomesečni rok, v katerem mora kritični subjekt ustrezno spremeniti načrt za odpornost prekratek, zato predlagamo, da se določi daljši rok.

- **k 28. členu predloga zakona (poročanje)**

V 1. odst. 28. člena predloga zakona je določeno, da nosilci sektorjev na podlagi letnih poročil kritičnih subjektov o zagotavljanju neprekinjenega delovanja kritične infrastrukture in opravljanju bistvene storitve za preteklo leto, ki jih ti pripravijo do konca januarja, pripravijo letno poročilo o zagotavljanju neprekinjenega delovanja kritične infrastrukture za sektor kritične infrastrukture iz svoje pristojnosti in ga do konca februarja pošljejo ministrstvu.

Opozarjamo na to, da gospodarski subjekti letna poročila za javno objavo predložijo do konca marca za preteklo koledarsko leto, revidirana letna poročila za javno objavo v 8, nerevidirana pa v 3 mesecih po koncu poslovnega leta. Opozarjamo, da je potrebno poenostaviti in poenotiti roke za poročanje, saj gre v nasprotnem primeru za novo administrativno obremenitev za kritične subjekte. Na GZS, tako na nivoju EU kot tudi na nivoju države, zagovarjamo sistem poročanja »vse na enem mestu« s čim manjšo obremenitvijo podjetij in čim manj dodatnih nesmiselnih kadrovskih, administrativnih in posledično finančnih obremenitev. Predlagamo, da se zagotovi enotna dostopna točka za poročanje za podjetja kar je tudi obljuba na ravni EU.

Predlagamo tudi, da se za lažjo pripravo poročila pripravijo in predvidijo vsi ustrezni obrazci za uniformno priglasitev.

- **k 29. členu predloga zakona (priglasitev izrednih dogodkov)**

29. člen predloga zakona pomeni pomembno spremembo z neposrednim vplivom, ki bo terjala določene prilagoditve. 29. člen je po našem mnenju neposredno povezan z bodočim zakonom o informacijski varnosti (EVA 2023-1544-0005: predlog ZInfV), ki je tudi v postopku sprejema. Opozarjamo na precejšnjo nedorečenost določil, ki urejajo priglasitev izrednih dogodkov – incidentov, ki vplivajo na delovanje kritične infrastrukture.

Opominjamo, da parametri za določitev pomembnosti motnje, ki so določeni v 1. odst. 29. člena predloga zakona, niso konkretizirani in ni jasno določeno, kako se bodo ugotavljali.

Predlagamo, da se pripravijo in predvidijo vsi ustrezni obrazci za uniformno priglasitev. Menimo, da v primeru nastanka izrednih dogodkov, poročanje ne sme biti naključno, prepuščeno vsakemu posamičnemu kritičnemu subjektu, pač pa mora biti pri vsakem kritičnem subjektu to poročanje avtomatizirano. Brez jasne definicije katere parametre je treba poročati, te avtomatizacije ne morejo zagotoviti. V trenutku, ko bo prišlo do kritičnega dogodka, namesto

da se kritični subjekt fokusira na detekcijo, izolacijo, odpravo in analizo dogodka, bo najverjetneje zbiral podatke za poročanje, kar pa ni namen samega predloga zakona in zagotavljanje navedenih aktivnosti.

Predlagamo, da se v 6. odst. pred zadnjim stavkom doda stavek, ki se glasi: »Sporočilo za javnost pristojni nosilec sektorja predhodno uskladi s kritičnim subjektom, na katerega se izredni dogodek nanaša.«.

Seznanjamo vas tudi s posebnimi pripombami in predlogi Sekcije operaterjev elektronskih komunikacij pri ZIT, GZS:

- **k 29. členu predloga zakona (priglasitev izrednih dogodkov)**

1. odst. 29. člena določa obveznost priglasitve izrednih dogodkov kar trem različnim naslovnikom, t.j. pristojnemu nosilcu sektorja, NCKU in ministrstvu. Kot izhaja iz pojasnil predlagatelja zakona to sicer ne pomeni treh poročanj, pač pa tako kot do sedaj, zgolj poročanje NCKU. Predlagamo, da se to bodisi jasno zapiše v prehodne določbe, bodisi jasno in nedvoumno napiše v obrazložitev tega člena (obrazložitev posamičnih členov), da se izognemo morebitnim nepotrebnim zapletom. V nasprotnem primeru (tri poročanja) bi šlo za nesorazmerno obveznost, saj je bolj pomembna detekcija in odprava izrednega dogodka.

Predlagamo, da se vzpostavi enotna točka za obveznosti poročanja po Zakonu o elektronskih komunikacijah, po novem Zakonu o informacijski varnosti in po novem Zakonu o kritični infrastrukturi. Na takšen način bi se zmanjšala bremena poročanja za tiste subjekte, ki so (bodo) zavezana za poročanje po vseh treh zakonih.

S platformo za obveznosti poročanja po Zakonu o elektronskih komunikacijah razpolaga AKOS, ki platformo ravno vzpostavlja, operaterji pa jo že testirajo. V skladu z novim Zakonom o informacijski varnosti in novim Zakonom o kritični infrastrukturi naj bi bila vzpostavljena platforma za poročanje pri URSIV. Opominjamo, da mora biti platforma za poročanje čim manj kompleksna - kritični subjekti poročajo o dogodku, a se morajo tisti moment ukvarjati z odpravo incidenta, ne pa z izpolnjevanjem izredno obsežnega in kompleksnega vprašalnika.

*****

Glede na navedene strokovne argumente predlagamo, da se smiselno upoštevajo pri sprejemu Zakona o kritični infrastrukturi. Za dodatna pojasnila in nadaljnje sodelovanje smo vam na voljo.

S spoštovanjem,

mag. Marko Djinović
izvršni direktor

Vesna Nahtigal
generalna direktorica