PRILOGA 3 **PREDLOG**
(EVA 2024-1911-0008)

ZAKON

O SPREMEMBAH IN DOPOLNITVAH ZAKONA O KRITIČNI INFRASTRUKTURI

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21-ZDU-1M, v nadaljnjem besedilu: ZKI) je bil sprejet leta 2017. Z ZKI se je sistemsko uredilo ugotavljanje in določanje kritične infrastrukture Republike Slovenije ter zaščito tovrstne infrastrukture, pri čemer se je izhajalo iz razumevanja, da obsega zaščita kritične infrastrukture vse dejavnosti, ki prispevajo k neprekinjenosti in celovitosti njenega delovanja. Ob upoštevanju dejstva, da so v posameznih sektorjih kritične infrastrukture obstoječi normativni dokumenti že urejali določene vidike kritične infrastrukture, predvsem njene zaščite, so bili cilji zakona, da se:

- z ustreznim celovitim predpisom uredi (tudi) področje kritične infrastrukture državnega pomena, torej »nacionalna« kritična infrastruktura;
- z normativnim ukrepom prispeva k dvigu ravni odpornosti slovenske družbe na sodobne varnostne grožnje in tveganja;
- vsem organom in organizacijam, ki so odgovorni za sektorje, ki so za slovensko družbo posebej pomembni, oziroma delujejo v njih, naloži, da pri svojem delu upoštevajo tudi zahteve glede zagotavljanja neprekinjenega delovanja kritične infrastrukture, torej vidik zaščite kritične infrastrukture;
- vsem organom in organizacijam pri zagotavljanju neprekinjenega in celovitega delovanja kritične infrastrukture naloži spoštovanje istih splošnih izhodišč in usmeritev (npr. načel);
- med organi in organizacijami, ki delujejo na področjih sektorjev kritične infrastrukture, vzpostavi primerna razmerja, predvsem z vidika delitve njihovih pristojnosti, odgovornosti in nalog pri zaščiti kritične infrastrukture;
- naloži dopolnitev normativne urejenosti ali sploh normativna ureditev, če ta še ne obstaja, v posameznih sektorjih kritične infrastrukture z vidika zaščite te infrastrukture.

K izvajanju zakona se je v naslednjih letih pristopilo sistematično, tako, da so bili s postopno uveljavitvijo zakonskih rešitev doseženi cilji zakona.

Tako je bila pripravljena metodologija za ocenjevanje tveganj za delovanje kritične infrastrukture. S strani Vlade Republike Slovenije (v nadaljnjem besedilu: vlada) so bili v letu 2018 določeni nosilci sektorjev kritične infrastrukture in z njimi sodelujoči državni organi ter sektorski in medsektorski kriteriji za določitev kritične infrastrukture, v letu 2019 pa je vlada, na podlagi drugega odstavka 9. člena ZKI s sklepom določila kritično infrastrukturo Republike Slovenije ter upravljavce kritične infrastrukture Republike Slovenije (v nadaljnjem besedilu: upravljavci). To so, gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti ali upravljajo kritično infrastrukturo, skupaj 53 upravljavcev v osmih sektorjih kritične infrastrukture.

Upravljavci so bili, na podlagi 11. člena ZKI, dolžni izdelati dokumente načrtovanja zaščite kritične infrastrukture, ki obsegajo oceno tveganj za delovanje kritične infrastrukture in ukrepe za zaščito

kritične infrastrukture. Oceno tveganj za delovanje kritične infrastrukture so upravljavci izdelali na podlagi Navodila ministra za obrambo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije (Uradni list RS, št. 7/19) in strokovnih usmeritev, ki so jih za posamezne sektorje kritične infrastrukture izdelali nosilci sektorjev kritične infrastrukture .

V skladu z ZKI se od določitve kritične infrastrukture Republike Slovenije v letu 2019 naprej letno poroča vladi o zagotavljanju neprekinjenega delovanja kritične infrastrukture Republike Slovenije.

Pri izvajanju zakona niso bile zaznane večje težave.

V letu 2022 je bila sprejeta Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov (v nadaljnjem besedilu: Direktiva 2022/2557) in razveljavitvi Direktive Sveta 2008/114/ES (UL L št. 333/142 z dne 27. 12. 2022, str. 164), ki so jo države članice dolžne implementirati v svojo zakonodajo do 17. oktobra 2024.

Cilj Direktive 2022/2557 je neprekinjeno opravljanje bistvenih storitev na notranjem trgu za ohranjanje ključnih družbenih funkcij ali gospodarskih dejavnosti in krepitve odpornosti kritičnih subjektov, ki opravljajo te storitve. Direktiva z namenom doseganja visoke ravni odpornosti kritičnih subjektov in neprekinjenega opravljanja bistvenih storitev, določa obveznosti za države članice in kritične subjekte. Državam članicam med drugim določa obveznost, da sprejmejo posebne ukrepe za neprekinjeno opravljanje bistvenih storitev, ki jih definira kot storitve, ki so ključne za ohranitev življenjsko pomembnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja, med katerimi posebej izpostavlja obveznost države članice, da identificira kritične subjekte v enajstih sektorjih (energetika, promet, bančništvo, infrastruktura finančnega trga, zdravje, pitna voda, odpadna voda, digitalna infrastruktura, javna uprava, vesolje ter pridelava, predelava in distribucija živil) in jih podpira pri izpolnjevanju njihovih obveznosti. Določene kritične subjekte zaradi opravljanja bistvenih storitev za šest ali več državam članicam ali v njih, celo povzdigne na raven kritičnih subjektov posebnega evropskega pomena.

V okviru nacionalnega okvira za odpornost kritičnih subjektov Direktiva 2022/2557 nalaga državam članicam pripravo strategije za odpornost kritičnih subjektov (v nadaljevanju: strategija) in nacionalne ocene tveganja za opravljanje bistvenih storitev (v nadaljevanju: nacionalna ocena tveganja). Določa kriterije za ugotavljanje kritičnih subjektov in kritičnih subjektov posebnega evropskega pomena. Kritičnim subjektom nalaga obveznost izdelave ocene tveganja in sprejetje ukrepov za krepitev njihove odpornosti, in jih tudi konkretizira po vsebinskih sklopih. V povezavi z ukrepi za zagotovitev ustreznega upravljanja varnosti zaposlenih opredeljuje podlago kritičnim subjektom za vzpostavitev postopkov preverjanja preteklosti zaposlenih. Kritičnim subjektom nalaga obveznost priglasitve incidentov in državam članicam vzpostavitev mehanizma za priglasitev določenih incidentov, da bi se pristojnim organom omogočil hiter in ustrezen odziv nanje. Državam članicam nalaga tudi obveznost posredovanja določenih informacij in aktov Evropski komisiji, sodelovanje in izmenjavo informacij s pristojnim nacionalnim organom na podlagi Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (v nadaljnjem besedilu: Direktiva (EU) 2022/2555) o incidentih in kibernetskih grožnjah. Nadalje Direktiva 2022/2557državam članicam določa pravila o nadzoru kritičnih subjektov, o izvrševanju in pravila za identifikacijo kritičnih subjektov posebnega evropskega pomena ter svetovalne misije za oceno ustreznosti ukrepov za odpornost teh kritičnih subjektov in še dodatno podporo pri izpolnjevanju obveznosti za ocenjevanje tveganj in sprejemanje ukrepov za povečanje njihove odpornosti. Direktiva 2022/2557 se sicer ne uporablja za vsebine, ki jih ureja Direktiva (EU) 2022/2555, z naslednjim dnem po poteku roka, do katerega so jo države članice dolžne implementirati v nacionalne zakonodaje pa razveljavlja Direktivo Sveta (ES) št. 114/2008 z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene

zaščite (v nadaljnjem besedilu: direktiva Sveta (ES) št. 114/2008). Slednjo je Slovenija prenesla v slovenski pravni red z Uredbo o evropski kritični infrastrukturi (Uradni list RS, št. 35/11).

Predlog zakona je treba sprejeti zaradi prenosa določb Direktive 2022/2557 v pravni red Republike Slovenije. Hkrati se s predlogom zakona natančneje ureja tudi določena vprašanja povezana z odzivanjem na izredne dogodke na področju kritične infrastrukture.

1.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji

Glavni cilj predloga zakona je zagotovitev prenosa Direktive 2022/2557 v pravni red Republike Slovenije.

2.2 Načela

Predlagane spremembe in dopolnitve sicer ne posegajo v načela ZKI, jih pa dopolnjujejo v smeri v zagotovitve čim višje ravni odpornosti in zmogljivosti kritičnih subjektov ter njihove kritične infrastrukture za neprekinjeno opravljanje bistvenih storitev ob soočanju z različnimi tveganji.

Temeljna načela predlaganih sprememb zakona so:
- predmet zakonskega urejanja je področje kritične infrastrukture Republike Slovenije, ugotavljanje in določanje kritičnih subjektov ter ugotavljanje kritičnih subjektov posebnega evropskega pomena in načrtovanje ukrepov za zagotavljanje odpornosti kritičnih subjektov in kritične infrastrukture;
- pri določanju obveznosti in odgovornosti organov in organizacij na področju kritične infrastrukture mora biti vodilo sorazmernost teh obveznosti oziroma odgovornosti ter izogibanje podvajanju in nepotrebnim obremenitvam;
- lastništvo kritične infrastrukture ni dejavnik, ki odločilno vpliva na ureditev področja kritične infrastrukture;
- kritična infrastruktura Republike Slovenije lahko dobi status objekta, ki je pomemben za obrambo države, če skladno z 29. členom Zakona o obrambi (Uradni list RS, št. 103/04– uradno prečiščeno besedilo, 95/15 in 139/20) tako odloči Vlada Republike Slovenije.

Načela, na katerih temelji odpornost kritičnih subjektov in kritične infrastrukture, predvidena s predlogom zakona, so: načelo celovitega pristopa, načelo odgovornosti, načelo zaščite pred različnimi vrstami nevarnosti, načelo neprekinjenega zagotavljanja odpornosti kritičnih subjektov in kritične infrastrukture ter načelo izmenjave podatkov in informacij.

2.3 Poglavitne rešitve

S Predlogom zakona se v slovenski pravni red prenaša Direktivo 2022/2557 (1. in 2. člen), pri čemer ji v celoti sledi tudi glede opredelitve področja uporabe (3. člen), ki ni enaka za vse subjekte. Zakon bo veljal za subjekte javne uprave ali zasebne subjekte, ki jih bo za kritične subjekte določila vlada ali jih bo kot kritične subjekte posebnega evropskega pomena določila Evropska komisija. Določbe poglavja o odpornosti kritičnih subjektov in kritične infrastrukture (III.), poglavja o kritičnih subjektih posebnega evropskega pomena (III.A) in poglavja o nadzoru (VII.) se za določene subjekte, zaradi njihovega specifičnega pomena, ne bodo uporabljale, prav tako se zakon ne bo uporabljal za vsebine, ki jih ureja zakon, ki ureja področje informacijske varnosti.

V predlogu zakona je prenovljen pomen izrazov, ki so terminološko in vsebinsko usklajeni s pojmi Direktive 2022/2557, ki v ospredje pravnega okvirja postavlja zagotavljanje bistvenih storitev na notranjem trgu Evropske unije (4. člen).

Novo poglavje, ki opredeljuje nacionalni okvir za odpornost kritičnih subjektov (5. člen), nalaga vladi sprejem strategije za odpornost kritičnih subjektov in nacionalne ocene tveganja za opravljanje bistvenih storitev ter opredeljuje osnovna izhodišča za njuno pripravo in obvezne vsebine obeh aktov.

Celotno poglavje ZKI o ugotavljanju in določanju kritične infrastrukture se vsebinsko spreminja in po predlogu zakona določa ugotavljanje in določanje kritičnih subjektov ter njihove kritične infrastrukture (6. člen). Temu sledi 7. člen, ki taksativno našteva enajst sektorjev kritične infrastrukture. 8. člen opredeljuje kriterije za ugotavljanje kritičnih subjektov, pri čemer vzpostavlja vsebinsko in funkcionalno razlikovanje med njimi. Prvi se nanašajo na presojanje nosilcev sektorjev kritične infrastrukture glede opravljanja bistvene storitve in ugotavljanje posledic izrednega dogodka na opravljanje posamezne bistvene storitve, drugi pa na določitev pomembnosti motečega učinka oziroma posledic izrednega dogodka na opravljanje bistvene storitve. Za uporabo slednjih bo treba opredeliti še njihove mejne vrednosti, kar bo določila vlada s predpisom. V skladu s postopkom, določenim z 10. členom predloga zakona vlada določi kritične subjekte in njihovo kritično infrastrukturo. Predlog zakona ministrstvu, pristojnemu za obrambo, v vlogi pristojnega nacionalnega organa na področju kritične infrastrukture in enotne kontaktne točke po določitvi kritičnih subjektov nalaga obveznosti, v prvi vrsti do kritičnih subjektov, pa tudi do Evropske komisije, še zlasti pa zagotavljanje podpore kritičnim subjektom pri krepitvi njihove odpornosti (11. člen).

Obseg obveznosti kritičnih subjektov ostaja enak obsegu njihovih obveznosti, kot so bile opredeljene v osnovnem zakonu. Kritični subjekti bodo tako kot do sedaj upravljavci kritične infrastrukture po zakonu dolžni izdelati oceno tveganja za bistveno storitev, ki jo zagotavljajo in na njeni podlagi sprejeti ukrepe za odpornost. Ti so v predlogu zakona razvrščeni po sklopih in v primerjavi s trenutno ureditvijo bolj konkretizirani. Ocena in ukrepi predstavljajo načrt kritičnega subjekta za odpornost. Predlog zakona daje podlago kritičnemu subjektu, da ta lahko ob upoštevanju nacionalne in svoje ocene tveganja predloži zahtevek za preverjanje preteklosti zaposlenih in kandidatov za zaposlitev na delovnih mestih, ki so pomembna za opravljanje bistvenih storitev kritičnega subjekta in imajo ali bodo imeli pooblaščen neposredni ali oddaljeni dostop do prostorov, informacij ali nadzornih sistemov kritičnega subjekta (spremenjeni 15. člen ZKI). Za kritične subjekte je pomembno tudi določilo o možni uporabi evropskih in mednarodnih standardov ter tehničnih specifikacij veljavnih ukrepov za varnost in odpornost kritičnih subjektov (15.a člen) .

Predlog zakona v okvir ZKI postavlja novo III.A poglavje, ki določa postopek ugotavljanja kritičnih subjektov posebnega evropskega pomena. Takšen status lahko dobi kritični subjekt, ki ga je kot takega določila vlada, če opravlja enake ali podobne bistvene storitve šestim ali več državam članicam ali v šestih ali več državah članicah in je bil uradno obveščen s strani Evropske komisije, da je določen kot kritični subjekt posebnega evropskega pomena. Ti so zaradi svojega pomena med drugim, s stani Evropske komisije deležni svetovanja in podpore, pa tudi ocenjevanja ustreznosti načrtovanih ukrepov za odpornost (13. člen).

V predlogu zakona so izvedene ustrezne terminološke prilagoditve. Na novo se določa imenovanje koordinacijske skupine za usklajen in učinkovit odziv na izredne dogodke na področju kritične infrastrukture (18. člen).

Ker se zakon ne bo uporabljal za Banko Slovenije in ker predlog zakona ne opredeljuje izraza »kriza« se 21. in 22. člen ZKI, ki se nanašata na naloge NCKU v primeru krize oziroma na Banko Slovenije, črtata (19. člen).

Dopolnjeno V. poglavje ZKI vsebuje glavna sistemska določila v zvezi z obveščanjem, poročanjem in zagotavljanjem podatkovne podpore odločanju na področju kritične infrastrukture. Vzpostavlja podlago za oblikovanje sistema zgodnjega opozarjanja na področju kritične infrastrukture in mehanizma priglasitve izrednih dogodkov. Namen vzpostavitve sistema zgodnjega opozarjanja je zaznavanje in analiza razlik v vrednostih kazalnikov po posameznih sektorjih, preden te prerastejo v

izredne dogodke ali motnje pri opravljanju bistvenih storitev. V povezavi z novim 24.a členom predloga zakona o obveznosti priglasitve izrednih dogodkov se pričakuje, da bodo kritični subjekti brez odlašanja posredovali vse razpoložljive informacije, ki jih pristojni organi in organizacije potrebujejo za odločanje. To pristojnim organom in organizacijam in telesom kriznega upravljanja omogoča hiter in ustrezen odziv na izredne dogodke ter celovit pregled vpliva, narave, vzroka in morebitnih posledic izrednih dogodkov, s katerimi se spoprijemajo kritični subjekti. Predvideno je, da bodo za ta namen uporabili digitalno platformo, ki jo bo vzpostavil pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost. Spremenjeni 25. člen ZKI, ki predstavlja zakonsko podlago za zbiranje, obdelovanje, uporabo in hrambo podatkov o odgovornih in kontaktnih osebah nosilcev sektorjev kritične infrastrukture in kritičnih subjektov je terminološko spremenjen in dopolnjen z navedbo podatka o elektronskem naslovu navedenih oseb (20. člen).

Podatke, ki se nanašajo na ugotavljanje, določanje in odpornost kritičnih subjektov ter kritične infrastrukture in so določeni kot tajni podatki ali poslovna skrivnost, se obravnava v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost (21. člena), pri čemer je treba poudariti, da zaupni podatki Banke Slovenije niso predmet urejanja predloga zakona, zato se 27. člen ZKI črta (22.člen).

V skladu z določbami Direktive 2022/2557 23. člen predloga zakona kljub temu, da inšpektorat, pristojen za obrambo, lahko v skladu z že obstoječimi predpisi in uveljavljenim načinom dela k inšpekcijskemu nadzoru lahko pritegne tudi druge inšpekcijske organe, ki imajo stvarne pristojnosti na področju sektorja kritične infrastrukture, vzpostavlja zakonsko podlago in možnost navedenemu inšpektoratu, da lahko od bistvenih subjektov, določenih na podlagi zakona, ki ureja informacijsko varnost, zahteva predložitev informacij za oceno, ali ukrepi, ki so jih le-ti sprejeli za zagotovitev svoje odpornosti, izpolnjujejo zahteve iz 13. člena predloga zakona in dokaze o učinkovitem izvajanju teh ukrepov. Hkrati vzpostavlja podlago tudi za to, da inšpektorat, pristojen za obrambo, lahko od inšpekcije pristojnega nacionalnega organa, na podlagi zakona, ki ureja informacijsko varnost, zahteva, da ta izvaja svoja nadzorna in izvršilna pooblastila glede subjekta, identificiranega na podlagi zakona, ki ureja informacijsko varnost, in določenega za kritični subjekt na podlagi tega predloga zakona, ter da mu v zvezi s tem posreduje informacije. Skladno z določbami Direktive 2022/2555 in predlogom novega zakona, ki bo urejal informacijsko varnost, bodo namreč vsi kritični subjekti, določeni na podlagi tega predloga zakona tudi zavezanci po predlogu zakonu, ki ureja informacijsko varnost, in je tako, v členu opredeljeno sodelovanje navedenih nadzornih organov, smiselno.

V predlogu zakona so taksativno našteti prekrški pri izvajanju zakona, zaradi katerih se kaznujeta kritični subjekt kot pravna oseba in odgovorna oseba kritičnega subjekta in obveznost ministrstva, pristojnega za obrambo, da o prekrških iz predloga zakona do nevednega roka obvesti Evropsko komisijo, in jo redno obvešča tudi o morebitnih spremembah (24 člen). 25. člen pa zagotavlja zakonsko podlago, da se lahko v hitrem postopku za prekrške po predlogu zakona izreče tudi globa v znesku, ki je višji od najnižje, ki jo predvideva predlog zakona.

Prehodne in končne določbe predloga zakona pristojnim organom in organizacijam (tj. vladi, ministrstvu, nosilcem sektorjev kritične infrastrukture in kritičnim subjektom) določajo rok, v katerem morajo izvesti glavne oziroma izhodiščne naloge (sprejem izvršilnega predpisa, aktov in poročanje Evropski komisiji), ki so povezane z ugotavljanjem, določanjem in odpornostjo kritičnih subjektov in njihove kritične infrastrukture za zagotavljanje neprekinjenega opravljanja bistvenih storitev in so jim naložene s predlogom zakona (26. člen).

V izogib pravni praznini se uporaba ZKI in Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije za kritično infrastrukturo Republike Slovenije in pristojne organe in organizacije, določene na podlagi ZKI podaljša do določitve kritičnih subjektov, na podlagi predloga zakona. Z uveljavitvijo predloga zakona bosta navedeno navodilo in Uredba o evropski kritični infrastrukturi prenehala veljati.(27. člen).

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA

Novela zakona nima vpliva na državni proračun. Izvajanje Zakona o kritični infrastrukturi ima lahko neposredne posledice za državni proračun samo v primeru, če bi ob prekinitvi delovanja kritične infrastrukture nosilec sektorja kritične infrastrukture za zagotovitev delovanja kritične infrastrukture v obsegu, ki še omogoča opravljanje bistvene storitve, pripravil predlog dodatnih ukrepov za odpornost na ravni sektorja kritične infrastrukture, izvedba teh ukrepov pa bi bila naložena kritičnemu subjektu. Zakon namreč predvideva, da bi se lahko v navedenem primeru sredstva za izvedbo obravnavanih ukrepov, ki jih naloži državni organ, zagotovila iz državnega proračuna. Višina potrebnih sredstev ter način njihovega zagotavljanja sta v takšnem primeru odvisna od konkretnih razmer in ju ni mogoče vnaprej oceniti.

Sprejem zakona ne bo imel finančnih posledic na druga javna sredstva.

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATERO JE BIL DRŽAVNI PRORAČUN ŽE SPREJET

2.

Za izvajanje zakona dodatnih finančnih sredstev v že sprejetem državnem proračunu ni treba zagotoviti.

3.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOSTI PREDLAGANE UREDITVE PRAVU EVROPSKE UNIJE

Evropska unija (EU)

Predlog zakona je treba sprejeti zaradi prenosa Direktive 2022/2557, ki je bila uveljavljena. 16. januarja 2023, v pravni red Republike Slovenije. Vse države članice Evropske unije so jo dolžne implementirati v svojo zakonodajo do 17. oktobra 2024, kar pomeni, da so vse države članice trenutno še v postopku njenega prenosa v nacionalno zakonodajo. Tako ni mogoče prikazati pravne ureditve drugih držav članic zaradi prenosa Direktive 2022/2557 v zakonodajo, pač je podan prikaz obstoječe ureditve področja kritične infrastrukture v Portugalski, Romuniji, Madžarski in Češki republiki.

Predlog zakona je prilagojen pravnemu redu EU, saj bo v vsebino ZKI vnesel določbe Direktive 2022/2557.

Portugalska

Portugalska je področje kritične infrastrukture normativno uredila leta 2022 z zakonom, s katerim je bila v nacionalno zakonodajo implementirana direktiva Sveta (ES) št. 114/2008. Z zakonom se je določila in prilagodila tudi struktura in naloge vladnega centra za upravljanje računalniških omrežij (CEGER) za prihodnje izzive, kot so izvajanje načrta za okrevanje in odpornost ter strategije za inovacije in posodobitev državne in javne uprave 2020–2023 ter akcijskega načrta za digitalni prehod Portugalske. V zakonu so jasno opredeljeni pojmi kot so "varnostno območje", "sektorski subjekt", "kritična infrastruktura", "evropska kritična infrastruktura" in drugi. Zakon se uporablja za opredelitev, določitev, zaščito in povečanje odpornosti nacionalne in evropske kritične infrastrukture v relevantnih sektorjih. Zakon operaterjem kritične infrastrukture in sektorskim subjektom nalaga zagotavljanje zaščite in odpornosti storitev. V zakonu je opredeljeno ravnanje z občutljivimi podatki in zagotovljena zakonska podlaga za varnostno preverjanje oseb, ki imajo dostope do občutljivih podatkov. Organ, pristojen za ugotavljanje in določanje kritične infrastrukture je nacionalni svet, pristojen za civilne nesreče. Evropska kritična infrastruktura je določena na podlagi utemeljenih predlogov sektorskih subjektov. Nacionalni svet za načrtovanje civilnih nesreč odloča o kategoriziranju nacionalne in

evropske kritične infrastrukture ter o tem obvešča pristojne organe. Za vsako nacionalno in evropsko kritično infrastrukturo je treba izdelati varnostni načrt, ki vključuje opredelitev kritičnih elementov, analizo tveganj in postopke kriznega upravljanja. Sektorji kritične infrastrukture, opredeljeni v zakonu so: energetika, promet, komunikacije, digitalne storitve, pitna in odpadna vode, prehrana, zdravstvo, finančne storitve ter sektor obrambe in varnosti.

Romunija

Romunija je z zakonom o opredelitvi, določitvi in zaščiti kritične infrastrukture iz leta 2010 v svoj pravni red prenesla direktivo Sveta (ES) št. 114/2008. Zakon ureja nacionalno in evropsko kritično infrastrukturo in določa merila za identifikacijo ter postopek za določitev nacionalne in evropske kritične infrastrukture. Sektorski kriteriji in njihove mejne vrednosti se določajo na podlagi usklajevanja pristojnih organov. Sektorski kriteriji za določanje kritične infrastrukture se oblikujejo na podlagi upoštevanja medsektorskih kriterijev, pri čemer upoštevajo število mrtvih in poškodovanih oseb, posledice prenehanja zagotavljanja dobrin in storitev za gospodarstvo in prebivalstvo itd. V zakonu opredeljeni sektorji kritične infrastrukture so: sektor energije, sektor informacijskih in komunikacijskih tehnologij, sektor voda, gozdov in okolja, sektor prehrane in kmetijstva, sektor zdravja, sektor nacionalne varnosti, sektor javne uprave, sektor prometa, sektor industrije, sektor vesolja in raziskav, sektor financ in bančništva in sektor kulture. Zakon opredeljuje tudi vlogo Nacionalnega koordinacijskega centra za zaščito kritične infrastrukture, ki deluje v sklopu ministrstva, pristojnega za notranje zadeve in zagotavlja strateško načrtovanje, usklajevanje in stalno spremljanje ter nadzor nad izvajanjem dejavnosti, opredeljenih v zakonu.

Madžarska

Madžarska je področje kritične infrastrukture uredila z zakonom, ki ga sprejela leta 2012. Zakon CLXVI o opredelitvi, določitvi in zaščiti kritičnih sistemov in objektov (mad. 2012. évi CLXVI. Törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről) je bil pripravljen zaradi prenosa direktive Sveta (ES) št. 114/2008 v nacionalno zakonodajo. Zakon med drugim določa pristojnosti in odgovornosti državnih organov pri zaščiti kritične infrastrukture. Določa sektorje kritične infrastrukture, ki so: energetika, kmetijstvo, zdravstvo, finance, informacijske in komunikacijske tehnologije, voda, zaščita javne varnosti, nacionalna obramba, promet in socialna varnost. Posamezni sektorji kritične infrastrukture so razdeljeni na podsektorje. Vsi gospodarski subjekti, ki opravljajo storitve na področju enega izmed opredeljenih sektorjev, morajo opraviti identifikacijsko oceno, ki vključuje analizo in oceno dejavnikov tveganja ogrožanja neprekinjenih storitev. Skladno z zakonom morajo poročilo o izvedeni identifikacijski oceni predložiti pristojnemu organu za posamezni sektor, ki ga pregleda ter oceni ustreznost izpolnjevanja horizontalnih in sektorskih meril za določitev izvajalcev bistvenih storitev. Če sta izpolnjena vsaj eno sektorsko merilo in vsaj eno horizontalno merilo, pristojni sektorski organ na podlagi zakona določi ključno sestavino ali storitev in odredi njeno registracijo, hkrati pa predvidi vključitev subjekta oziroma izvajalca na seznam izvajalcev bistvenih storitev.

Češka republika

Češka republika je področje kritične infrastrukture uredila z zakonom, sprejetim leta 2000, v katerem je kritična infrastruktura opredeljena, kot tista infrastruktura, katere motnje bi resno vplivale na varnost države, zadovoljevanje osnovnih potreb prebivalstva, zdravje ljudi ali gospodarstvo države. Vlada je na podlagi zakona leta 2010 z uredbo določila presečna in sektorska merila za ugotavljanje in določanje elementov kritične infrastrukture. Presečna merila za določitev elementa kritične infrastrukture, kot jih opredeljuje zakon, so naslednja: 250 smrtnih žrtev ali več kot 2500 oseb potrebnih hospitalizacije; gospodarski vpliv na bruto domači proizvod v višini več kot 0,5 %; vpliv na zmanjšanje zagotavljanja osnovnih storitev, ki bi prizadelo več kot 125 000 ljudi. Uredba določa devet sektorjev in sicer: energetika, upravljanje voda, prehrana in kmetijstvo, zdravstvo, promet, komunikacijski in informacijski sistemi, finančni trgi, reševalne službe in javna uprava. Sektorji so razdeljeni v podsektorje.

6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA

6.1 Presoja administrativnih posledic

a) v postopkih oziroma poslovanju javne uprave ali pravosodnih organov:

V ministrstvih, ki bodo na podlagi predloga zakona določeni za nosilce novih sektorjev kritične infrastrukture bo lahko uuresničevanje njihovih pristojnosti in odgovornosti na področju kritične infrastrukture zahtevalo zaposlitev dodatnih javnih uslužbencev, vsekakor pa bo potrebno dodatno usposabljanje že zaposlenih izvajalcev nalog na področju kritične infrastrukture. Po predlogu zakona so subjekti javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, notranje varnosti, obrambe ali kazenskega pregona, vključno s preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, oziroma kritični subjekti, ki opravljajo storitve le na področju javne uprave in za sodstvo, parlament ter Banko Slovenije, izključeni iz njegove uporabe.

4.

b) pri obveznostih strank do javne uprave ali pravosodnih organov:

5.

6. Zakon ne bo imel posledic na obveznosti strank do javne uprave ali pravosodnih organov.

7.

6.2 Presoja posledic za okolje, vključno s prostorskimi in varstvenimi vidiki, in sicer za:

Zakon ne bo imel posledic na okolje.

6.3 Presoja posledic za gospodarstvo, in sicer za:

Izvajanje zakona bo vplivalo na poslovne stroške tistih kritičnih subjektov, ki doslej na podlagi Zakona o kritični infrastrukturi niso imeli statusa upravljavca kritične infrastrukture Republike Slovenije in niso bili zavezani k izdelavi dokumentov načrtovanja zaščite kritične infrastrukture. Subjekti, ki bodo na podlagi predloga zakona povsem na novo določeni za kritične subjekte, bodo morali izdelati oceno tveganja za bistveno storitev, ki jo zagotavljajo, in sprejeti ukrepe za odpornost, kar bo zahtevalo precejšen delovni napor in tudi finančni vložek. Če bodo kritični subjekti gospodarske družbe, bodo lahko ti poslovni stroški delno neposredno neugodno vplivali na konkurenčnost teh podjetij oziroma gospodarskih družb. V zvezi s tem je pomembno določilo predloga zakona, da lahko kritični subjekti pri izdelavi načrta za odpornost smiselno upoštevajo dokumente, ukrepe, postopke in rešitve, ki so jih izdelali oziroma sprejeli na podlagi drugih predpisov ali svojih poslovnih odločitev. Upoštevaje vse navedeno je celovita ocena vplivov izvajanja zakona na gospodarstvo, predvsem na mala in srednja podjetja, ki bo izvedena s pomočjo testa MSP, pokazala, da bodo skupni predvideni letni stroški izvajanja tega zakona, ko gre za kritične subjekte s statusom gospodarske družbe, znašali okoli ___.

Toda pri ocenjevanju poslovnih stroškov kritičnih subjektov iz gospodarskega okolja, povezanih z izvajanjem zakona, je treba upoštevati tudi mogoč vzvratni vpliv ukrepov za odpornost, ki je ugoden. Z izvajanjem teh ukrepov bo kritični subjekt povečal svojo odpornost na motnje v delovanju ali prekinitev delovanja infrastrukture, ki jo upravlja, naložba subjekta v lastno varnost in zaščito pa dolgoročno običajno vpliva na njegovo poslovanje. Izvajanje zakona bo vsaj posredno ugodno vplivalo na potrošnike in gospodinjstva, saj naj bi prispevalo k neprekinjenemu zagotavljanju bistvenih storitev, ki so ključne za nemoteno delovanje države, ohranitev življenjsko pomembnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja.

6.4 Presoja posledic za socialno področje, in sicer za:

Zakon ne bo imel posledic za socialno področje.

6.5 Presoja posledic za dokumente razvojnega načrtovanja, in sicer za:

Zakon ne bo imel posledic za dokumente razvojnega načrtovanja.

6.6 Presoja posledic za druga področja

Zakon ne bo imel posledic za druga področja.

6.7 Izvajanje sprejetega predpisa:
a) Predstavitev sprejetega zakona:

Ministrstvo za obrambo bo sprejeti zakon predstavilo ciljnim skupinam (ministrstva in vladne službe kot nosilci sektorjev kritične infrastrukture, kritični subjekti) preko seminarjev oziroma delavnic, širši javnosti pa s spletno predstavitvijo.

b) Spremljanje izvajanja sprejetega predpisa:

Izvajanje tega zakona bo spremljalo Ministrstvo za obrambo, ki strokovno usmerja in usklajuje dejavnosti na področju kritične infrastrukture. Metodologija za spremljanje doseganja ciljev zakona ni predvidena.

6.8 Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona
V zvezi s predlogom zakona ni drugih pomembnih okoliščin.

7. Prikaz sodelovanja javnosti pri pripravi predloga zakona:
Javna objava predloga zakona na portalu E-demokracija, kamor je bilo mogoče sporočiti mnenja, predloge in pripombe, je trajala od _____. Sočasno je bil predlog zakona objavljen na spletnih straneh Ministrstva za obrambo.

Javna predstavitev predloga zakona je potekala _____. Javna obravnava predloga zakona je potekala v prostorih Državnega sveta Republike Slovenije od _____.

8. Podatek o zunanjem strokovnjaku oziroma pravni osebi, ki je sodelovala pri pripravi predloga zakona, in znesku plačila za ta namen:
Pri pripravi zakona ni sodeloval zunanji strokovnjak oziroma pravna oseba.

9. Navedba, kateri predstavniki predlagatelja bodo sodelovali pri delu državnega zbora in delovnih teles
- Marjan Šarec, minister za obrambo,
- dr. Damir Črnčec, državni sekretar na Ministrstvu za obrambo,
- Boštjan Pavlin, mag., generalni direktor Direktorata za obrambne zadeve, Ministrstvo za obrambo,
- Anica Ferlin, vodja Sektorja za civilno obrambo v Direktoratu za obrambne zadeve, Ministrstvo za obrambo,
- Igor Nered, sekretar v Kabinetu ministra za obrambo.

II. BESEDILO ČLENOV

Zakon o spremembah in dopolnitvah Zakona o kritični infrastrukturi

1. člen

V Zakonu kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M) se besedilo 1. člena spremeni tako, da se glasi:

»(1) Ta zakon ureja področje kritične infrastrukture, postopek ugotavljanja in določanja kritičnih subjektov ter ugotavljanja kritičnih subjektov posebnega evropskega pomena, opredeljuje nacionalni okvir za odpornost kritičnih subjektov in ukrepe za zagotavljanje odpornosti kritičnih subjektov pri opravljanju bistvenih storitev.

(2) Ta zakon določa pristojnosti in naloge pristojnih organov in organizacij, pristojnega nacionalnega organa in enotne kontaktne točke ter okvir za zgodnje opozarjanje, zagotavljanje podpore odločanju, poročanje in nadzor na področju kritične infrastrukture.«.

2. člen

2. člen se spremeni tako, da se glasi:

»2. člen
(prenos direktive)

S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov (v nadaljnjem besedilu: Direktiva 2022/2557) in razveljavitvi Direktive Sveta 2008/114/ES (UL L št. 333/142 z dne 27. 12. 2022, str. 164).«.

3. člen

Za 2. členom se doda nov, 2.a člen, ki se glasi:

»2.a člen
(področje uporabe zakona)

(1) Ta zakon se uporablja za subjekte javne uprave ali zasebne subjekte, ki so v skladu s tem zakonom določeni kot kritični subjekti ali jih je kot kritične subjekte posebnega evropskega pomena določila Evropska komisija.

(2) Za kritične subjekte v sektorjih bančništva, infrastrukture finančnega trga in digitalne infrastrukture se III., III.A in VII. poglavje tega zakona ne uporabljajo.

(3) Ta zakon se ne uporablja za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, notranje varnosti, obrambe ali kazenskega pregona, vključno s preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, oziroma za kritične subjekte, ki opravljajo storitve le na področju javne uprave iz tega člena in za sodstvo, Državni zbor Republike Slovenije ter Banko Slovenije.

(4) Ta zakon se ne uporablja za vsebine, ki jih ureja zakon, ki ureja področje informacijske varnosti.«.

4. člen

3. člen se spremeni tako, da se glasi:

»3. člen
(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, pomenijo:

1. bistvena storitev je storitev, ki je ključna za nemoteno delovanje države, ohranitev življenjsko pomembnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja;
2. izredni dogodek po tem zakonu je nekibernetski incident, ki pomeni dogodek, ki bi lahko povzročil pomembne motnje ali ki povzroči motnje v opravljanju bistvene storitve, tudi kadar vpliva na sisteme, ki varujejo pravno državo;
3. kategorije subjektov so skupine subjektov, ki so povezane glede na vrsto in namen bistvene storitve, ki jo opravljajo in izmed katerih nosilci sektorjev ugotavljajo kritične subjekte;
4. kibernetski incident je dogodek kot ga določa zakon, ki ureja informacijsko varnost;
5. kritična infrastruktura Republike Slovenije je sredstvo, objekt, oprema, omrežje ali sistem oziroma njegov del, ki je nujen za oziroma omogoča opravljanje bistvenih storitev (v nadaljnjem besedilu: kritična infrastruktura);
6. kritični subjekt je javni ali zasebni subjekt, ki opravlja bistveno storitev in je določen kot tak (v nadaljnjem besedilu: kritični subjekt);
7. nosilci sektorjev kritične infrastrukture so posamezna ministrstva in službe Vlade Republike Slovenije (v nadaljnjem besedilu: vlada), ki so odgovorni za delovna področja, na katera spada kritična infrastruktura;
8. ocena tveganja je celoten postopek ugotavljanja narave in obsega tveganja, in sicer s prepoznavanjem in analiziranjem morebitnih pomembnih groženj, ranljivosti in nevarnosti, ki bi lahko privedle do izrednega dogodka, ter z vrednotenjem možnosti izgube ali motenj, ki jih ta izredni dogodek povzroči pri opravljanju bistvene storitve;
9. odpornost kritičnega subjekta je sposobnost kritičnega subjekta, da prepreči izredni dogodek, se pred njim zavaruje, se nanj odzove, se mu zoperstavi, ga ublaži in absorbira, se nanj prilagodi ter po njem okreva;
10. področje kritične infrastrukture obsega dejavnosti, povezane z ugotavljanjem in določitvijo kritičnih subjektov ter načrtovanjem ukrepov za zagotavljanje odpornosti kritičnih subjektov in kritične infrastrukture (v nadaljnjem besedilu: ukrepi za odpornost);
11. povečana ogroženost kritične infrastrukture je stanje, ki ga zazna pristojni državni organ in za katerega oceni, da bi lahko povzročil izredni dogodek;
12. pristojni organi in organizacije na področju kritične infrastrukture so vlada, pristojni nacionalni organ, nosilci sektorjev kritične infrastrukture, organi, ki sodelujejo z nosilci sektorjev kritične infrastrukture pri izvajanju njihovih nalog po tem zakonu (v nadaljnjem besedilu: sodelujoči organi), kritični subjekti, kritični subjekti posebnega evropskega pomena, koordinacijska skupina, Nacionalni center za krizno upravljanje (v nadaljnjem besedilu: NCKU) in inšpektorat, pristojen za obrambo;
13. pristojni nacionalni organ na področju kritične infrastrukture je ministrstvo, pristojno za obrambo (nadaljnjem besedilu: ministrstvo);
14. sektorji kritične infrastrukture so posamezne vsebinsko zaokrožene celote delovanja kritične infrastrukture, ki omogočajo opravljanje bistvenih storitev, sestavljene iz podsektorjev;
15. tveganje predstavlja možnost izgube ali motnje pri opravljanju bistvenih storitev, zaradi izrednega dogodka in je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi do izrednega dogodka prišlo.«.

5. člen

Za 3. členom se doda novo, I.A poglavje, ki se glasi:

»I.A NACIONALNI OKVIR ZA ODPORNOST KRITIČNIH SUBJEKTOV

3.a člen
(strategija za odpornost kritičnih subjektov)

(1) Vlada sprejme strategijo za odpornost kritičnih subjektov (v nadaljnjem besedilu: strategija). V strategiji se določijo cilji in ukrepi, za doseganje in ohranjanje visoke ravni odpornosti kritičnih subjektov v vseh sektorjih kritične infrastrukture.

(2) Strategija vsebuje vsaj naslednje elemente:

1. strateške cilje in prednostne naloge za okrepitev odpornosti kritičnih subjektov ob upoštevanju čezmejne ter medsektorske odvisnosti in soodvisnosti;
2. upravljanje za doseganje strateških ciljev in prednostnih nalog, vključno z navedbo nalog pristojnih organov in organizacij na področju kritične infrastrukture pri izvajanju strategije;
3. ukrepi za odpornost kritičnih subjektov, vključno z opisom elementov nacionalne ocene tveganja za opravljanje bistvenih storitev;
4. postopek ugotavljanja kritičnih subjektov;
5. postopek za podporo kritičnih subjektov vključno z ukrepi za okrepitev sodelovanja med subjekti javne uprave in zasebnimi subjekti;
6. seznam drugih organov in organizacij, ki sodelujejo pri izvajanju strategije;
7. upravljanje z namenom usklajevanja med pristojnimi organi in organizacijami na področju kritične infrastrukture in pristojnimi organi na podlagi zakona, ki ureja informacijsko varnost za izmenjavo informacij o tveganjih za kibernetsko varnost, o kibernetskih grožnjah in kibernetskih incidentih ter nekibernetskih tveganjih, grožnjah in izrednih dogodkih ter opravljanju nadzora;
8. veljavne, sprejete ukrepe malih in srednjih podjetij za lažje izvajanje obveznosti iz III. poglavja zakona.
8.

(3) Nosilci sektorjev kritične infrastrukture redno oziroma vsaj na vsaka štiri leta ministrstvu posredujejo podatke za posodobitev strategije. Ob vsaki večji posodobitvi ministrstvo novo strategijo posreduje v vednost Evropski komisiji.

3.b člen
(nacionalna ocena tveganja za opravljanje bistvenih storitev)

(1) Vlada določi seznam bistvenih storitev in sprejme nacionalno oceno tveganja za opravljanje bistvenih storitev.

(2) V nacionalni oceni tveganja se upoštevajo relevantna tveganja in tveganja, ki jih povzroči človek, vključno s tveganji medsektorske in čezmejne narave, nesrečami, naravnimi nesrečami, izrednimi razmerami v javnem zdravju in s hibridnimi grožnjami ali drugimi antagonističnimi grožnjami, in terorističnimi kaznivimi dejanji.

(3) Pri izdelavi nacionalne ocene iz prvega odstavka se upoštevajo tudi:

1. splošna ocena tveganja, opravljena na podlagi predpisa, ki ureja izvajanje Sklepa o mehanizmu Unije na področju civilne zaščite;
2. druge ocene tveganja, izdelane v skladu z zahtevami sektorskih pravnih aktov Evropske unije, vključno z uredbama (EU) 2017/1983 Evropskega parlamenta in Sveta o ukrepih za zagotavljanje zanesljivosti oskrbe s plinom in (EU) 2019/941 Evropskega parlamenta in Sveta o pripravljenosti na tveganja v sektorju električne energije ter direktivama 2007/60/ES o oceni in

obvladovanju poplavne ogroženosti in 2012/18/EU Evropskega parlamenta in Sveta o obvladovanju nevarnosti večjih nesreč, v katere so vključene nevarne snovi;
3. relevantna tveganja, ki izhajajo iz soodvisnosti sektorjev in odvisnosti sektorjev od subjektov in koliko so sektorji odvisni od subjektov, ki so v drugih državah članicah ter tretjih državah;
4. vpliv, ki bi ga pomembna motnja v enem sektorju lahko imela v drugih sektorjih, vključno z vsemi pomembnimi tveganji za državljane in notranji trg;
5. informacije o izrednih dogodkih, priglašenih v skladu s 24.a členom tega zakona.

(4) Za namen izdelave ocene tveganja in sprejemanja ukrepov za odpornost, ministrstvo in nosilci sektorjev kritične infrastrukture kritičnim subjektom posredujejo potrebne informacije o nacionalni oceni tveganja, prepoznanih tveganjih in drugih bistvenih elementih, ki so jim v pomoč pri izvedbi njihove ocene tveganja in sprejemanju ukrepov za odpornost.

(5) Nosilci sektorjev kritične infrastrukture redno oziroma vsaj na vsaka štiri leta ministrstvu posredujejo podatke za posodobitev nacionalne ocene tveganja.«.

6. člen

Naslov II. poglavja se spremeni tako, da se glasi:

»II. UGOTAVLJANJE IN DOLOČANJE KRITIČNIH SUBJEKTOV TER KRITIČNE INFRASTRUKTURE«.

7. člen

Besedilo 4. člena se spremeni tako, da se glasi:

»(1) Sektorji kritične infrastrukture so sektor energetike, sektor prometa, sektor bančništva, sektor infrastrukture finančnega trga, sektor zdravja, sektor pitne vode, sektor odpadne vode, sektor digitalne infrastrukture, sektor javne uprave, sektor vesolja ter sektor pridelave, predelave in distribucije živil.

(2) Sektorji iz prejšnjega odstavka imajo nosilca in enega ali več sodelujočih organov.

(3) Vlada določi podsektorje in nosilce sektorjev iz prvega odstavka ter sodelujoče organe.

8. člen

5. člen se spremeni tako, da se glasi:

»5. člen
(kriteriji za ugotavljanje kritičnih subjektov)

(1) Vlada določi kategorije subjektov, izmed katerih nosilci sektorjev ugotavljajo kritične subjekte.

(2) Nosilci sektorjev pri ugotavljanju kritičnih subjektov upoštevajo strategijo in rezultate nacionalne ocene tveganja ter naslednje kriterije:
– subjekt opravlja eno ali več bistvenih storitev;
– subjekt deluje in njegova kritična infrastruktura se nahaja v Republiki Sloveniji;
– izredni dogodek bi imel pomembne moteče učinke, določene v skladu s tretjim odstavkom tega člena, na opravljanje bistvene storitve subjekta ali opravljanje odvisnih bistvenih storitev v drugih sektorjih kritične infrastrukture.

(3) Nosilci sektorjev pri določanju pomembnosti motečega učinka iz prejšnjega odstavka upoštevajo naslednje kriterije:

1. število uporabnikov, ki so odvisni od bistvene storitve subjekta;
2. stopnjo odvisnosti drugih sektorjev in podsektorjev od bistvene storitve subjekta;
3. stopnjo in trajanje vpliva, ki bi ga izredni dogodek lahko imeli na gospodarske in družbene dejavnosti, okolje, javno varnost in varovanje ali zdravje prebivalstva;
4. tržni delež subjekta na trgu te bistvene storitve;
5. geografsko razširjenost, kar zadeva območje, ki bi ga izredni dogodek lahko prizadel;
6. pomen subjekta pri ohranjanju zadostne ravni bistvene storitve ob upoštevanju alternativnih načinov za opravljanje te bistvene storitve.

(4) Mejne vrednosti kriterijev, ki se uporabljajo za določitev enega ali več kriterijev iz prejšnjega odstavka, določi vlada.«.

9. člen

6., 7. in 8. člen se črtajo.

10. člen

9. člen se spremeni tako, da se glasi:

»9. člen
(določitev kritičnih subjektov)

(1) Ministrstvo na podlagi kriterijev iz 5. člena in minimalne mejne vrednosti vsaj enega kriterija za določitev pomembnega motečega učinka iz tretjega odstavka 5. člena zakona pripravi seznam kritičnih subjektov in njihove kritične infrastrukture.

(2) Vlada, na podlagi seznama iz prejšnjega odstavka, določi kritične subjekte in njihovo kritično infrastrukturo, o čemer kritične subjekte obvesti ministrstvo v roku enega meseca.

(3) Ministrstvo v roku enega meseca obvesti kritične subjekte v sektorjih bančništva, infrastrukture finančnega trga in digitalne infrastrukture, da nimajo obveznosti iz III. poglavja in da zanje ne velja VII. poglavje zakona.

(4) Ministrstvo roku enega meseca od določitve kritičnih subjektov obvesti nosilce sektorjev bančništva, infrastrukture finančnega trga in digitalne infrastrukture o identiteti kritičnih subjektov iz prejšnjega odstavka in o tem, da nimajo obveznosti iz III. poglavja in da zanje ne velja VII. poglavje zakona.

(5) Ministrstvo Evropski komisiji predloži:

– seznam bistvenih storitev, če se ta spremeni in vsaj na vsaka štiri leta;
– število kritičnih subjektov, ugotovljenih za vsak sektor in podsektor kritične infrastrukture ter za vsako bistveno storitev, ko jih vlada določi, in vsaj na vsaka štiri leta;
– mejne vrednosti kriterijev, ki se uporabljajo za določitev pomembnosti motečega učinka, ki se lahko predložijo kot take ali v zbirni obliki.

(6) Ministrstvo kritične subjekte, ki jim preneha status kritičnega subjekta, obvesti o tem in tem, da zanje od datuma tega uradnega obvestila ne veljajo več obveznosti iz III. poglavja.«.

11. člen

Za 9. členom se dodata nova, 9.a in 9.b člen, ki se glasita:

»9.a člen
(enotna kontaktna točka)

(1) Ministrstvo je enotna kontaktna točka, ki ima povezovalno vlogo in zagotavlja sodelovanje med pristojnimi organi in organizacijami ter čezmejno sodelovanje z enotnimi kontaktnimi točkami drugih držav članic ter z Evropsko komisijo ter sodelovanje s tretjimi državami.

(2) Ministrstvo sodeluje in si izmenjuje informacije s pristojnim nacionalnim organom na podlagi zakona, ki ureja informacijsko varnost, glede tveganj za kibernetsko varnost, kibernetskih groženj in kibernetskih izrednih dogodkov ter nekibernetskih tveganj, groženj in izrednih dogodkov, ki vplivajo na kritične subjekte, tudi glede bistvenih ukrepov, ki so jih sprejeli nosilci sektorjev in pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost.

9.b člen
(podpora kritičnim subjektom)

(1) Ministrstvo in nosilci sektorjev kritičnim subjektom pri krepitvi njihove odpornosti zagotavljajo podporo z različnimi ukrepi, kot so zlasti organizacija usposabljanja kadra in izvajanje vaj za preverjanje njihove odpornosti.

(2) Ministrstvo in nosilci sektorjev medsebojno sodelujejo ter si izmenjujejo informacije in dobre prakse. Za izmenjavo informacij in podatkov, določenih v skladu s predpisi, ki urejajo področje tajnih podatkov, področje osebnih podatkov in poslovno skrivnost, uporabijo zaščiteno komunikacijsko in informacijsko omrežje NCKU.

(3) Ministrstvo kritičnim subjektom zagotavlja podporo tudi preko komunikacijskega in informacijskega omrežja NCKU omogoča sprejemanje, spremljanje in obdelavo podatkov za vzpostavitev centralne slike delovanja kritične infrastrukture in sistema zgodnjega opozarjanja ter predikcije potencialnih izrednih dogodkih na podlagi obvestil kritičnih subjektov. V ta namen NCKU omogoča zaščiteno komunikacijsko in informacijsko omrežje ter neprekinjeno zagotavljanje razpoložljivosti svojih komunikacijskih kanalov in zaupnost in zanesljivost svojih dejavnosti.

(4) Izmenjava informacij o izrednih dogodkih, kibernetskih grožnjah in skorajšnjih incidentih poteka v skladu z zakonom, ki ureja informacijsko varnost, z uporabo digitalne platforme, ki jo vzpostavi pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost.«.

12. člen

III. poglavje se spremeni tako, da se glasi:

»III. ODPORNOST KRITIČNIH SUBJEKTOV IN KRITIČNE INFRASTRUKTURE

10. člen
(načela odpornosti kritičnih subjektov in kritične infrastrukture)

Načela odpornosti kritičnih subjektov in kritične infrastrukture so:

1. načelo celovitega pristopa, ki zahteva, da so v krepitev odpornosti in zaščito kritične infrastrukture pred in med motnjami v delovanju ali ob prekinitvi delovanja kritične infrastrukture ter po njih vključeni pristojni organi in organizacije in da se pri tem upoštevajo različne vrste

nevarnosti, izhaja iz ocen tveganja ter upošteva soodvisnost sektorjev kritične infrastrukture in njihov medsebojni vpliv;
2. načelo odgovornosti, po katerem so za zagotavljanje bistvenih storitev in delovanje kritične infrastrukture neposredno odgovorni kritični subjekti, za krepitev odpornosti kritične infrastrukture pa vsi pristojni organi in organizacije;
3. načelo zaščite pred različnimi vrstami nevarnosti, ki zahteva, da pristojni organi in organizacije pri zagotavljanju bistvenih storitev in neprekinjenega delovanja kritične infrastrukture upoštevajo različne vrste naravnih in tehnoloških nevarnosti;
4. načelo neprekinjenega zagotavljanja odpornosti kritičnih subjektov in kritične infrastrukture, ki zahteva, da je načrtovanje ukrepov za odpornost kritičnih subjektov in kritične infrastrukture podprto z nenehnim ocenjevanjem tveganj za opravljanje bistvenih storitev, delovanje kritične infrastrukture in presoje ustreznosti ukrepov za njeno zaščito in odpornost;
5. načelo izmenjave podatkov in informacij ter varovanja podatkov, ki zahteva od pristojnih organov in organizacij redno, pravočasno ter na zaupanju temelječo izmenjavo podatkov in informacij ob hkratnem varovanju podatkov, povezanih s kritičnimi subjekti in njihovo kritično infrastrukturo, v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.

11. člen
(načrt za odpornost)

(1) Načrt za odpornost kritičnih subjektov (v nadaljnjem besedilu: načrt za odpornost) obsega oceno tveganja kritičnega subjekta in ukrepe za odpornost.

(2) Načrt za odpornost pripravijo in hranijo kritični subjekti.

(3) Kritični subjekti pripravljeni načrt za odpornost posredujejo nosilcu sektorja, ki načrt odobri oziroma predlaga njegovo dopolnitev.

(4) Kritični subjekt pristojnemu nosilcu sektorja oziroma ministrstvu na njegovo zahtevo pošlje načrt za odpornost.

12. člen
(ocena tveganja kritičnega subjekta)

(1) Kritični subjekti na podlagi nacionalne ocene tveganja in drugih ustreznih virov informacij ter strokovnih usmeritev, ki jih za posamezne sektorje kritične infrastrukture pripravijo nosilci sektorjev, pripravijo oceno tveganja, v kateri ocenijo bistvena tveganja, ki bi lahko povzročila motnje v opravljanju njihovih bistvenih storitev (v nadaljnjem besedilu: ocena tveganja kritičnega subjekta).

(2) V ocenah tveganja kritični subjekti upoštevajo naravna tveganja in tveganja, ki jih povzroči človek, ki bi lahko povzročila izredni dogodek, vključno s tistimi, ki imajo medsektorsko in čezmejno naravo, nesreče, naravne nesreče, izredne razmere v javnem zdravju, hibridne grožnje ter druge antagonistične grožnje, vključno s terorističnimi kaznivimi dejanji. V oceni tveganja kritični subjekti upoštevajo stopnjo odvisnosti drugih sektorjev od bistvene storitve, ki jo opravlja ta kritični subjekt in stopnjo odvisnosti tega kritičnega subjekta od bistvenih storitev, ki jih opravljajo kritični subjekti drugih sektorjev ter tudi v sosednjih državah članicah in tretjih državah.

(3) Za izdelavo ocene, lahko kritični subjekt uporabi druge ocene tveganja ali druge dokumente pomembne za izdelavo njegovo oceno tveganja. Pristojni nosilec sektorja to ugotovi ob odobritvi načrta za odpornost.

13. člen

(ukrepi za odpornost)

(1) Kritični subjekt na podlagi rezultatov in informacij iz nacionalne ocene tveganja in rezultatov svoje ocene tveganja sprejme ustrezne ter sorazmerne tehnične, varnostne in organizacijske ukrepe za odpornost, vključno z ukrepi, potrebnimi za:

1. preprečevanje nastanka izrednega dogodka;
2. zagotovitev ustrezne fizične zaščite svojih prostorov in kritične infrastrukture;
3. 3.neprekinjeno zagotovitev bistvene storitve in delovanja kritične infrastrukture ob upoštevanju medsebojne soodvisnosti sektorjev kritične infrastrukture;
4. zagotovitev redundance sistemov in omrežij za zagotavljanje bistvene storitve;
5. zagotovitev ustreznega upravljanja in nadzora primarnih dobavnih verig;
6. zagotovitev zadostnih zalog;
7. odzivanje na izredne dogodke, zoperstavljanje in blaženje njihovih posledic ob ustreznem izvajanju postopkov in protokolov za obvladovanje tveganj in kriz ter postopkov opozarjanja;
8. okrevanje po izrednih dogodkih;
9. zagotovitev ustreznega upravljanja varnosti zaposlenih;
10. ozaveščanje zaposlenih o ukrepih za odpornost.

(2) Kritični subjekti pri izbiri zaposlenih, ki opravljajo naloge na delovnih mestih, posebnega pomena za opravljanje bistvene storitve, upoštevajo tudi vloge kandidatov zunanjih ponudnikov teh storitev.

(3) Ukrepi za odpornost so stalni in dodatni. Stalni ukrepi za odpornost se izvajajo v vseh razmerah, ob povečani ogroženosti kritične infrastrukture ali izrednem dogodku pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi za odpornost se izvajajo ob povečani ogroženosti kritične infrastrukture ali izrednem dogodku, če stalni ukrepi za odpornost, tudi če se njihovo izvajanje stopnjuje, ne zadostujejo.

(4) Stalne ukrepe za odpornost na podlagi ocene tveganja načrtujejo in izvajajo kritični subjekti.

(5) Kritični subjekti dodatne ukrepe za odpornost načrtujejo na podlagi ocene tveganja ali sprejmejo na podlagi nastalih in pričakovanih posledic povečane ogroženosti kritične infrastrukture ali izrednega dogodka.

(6) Nosilci sektorjev lahko za zagotovitev delovanja kritične infrastrukture v obsegu, ki še omogoča opravljanje bistvene storitve, sprejmejo dodatne ukrepe za odpornost na ravni sektorja kritične infrastrukture iz svoje pristojnosti ali pripravijo predlog dodatnih ukrepov za odpornost, ki ga sprejme vlada.

(7) Če morajo dodatne ukrepe za odpornost izvesti kritični subjekti, lahko vlada odloči o dodelitvi sredstev za izvedbo teh ukrepov za odpornost.

(8) Za zagotovitev ukrepov za odpornost iz 2. točke prvega odstavka se kritični subjekti na predlog nosilcev sektorjev v skladu s predpisi, ki urejajo področje zasebnega varovanja, določijo za zavezance obveznega organiziranja varovanja, ki morajo varovati kritično infrastrukturo v skladu s temi predpisi.

(9) Kritični subjekt lahko sprejme ukrepe za odpornost na podlagi že pripravljenih načrtov ali dokumentov pomembnih za opredelitev teh ukrepov za odpornost. Pristojni nosilec sektorja to ugotovi ob odobritvi načrta za odpornost.

14. člen

(posodabljanje načrta za odpornost)

(1) Kritični subjekti morajo načrt za odpornost redno posodabljati, najmanj pa enkrat na dve leti.

(2) Ob nastanku novih okoliščin, ki lahko pomembno vplivajo na zagotavljanje bistvene storitve in delovanje kritične infrastrukture, kritični subjekt ustrezno spremeni načrt za odpornost spremeniti najpozneje v roku enega meseca. K tako spremenjenemu načrtu za odpornost je treba pridobiti odobritev pristojnega nosilca sektorja.

15. člen
(preverjanje preteklosti)

(1) Kritični subjekt ob upoštevanju nacionalne in svoje ocene tveganja lahko predloži zahtevek za preverjanje preteklosti zaposlenih in kandidatov za zaposlitev na delovnih mestih, ki so pomembna za opravljanje bistvenih storitev kritičnega subjekta in imajo ali bodo imeli pooblaščen neposredni ali oddaljeni dostop do prostorov, informacij ali nadzornih sistemov kritičnega subjekta.

(2) Preverjanje preteklosti osebe iz prejšnjega odstavka se po njenem predhodnem soglasju opravi z namenom, da se:
– potrdi identiteta osebe, katere preteklost se preverja;
– preverijo kazenske evidence Republike Slovenije, drugih držav članic in tretjih držav glede kaznivih dejanj, ki po oceni kritičnega subjekta sodijo v opis delovnega mesta, pomembnega za opravljanje bistvene storitve.

(3) Preverjanje preteklosti osebe iz prvega odstavka tega člena, ki je državljan Republike Slovenije ali državljan tuje države, po predložitvi zahtevka kritičnega subjekta in soglasja osebe iz prvega odstavka tega člena opravijo zaprošeni državni organi, ki pridobijo dokazila iz prejšnjega odstavka po uradni dolžnosti iz uradnih evidenc. Zahtevki iz prvega odstavka tega člena se obravnavajo takoj oziroma najkasneje v roku 15 dni in v skladu s predpisi, ki urejajo področje osebnih podatkov. Preverjanja preteklosti so sorazmerna in omejena na vrednotenje morebitnega tveganja za opravljanje bistvene storitve kritičnega subjekta.

15.a člen
(standardi)

Kritični subjekti lahko pri načrtovanju in sprejemanju ukrepov za odpornost uporabijo uveljavljene evropske in mednarodne standarde ter tehnične specifikacije veljavnih ukrepov za zagotavljanje varnosti in odpornosti kritičnih subjektov.

16. člen
(izvršba in stečaj kritičnega subjekta)

(1) Kritični subjekt o dejstvih in okoliščinah, ki kažejo na možnost njegovega prenehanja poslovanja ali stečaja, obvesti nosilca sektorja, ta pa NCKU in ministrstvo.

(2) Kritična infrastruktura kritičnega subjekta, ki je nujna za oziroma omogoča opravljanje bistvenih storitev kritičnega subjekta in njegove premoženjske pravice, ne more biti predmet izvršbe ali prodaje v stečajnem postopku ali postopku prisilne likvidacije v skladu z zakonom, ki ureja izvršbo, ter zakonom, ki ureja postopke zaradi insolventnosti in prisilnega prenehanja, razen če se z izvršbo ali prodajo v postopku stečaja ali prisilne likvidacije zagotavljata celovitost in nemoteno delovanje kritične infrastrukture za opravljanje bistvenih storitev v skladu s tem zakonom.

(3) Ne glede na predpise, ki urejajo poslovanje stečajnega dolžnika po začetku stečajnega postopka, se kritičnemu subjektu kot stečajnemu dolžniku dovoli nadaljevanje poslovanja v zadevah, ki so nujne za zagotavljanje bistvene storitve in neprekinjenega delovanja kritične infrastrukture. Stečajni upravitelj kritičnega subjekta poskrbi, da se naloge, nujne za nemoteno opravljanje bistvenih storitev in neprekinjenega delovanja kritične infrastrukture opravljajo v nezmanjšanem obsegu.«.

13. člen

Z 16. členom se doda novo, III.A poglavje, ki se glasi:

»III.A KRITIČNI SUBJEKTI POSEBNEGA EVROPSKEGA POMENA

16.a člen
(ugotavljanje in določitev kritičnih subjektov posebnega evropskega pomena)

(1) Kritični subjekt se šteje za kritični subjekt posebnega evropskega pomena, če:
– je določen kot kritični subjekt na podlagi drugega odstavka 9. člena zakona;
– opravlja enake ali podobne bistvene storitve šestim ali več državam članicam ali v šestih ali več državah članicah;
– je bil uradno obveščen na podlagi tretjega odstavka tega člena, da je določen kot kritični subjekt posebnega evropskega pomena.

(2) Kritični subjekt, ki opravlja bistvene storitve za šest ali več držav članic ali v šestih ali več državah članicah, o tem obvesti nosilca sektorja, ta pa ministrstvo. Ministrstvo brez odlašanja Evropski komisiji posreduje podatke kritičnega subjekta iz prvega odstavka tega člena.

(3) Evropska komisija na podlagi posvetovanj z ministrstvom, pristojnimi nacionalnimi organi držav članic, za katere ali v katerih kritični subjekt opravlja bistvene storitve, in kritičnim subjektom ugotovi, ali so storitve, ki jih kritični subjekt opravlja bistvene storitve tudi v teh državah članicah. Če ugotovi, da ta kritični subjekt opravlja bistvene storitve za šest ali več držav članic ali v šestih ali več državah članicah, ta kritični subjekt prek ministrstva uradno obvesti, da se šteje za kritični subjekt posebnega evropskega pomena, in o njegovih obveznostih iz tega poglavja ter o datumu, od katerega začnejo te obveznosti veljati.

16.b člen
(svetovalne misije)

(1) Ministrstvo lahko od Evropske komisije zahteva organiziranje svetovalne misije za oceno ukrepov za odpornost kritičnih subjektov posebnega evropskega pomena.

(2) Nosilec sektorja, odgovoren za delovno področje, na katerega spada kritični subjekt posebnega evropskega pomena, v sodelovanju s kritičnim subjektom posebnega evropskega pomena na obrazloženo pobudo Evropske komisije ali zahteve ene oziroma več držav članic, za katere se oziroma v katerih se opravlja bistvena storitev, Evropski komisiji zagotovi:

– oceno tveganja kritičnega subjekta;
– seznam ukrepov kritičnega subjekta;
– informacije o ukrepih kritičnega subjekta, vključno z ocenami skladnosti ali izdanimi odredbami, ki jih je glede tega kritičnega subjekta sprejel inšpektorat, pristojen za obrambo.

(3) Kritični subjekti posebnega evropskega pomena svetovalnim misijam omogočijo dostop do informacij, sistemov in objektov, povezanih z opravljanjem njihovih bistvenih storitev za izvajanje te svetovalne misije v skladu s predpisi, ki urejajo področje tajnih podatkov oziroma mednarodnimi sporazumi, ki jih je na področju izmenjave in varovanja tajnih podatkov z drugimi državami ali mednarodnimi organizacijami, sprejela Republika Slovenija.

(4) Ministrstvo zagotovi, da kritični subjekt posebnega evropskega pomena upošteva poročilo svetovalne misije in mnenje Evropske komisije o svojih ugotovitvah glede ustreznosti ukrepov za odpornost. «.

14. člen

17. člen se spremeni tako, da se glasi:

»17. člen
(vlada)

Vlada na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, določa politiko na tem področju in po potrebi od nosilcev sektorjev, kritičnih subjektov, ministrstva in inšpektorata, pristojnega za obrambo zahteva dodatna poročila o opravljanju nalog iz njihove pristojnosti, ki niso zajeta v V. poglavju tega zakona.«.

15. člen

18. člen se spremeni tako, da se glasi:

»18. člen

(nosilci sektorjev kritične infrastrukture)

(1) Nosilci sektorjev opravljajo na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, naslednje naloge:

1. oblikujejo pobudo in sodelujejo pri pripravi predloga kriterijev za ugotavljanje kritičnih subjektov ter njihovih mejnih vrednosti;
2. oblikujejo pobudo in sodelujejo pri pripravi predloga za določitev kritičnih subjektov in njihove kritične infrastrukture iz svoje pristojnosti;
3. usklajujejo predloge ukrepov za odpornost kritičnih subjektov v sektorju kritične infrastrukture iz svoje pristojnosti;
4. usmerjajo kritične subjekte pri njihovem načrtovanju ukrepov za odpornost;
5. po potrebi predlagajo spremembo predpisov s področja sektorja kritične infrastrukture iz svoje pristojnosti z vidika krepitve odpornosti kritičnih subjektov in zaščite kritične infrastrukture.

(2) Nosilci sektorjev določijo kontaktno osebo za sodelovanje na področju kritične infrastrukture s kritičnimi subjekti, drugimi nosilci sektorjev kritične infrastrukture in ministrstvom (v nadaljnjem besedilu: kontaktna oseba nosilca sektorja).«.

16. člen

19. člen se spremeni tako, da se glasi:

»19. člen

(kritični subjekti)

(1) Kritični subjekti zagotavljajo neprekinjeno opravljanje bistvenih storitev in delovanje kritične infrastrukture.

(2) Kritični subjekti imenujejo kontaktno osebo za sodelovanje na področju kritične infrastrukture z drugimi kritičnimi subjekti, nosilci sektorjev in ministrstvom (v nadaljnjem besedilu: kontaktna oseba kritičnega subjekta).«.

17. člen

20. člen se spremeni tako, da se glasi:

»20. člen

(ministrstvo)

(1) Ministrstvo strokovno usmerja in usklajuje dejavnosti na področju kritične infrastrukture.

(2) Ministrstvo opravlja na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, naslednji nalogi:
– pripravlja predloge za določitev kriterijev za ugotavljanja kritičnih subjektov in njihovih mejnih vrednosti, pri čemer obravnava pobude in predloge nosilcev sektorjev;
– pripravlja predloge za določitev kritičnih subjektov, pri čemer obravnava pobude in predloge pristojnih nosilcev sektorjev.«.

18. člen

Za 20. členom se doda nov, 20.a člen, ki se glasi:

»20.a člen
(koordinacijska skupina)

(1) Vlada imenuje koordinacijsko skupino, ki jo vodi ministrstvo, ki v ta namen vodi in posodablja seznam članov in nadomestnih članov in ji zagotavlja administrativno-tehnično podporo.

(2) Koordinacijsko skupino sestavljajo predstavniki nosilcev sektorjev in ministrstva, ministrstev, pristojnih za notranje zadeve ter zunanje in evropske zadeve, pristojnega nacionalnega organa po zakonu, ki ureja informacijsko varnost, ter Slovenske obveščevalno-varnostne agencije.

(3) Koordinacijsko skupino aktivira ministrstvo ob izrednih dogodkih iz 24.a člena tega zakona, kadar sta potrebna usklajen in učinkovit odziv na izredni dogodek.

(4) Koordinacijska skupina usklajuje upravljanje izrednega dogodka in ukrepe za ublažitev posledic izrednega dogodka ter zagotovitev čimprejšnjega ponovnega nemotenega delovanja kritične infrastrukture in opravljanje bistvenih storitev, ki jih predlagajo nosilci sektorjev, in jih predloži vladi.

(5) Ministrstvo skupino skliče najmanj enkrat na leto, po potrebi pa pogosteje in o tem poroča vladi.«.

19. člen

21. in 22. člen se črtata.

20. člen

V. poglavje se spremeni tako, da se glasi:

»V. ZGODNJE OPOZARJANJE, ZAGOTAVLJANJE PODPORE ODLOČANJU IN POROČANJE

23. člen
(zgodnje opozarjanje, zagotavljanje podpore odločanju in posredovanje podatkov)

(1) Zagotavljanje podpore odločanju temelji na načelu izmenjave podatkov in informacij ter varovanja podatkov iz 10. člena zakona, ki zahteva od pristojnih organov in kritičnih subjektov redno, pravočasno ter na zaupno izmenjavo podatkov in informacij ob hkratnem varovanju podatkov, povezanih s kritično infrastrukturo ter opravljanjem bistvenih storitev, v skladu s predpisi, ki urejajo področje tajnih podatkov ali poslovno skrivnost.

(2) Z namenom zgodnjega opozarjanja na področju kritične infrastrukture, nosilci sektorjev in kritični subjekti posredujejo NCKU podatke iz svoje pristojnosti, ki pristojnim organom in organizacijam omogočajo hiter in ustrezen odziv na izredni dogodek ter celovit pregled vpliva, narave, vzroka in morebitnih posledic izrednega dogodka, s katerimi se spoprijemajo kritični subjekti. Ta sistem omogoča zaznavanje in analizo razlik v vrednostih kazalnikov po posameznih sektorjih, preden te prerastejo v izredni dogodek ali motnje pri opravljanju bistvenih storitev.

(3) NCKU med spremljanjem in analiziranjem podatkov v okviru sistema zgodnjega opozarjanja in mehanizma priglasitev izrednih dogodkov iz 24.a člena zakona zbira, obdeluje, uporablja ter hrani digitalizirane, avtomatizirane, agregirane in anonimizirane podatke.

(4) NCKU o nepravilnostih in morebitnih grožnjah obvesti telesa kriznega upravljanja ter pristojne nosilce sektorjev, ti pa kritične subjekte, ki vrednotijo razlike in nepravilnosti ter na tej podlagi okrepijo ukrepe za odpornost oziroma jih stopnjujejo ali sprejmejo dodatne ukrepe za odpornost

(5) Ob zaznani povečani ogroženosti kritične infrastrukture pristojni državni organi na področju nacionalne varnosti o morebitni grožnji seznanijo NCKU, ministrstvo in nosilca sektorja, ta pa kritični subjekt.

24. člen
(poročanje)

(1) 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. Ta pripravi skupno letno poročilo o zagotavljanju neprekinjenega delovanja kritične infrastrukture in ga do konca marca za preteklo leto predloži vladi.

(2) V poročilih iz prejšnjega odstavka se navedejo izredni dogodki, ki so povzročili prekinitev zagotavljanja bistvene storitve z negativnimi materialnimi in drugimi posledicami za delovanje sektorja, glede tega izvedeni ukrepi ter rešitve in sprejeti ali predlagani ukrepi za izboljšanje odpornosti kritičnega subjekta in zaščite kritične infrastrukture. Predlogi ukrepov za izboljšanje stanja na področju kritične infrastrukture morajo biti finančno, materialno in kadrovsko utemeljeni.

24.a člen
(priglasitev izrednih dogodkov)

(1) Kritični subjekti pristojnemu nosilcu sektorja, NCKU in ministrstvu takoj priglasijo izredne dogodke, ki povzročijo ali bi lahko povzročili pomembno motnjo pri opravljanju bistvenih storitev, oziroma predložijo začetno priglasitev najpozneje v 24 urah po tem, ko se seznanijo z izrednim dogodkom, razen če so operativno nesposobni. Najpozneje v roku enega meseca ji sledi natančno poročilo o tem izrednem dogodku. Za določitev pomembnosti motnje se upoštevajo zlasti naslednji parametri:

– število in delež uporabnikov, prizadetih zaradi motnje;
– trajanje motnje;
– območje, prizadeto zaradi motnje, ob upoštevanju morebitne geografske izoliranosti območja.

(2) Priglasitev izrednega dogodka iz prejšnjega odstavka poteka po digitalni platformi, ki jo vzpostavi pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost. Do vzpostavitve navedene platforme se zagotovi varnost prenesenih podatkov preko zaščitenega komunikacijskega in informacijskega omrežja NCKU.

(3) Če izredni dogodek pomembno vpliva ali bi lahko pomembno vplival na neprekinjeno opravljanje bistvenih storitev v šestih ali več državah članicah, ministrstvo tak izredni dogodek priglasi Evropski komisiji.

(4) Priglasitve izrednih dogodkov iz prvega odstavka tega člena vsebujejo informacije, ki jih potrebujejo nosilec sektorja, ministrstvo in NCKU za razumevanje narave, vzroka in mogočih posledic izrednih dogodkov, vključno z navedbo ukrepov, ki jih je sprejel kritični subjekt ob zaznanem izrednem dogodku in informacijami za ugotovitev vsakega čezmejnega vpliva izrednega dogodka. Take priglasitve ne smejo povzročiti dodatnih odgovornosti za kritične subjekte.

(5) Ministrstvo na podlagi informacij, ki jih v priglasitvi iz prvega odstavka tega člena predloži kritični subjekt, obvesti enotno kontaktno točko drugih prizadetih držav članic, kadar izredni dogodek pomembno vpliva ali bi lahko pomembno vplival na kritične subjekte in neprekinjeno opravljanje bistvenih storitev za eno ali več drugih držav članic ali v eni ali več drugih državah članicah. Enotne kontaktne točke prizadetih držav informacije obravnavajo tako, da spoštujejo njihovo zaupnost ter varujejo varnost in poslovne interese tega kritičnega subjekta.

(6) Pristojni nosilec sektorja po prejemu priglasitve iz prvega odstavka tega člena temu kritičnemu subjektu, ministrstvu in NCKU brez odlašanja predloži ustrezne informacije o nadaljnjem ukrepanju, vključno z informacijami, ki bi lahko podprle učinkovit odziv tega kritičnega subjekta na izredni dogodek. Kadar je to v javnem interesu in glede na pomembnost motnje ter razsežnosti izrednega dogodka, o njem obvestijo javnost. Če pristojni nosilec sektorja skupaj s službo vlade, pristojno za komuniciranje z javnostjo in ministrstvom, pripravi sporočilo za javno objavo z navedbo pomembnih dejstev in izvedenih ukrepov, ga mediji smejo objaviti le v nespremenjeni obliki.

(7) Ministrstvo prvič do 17. julija 2028 in nato na vsaki dve leti Evropski komisiji predloži zbirno poročilo o prejetih priglasitvah izrednih dogodkov, vključno s številom priglasitev, naravo priglašenih izrednih dogodkov in ukrepi.

25. člen
(podatki o odgovornih osebah in kontaktnih osebah)

(1) Da se zagotovi podpora odločanju na področju kritične infrastrukture, se zbirajo, obdelujejo, uporabljajo in hranijo naslednji podatki o odgovorni in kontaktni osebi nosilca sektorja ter odgovorni osebi in kontaktni osebi kritičnega subjekta:

1. ime in priimek,
2. stalno ali začasno prebivališče,

3. številka telefona,
4. naziv delovnega mesta,
5. naslov elektronske pošte.

(2) Podatke o odgovornih osebah in kontaktnih osebah nosilcev sektorjev ter kritičnih subjektov zbira, obdeluje, uporablja in hrani NCKU.

(3) Nosilci sektorjev zbirajo, obdelujejo, uporabljajo in hranijo podatke o odgovornih osebah ter kontaktnih osebah kritičnih subjektov, ki delujejo v sektorju kritične infrastrukture iz njihove pristojnosti.«.

21. člen

Besedilo 26. člena se spremeni tako, da se glasi:

»Podatek, ki se nanaša na ugotavljanje, določanje in odpornost kritičnih subjektov ter kritične infrastrukture in je določen kot tajni podatek ali poslovna skrivnost, se obravnava v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.«.

22. člen

27. člen se črta.

23. člen

Za besedilom 28. člena, ki se označi kot prvi odstavek se dodata nova, drugi in tretji odstavek, ki se glasita:

»(2) Od subjektov, ki so kot bistveni določeni na podlagi zakona, ki ureja informacijsko varnost lahko inšpektorat, pristojen za obrambo, kadar oceni, da je to potrebno za opravljanje njihovih nalog iz tega zakona, zahteva, da predložijo informacije potrebne za oceno ali ukrepi, ki so jih subjekti sprejeli za zagotovitev svoje odpornosti izpolnjujejo zahteve iz 13. člena tega zakona in dokaze o učinkovitem izvajanju teh ukrepov. Kadar inšpektorat, pristojen za obrambo zahteva take informacije ali dokaze, navede namen te zahteve, opredeli, katere informacije zahteva, in določi razumen rok za izpolnitev zahteve.

(3) Inšpektorat, pristojen za obrambo lahko zahteva od inšpekcije pristojnega nacionalnega organa, na podlagi zakona, ki ureja informacijsko varnost, da izvaja svoja nadzorna in izvršilna pooblastila glede subjekta, identificiranega na podlagi zakona, ki ureja informacijsko varnost, in določenega za kritični subjekt na podlagi tega zakona, ter da mu v zvezi s tem posreduje informacije.«.

24. člen

29. člen se spremeni tako, da se glasi:

»29. člen
(prekrški)

(1) Z globo od 4.000 do 12.000 evrov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če ne izpolni obveznosti iz:
1. drugega in tretjega odstavka 11. člena tega zakona;

2. prvega ali drugega odstavka 12. člena tega zakona;
3. prvega, drugega ali osmega odstavka 13. člena tega zakona;
4. 14. člena tega zakona;
5. prvega odstavka 16. člena tega zakona;
6. drugega odstavka 18. člena tega zakona;
7. 19. člena tega zakona;
8. drugega odstavka 24. člena tega zakona;
9. 24.a člena tega zakona.

(2) Z globo od 600 do 1.200 evrov se kaznuje odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost, ali odgovorna oseba v državnem organu ali samoupravni lokalni skupnosti, če naredi prekršek iz prejšnjega odstavka.

(3) Z globo od 600 do 1.200 evrov se kaznuje posameznik, če naredi prekršek iz prvega odstavka tega člena.

(4) Ministrstvo o prekrških, ki se uporabljajo za kršitve ukrepov, sprejetih na podlagi tega zakona, uradno obvesti Evropsko komisijo do 17. oktobra 2024 in jo takoj obvesti tudi o vsakršni njihovi naknadni spremembi.«.

25. člen

30. člen se spremeni tako, da se glasi:

»30. člen

(višina globe v hitrem prekrškovnem postopku)

Za prekrške iz tega zakona se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.«.

PREHODNA IN KONČNI DOLOČBI

26. člen
(sprejem aktov in poročanje)

(1) Vlada do 17. januarja 2026 sprejme strategijo in nacionalno oceno tveganja.

(2) Vlada v šestih mesecih po uveljavitvi tega zakona določi bistvene storitve iz 3.b člena tega zakona, podsektorje sektorjev kritične infrastrukture, nosilce sektorjev kritične infrastrukture in sodelujoče organe iz 7. člena zakona, kategorije subjektov ter mejne vrednosti kriterijev za ugotavljanja kritičnih subjektov iz 8. člena tega zakona.

(3) Vlada do 17. julija 2026 določi kritične subjekte in njihove kritične infrastrukture iz 9. člena zakona.

(4) Ministrstvo v treh mesecih po uveljavitvi tega zakona Evropski komisiji sporoči, da je pristojni nacionalni organ in tudi enotna kontaktna točka, pri čemer navede kontaktne podatke in morebitne poznejše spremembe.

(5) Ministrstvo Evropski komisiji posreduje strategijo in nacionalno oceno tveganja v treh mesecih od njunega sprejema.

(6) Za kritične subjekte se spremenjeno III. poglavje zakona začne uporabljati deset mesecev po njihovi določitvi v skladu s spremenjenim 9. členom zakona.

27. člen
(prenehanje veljavnosti in podaljšanje uporabe)

(1) Za kritično infrastrukturo Republike Slovenije iz 3. točke 3. člena in pristojne organe in organizacije iz 12. točke 3. člena Zakona o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M) se uporablja Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M) in Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije (Uradni list RS, št. 7/19) do določitve kritičnih subjektov iz spremenjenega 9. člena zakona.

(2) Z dnem uveljavitve tega zakona prenehata veljati:
– Uredba o evropski kritični infrastrukturi (Uradni list RS, št. 35/11) in
– Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije (Uradni list RS, št. 7/19).

28. člen
(začetek veljavnosti)

Ta zakon začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

III. OBRAZLOŽITEV

K 1. členu

Predlog zakona povzema vsebino spremenjenega 1. člena ZKI tako, da navaja najpomembnejše sistemske elemente v zvezi s področjem kritične infrastrukture in kritično infrastrukturo Republike Slovenije in postopkom ugotavljanja in določanja kritičnih subjektov ter ugotavljanja kritičnih subjektov posebnega evropskega pomena, opredeljuje nacionalni okvir za odpornost kritičnih subjektov in ukrepe za zagotavljanje odpornosti kritičnih subjektov pri opravljanju bistvenih storitev. Določa tudi pristojnosti in naloge pristojnih organov in organizacij na področju kritične infrastrukture, pristojnega nacionalnega organa in enotne kontaktne točke (to je, skladno z opredelitvijo v 13. točki 3. člena oziroma v novem 9.a členu predloga zakona ministrstvo, pristojno za obrambo, v nadaljnjem besedilu: ministrstvo) ter okvir za zgodnje opozarjanje, zagotavljanje podpore odločanju, poročanje in nadzor na področju kritične infrastrukture.

K 2. členu

Predlog zakona v pravni red Republike Slovenije prenaša določbe Direktive 2022/2557, zato je potrebna sprememba 2. člena ZKI.

K 3. členu

Z novim 2.a členom predloga zakona se določa področje uporabe zakona. Iz navedenega člena predloga zakona je razvidno, da uporaba zakona ni enaka za vse subjekte. Za določene subjekte se bo uporabljal v celoti, za druge subjekte so določena poglavja izključena, medtem ko se za posamezne subjekte zakon sploh ne bo uporabljal.

V prvem odstavku 2.a člena predlog zakona kot zavezance naslavlja subjekte javne uprave in zasebne subjekte, ki so na podlagi tega zakona določeni kot kritični subjekti ali jih je kot kritične subjekte posebnega evropskega pomena določila Evropska komisija. Tovrstni subjekti bodo uporabljali zakon v celoti.

V drugem odstavku so navedeni subjekti, ki bodo na podlagi tega zakona sicer lahko določeni kot kritični subjekti po tem zakonu, vendar se zanje III. poglavje predloga (Odpornost kritičnih subjektov in kritične infrastrukture), III.A poglavje (Kritični subjekti posebnega evropskega pomena) in VII. Poglavje predloga zakona (Izvajanje nadzora) ne bodo uporabljala, kar tudi pomeni, da zanje obveznosti, ki izhajajo iz navedenih poglavij ne bodo veljala. Navedena določba sicer sledi določbi 8. člena Direktive 2022/2557 in je obrazložena z njeno uvodno izjavo 20, ki se glasi: »Glede na to, da so zahteve iz Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (v nadaljnjem besedilu: Direktiva 2022/2555), vsaj enakovredne ustreznim obveznostim iz te direktive, se obveznosti iz člena 11 ter poglavij III, IV in VI te direktive ne bi smele uporabljati za subjekte, ki spadajo v sektor digitalne infrastrukture, da bi se izognili podvajanju in nepotrebnemu upravnemu bremenu.«. Prav tako tudi uvodna izjava 21 Direktive 2022/2555, ki med drugim navaja: »Ta pravni okvir dopolnjuje Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta, ki določa zahteve, ki se uporabljajo za finančne subjekte glede obvladovanja tveganj na področju informacijskih in komunikacijskih tehnologij (IKT), vključno v zvezi z zaščito fizične infrastrukture IKT. Ker je torej odpornost teh subjektov celovito zajeta, se člen 11 ter poglavja III, IV in VI te direktive ne bi smeli uporabljati za te subjekte, ki spadajo v sektor digitalne infrastrukture, da bi se izognili podvajanju in nepotrebnemu upravnemu bremenu.«.

Tretji odstavek določa subjekte, za katere se ta zakon zaradi njihovega specifičnega pomena ne bo uporabljal. Med te subjekte sodijo subjekti javne uprave (subjekt javne uprave po Direktivi 2022/2557 pomeni javni sektor), ki izvajajo svoje dejavnosti na področju nacionalne varnosti, notranje varnosti, obrambe ali kazenskega pregona, vključno s preiskovanjem, odkrivanjem in pregonom kaznivih

dejanj, oziroma kritični subjekti, ki opravljajo storitve le na področju javne uprave iz tega člena in za sodstvo, Državni zbor Republike Slovenije ter Banko Slovenije, kot to določa peti odstavek 1. člena Direktive 2022/2557.

Zadnji odstavek 2.a člena sledi določbi drugega odstavka 1. člena Direktive 2022/2557, ki iz uporabe Direktive 2022/2557 izključuje vsebine, ki jih ureja Direktiva 2022/2555, in tudi njeni uvodni izjavi 9, ki pojasnjuje, da »Glede na večjo pogostost in posebne značilnosti kibernetskih tveganj Direktiva (EU) 2022/2555 nalaga celovite zahteve za velik sklop subjektov, da se zagotovi njihova kibernetska varnost. Glede na to, da je kibernetska varnost zadostno obravnavana v Direktivi (EU) 2022/2555, bi bilo treba zadeve, ki jih navedena direktiva zajema, izključiti iz uporabe te direktive, brez poseganja v posebno ureditev za subjekte v sektorju digitalne infrastrukture.«. Pomembno je omeniti še uvodno izjavo 20 Direktive (EU) 2022/2555, ki med drugim navaja: »Ker imajo grožnje za varnost omrežnih in informacijskih sistemov različen izvor, se v Direktivi (EU) 2022/2555 uporablja pristop, ki upošteva vse nevarnosti in vključuje odpornost omrežnih in informacijskih sistemov, pa tudi fizične komponente in okolje teh sistemov.«.

K 4. členu

S 4. členom predloga zakona se spreminja 3. člen ZKI, ki opredeljuje pojme. S spremembo člena se pojmi, določeni v 3. členu ZKI dopolnjujejo s pojmi, ki jih definira Direktiva 2022/2557, ki v ospredje pravnega okvira postavlja zagotavljanje bistvenih storitev na notranjem trgu Evropske unije in v ta namen oblikuje pojme, ki so v primerjavi z ZKI nekoliko drugače zastavljeni.

Večina pojmov iz 3. člena ZKI je ohranjenih in preoblikovanih v skladu s spremenjenim konceptom zaščite kritične infrastrukture in prehodom h krepitvi odpornosti kritičnih subjektov in kritične infrastrukture, ki omogoča zagotavljanje bistvenih storitev. Med slednje sodijo pojmi: izredni dogodek pri delovanju kritične infrastrukture, kritična infrastruktura Republike Slovenije, nosilci sektorjev kritične infrastrukture, ocena tveganj za delovanje kritične infrastrukture, področje kritične infrastrukture, povečana ogroženost kritične infrastrukture, pristojni organi in organizacije in sektorji kritične infrastrukture. V skladu z Direktivo 2022/2557, ki je osredotočena na kritične subjekte, je spremenjen pojem iz ZKI »upravljavci kritične infrastrukture«, ki je v noveli zakona pojasnjen pod izrazom »kritični subjekt«. Pojasnjen je pomen dodatnih izrazov kot so: »bistvena storitev« (storitev, ki je ključna za nemoteno delovanje države, ohranitev življenjsko pomembnih družbenih funkcij, gospodarskih dejavnosti, javnega zdravja in varnosti ali okolja), »odpornost kritičnega subjekta« (sposobnost kritičnega subjekta, da prepreči izredni dogodek, se pred njim zavaruje, se nanj odzove, se mu zoperstavi, ga ublaži in absorbira, se nanj prilagodi ter po njem okreva), »kibernetski incident« (dogodek kot ga določa zakon, ki ureja informacijsko varnost), »kategorije subjektov« (skupine subjektov, ki so povezane glede na vrsto in namen bistvene storitve, ki jo opravljajo in izmed katerih nosilci sektorjev ugotavljajo kritične subjekte) in »tveganje« (možnost izgube ali motnje pri opravljanju bistvenih storitev zaradi izrednega dogodka in je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi do izrednega dogodka prišlo). Z omenjenim dodatnim izrazom »kibernetski incident« je poudarjeno ločevanje oziroma razmejevanje med njim in izrazom izredni dogodek po predlogu zakona (nekibernetski incident, ki pomeni dogodek, ki bi lahko povzročil pomembne motnje ali ki povzroči motnje v opravljanju bistvene storitve, tudi kadar vpliva na sisteme, ki varujejo pravno državo).

V pojmih ZKI kot so »evropska kritična infrastruktura«, »kriza«, »načrtovanje zaščite kritične infrastrukture«, »prioriteta delovanja sektorjev kritične infrastrukture«, »ukrepi za zaščito kritične infrastrukture« in »zaščita kritične infrastrukture« v luči spremenjenega koncepta krepitve odpornosti kritičnih subjektov ni izkazan njihov vsebinski prispevek in jih predlog zakona ne vsebuje. Z navedenimi spremembami 3. člena ZKI se je tako terminološko in vsebinsko zadostilo zahtevi 2. člena Direktive 2022/2557, ki je posvečena opredelitvi pojmov.

K 5. členu

S 5. členom predloga zakona se dodaja novo I.A poglavje, ki vsebuje dva nova, 3.a in 3.b člen. Navedeno poglavje opredeljuje nacionalni okvir za odpornost kritičnih subjektov, s čimer se sledi določbam II. poglavja Direktive 2022/2557. Namen strategije je doseči in ohraniti visoko raven odpornosti kritičnih subjektov za vse sektorje kritične infrastrukture in tako zagotoviti nemoteno opravljanje bistvenih storitev. Predlog zakona z novim 3.a členom predstavi minimalna, temeljna izhodišča za izdelavo strategije, s čimer prispeva k njeni bolj jasni in določni izdelavi. Zaradi skladnosti in učinkovitosti je pri pripravi strategije med drugimi treba upoštevati sektorske politike in strategije, že izdelane načrte, že sprejete ukrepe in podobne dokumente ter tudi hibridno naravo groženj za kritične subjekte. V strategiji je treba opredeliti tudi sodelovanje in izmenjavo informacij med pristojnim nacionalnim organom na podlagi zakona, ki ureja informacijsko varnost in drugimi relevantnimi organi in organizacijami. Predlog strategije pripravi ministrstvo v sodelovanju z nosilci sektorjev kritične infrastrukture in ga posreduje vladi v sprejem.

Novo poglavje je 3.b člen posvetilo nacionalni oceni tveganja. Člen določa obveznost vladi izdelati seznam bistvenih storitev, ki predstavlja izhodišče za izdelavo nacionalne ocene in sprejeti nacionalno oceno, medtem ko je postopek izdelave nacionalne ocene tveganja zaupan ministrstvu, ki v ta namen sodeluje z nosilci sektorjev kritične infrastrukture. V skladu z uvodno izjavo 15 Direktive 2022/2557 je treba »pri zagotavljanju odpornosti kritičnih subjektov slediti pristopu, ki temelji na tveganju in je osredotočen na subjekte, ki so najpomembnejši za izvajanje ključnih družbenih funkcij ali gospodarskih dejavnosti.«. Predlog zakona v 3.b členu predstavi temeljna izhodišča za izdelavo nacionalne ocene tveganja z navedbo elementov, ki jih je treba upoštevati, s čimer se zagotovi ciljno usmerjen in usklajen pristop k njeni izdelavi. Pri izdelavi nacionalne ocene tveganja je treba upoštevati oceno relevantnih naravnih tveganj in tveganj, ki jih povzroči človek, vključno s tveganji medsektorske in čezmejne narave, ki bi lahko vplivala na opravljanje bistvenih storitev, vključno z nesrečami, naravnimi nesrečami, izrednimi razmerami v javnem zdravju, kot so pandemije, in hibridnimi grožnjami ali drugimi antagonističnimi grožnjami, vključno s terorističnimi kaznivimi dejanji, infiltracijo kriminala in sabotažo. Pri tem je treba upoštevati že obstoječe splošne ali sektorske ocene tveganja, izvedene na podlagi drugih pravnih aktov in tudi, v kolikšni meri so sektorji soodvisni, tudi tisti iz drugih držav članic in tretjih držav, in tudi informacije o preteklih priglašenih izrednih dogodkih.

Strategija in nacionalna ocena tveganja predstavljata podlago za ugotavljanje kritičnih subjektov in tudi podlago za izdelavo ocene tveganj kritičnih subjektov. Rok za sprejem obeh navedenih dokumentov je določen v 26. členu predloga zakona, tj. do 17. januarja 2026.

K 6. členu

S 6. členom predloga zakona se spreminja naslov II. poglavja ZKI, ki se po novem glasi »Ugotavljanje in določanje kritičnih subjektov ter kritične infrastrukture«. Z navedeno spremembo se poudari pomembnost kritičnih subjektov, njihovo ugotavljanje in določanje pa opredeljujeta 8. in 10. člen predloga zakona.

K 7. členu

Obseg sektorjev kritične infrastrukture, ki jih določa predlog zakona v spremenjenem 4. členu ZKI je v skladu s prilogo Direktive 2022/2557 razširjen. Poleg obstoječih osmih sektorjev z nekoliko spremenjenimi nazivi v skladu z določbami navedene direktive predlog zakona dodatno določa še tri nove, in sicer: sektor odpadne vode, sektor javne uprave in sektor vesolja. in nekoliko spreminja nazive obstoječih sektorjev. Nov naziv sektorja prehrane je sektor pridelave, predelave in distribucije živil; sektorja preskrbe s pitno vodo sektor pitne vode; sektorja informacijsko-komunikacijskih omrežij in sistemov sektor digitalne infrastrukture. Sektor financ je razdeljen na sektor bančništva in sektor infrastrukture finančnega trga. Direktiva 2022/2557 sektorja varovanja okolja v svojih določbah ne opredeljuje zato ga predlog zakona ne vsebuje. Sektorja energetike in prometa imata v skladu s prilogo Direktive 2022/2557 tudi podsektorje (sektor energetike tako obsega podsektorje: elektrika, daljinsko ogrevanje in hlajenje, nafta, plin in vodik; sektor prometa pa: zračni, železniški, vodni, cestni in javni prevoz), le-te določi vlada s predpisom. Sektorji imajo svojega nosilca in z njimi sodelujoče

organe. Tudi slednje določi vlada. Nosilci sektorjev kritične infrastrukture so odgovorni za delovna področja, na katera spada kritična infrastruktura, njihova vloga je usmerjati in podpirati kritični subjekt pri njihovem načrtovanju ukrepov za odpornost. Upoštevajoč koncept odpornosti kritičnih subjektov, s katerim se želi doseči visoka raven odpornosti kritičnih subjektov v vseh sektorjih, se je določanje prioritete delovanja sektorjev kritične infrastrukture izkazalo kot odvečno in jo predlog zakona ne vsebuje.

K 8. členu
S tem členom se določa kriterije za ugotavljanje kritičnih subjektov. V skladu s prvim odstavkom spremenjenega 5. člena ZKI bo kategorije subjektov, izmed katerih bodo nosilci sektorjev kritične infrastrukture ugotavljali kritične subjekte, znotraj vsakega sektorja in podsektorja kritične infrastrukture določila vlada s podzakonskim aktom.

Člen določa postopek ugotavljanja kritičnih subjektov. Ob upoštevanju strategije in rezultatov nacionalne ocene tveganja je prvi korak nosilcev sektorjev ugotavljanje subjektov, ki opravljajo eno ali več bistvenih storitev, ki jih bo določila vlada v podzakonskem predpisu. Nadalje sledi ugotavljanje ali subjektova kritična infrastruktura, ki se uporablja za opravljanje bistvene storitve oziroma omogoča njeno opravljanje, deluje oziroma se nahaja v Republiki Sloveniji, in ugotavljanje ali bi izredni dogodek, kot je opredeljen v 3. členu predloga zakona imel pomembne moteče učinke (posledice) na subjektovo zagotavljanje bistvene storitve ali drugih bistvenih storitev v drugih sektorjih kritične infrastrukture.

V tretjem odstavku spremenjenega 5. člena ZKI se določa kriterije, ki jih morajo nosilci sektorjev upoštevati pri določitvi pomembnega motečega učinka na subjektovo zagotavljanje bistvene storitve, pri čemer besedilo v celoti sledi določbam Direktive 2022/2557 in še zlasti njeni uvodni izjavi 18, ki se glasi: »Velike krize, kot je pandemija COVID-19, so pokazale, kako pomembno je zagotoviti varnost dobavne verige, pa tudi, kakšen negativen gospodarski in družbeni vpliv v velikem številu sektorjev in preko meja lahko imajo motnje v tej verigi. Zato bi morale države članice pri ugotavljanju v kolikšni meri so drugi sektorji in podsektorji odvisni od bistvene storitve, ki jo opravlja kritični subjekt, kolikor je mogoče upoštevati tudi vpliv na dobavno verigo.«.

Mejne vrednosti kriterijev, ki se bodo uporabljale za določitev enega ali več kriterijev za ugotavljanje kritičnih subjektov v posameznem sektorju kritične infrastrukture in njegovih podsektorjih bo določila vlada v podzakonskem predpisu.

K 9. členu
Glede na v Direktivi 2022/2557 določen koncept odpornosti kritičnih subjektov in pristop k ugotavljanju in določanju kritičnih subjektov člen narekuje črtanje 6., 7. in 8. člena ZKI. Določbe so se nanašale na sektorske oziroma medsektorske kriterije za ugotavljanje kritične infrastrukture ter mejne vrednosti kriterijev za ugotavljanje kritične infrastrukture.

K 10. členu
Člen določa postopek določitve kritičnih subjektov in spreminja 9. člen ZKI, ki je urejal določitev kritične infrastrukture. Predlog zakona sledi zahtevam Direktive 2022/2557, ki v ospredje postavlja bistvene storitve, v okviru postopka določitve kritičnih subjektov pa osnovo predstavlja seznam bistvenih storitev, temu sledi ugotavljanje in določitev kritičnih subjektov.

Prvi odstavek spremenjenega 9. člena nalaga obveznost ministrstvu, da na podlagi prejetih predlogov pristojnih nosilcev sektorjev kritične infrastrukture za določitev kritičnih subjektov pripravi seznam kritičnih subjektov in njihove kritične infrastrukture. Ti morajo izpolnjevati kriterije za ugotavljanje kritičnih subjektov in zadostiti minimalni mejni vrednosti vsaj enega kriterija za določitev pomembnega motečega učinka izrednega dogodka na opravljanje bistvene storitve, ki jo zagotavljajo ali na opravljanje odvisnih bistvenih storitev v drugih sektorjih kritične infrastrukture. Predlog za določitev

kritičnih subjektov in njihove kritične infrastrukture (tj. sredstvo, objekt, oprema, omrežje ali sistem oziroma njegov del, ki je nujen za oziroma omogoča opravljanje bistvene storitve) z utemeljitvijo se posreduje vladi.

Kritične subjekte in njihovo kritično infrastrukturo določi vlada s sklepom.

Člen določa naloge ministrstva po sprejemu sklepa vlade o določitvi kritičnih subjektov in kritične infrastrukture Republike Slovenije, od obveščanja kritičnih subjektov o njihovem statusu v posameznih sektorjih kritične infrastrukture in njihovih obveznostih ter pristojnih nosilcev sektorjev kritične infrastrukture, do posredovanja določenih dokumentov oziroma informacij Evropski komisiji ter roke za izvedbo teh nalog. Pri tem kritične subjekte, ki so določeni kot taki v sektorjih bančništva, infrastrukture finančnega trga in digitalne infrastrukture, obvesti o tem, da nimajo obveznosti iz poglavja o odpornosti kritičnih subjektov in kritične infrastrukture, in tudi da zanje ne velja poglavje o nadzoru. Kritični subjekti v navedenih treh sektorjih kritične infrastrukture so teh obveznosti razbremenjeni, saj zanje določbe tega zakona ne veljajo, kar je že bilo obrazloženo pri 2. členu predloga zakona.

K 11. členu

S členom se v okvir ZKI dodajata nova člena 9.a in 9.b. Novi 9.a člen v skladu z uvodno izjavo 23 in določbo drugega odstavka 9. člena Direktive 2022/2557 določa vzpostavitev, določitev ter delovanje enotne kontaktne točke, ki ima povezovalno vlogo in zagotavlja sodelovanje med pristojnimi organi in organizacijami ter čezmejno sodelovanje z enotnimi kontaktnimi točkami drugih držav članic ter z Evropsko komisijo ter sodelovanje s tretjimi državami. To je ministrstvo, ki je tudi pristojni nacionalni organ na področju kritične infrastrukture, kot je opredeljeno v 3. členu predloga zakona pod zaporedno številko 11. Besedilo člena sledi tudi uvodni izjavi 24 navedene direktive, ki se glasi: »Pristojni organi iz te direktive, in pristojni organi iz Direktive (EU) 2022/2555, bi morali sodelovati in si izmenjevati informacije, kar zadeva tveganja za kibernetsko varnost, kibernetske grožnje in incidente ter nekibernetska tveganja, grožnje in incidente, ki vplivajo na kritične subjekte, ter kar zadeva ustrezne ukrepe, ki jih sprejmejo pristojni organi iz te direktive in pristojni organi iz Direktive (EU) 2022/2555. Pomembno je, da države članice zagotovijo, da se zahteve iz te direktive in iz Direktive (EU) 2022/2555 izvajajo na dopolnjujoč način ter da za kritične subjekte ne nastaja upravno breme, ki bi preseglo, kar je potrebno za doseganje ciljev te in navedene direktive,« in tudi šestemu odstavku 9. člena Direktive 2022/2557 in tako opredeljuje sodelovanje in izmenjavo informacij s pristojnim nacionalnim organom na podlagi zakona, ki ureja informacijsko varnost.

S predlogom dodatnega, 9.b člena se sledi določbi 10. člena Direktive 2022/2557 o podpori držav članic kritičnim subjektom pri krepitvi njihove odpornosti. V ta namen je predvideno, da se organizira usposabljanje zaposlenega kadra v kritičnih subjektih, izvaja ter preverja njihovo pripravljenost in odpornost, si medsebojno izmenjuje informacije, izkušnje, dobre prakse itd.

Za namen izmenjave informacij in podatkov, določenih v skladu s predpisi, ki urejajo področje tajnih podatkov, osebnih podatkov in poslovno skrivnost se uporabi zaščiteno komunikacijsko in informacijsko omrežje NCKU, v katerega so sicer že vključeni vsi nosilci sektorjev kritične infrastrukture in upravljavci kritične infrastrukture, določeni na podlagi ZKI.

S členom se ministrstvu oziroma NCKU nalaga obveznost zagotavljanja podpore kritičnim subjektom, in sicer v vlogi nacionalnega odzivnega centra, ki ga predstavlja NCKU, ki s svojimi zaščitenim komunikacijskim in informacijskim omrežjem ter drugimi, v tretjem odstavku navedenimi zmožnostmi omogoča sprejemanje, spremljanje in obdelavo podatkov za vzpostavitev centralne slike delovanja kritične infrastrukture kritičnih subjektov, in sistema zgodnjega opozarjanja na področju kritične infrastrukture ter napovedi ali predvidevanja potencialnih izrednih dogodkov, in sicer na podlagi sporočil kritičnih subjektov.

Predlog zakona tudi določa, da medsebojna izmenjava informacij o izrednih dogodkih in kibernetskih grožnjah poteka z uporabo namenske digitalne platforme, ko jo v skladu z določbo šestega odstavka 13. člena Direktive 2022/2555 za ta namen vzpostavi pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost. S to rešitvijo se zasleduje racionalnost in nepotrebno podvajanje.

K 12. členu

S predlogom člena se spreminja celotno III. poglavje ZKI, ki je prilagojeno določbam Direktive 2022/2557 in že omenjenemu spremenjenemu konceptu zaščite kritične infrastrukture in osredotočenosti na odpornost kritičnih subjektov in njihove kritične infrastrukture.

Načela odpornosti kritičnih subjektov in kritične infrastrukture, opredeljena v spremenjenem 10. členu so zgolj terminološko prilagojena navedeni direktivi. Prav tako določba spremenjena 11. člena, ki kritičnim subjektom nalaga obveznost izdelave in hrambe načrta za odpornost, ki obsega oceno tveganja kritičnega subjekta in ukrepe za odpornost. K izdelanemu načrtu morajo pridobiti odobritev pristojnega nosilca sektorja kritične infrastrukture.

Spremenjeni 12. člen v celoti sledi določbi 12. člena Direktive 2022/2557 in opredeljuje glavne elemente ocene tveganja kritičnega subjekta za bistveno storitev, ki jo zagotavlja. Ocena tveganja je kot pisni rezultat celovitega postopka ugotavljanja narave in obsega tveganja, in sicer s prepoznavanjem in analiziranjem morebitnih pomembnih groženj, ranljivosti in nevarnosti, ki bi lahko privedle do izrednega dogodka, ter z vrednotenjem možnosti izgube ali motenj, ki jih ta izredni dogodek povzroči pri opravljanju bistvene storitve. Z določbo tretjega odstavka člen, v izogib nepotrebnemu obremenjevanju kritičnih subjektov le-tem daje možnost uporabiti že izdelane ocene tveganja ali druge dokumente na podlagi obveznostih iz drugih pravnih aktov, ki so relevantni za njegovo oceno tveganja za izpolnjevanje obveznostih po tem členu. To lahko ugotovi pristojni nosilec sektorja kritične infrastrukture ob odobritvi načrta za odpornost.

Spremenjeni 13. člen sledi določbam 13. člena Direktive 2022/2557. V prvem odstavku opredeljuje sklope ukrepov, ki jih morajo sprejeti kritični subjekti za zagotavljanje svoje odpornosti. Kritični subjekti bi morali sprejeti tehnične, varnostne in organizacijske ukrepe, ki so ustrezni in sorazmerni glede na tveganja, s katerimi se soočajo, da bi preprečili izredne dogodke, se zavarovali pred njimi, se odzvali nanje, se jim bili zmožni zoperstaviti, jih ublažili, jih absorbirali, se jim prilagodili in okrevali po njih. Podrobnosti, specifike in obseg takih ukrepov bi morali ustrezno in sorazmerno odražati različna tveganja, ki jih je vsak kritični subjekt prepoznal v okviru svoje ocene tveganja kritičnega subjekta, in posebnosti takega subjekta. V povezavi z zagotovitvijo ustreznega upravljanja varnosti zaposlenih predlog zakona kritične subjekte obvezuje, da pri izbiri zaposlenih, ki opravljajo naloge na delovnih mestih, posebnega pomena za opravljanje bistvene storitve, upoštevajo tudi vloge kandidatov zunanjih ponudnikov teh storitev. Ukrepi za odpornost se delijo na stalne in dodatne, pri čemer je predvideno, da se stalni ukrepi izvajajo v vseh razmerah, ob izrednem dogodku ali zaznani povečani ogroženosti kritične infrastrukture pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi se izvajajo ob izrednem dogodku ali povečani ogroženosti kritične infrastrukture, če stalni ukrepi, tudi če so stopnjevani, ne zadostujejo. Stalne ukrepe za odpornost načrtujejo in izvajajo (samo) kritični subjekti, dodatne ukrepe pa lahko poleg kritičnih subjektov sprejmejo še nosilci sektorjev kritične infrastrukture, če gre za ukrepe za odpornost na ravni sektorja kritične infrastrukture iz njihove pristojnosti, ali na predlog nosilcev sektorjev kritične infrastrukture za zagotovitev delovanja kritične infrastrukture v obsegu, ki še omogoča opravljanje bistvene storitve tudi vlada, če gre za ukrepe, ki presegajo pristojnost posameznega kritičnega subjekta (npr. okrepitev varovanja kritične infrastrukture, sprostitev blagovnih rezerv ali zaprosilo za mednarodno pomoč). Dodatni ukrepi, ki jih nosilci sektorjev kritične infrastrukture ali sprejmejo sami ali predlagajo v sprejetje vladi, zakonsko niso obvezni, saj jih nosilci lahko sprejmejo ali predlagajo le, če to ocenijo za potrebno. Če morajo tovrstne dodatne ukrepe za odpornost izvesti kritični subjekti, lahko vlada odloči, da se sredstva za izvedbo teh ukrepov zagotovijo iz državnega proračuna. Za zagotovitev ustrezne fizične zaščite svojih prostorov in kritične infrastrukture (pri čemer se upošteva na primer tudi postavitev ograje, izgradnja

pregrad, orodja in postopki za nadziranje zavarovanega območja, oprema za odkrivanje in nadzor dostopa itd.) predlog zakona z navezavo na predpise, ki urejajo zasebno varovanje, nosilcem sektorja kritične infrastrukture nalaga, naj poskrbijo, da so kritični subjekti določeni za zavezance obveznega organiziranja varovanja, ki morajo zagotavljati varovanje prostorov in kritične infrastrukture v skladu s predpisi s področja zasebnega varovanja. Določba devetega odstavka enako kot v primeru ocene tveganj kritičnim subjektom tudi za ukrepe za odpornost daje podlago za uporabo že sprejetih ukrepov na podlagi obveznosti iz drugih aktov kot enakovrednih ukrepom iz tega člena, kar lahko ugotovijo nosilci sektorjev kritične infrastrukture ob podaji odobritve k načrtu za odpornost.

Spremenjeni 14. člen določa obveznost kritičnega subjekta, da svoj načrt za odpornost posodobi najmanj enkrat na dve leti.

Spremenjeni 15. člen prenaša v slovensko zakonodajo določbo 14. člena Direktive 2022/2557, ki je obrazložen z njeno uvodno izjavo 32, ki se glasi: »Tveganje, da bi zaposleni v kritičnih subjektih ali njihovi zunanji izvajalci zlorabljali na primer svoje pravice do dostopa v organizaciji kritičnega subjekta za ogrožanje in povzročanje škode, je čedalje bolj zaskrbljujoče. Države članice bi zato morale podrobneje določiti pogoje, pod katerimi se kritičnim subjektom v ustrezno utemeljenih primerih in ob upoštevanju ocen tveganja držav članic dovoli, da predložijo zahtevke za preverjanje preteklosti oseb, ki spadajo v posebne kategorije njihovega osebja. Zagotoviti bi bilo treba, da ustrezni organi zahtevke v razumnem roku ocenijo in jih obravnavajo v skladu z nacionalnim pravom in postopki ter ustreznim in veljavnim pravom Unije, vključno v zvezi z varstvom osebnih podatkov. Za potrditev identitete osebe, katere preteklost se preverja, je ustrezno, da države članice zahtevajo dokazilo o identiteti, na primer potni list, nacionalno osebno izkaznico ali digitalno obliko identifikacije, v skladu z veljavnim pravom. Preverjanje preteklosti bi moralo vključevati preverjanje kazenske evidence zadevne osebe. Države članice bi morale za namen pridobitve informacije iz kazenskih evidenc drugih držav članic uporabiti evropski informacijski sistem kazenskih evidenc v skladu s postopki iz Okvirnega sklepa Sveta 2009/315/PNZ[1] in, kadar je ustrezno in potrebno, Uredbe (EU) 2019/816 Evropskega parlamenta in Sveta[2]. Države članice bi se lahko, kadar je relevantno in ustrezno, oprle tudi na Schengenski informacijski sistem druge generacije (SIS II), vzpostavljen z Uredbo (EU) 2018/1862 Evropskega parlamenta in Sveta[3], na obveščevalne podatke in vse druge razpoložljive objektivne informacije, ki so lahko potrebne za ugotavljanje ustreznosti zadevne osebe za delo na položaju, glede katerega je kritični subjekt zahteval preverjanje preteklosti«. Člen predstavlja pravno podlago kritičnim subjektom, da ob upoštevanju nacionalne ocene tveganja za opravljanje bistvenih storitev in na podlagi svoje lastne ocene tveganja, v svojih aktih opredelijo delovna mesta, ki so pomembna za opravljanje bistvene storitve in na katerih imajo ali bodo imeli zaposleni pooblaščen neposredni ali oddaljeni dostop do prostorov, informacij ali nadzornih sistemov kritičnega subjekta, in določi, da se za zaposlene, ki zasedajo ali bodo zasedli ta delovna mesta preveri njihovo preteklost.

Ne gre za obveznost pač pa za možnost, po predhodni utemeljitvi potrebe po preverjanju preteklosti zaposlenih. Če pa iz ocene tveganja kritičnega subjekta izhaja potreba po preverjanju preteklosti vseh zaposlenih, mora kritični subjekt v izogib morebitnemu diskriminatornemu ravnanju kritičnega subjekta to v svojih aktih tudi ustrezno opredeliti.

---

[1] Okvirni sklep Sveta 2009/315/PNZ z dne 26. februarja 2009 o organizaciji in vsebini izmenjave informacij iz kazenske evidence med državami članicami (UL L 93, 7.4.2009, str. 23).

[2] Uredba (EU) 2019/816 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o vzpostavitvi centraliziranega sistema za določitev držav članic, ki imajo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva (sistem ECRIS-TCN), z namenom dopolnitve evropskega informacijskega sistema kazenskih evidenc ter o spremembi Uredbe (EU) 2018/1726 (UL L 135, 22.5.2019, str. 1).

[3] Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56).

Kritični subjekt zahtevek za preverjanje skupaj s soglasjem preverjane osebe naslovi na pristojne državne organe. Preverjanje preteklosti zaposlenih se lahko opravi zgolj s predhodnim pisnim soglasjem vsake posamezne preverjane osebe. Z njenim soglasjem se preverjanje preteklosti opravi z namenom, da se potrdi identiteta osebe, katere preteklost se preverja in preverijo kazenske evidence navedene osebe glede kaznivih dejanj, ki jih kritični subjekt opredeli kot bistvena za določeno delovno mesto. Za potrditev identitete osebe, katere preteklost se preverja, se lahko zahteva dokazilo o identiteti, kot je potni list, osebna izkaznica ali digitalna oblika identifikacije. Navedeno izhaja tudi iz predhodno citirane uvodne izjave 32 Direktive 2022/2557. Določba tretjega odstavka narekuje tudi obravnavo zahtevkov za preverjanje preteklosti v skladu s predpisi, ki urejajo osebne podatke in zapoveduje sorazmernost preverjanja. Z določbo se zapoveduje, da morajo biti preverjanja preteklosti sorazmerna in strogo omejena na to, kar je potrebno ter opravljena le za vrednotenje morebitnega varnostnega tveganja za konkretni kritični subjekt. Prejete zahtevke za preverjanje preteklosti se obravnava takoj oziroma najkasneje v roku 15 dni, kar je skladno s četrtim odstavkom 139. člena Zakona o splošnem upravnem postopku (Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10, 82/13, 175/20-ZIUOPDVE in 3/22-ZDeb).

S predlogom člena je dodan nov 15.a. člen, s katerim se sledi določbi 16. člena Direktive 2022/2557 o uporabi evropskih in mednarodnih standardov ter tehničnih specifikacij veljavnih ukrepov za varnost in odpornost kritičnih subjektov. Po navedeni direktivi standard pomeni standard, ki je opredeljen v prvi točki 2. člena Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L št. 316 z dne 14. 11. 2012, str. 12). Tehnična specifikacija pa pomeni tehnično specifikacijo, kot je opredeljena v 4. točki 2. člena Uredbe (EU) št. 1025/2012.

Spremenjeni 16. člen predloga zakona ureja določena vprašanja, povezana z izvršbo in stečajem kritičnih subjektov. Kritičnim subjektom nalaga obveznost, da pristojnega nosilca sektorja kritične infrastrukture, ta pa NCKU in ministrstvo, obvestijo o dejstvih in okoliščinah, ki nakazujejo možnost njihovega prenehanja poslovanja ali stečaja. Po prvem stavku prvega odstavka 5. člena Ustave Republike Slovenije mora Republika Slovenija zagotavljati človekove pravice in temeljne svoboščine na svojem ozemlju. Po prvem odstavku 67. člena Ustave Republike Slovenije je lastninska pravica na primer omejena z njeno družbeno ali ekološko vlogo. Javni interes glede zagotavljanja bistvenih storitev, ki je sočasno tudi splošni interes, zahteva posebno ureditev glede stečajev in izvršb kritičnih subjektov, tako da so bistvene storitve zagotovljene v splošnem interesu. Z vidika načela sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) je v tem členu predlagana ureditev primerna in nujna (test sorazmernosti), saj če ne obstajajo ukrepi za odpornost kritičnih subjektov in zaščito kritične infrastrukture, ki omogoča opravljanje bistvenih storitev, tudi na področju civilnega in gospodarskega prava, prenehajo delovati sistemi, ki sploh omogočajo izvajanje človekovih pravic in temeljnih svoboščin. To pa glede na določbe 15. in 5. člena Ustave Republike Slovenije ni dopustno – torej, da se ne bi izvajale ali uresničevale in varovale človekove pravice in temeljne svoboščine.

K 13. členu

S tem členom se v ZKI, v skladu z določili Direktive 2022/2557, dodaja novo III.A poglavje z naslovom »Kritični subjekti posebnega evropskega pomena«, ki obsega dva člena, 16.a. in 16.b.

16.a člen ureja postopek ugotavljanja in določanja kritičnih subjektov posebnega evropskega pomena
Kritični subjekt, ki je kot tak določen na podlagi drugega odstavka 9. člena tega zakona lahko dobi dodatno še status »kritičnega subjekta posebnega evropskega pomena«, če opravlja enake ali podobne bistvene storitve šestim ali več državam članicam ali v šestih ali več državah članicah in je

bil na podlagi tretjega odstavka tega člena uradno obveščen, da je določen kot kritični subjekt posebnega evropskega pomena.

Drugi odstavek kritičnemu subjektu nalaga obveznost, da, če opravlja bistvene storitve za šest ali več držav članic ali v šestih ali več državah članicah, o tem obvesti nosilca sektorja, ta pa ministrstvo. Ministrstvo posreduje podatke kritičnega subjekta Evropski komisiji, ki opravi posvetovanja z vsemi relevantnimi organi in v primeru, da ugotovi, da kritični subjekt dejansko izpolnjuje kriterije, navedene v prvem odstavku tega člena konkretni kritični subjekt preko ministrstva uradno obvesti o tem, da se šteje za kritični subjekt posebnega evropskega pomena in o njegovih obveznostih.

16.b člen ureja organizacijo in izvedbo svetovalnih misij Evropske komisije, ki se izvedejo z namenom, da se oceni sprejete ukrepe za odpornost kritičnega subjekta posebnega evropskega pomena, s čimer se sledi določbi 18. člena Direktive 2022/2557. Gre za kritične subjekte, ki so še posebej pomembni za Evropsko unijo in njen notranji trg zato je pomembno, da se jim svetuje pri izpolnjevanju njihovih obveznosti po tem zakonu in se oceni ali dejansko izpolnjujejo obveznosti, ki se nanaša od njihovo odpornost in zaščito njihove kritične infrastrukture. Člen opredeljuje možnost, da ministrstvo od Evropske komisije zahteva izvedbo svetovalne misije, nalaga obveznost nosilcu sektorja kritične infrastrukture, da Evropski komisiji zagotovi vse relevantne dokumente in podatke (oceno tveganja, seznam ukrepov, informacije o ukrepih in tudi o ugotovitvah o izvedenem nadzoru nad izvajanjem določb tega zakona), pri čemer se upošteva predpise, ki urejajo področje tajnih podatkov in nalaga obveznost ministrstvu, da zagotovi, da kritični subjekt posebnega evropskega pomena upošteva poročilo svetovalne misije in mnenje Evropske komisije glede ustreznosti ukrepov za odpornost.

K 14. členu
Člen zgolj terminološko in ne tudi vsebinsko spreminja določbo 17. člena ZKI v skladu z Direktivo 2022/2557. Člen določa, da vlada kot najvišji organ državne uprave poleg nalog, ki jih ima po drugih členih tega zakona, skrbi za določanje, usmerjanje in usklajevanje politike na področju kritične infrastrukture, poleg tega pa lahko po potrebi zahteva, da ji nosilci sektorjev kritične infrastrukture, kritični subjekti, ministrstvo, in inšpektorat, pristojen za obrambo, predložijo poročilo o izvajanju nalog, za katere so sicer pristojni, vendar niso zajete v V. poglavju predloga zakona, ki ureja zgodnje opozarjanje, zagotavljanje podpore odločanju in poročanje.

K 15. členu
Člen zgolj terminološko, ne pa tudi vsebinsko spreminja določbo 18. člena ZKI v skladu z Direktivo 2022/2557. Določa tiste naloge nosilcev sektorjev kritične infrastrukture na področju kritične infrastrukture, ki niso navedene v drugih členih tega zakona, od oblikovanja pobude in sodelovanja pri pripravi predloga kriterijev za ugotavljanje kritičnih subjektov in njihovih mejnih vrednosti ter za določitev kritičnih subjektov in njihove kritične infrastrukture, usklajevanja predlogov za odpornost kritičnih subjektov v sektorju, usmerjanja kritičnih subjektov pri njihovem načrtovanju ukrepov za odpornost, do predlaganja sprememb predpisov s področja sektorja kritične infrastrukture iz njihove pristojnosti z vidika krepitve odpornosti in zaščite kritične infrastrukture. Nosilec sektorja kritične infrastrukture mora tudi določiti najmanj eno kontaktno osebo za njegovo sodelovanje na področju kritične infrastrukture s kritičnimi subjekti, drugimi nosilci sektorjev kritične infrastrukture in ministrstvom.

K 16. členu
Člen prilagojeno pojmom, opredeljenim v Direktivi 2022/2557 spreminja 19. člen ZKI, ki pa se sicer po vsebini ne spreminja. Določa, da je glavna naloga kritičnih subjektov na področju kritične infrastrukture zagotavljati neprekinjeno opravljanje bistvenih storitev in delovanje kritične infrastrukture. Kar pomeni njeno delovanje v vseh razmerah, pri čemer so seveda izključene okoliščine, na nastanek katerih subjekt kritične infrastrukture ne more vplivati in se nanje pripraviti. Izhajajoč tudi iz načela odgovornosti, določenega v 10. členu predloga zakona, po katerem so za zagotavljanje bistvenih storitev in delovanje kritične infrastrukture neposredno odgovorni kritični

subjekti, so ti dolžni zagotavljati ustrezne materialne (finančna in materialna sredstva) in tudi organizacijske pogoje (npr. usposabljanje vodstvenega kadra in drugih zaposlenih) za neprekinjeno zagotavljanje bistvene storitve in delovanje kritične infrastrukture. Tudi kritični subjekt mora določiti kontaktno osebo za njegovo sodelovanje na področju kritične infrastrukture predvsem s pristojnim nosilcem sektorja kritične infrastrukture, drugimi kritičnimi subjekti in drugimi nosilci sektorjev kritične infrastrukture ter z ministrstvom.

K 17. členu

S členom se terminološko prilagaja 20. člen ZKI v skladu z Direktivo 2022/2557. Določa, da strokovno usmerjanje in usklajevanje dejavnosti na področju kritične infrastrukture izvaja ministrstvo, ki je s predlogom zakona določeno tudi za pristojni nacionalni organ na področju kritične infrastrukture (13. točka 3. člena) in enotno kontaktno točka (9.a člen). Kot tako je pristojno za strokovno usmerjanje dejavnosti vseh déležnikov na področju kritične infrastrukture, poleg tega pa pripravljavec in končni nosilec vseh predlogov, povezanih z ugotavljanjem in določanjem kritičnih subjektov in njihove kritične infrastrukture, ki bodo predloženi v obravnavo vladi.

K 18. členu

S členom se v okvir ZKI dodaja nov 20.a, ki narekuje ustanovitev in delovanje koordinacijske skupine. Imenuje jo vlada, sestavljena iz predstavnikov nosilcev sektorjev in ministrstev pristojnih za obrambo, notranjih zadev, zunanjih in evropskih zadev, ter Slovenske obveščevalno-varnostne agencije. Vodi jo ministrstvo, ki tudi vodi in posodablja seznam članov in nadomestnih članov in skupini zagotavlja administrativno-tehnično podporo. Predvideno je, da se skupino aktivira ob izrednih dogodkih z namenom usklajevanja upravljanja izrednega dogodka, čimprejšnjega in učinkovitega odziva nanj, ukrepov nosilcev sektorjev kritične infrastrukture za ublažitev posledic ter zagotovitev čimprejšnjega ponovnega nemotenega delovanja kritične infrastrukture in opravljanje bistvenih storitev. Skupina se sicer sestane najmanj enkrat na leto oziroma po potrebi in o tem poroča vladi.

K 19. členu

Člen določa črtanje 21. in 22. člena ZKI. 21. člen določa vlogo NCKU v primeru krize, ki bi nastala zaradi prekinitve delovanja kritične infrastrukture, torej ob krizi, kot je opredeljena v ZKI. Ker je pojem »kriza« po predlogu 4. člena tega zakona črtan in so tudi vloga in naloge NCKU, ki je eno izmed teles kriznega upravljanja opredeljene v Uredbi o kriznem upravljanju in vodenju ter Nacionalnem centru krizno upravljanje (Uradni list RS, št. 28/18, nadaljnjem besedilu: Uredba), je smiselno njegovo črtanje.

22. člena ZKI ureja položaj Banke Slovenije na področju kritične infrastrukture. Ker je Banka Slovenije na podlagi tretjega odstavka novega 2.a člena predloga zakona izključena iz uporabe tega zakona (obrazložitev je podana v okviru obrazložitve k 3. členu tega zakona), posebna ureditev njenega položaja na področju kritične infrastrukture zaradi njene neodvisnosti ni potrebna in smiselna.

K 20. členu

S členom predloga zakona se vsebinsko spreminja in dopolnjuje celotno V. poglavje ZKI. Spremenjeni 23. člen ZKI podrobneje določa izmenjavo podatkov in informacij v skladu s 5. načelom odpornosti kritičnih subjektov in kritične infrastrukture iz 10. člena predloga zakona. Izmenjava podatkov je ključna za delovanje NCKU, ki je skladno z 9. členom Uredbe, osrednji informacijsko operativni center kriznega upravljanja, ki izvaja naloge spremljanja in obveščanja v podporo odločanju tudi po tem zakonu. Člen se povezuje z novim 24.a člen, s katerim se vzpostavlja mehanizem priglasitve izrednih dogodkov in obveznost kritičnih subjektov priglasitve in poročanja o izrednih dogodkov, pri čemer se pričakuje, da kritični subjekti brez odlašanja posredujejo vse razpoložljive informacije, ki jih pristojni organi in organizacije potrebujejo za odločanje. Zaradi navedenega je smiselno in potrebno vzpostaviti sistem zgodnjega opozarjanja na področju kritične infrastrukture, za delovanje katerega nosilci sektorjev kritične infrastrukture in kritični subjekti NCKU posredujejo podatke iz svoje pristojnosti. To pristojnim organom in organizacijam omogoča hiter in ustrezen odziv na izredne

dogodke ter celovit pregled vpliva, narave, vzroka in morebitnih posledic izrednih dogodkov, s katerimi se spoprijemajo kritični subjekti. NCKU skladno s 4. odstavkom 8. člena Uredbe izvaja naloge spremljanja in obveščanja v podporo odločanju in deluje neprekinjeno. Prav tako NCKU zagotavlja varne informacijske in komunikacijske povezave za izmenjavo podatkov med vsemi subjekti, ki so že vključeni v komunikacijsko informacijski sistem NCKU, med njimi so tudi nosilci sektorjev kritične infrastrukture in vsi upravljavci kritične infrastrukture, določeni na podlagi ZKI. Z namenom, da pri tem ne bi prihajalo do dodatnih odgovornosti in obremenitev za kritične subjekte, mora ta izmenjava podatkov potekati digitalizirano in čim bolj avtomatizirano. Z vidika varovanja osebnih in podatkov, povezanih s kritično infrastrukturo ter opravljanjem bistvenih storitev je pomembno, da so podatki agregirani in anonimizirani. Posredovanje podatkov NCKU po zaščitenem komunikacijskem in informacijskem sistemu NCKU je opredeljeno tudi v 4. odstavku 3. člena Uredbe. Namen vzpostavitve sistema zgodnjega opozarjanja je zaznavanje in analiza razlik v vrednostih kazalnikov po posameznih sektorjih, preden te prerastejo v izredne dogodke ali motnje pri opravljanju bistvenih storitev. Ta člen tudi nalaga, da pristojni državni organi in službe (tj. Slovenska obveščevalno-varnostna agencija, policija in Obveščevalno-varnostna služba Ministrstva za obrambo), če zaznajo povečano ogroženost kritične infrastrukture, s tem seznanijo NCKU, ministrstvo in nosilca sektorja kritične infrastrukture, ta pa nato seznani kritični subjekt. S tem določilom se želi h krepitvi odpornosti kritičnega subjekta in k zaščiti njegove kritične infrastrukture vsaj posredno dejavneje pritegniti tudi nosilce obveščevalno-varnostne dejavnosti v naši državi.

24. člen nalaga kritičnim subjektom in nosilcem sektorjev kritične infrastrukture, seveda vsakemu za njegovo raven, pripravo letnega poročila o zagotavljanju neprekinjenega delovanja kritične infrastrukture in opravljanju bistvenih storitev, od ministrstva, pa zahteva, da na podlagi sektorskih poročil pripravi skupno poročilo o zagotavljanju neprekinjenega delovanja vse kritične infrastrukture in to skupno poročilo za preteklo leto najpozneje do konca marca predloži v obravnavo vladi. Člen določa tudi tri obvezne vsebine vsakega letnega poročila, in sicer: navedbo izrednih dogodkov, ki so povzročili prekinitev zagotavljanja bistvene storitve z negativnimi materialnimi in drugimi posledicami za delovanje sektorja (gre za izredne dogodke, ki jih mora kritični subjekt v skladu s prvim odstavkom novega 24.a člena priglasiti takoj, ko je mogoče, obvestiti nosilca sektorja kritične infrastrukture, NCKU in ministrstvo), navedbo izvedenih ukrepov ter rešitev in navedbo sprejetih ali predlaganih ukrepov za izboljšanje odpornosti kritičnega subjekta in zaščite kritične infrastrukture. Slednji morajo biti tudi finančno, materialno in kadrovsko utemeljeni.

Novi 24.a člen nalaga kritičnim subjektom obveznost priglasitve izrednih dogodkov in v celoti sledi določbi 15. člena Direktive 2022/2557 in njeni uvodni izjavi 33, ki se glasi: »Vzpostaviti bi bilo treba mehanizem za priglasitev določenih incidentov, da bi se pristojnim organom omogočil hiter in ustrezen odziv na incidente ter celovit pregled vpliva, narave, vzroka in morebitnih posledic incidentov, s katerim se spopadajo kritični subjekti. Kritični subjekti bi morali brez nepotrebnega odlašanja pristojnim organom priglasiti incidente, ki povzročijo ali bi lahko povzročili pomembne motnje v opravljanju bistvenih storitev. Kritični subjekti bi morali začetno priglasitev predložiti najpozneje 24 ur po seznanitvi z incidenti, razen če to operativno ni mogoče. Začetna priglasitev bi morala vključevati le informacije, ki so nujno potrebne za seznanitev pristojnega organa z incidenti in ki kritičnemu subjektu omogočajo, da po potrebi zaprosi za pomoč. V taki priglasitvi bi bilo treba, kadar je mogoče, navesti domnevni vzrok incidenta. Države članice bi morale zagotoviti, da se z zahtevo po predložitvi začetne priglasitve sredstva kritičnega subjekta ne preusmerijo z dejavnosti, povezanih z obvladovanjem incidenta, ki bi moralo biti prednostna naloga. Začetni priglasitvi bi moralo, kadar je ustrezno, slediti podrobno poročilo, in sicer najpozneje en mesec po incidentu. Podrobno poročilo bi moralo dopolnjevati začetno priglasitev in zagotoviti celovitejši pregled incidenta.« Uvodna izjava 24 Direktiva 2022/2557e nadalje napotuje, da se zahteve iz Direktive 2022/2557 in zahteve iz Direktive (EU) 2022/2555 izvajajo na dopolnjujoč način ter, da za kritične subjekte ne nastaja upravno breme. Direktivi se v slovenski pravni red prenašata istočasno, 2. člen Direktive 2022/2555 pa določa, da se direktiva uporablja tudi za subjekte, ki bodo na podlagi tega zakona določeni kot kritični. 13. člen Direktive 2022/2555 govori o sodelovanju na nacionalni ravni in obveznosti medsebojne izmenjave

informacij o izrednih dogodkih, kibernetskih grožnjah in skorajšnjih izrednih dogodkih. Za ta namen pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost vzpostavi digitalno platformo. Zaradi povezav med obema navedenima direktivama, predvsem pa v izogib podvajanju člen določa uporabo digitalne platforme tudi za potrebe tega zakona.

Člen opredeljuje parametre, ki jih morajo kritični subjekti upoštevati pri opredelitvi pomembnosti motnje pri opravljanju bistvene storitve in določa obvezno vsebino vsake začetne priglasitve izrednega dogodka, in sicer so to: informacije, potrebne za nadaljnje ukrepanje pristojnega nosilca sektorja in podporo kritičnemu subjektu za učinkovit odziv na izredni dogodek; informacije potrebne ministrstvu za ugotovitev čezmejnega vpliva izrednega dogodka in priglasitev izrednega dogodka z vplivom na neprekinjeno opravljanje bistvenih storitev v šestih ali več državah članicah Evropski komisiji ter obveščanje enotnih kontaktnih točk prizadetih držav članic; in informacije, potrebne NCKU za namen izvajanja nalog v sistemu zgodnjega opozarjanja ter zagotavljanja podpore odločanju telesom kriznega upravljanja. Člen določa tudi kriterij za obveščanje javnosti in pripravo sporočila za javno objavo, ministrstvu pa nalaga obveznost rednega poročanja o prejetih priglasitvah izrednih dogodkov Evropski komisiji in določa vsebino poročila.

25. člen predstavlja podlago za zbiranje, obdelovanje, uporabo in hrambo podatkov o odgovornih in kontaktnih osebah nosilcev sektorjev kritične infrastrukture in kritičnih subjektov, z namenom, da se zagotovi podpora odločanju na področju kritične infrastrukture. Nosilec sektorja kritične infrastrukture mora zbirati, obdelovati in hraniti podatke (tj. ime in priimek osebe, naslov njenega prebivališča, številko telefona, naziv njenega delovnega mesta in naslov elektronske pošte) o odgovornih in kontaktnih osebah kritičnih subjektov, ki delujejo v sektorju kritične infrastrukture iz njegove pristojnosti, NCKU pa mora zbirati, obdelovati, uporabljati in hraniti iste vrste podatkov o odgovornih in kontaktnih osebah vseh nosilcev sektorjev kritične infrastrukture in vseh kritičnih subjektih. Obveznost NCKU in nosilcev sektorjev kritične infrastrukture v zvezi z zbiranjem, obdelovanjem in hrambo podatkov o odgovornih in kontaktnih osebah vključuje tudi obveznost ažuriranja ustreznih evidenc podatkov.

K 21. členu
S tem členom predloga zakona se spreminja 26. člen ZKI zaradi terminološke uskladitve z izrazi, opredeljenimi v 4. členu predloga zakona.

K 22. členu
Člen določa črtanje 27. člena ZKI, ki ureja zaupne podatke Banke Slovenije, kar je, glede na to, da je Banka Slovenije na podlagi tretjega odstavka novega 2.a člena predloga zakona izključena iz uporabe tega zakona smiselno in potrebno.

K 23. členu
Člen dopolnjujejo vsebino 28. člena ZKI o izvajanju nadzora v skladu z določbami Direktive 2022/2557 in sledi njeni uvodni izjavi 40, ki se glasi: »Države članice bi morale zagotoviti, da imajo njihovi pristojni organi nekatera posebna pooblastila za pravilno uporabo in izvrševanje te direktive v zvezi s kritičnimi subjekti, kadar ti spadajo v njihovo pristojnost, kot je določeno v tej direktivi. Ta pooblastila bi morala vključevati zlasti pooblastilo za izvajanje inšpekcijskih pregledov in revizij, pooblastilo za nadzor, pooblastilo da lahko od kritičnih subjektov zahtevajo predložitev informacij in dokazov v zvezi z ukrepi, ki so jih sprejeli za izpolnitev svojih obveznosti, in, kadar je ustrezno, pooblastilo, da izdajo odredbe za odpravo ugotovljenih kršitev. Države članice pri izdaji takih odredb ne bi smele zahtevati ukrepov, ki presegajo tisto, kar je potrebno in sorazmerno za zagotovitev skladnosti zadevnega kritičnega subjekta, ter pri tem zlasti upoštevati resnost kršitve in gospodarsko zmogljivost zadevnega kritičnega subjekta. Splošneje, ta pooblastila bi morali spremljati ustrezni in učinkoviti zaščitni ukrepi, ki bi jih bilo treba določiti v nacionalnem pravu v skladu z Listino Evropske unije o temeljnih pravicah. Pristojni organi iz te direktive, bi morali imeti pri ocenjevanju, ali kritični subjekt izpolnjuje svoje obveznosti iz te direktive, možnost, da od pristojnih organov iz Direktive (EU) 2022/2555 zahtevajo, da izvajajo

svoja nadzorna in izvršilna pooblastila v zvezi s subjektom, ki spada v okvir navedene direktive in je identificiran kot kritičen subjekt na podlagi te direktive. Pristojni organi iz te direktive in pristojni organi iz Direktive (EU) 2022/2555 bi morali v ta namen sodelovati in si izmenjevati informacije.«

Predlog zakona kljub temu, da inšpektorat, pristojen za obrambo lahko, v skladu z že obstoječimi predpisi in uveljavljenim načinom dela k inšpekcijskemu nadzoru lahko pritegne tudi druge inšpekcijske organe, ki imajo stvarne pristojnosti na področju sektorja kritične infrastrukture, vzpostavlja zakonsko podlago in možnost navedenemu inšpektoratu, da lahko od bistvenih subjektov, določenih na podlagi zakona, ki ureja informacijsko varnost zahteva predložitev informacij za oceno ali ukrepi, ki so jih le-ti sprejeli za zagotovitev svoje odpornosti izpolnjujejo zahteve iz 13. člena predloga zakona in dokaze o učinkovitem izvajanju teh ukrepov. Hkrati vzpostavlja podlago tudi za to, da inšpektorat, pristojen za obrambo lahko od inšpekcije pristojnega nacionalnega organa, na podlagi zakona, ki ureja informacijsko varnost zahteva, da ta izvaja svoja nadzorna in izvršilna pooblastila glede subjekta, identificiranega na podlagi zakona, ki ureja informacijsko varnost, in določenega za kritični subjekt na podlagi tega predloga zakona, ter da mu v zvezi s tem posreduje informacije. Skladno z določbami Direktive 2022/2555 in predlogom novega zakona, ki bo urejal informacijsko varnost bodo namreč vsi kritični subjekti, določeni na podlagi tega predloga zakona tudi zavezanci po predlogu zakonu, ki ureja informacijsko varnost in je tako, v členu opredeljeno sodelovanje navedenih nadzornih organov smiselno.

K 24. členu
Člen določa prekrške pri izvajanju tega zakona in višino zagroženih glob, zaradi katerih sta kaznovana kritični subjekt kot pravna oseba, in odgovorna oseba kritičnega subjekta. Ne gre za kaznovanje kritičnega subjekta ali njegove odgovorne osebe zaradi morebitnega nedelovanja kritične infrastrukture na splošno, ampak zaradi njegove ali njune opustitve s predlogom zakona določenih ravnanj, katerih izvajanje načelno prispeva k zagotavljanju neprekinjenega opravljanja bistvenih storitev in celovitosti delovanja kritične infrastrukture. Člen ministrstvu nalaga obveznost o prekrških, ki se uporabljajo za kršitve ukrepov, sprejetih na podlagi predloga zakona obvestiti Evropsko komisijo, in sicer do 17. oktobra 2024. Evropsko komisijo mora obveščati tudi o vseh njihovih naknadnih spremembah.

K 25. členu
Člen zagotavlja zakonsko podlago, da se lahko v hitrem postopku za prekrške, določene v 24. členu predloga zakona, izreče tudi globa v znesku, ki je višji od najnižje, ki jo predvideva predlog zakona.

K 26. členu
Člena določa rok za sprejem strategije in nacionalne ocene tveganja ter za izdajo obveznih podzakonskih aktov po predlogu tega zakona, s katerimi bo vlada določila bistvene storitve, podsektorje sektorjev kritične infrastrukture, nosilce sektorjev kritične infrastrukture in sodelujoče organe, kategorije subjektov, mejne vrednosti kriterijev za ugotavljanja kritičnih subjektov ter kritične subjekte in njihove kritične infrastrukture.

Člen nalaga ministrstvu posredovanje podatkov Evropski komisiji o tem, da je pristojni nacionalni organ in tudi enotna kontaktna točka in določa rok za posredovanje navedenih podatkov ter obveznost sporočanja morebitnih poznejših sprememb Člen ministrstvu nalaga tudi obveznost in rok za posredovanje strategije in nacionalna ocene Evropski komisiji.

Člen določa rok, s katerim je kritičnim subjektom naložena uporaba III. poglavja predloga zakona z naslovom Odpornost kritičnih subjektov in kritične infrastrukture in izpolnjevanje obveznosti, ki izhajajo iz členov tega poglavja, in sicer je to deset mesecev po njihovi določitvi za kritične subjekte.

K 27. členu

S členom se ureja podaljšanje uporabe ZKI in Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije. Veljavnost Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije sicer preneha z dnem uveljavitve predloga zakona. Navedena predpisa se uporabljata do določitve kritičnih subjektov na podlagi predloga zakona. Z uveljavitvijo predloga zakona bo prenehala veljati tudi Uredba o evropski kritični infrastrukturi.

K 28. členu
Člen določa petnajstdnevni rok za uveljavitev predloga zakona.

IV. BESEDILO ČLENOV, KI SE SPREMINJAJO

Zakon o kritični infrastrukturi

1. člen
(vsebina zakona)

Ta zakon ureja ugotavljanje in določanje kritične infrastrukture Republike Slovenije, načela in načrtovanje zaščite kritične infrastrukture, naloge organov in organizacij na področju kritične infrastrukture ter obveščanje, poročanje, zagotavljanje podpore odločanju, varovanje podatkov in nadzor na področju kritične infrastrukture.

2. člen
(razmerje med evropsko kritično infrastrukturo Republike Slovenije in kritično infrastrukturo Republike Slovenije)

(1) Evropska kritična infrastruktura, določena na območju Republike Slovenije, je tudi kritična infrastruktura Republike Slovenije (v nadaljnjem besedilu: kritična infrastruktura).

(2) Pri zaščiti kritične infrastrukture iz prejšnjega odstavka se upoštevajo tudi predpisi, ki urejajo evropsko kritično infrastrukturo.

3. člen
(pomen pojmov)

V tem zakonu uporabljeni pojmi imajo naslednji pomen:

1. Evropska kritična infrastruktura Republike Slovenije je infrastruktura, ki se nahaja na ozemlju Republike Slovenije in je določena v skladu s predpisi, ki urejajo evropsko kritično infrastrukturo.
2. Izredni dogodek pri delovanju kritične infrastrukture (v nadaljnjem besedilu: izredni dogodek) je resna motnja v delovanju ali prekinitev delovanja kritične infrastrukture, ki vpliva ali bi lahko vplivala tudi na njeno varnost.
3. Kritična infrastruktura Republike Slovenije obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo, in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi.
4. Kriza je stanje, v katerem so zaradi prekinitve delovanja kritične infrastrukture nastale ali lahko nastanejo posledice, ki presegajo mejno vrednost vsaj enega medsektorskega kriterija za ugotavljanje kritične infrastrukture.
5. Lastniki ali upravljavci kritične infrastrukture (v nadaljnjem besedilu: upravljavci kritične infrastrukture) so gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti ali upravljajo kritično infrastrukturo.
6. Načrtovanje zaščite kritične infrastrukture obsega ocenjevanje tveganj za delovanje kritične infrastrukture in oblikovanje ukrepov za zaščito kritične infrastrukture.
7. Nosilci sektorjev kritične infrastrukture so posamezna ministrstva in službe Vlade Republike Slovenije, ki so odgovorni za delovna področja, na katera spada kritična infrastruktura, in Banka Slovenije.
8. Ocena tveganj za delovanje kritične infrastrukture (v nadaljnjem besedilu: ocena tveganj) je rezultat celovitega postopka identifikacije, analize in ovrednotenja različnih virov tveganj za delovanje kritične infrastrukture, ki se izvede za zagotovitev podlage za oblikovanje ukrepov za zaščito kritične infrastrukture.
9. Področje kritične infrastrukture obsega dejavnosti, povezane z ugotavljanjem, določanjem in zaščito kritične infrastrukture.
10. Povečana ogroženost kritične infrastrukture je stanje, ki ga zazna pristojni državni organ in za katerega oceni, da bi lahko povzročilo nastanek izrednega dogodka ali krize.
11. Prioriteta delovanja sektorjev kritične infrastrukture je določitev prednostnega vrstnega reda sektorjev kritične infrastrukture z vidika posledic resnih motenj v njihovem delovanju ali prekinitve njihovega delovanja.

12. Pristojni organi in organizacije so Vlada Republike Slovenije (v nadaljnjem besedilu: vlada), ministrstvo, pristojno za obrambo (v nadaljnjem besedilu: ministrstvo), nosilci sektorjev kritične infrastrukture, državni organi, ki sodelujejo z nosilci sektorjev kritične infrastrukture pri izvajanju njihovih nalog po tem zakonu, upravljavci kritične infrastrukture, Nacionalni center za krizno upravljanje (v nadaljnjem besedilu: NCKU) in inšpektorat, pristojen za obrambo.
13. Sektorji kritične infrastrukture so posamezne vsebinsko zaokrožene celote delovanja kritične infrastrukture, med katere se štejejo tudi objekti, ki zagotavljajo sistemsko odpornost in redundanco.
14. Ukrepi za zaščito kritične infrastrukture so dejavnosti, katerih namen je zagotoviti varnost kritične infrastrukture, preprečiti motnje v njenem delovanju ali prekinitev njenega delovanja in ublažiti posledice tega, po potrebi vzpostaviti nadomestno ali obhodno delovanje kritične infrastrukture in zagotoviti njeno čimprejšnje ponovno nemoteno delovanje.
15. Zaščita kritične infrastrukture kot del področja kritične infrastrukture je dejavnost, ki se izvaja za zagotovitev neprekinjenosti delovanja kritične infrastrukture.

II. UGOTAVLJANJE IN DOLOČANJE KRITIČNE INFRASTRUKTURE

4. člen
(sektorji kritične infrastrukture)

(1) Sektorji kritične infrastrukture so sektor energetike, sektor prometa, sektor prehrane, sektor preskrbe s pitno vodo, sektor zdravstva, sektor financ, sektor varovanja okolja ter sektor informacijsko-komunikacijskih omrežij in sistemov.

(2) Sektor iz prejšnjega odstavka ima nosilca in državni organ ali več teh, ki sodelujejo z nosilcem sektorja kritične infrastrukture pri izvajanju njegovih nalog po tem zakonu.

(3) Nosilce sektorjev kritične infrastrukture in z njimi sodelujoče državne organe iz prejšnjega odstavka ter prioriteto delovanja sektorjev kritične infrastrukture določi vlada.

5. člen
(kriteriji za ugotavljanje kritične infrastrukture)

(1) Kriteriji za ugotavljanje kritične infrastrukture se oblikujejo na podlagi presoje mogočih posledic zaradi resnih motenj v delovanju ali prekinitve delovanja kritične infrastrukture za nacionalno varnost, gospodarstvo in druge ključne družbene funkcije, ter zdravje, varnost, zaščito in blaginjo ljudi.

(2) Kriteriji za ugotavljanje kritične infrastrukture so podlaga za določitev kritične infrastrukture in jih podrobneje določi vlada.

(3) Kriteriji za ugotavljanje kritične infrastrukture so sektorski in medsektorski.

6. člen
(sektorski kriteriji za ugotavljanje kritične infrastrukture)

(1) Sektorski kriteriji za ugotavljanje kritične infrastrukture se ob upoštevanju značilnosti posameznega sektorja kritične infrastrukture oblikujejo na podlagi presoje mogočih posledic zaradi resnih motenj v delovanju ali prekinitve delovanja kritične infrastrukture za posamezen sektor kritične infrastrukture.

(2) Sektorski kriteriji za ugotavljanje kritične infrastrukture so podlaga za prvi izbor kritične infrastrukture v sektorju kritične infrastrukture.

7. člen
(medsektorski kriteriji za ugotavljanje kritične infrastrukture)

(1) Medsektorski kriteriji za ugotavljanje kritične infrastrukture se oblikujejo na podlagi presoje mogočih posledic zaradi resnih motenj v delovanju ali prekinitve delovanja kritične infrastrukture za vse sektorje kritične infrastrukture.

(2) Medsektorski kriteriji za ugotavljanje kritične infrastrukture iz prejšnjega odstavka se nanašajo na posledice resnih motenj v delovanju ali prekinitve delovanja kritične infrastrukture, pri čemer se upoštevajo:
– število žrtev, pri čemer se oceni mogoče število mrtvih ali poškodovanih;
– gospodarske posledice, pri čemer se oceni mogoča gospodarska izguba ali poslabšanje kakovosti proizvodov ali storitev, vključno z morebitnimi posledicami za okolje;
– vpliv na javnost, pri čemer se ocenijo mogoče posledice za zaupanje javnosti, fizično trpljenje in motnje v vsakodnevnem življenju ljudi, vključno s prekinitvijo zagotavljanja osnovnih storitev.

8. člen
(mejne vrednosti kriterijev za ugotavljanje kritične infrastrukture)

(1) Mejne vrednosti kriterijev za ugotavljanje kritične infrastrukture se oblikujejo na podlagi presoje teže mogočih posledic, nastalih zaradi resnih motenj v delovanju ali prekinitve delovanja kritične infrastrukture.

(2) Mejne vrednosti kriterijev za ugotavljanje kritične infrastrukture podrobneje določi vlada.

9. člen
(določitev kritične infrastrukture)

(1) Kritična infrastruktura mora zadostiti minimalni vrednosti vsaj enega medsektorskega kriterija za ugotavljanje kritične infrastrukture.

(2) Kritično infrastrukturo in upravljavce kritične infrastrukture določi vlada.

III. ZAŠČITA KRITIČNE INFRASTRUKTURE

10 člen
(načela zaščite kritične infrastrukture)

Načela zaščite kritične infrastrukture so:
1. Načelo celovitega pristopa, ki zahteva, da so v zaščito kritične infrastrukture pred in med motnjami v delovanju ali prekinitvi delovanja kritične infrastrukture ter po njih vključeni vsi pristojni organi in organizacije in da se pri tem upoštevajo različne vrste nevarnosti, izhaja iz ocene tveganj ter upošteva soodvisnost sektorjev kritične infrastrukture in njihov medsebojni vpliv.
2. Načelo odgovornosti, po katerem so za delovanje kritične infrastrukture neposredno odgovorni upravljavci kritične infrastrukture, za krepitev zaščite kritične infrastrukture pa vsi pristojni organi in organizacije.
3. Načelo zaščite pred različnimi vrstami nevarnosti, ki zahteva, da vsi pristojni organi in organizacije pri zagotavljanju neprekinjenega delovanja kritične infrastrukture upoštevajo različne vrste naravnih in tehnoloških nevarnosti.
4. Načelo stalnega načrtovanja zaščite kritične infrastrukture, ki zahteva, da je načrtovanje zaščite kritične infrastrukture podprto s stalnim procesom ocenjevanja tveganj za delovanje kritične infrastrukture in presoje ustreznosti ukrepov za njeno zaščito.
5. Načelo izmenjave podatkov in informacij ter varovanja podatkov, ki zahteva od vseh pristojnih organov in organizacij redno, pravočasno in na zaupanju temelječo izmenjavo podatkov in informacij ob hkratnem varovanju podatkov, povezanih s kritično infrastrukturo, v skladu s predpisi, ki urejajo varovanje tajnih podatkov ali poslovno skrivnost.

11. člen
(dokumenti načrtovanja zaščite kritične infrastrukture)

(1) Dokumenti načrtovanja zaščite kritične infrastrukture (v nadaljnjem besedilu: dokumenti načrtovanja) obsegajo oceno tveganj in ukrepe za zaščito kritične infrastrukture.

(2) Dokumente načrtovanja izdelajo in hranijo upravljavci kritične infrastrukture.

(3) Upravljavci kritične infrastrukture morajo k izdelanim dokumentom načrtovanja pridobiti soglasje nosilca sektorja kritične infrastrukture.

(4) Upravljavec kritične infrastrukture je pristojnemu nosilcu sektorja kritične infrastrukture oziroma ministrstvu na njuno zahtevo dolžen poslati dokumente načrtovanja.

12. člen
(ocena tveganj)

Upravljavci kritične infrastrukture izdelajo oceno tveganj na podlagi navodila za ocenjevanje tveganj za delovanje kritične infrastrukture (v nadaljnjem besedilu: navodilo), ki ga sprejme ministrstvo, in strokovnih usmeritev, ki jih za posamezne sektorje kritične infrastrukture izdelajo nosilci sektorjev kritične infrastrukture.

13. člen
(ukrepi za zaščito kritične infrastrukture)

(1) Ukrepi za zaščito kritične infrastrukture so stalni in dodatni. Stalni ukrepi se izvajajo v vseh razmerah, ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi se izvajajo ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi, če stalni ukrepi, tudi če se njihovo izvajanje stopnjuje, ne zadostujejo.

(2) Stalne ukrepe za zaščito kritične infrastrukture na podlagi ocene tveganj načrtujejo in izvajajo upravljavci kritične infrastrukture.

(3) Upravljavci kritične infrastrukture dodatne ukrepe za zaščito kritične infrastrukture načrtujejo na podlagi ocene tveganj ali sprejmejo na podlagi nastalih in pričakovanih posledic povečane ogroženosti kritične infrastrukture, izrednega dogodka ali krize.

(4) Nosilci sektorjev kritične infrastrukture lahko sprejmejo dodatne ukrepe za zaščito kritične infrastrukture na ravni sektorja kritične infrastrukture iz svoje pristojnosti ali pripravijo predlog dodatnih ukrepov za zaščito kritične infrastrukture, ki ga sprejme vlada.

(5) Če morajo dodatne ukrepe za zaščito kritične infrastrukture iz prejšnjega odstavka izvesti upravljavci kritične infrastrukture, lahko vlada odloči o dodelitvi sredstev za izvedbo teh ukrepov.

(6) Na predlog nosilcev sektorjev kritične infrastrukture se upravljavce kritične infrastrukture v skladu s predpisi, ki urejajo zasebno varovanje, določi za zavezance obveznega organiziranja varovanja, ki morajo izvajati varovanje kritične infrastrukture v skladu s temi predpisi.

14. člen
(ažuriranje dokumentov načrtovanja)

(1) Upravljavci kritične infrastrukture morajo dokumente načrtovanja redno ažurirati, najmanj pa enkrat na leto.

(2) Ob nastanku novih okoliščin, ki lahko pomembno vplivajo na delovanje kritične infrastrukture, je treba dokumente načrtovanja spremeniti najpozneje v mesecu dni. K tako spremenjenim dokumentom načrtovanja je treba pridobiti soglasje pristojnega nosilca sektorja kritične infrastrukture.

15. člen
(upoštevanje obstoječih dokumentov)

Pri izdelavi dokumentov načrtovanja se lahko upoštevajo dokumenti, ukrepi, postopki in rešitve, izdelani ali sprejeti na podlagi veljavnih predpisov, zlasti s področja zasebnega varovanja, varstva pred naravnimi in drugimi nesrečami in tehnološke varnosti, in poslovnih odločitev upravljavcev kritične infrastrukture.

16. člen
(izvršba in stečaj upravljavca kritične infrastrukture)

(1) Objekti, naprave, sistemi in zmogljivosti upravljavcev kritične infrastrukture in njihove premoženjske pravice, ki so nujno potrebni za nemoteno delovanje kritične infrastrukture, ne morejo biti predmet izvršbe ali prodaje v stečajnem postopku ali postopku prisilne likvidacije v skladu z zakonom, ki ureja izvršbo, ter zakonom, ki ureja postopke zaradi insolventnosti in prisilnega prenehanja, razen če se z izvršbo ali prodajo v postopku stečaja ali prisilne likvidacije zagotavljata celovitost in nemoteno delovanje kritične infrastrukture v skladu s tem zakonom.

(2) Ne glede na predpise, ki urejajo poslovanje stečajnega dolžnika po začetku stečajnega postopka, je stečajnemu dolžniku, ki je upravljavec kritične infrastrukture, dovoljeno nadaljevanje poslovanja v zadevah, ki so nujno potrebne za zagotavljanje neprekinjenega delovanja kritične infrastrukture. Stečajni upravitelj mora v tem primeru poskrbeti, da se opravljanje nalog, ki so nujno potrebne za zagotavljanje neprekinjenega delovanja kritične infrastrukture, zagotovi v neokrnjenem obsegu.

17. člen
(vlada)

Vlada na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, določa politiko na tem področju ter po potrebi od nosilcev sektorjev kritične infrastrukture, upravljavcev kritične infrastrukture, ministrstva in inšpektorata, pristojnega za obrambo, zahteva dodatna poročila o izvajanju nalog iz njihove pristojnosti, ki niso zajeta v petem poglavju tega zakona.

18. člen
(nosilci sektorjev kritične infrastrukture)

(1) Nosilci sektorjev kritične infrastrukture opravljajo na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, te naloge:
- oblikujejo pobudo in sodelujejo pri pripravi predloga za določitev sektorskih kriterijev za ugotavljanje kritične infrastrukture in njihovih mejnih vrednosti;
- sodelujejo pri pripravi predloga za določitev medsektorskih kriterijev za ugotavljanje kritične infrastrukture in njihovih mejnih vrednosti;
- oblikujejo pobudo in sodelujejo pri pripravi predloga za določitev kritične infrastrukture iz svoje pristojnosti;
- usklajujejo predloge ukrepov za zaščito kritične infrastrukture v sektorju kritične infrastrukture iz svoje pristojnosti;
- usmerjajo in nudijo strokovno pomoč upravljavcem kritične infrastrukture pri njihovem načrtovanju zaščite kritične infrastrukture;
- pripravljajo ali dopolnjujejo predpise s področja sektorja kritične infrastrukture iz svoje pristojnosti z vidika zaščite kritične infrastrukture.

(2) Nosilci sektorjev kritične infrastrukture določijo kontaktno osebo ali več takih oseb za sodelovanje na področju kritične infrastrukture z upravljavci kritične infrastrukture, drugimi nosilci sektorjev kritične infrastrukture in ministrstvom.

19. člen
(upravljavci kritične infrastrukture)

(1) Upravljavci kritične infrastrukture zagotavljajo neprekinjeno delovanje kritične infrastrukture.

(2) Upravljavci kritične infrastrukture določijo kontaktno osebo ali več takih oseb za sodelovanje na področju kritične infrastrukture z drugimi upravljavci kritične infrastrukture, nosilci sektorjev kritične infrastrukture in ministrstvom.

20. člen
(ministrstvo)

(1) Strokovno usmerjanje in usklajevanje dejavnosti na področju kritične infrastrukture izvaja ministrstvo.

(2) Ministrstvo opravlja na področju kritične infrastrukture poleg drugih nalog, določenih s tem zakonom, naslednje naloge:
– pripravlja predloge za določitev sektorskih in medsektorskih kriterijev za ugotavljanje kritične infrastrukture in mejnih vrednosti teh kriterijev, pri čemer obravnava pobude in predloge nosilcev sektorjev kritične infrastrukture;
– pripravlja predloge za določitev kritične infrastrukture, pri čemer obravnava pobude in predloge pristojnih nosilcev sektorjev kritične infrastrukture;
– usklajuje predloge ukrepov za zaščito kritične infrastrukture med sektorji kritične infrastrukture.

(3) Ministrstvo je kontaktni organ za sodelovanje med pristojnimi organi in organizacijami.

21. člen
(Nacionalni center za krizno upravljanje)

V primeru krize po tem zakonu NCKU opravlja svoje naloge tako, kot je določeno s predpisi o njegovi organizaciji in delovanju.

22. člen
(Banka Slovenije)

(1) Ta zakon se ne uporablja za kritično infrastrukturo, ki jo upravlja Evropski sistem centralnih bank.

(2) Ta zakon se ne uporablja za kritično infrastrukturo v upravljanju Banke Slovenije, ki jo nadzira Evropski sistem centralnih bank.

(3) Ta zakon ne posega v nadzor kritične infrastrukture s področja pristojnosti Banke Slovenije ali Evropskega sistema centralnih bank, ki ga urejajo predpisi Evropske unije in na njihovi podlagi sprejeti predpisi Republike Slovenije.

(4) Za kritično infrastrukturo Banke Slovenije, ki ni infrastruktura iz prvega in drugega odstavka tega člena in jo Banka Slovenije uporablja za izvajanje svojih nalog po Zakonu o Banki Slovenije (Uradni list RS, št. 72/06 – uradno prečiščeno besedilo, 59/11 in 55/17; v nadaljnjem besedilu: ZBS-1), Statutu Evropskega sistema centralnih bank in Evropske centralne banke (UL C št. 326 z dne 26. 10. 2012, str. 230; v nadaljnjem besedilu: Statut) in predpisih Evropske unije, lahko

pristojni organi in organizacije sprejemajo odločitve o delovanju te infrastrukture le s soglasjem Banke Slovenije.

V. OBVEŠČANJE, POROČANJE IN ZAGOTAVLJANJE PODPORE ODLOČANJU

23. člen
(obveščanje)

(1) Upravljavec kritične infrastrukture takoj, ko je mogoče, obvesti nosilca sektorja kritične infrastrukture in NCKU o prekinitvi delovanja kritične infrastrukture, za katero oceni, da lahko ima negativne materialne in druge posledice za delovanje sektorja kritične infrastrukture, in o že izvedenih ukrepih za zaščito kritične infrastrukture.

(2) O prekinitvi delovanja kritične infrastrukture z znaki možnosti nastanka krize nosilec sektorja kritične infrastrukture obvesti vlado ter skupaj z upravljavcem kritične infrastrukture poskrbi za čimprejšnje obveščanje javnosti o pomembnih dejstvih in izvedenih ukrepih za zaščito kritične infrastrukture.

(3) V primeru povečane ogroženosti kritične infrastrukture pristojni državni organi z zaznano grožnjo seznanijo nosilca sektorja kritične infrastrukture, ta pa upravljavca kritične infrastrukture.

(4) Upravljavec kritične infrastrukture o dejstvih in okoliščinah, ki kažejo na možnost njegovega prenehanja poslovanja ali stečaja, obvesti nosilca sektorja kritične infrastrukture.

24. člen
(poročanje)

(1) Nosilci sektorjev kritične infrastrukture na podlagi letnih poročil upravljavcev kritične infrastrukture o zagotavljanju neprekinjenega delovanja kritične infrastrukture za preteklo leto, ki jih ti pripravijo do konca februarja, pripravijo letno poročilo o zagotavljanju neprekinjenega delovanja kritične infrastrukture za sektor kritične infrastrukture iz svoje pristojnosti in ga do konca aprila pošljejo ministrstvu, ki pripravi skupno letno poročilo o zagotavljanju neprekinjenega delovanja kritične infrastrukture Republike Slovenije in ga do konca maja za preteklo leto predloži vladi.

(2) V poročilih iz prejšnjega odstavka se navedejo izredni dogodki, ki so povzročili prekinitev delovanja kritične infrastrukture z negativnimi materialnimi in drugimi posledicami za delovanje sektorja kritične infrastrukture, v zvezi s tem izvedeni ukrepi za zaščito kritične infrastrukture ter rešitve in sprejeti ali predlagani ukrepi za izboljšanje zaščite kritične infrastrukture.

25. člen
(podatki o odgovornih in kontaktnih osebah)

(1) Da se zagotovi podpora odločanju na področju kritične infrastrukture, se zbirajo, obdelujejo, uporabljajo in hranijo ti podatki o odgovorni in kontaktni osebi nosilca sektorja kritične infrastrukture in upravljavca kritične infrastrukture:
– ime in priimek,
– stalno ali začasno prebivališče,
– številka telefona,
– naziv delovnega mesta.

(2) Podatke o odgovornih in kontaktnih osebah nosilcev sektorjev kritične infrastrukture in upravljavcev kritične infrastrukture zbira, obdeluje, uporablja in hrani NCKU.

(3) Nosilci sektorjev kritične infrastrukture zbirajo, obdelujejo, uporabljajo in hranijo podatke o odgovornih in kontaktnih osebah upravljavcev kritične infrastrukture, ki delujejo v sektorju kritične infrastrukture iz njihove pristojnosti.

26. člen
(varovanje podatkov)

Podatki, ki se nanašajo na ugotavljanje, določanje in zaščito kritične infrastrukture in so določeni kot tajni ali poslovna skrivnost, se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.

27. člen
(zaupni podatki Banke Slovenije)

Podatki, ki jih ima na voljo Banka Slovenije in so v skladu z ZBS-1, Statutom in drugimi predpisi določeni kot zaupni, se lahko uporabijo le v skladu s temi predpisi.

28. člen
(izvajanje nadzora)

Nadzor nad izvajanjem določb tega zakona izvaja inšpektorat, pristojen za obrambo.

29. člen
(prekrški)

(1) Z globo od 5.000 do 15.000 eurov je za prekršek kaznovan upravljavec kritične infrastrukture, če:
- ne izdela ali hrani dokumentov načrtovanja (drugi odstavek 11. člena);
- k izdelanim dokumentom načrtovanja ne pridobi soglasja nosilca sektorja kritične infrastrukture (tretji odstavek 11. člena);
- ne izvaja rednega ažuriranja dokumentov načrtovanja (prvi odstavek 14. člena);
- ob nastanku novih okoliščin, ki lahko pomembno vplivajo na delovanje kritične infrastrukture, v predpisanem roku ne spremeni dokumentov načrtovanja ali k tako spremenjenim dokumentom načrtovanja ne pridobi soglasja pristojnega nosilca sektorja kritične infrastrukture (drugi odstavek 14. člena);
- ne določi kontaktne osebe za sodelovanje na področju kritične infrastrukture z drugimi upravljavci kritične infrastrukture, nosilci sektorjev kritične infrastrukture in ministrstvom (drugi odstavek 19. člena);
- nosilca sektorja kritične infrastrukture in NCKU takoj, ko je mogoče, ne obvesti o prekinitvi delovanja kritične infrastrukture, za katero oceni, da ima lahko negativne materialne in druge posledice za delovanje sektorja kritične infrastrukture, in o že izvedenih ukrepih za zaščito kritične infrastrukture (prvi odstavek 23. člena);
- nosilca sektorja kritične infrastrukture ne obvesti o dejstvih in okoliščinah, ki kažejo na možnost njegovega prenehanja poslovanja ali stečaja (četrti odstavek 23. člena);
- ne izdela vsebinsko ustreznega letnega poročila o zagotavljanju neprekinjenega delovanja kritične infrastrukture, ki jo upravlja (drugi odstavek 24. člena);
- podatkov, ki se nanašajo na kritično infrastrukturo in so določeni kot tajni ali poslovna skrivnost, ne obravnava v skladu s predpisi, ki urejajo varovanje tajnih podatkov in poslovno skrivnost (26. člen).

(2) Z globo od 400 do 1.000 eurov je kaznovana odgovorna oseba upravljavca kritične infrastrukture, ki stori prekršek iz prejšnjega odstavka.

30. člen

(višina globe v hitrem prekrškovnem postopku)

Za prekrške po tem zakonu se v hitrem prekrškovnem postopku lahko izreče globa v znesku, ki je višji od najnižje globe, določene po tem zakonu.

V. PREDLOG, DA SE PREDLOG ZAKONA OBRAVNAVA PO NUJNEM OZIROMA SKRAJŠANEM POSTOPKU

/