



## PRILOGA 3

## PREDLOG (EVA 2024-1911-0008)

### ZAKON O KRITIČNI INFRASTRUKTURI

#### I. UVOD

#### 1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Nov Zakon o kritični infrastrukturi bo nadomestil Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M, v nadaljnjem besedilu: ZKI), ki je bil sprejet leta 2017. Z ZKI so se sistemsko uredili ugotavljanje in določanje kritične infrastrukture Republike Slovenije ter zaščita tovrstne infrastrukture, pri čemer se je izhajalo iz razumevanja, da zaščita kritične infrastrukture obsega 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) kritična infrastruktura državnega pomena, torej »nacionalna« kritična infrastruktura;
- z normativnim ukrepom prispeva k dvigu ravni odpornosti slovenske družbe na sodobne varnostne grožnje in tveganja;
- organom in organizacijam, ki so odgovorni za sektorje, ki so za slovensko družbo posebno pomembni, oziroma delujejo v njih, naloži, da pri svojem delu upoštevajo tudi zahteve glede zagotavljanja neprekinjenega delovanja kritične infrastrukture, torej vidik zaščite kritične infrastrukture;
- organom in organizacijam pri zagotavljanju neprekinjenega ter celovitega delovanja kritične infrastrukture naloži spoštovanje istih splošnih izhodišč in usmeritev (npr. načel);
- med organi in organizacijami, ki delujejo v sektorjih kritične infrastrukture, vzpostavijo primerna razmerja, predvsem z vidika delitve njihovih pristojnosti, odgovornosti in nalog pri zaščiti kritične infrastrukture;
- naloži dopolnitev normativne urejenosti ali normativne ureditve, če te še ni, v posameznih sektorjih kritične infrastrukture z vidika zaščite te infrastrukture.

Izvajanje zakona je v naslednjih letih potekalo 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. Vlada Republike Slovenije (v nadaljnjem besedilu: vlada) je leta 2018 določila nosilce sektorjev kritične infrastrukture in z njimi sodelujoče državne organe ter sektorske in medsektorske kriterije za določitev kritične infrastrukture, leta 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 torej 53 upravljavcev v osmih sektorjih kritične infrastrukture.

Upravljavci so morali na podlagi 11. člena ZKI 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 leta 2019 vsako leto poroča vladi o zagotavljanju neprekinjenega delovanja kritične infrastrukture Republike Slovenije.

Pri izvajanju zakona niso bile zaznane večje težave.

Leta 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 jo morajo države članice implementirati v svojo zakonodajo do 17. oktobra 2024.

Cilj Direktive 2022/2557 sta neprekinjeno opravljanje bistvenih storitev na notranjem trgu za ohranjanje ključnih družbenih funkcij ali gospodarskih dejavnosti in krepitev odpornosti kritičnih subjektov, ki opravljajo te storitve. Direktiva za doseganje visoke ravni odpornosti kritičnih subjektov in neprekinjenega opravljanja bistvenih storitev določa obveznosti za države članice ter 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 11 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 držav članic oziroma 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 ter 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 kibernetске varnosti v Uniji, o 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 kibernetских grožnjah. V Direktivi 2022/2557 so za države članice določena pravila o nadzoru kritičnih subjektov, izvrševanju in 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 jo morajo države članice 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 urejajo tudi določena vprašanja, povezana z odzivanjem na izredne dogodke na področju kritične infrastrukture.

## **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**

Temeljna načela predloga zakona so:

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

Načela, na katerih temelji odpornost kritičnih subjektov in kritične infrastrukture, predvidena s predlogom zakona, so kot splošne usmeritve pri krepitvi odpornosti kritičnih subjektov določena v 12. členu predloga zakona.

### **2.3 Poglavitne rešitve**

S predlogom zakona se v slovenski pravni red prenaša Direktiva 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 in 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 (IV.), poglavja o kritičnih subjektih posebnega evropskega pomena (V.) in poglavja o nadzoru (IX.) se za določene subjekte zaradi njihovega posebnega pomena ne bodo uporabljale, prav tako se zakon ne bo uporabljal za vsebine, ki jih opredeljuje zakon, ki ureja področje informacijske varnosti.

V predlogu zakona je opredeljen pomen 14 izrazov, ki so terminološko in vsebinsko usklajeni s pojmi Direktive 2022/2557, ki v ospredje pravnega okvira postavlja zagotavljanje bistvenih storitev na notranjem trgu Evropske unije (4. člen).

II. poglavje, ki opredeljuje nacionalni okvir za odpornost kritičnih subjektov, nalaga vladi sprejem strategije za odpornost kritičnih subjektov (5. člen) in nacionalne ocene tveganja za opravljanje bistvenih storitev (6. člen) ter opredeljuje osnovna izhodišča za njuno pripravo in obvezne vsebine obeh aktov.

III. poglavje predloga zakona določa ugotavljanje in določanje kritičnih subjektov ter njihove kritične infrastrukture. Besedilo predloga zakona navaja 11 sektorjev kritične infrastrukture (7. člen). V 8. členu so opredeljeni kriteriji za ugotavljanje kritičnih subjektov, pri čemer se vzpostavlja vsebinsko in funkcionalno ločevanje med njimi. Prvi se nanašajo na presojanje nosilcev sektorjev kritične infrastrukture glede opravljanja bistvene storitve in na 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 9. 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 predvsem do kritičnih subjektov in tudi do Evropske komisije (10. člen), še zlasti pa zagotavljanje podpore kritičnim subjektom pri krepitvi njihove odpornosti (11. člen).

IV. poglavje o odpornosti kritičnih subjektov in kritične infrastrukture opredeljuje najpomembnejše dejavnosti, ki se izvajajo za zagotovitev neprekinjenosti opravljanja bistvene storitve in delovanja kritične infrastrukture. Načela odpornosti kritičnih subjektov in kritične infrastrukture 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 (12. člen). V 13. členu predloga zakona je opredeljen obseg obveznosti kritičnih subjektov. Ta ostaja enak obsegu njihovih obveznosti, kot so bile opredeljene v ZKI. Kritični subjekti bodo morali tako kot do zdaj upravljavci kritične infrastrukture po ZKI izdelati oceno tveganja za bistveno storitev (14. člen), 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. Stalne ukrepe za odpornost na podlagi ocene tveganja kritičnega subjekta načrtujejo in izvajajo kritični subjekti. Stalni ukrepi, ki so lahko po vsebini organizacijski, materialno-tehnični, kadrovski, varnostni itd., se izvajajo v vseh razmerah, ob zaznani povečani ogroženosti kritične infrastrukture ali izrednem dogodku pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi za odpornost pa se vsebinsko razlikujejo od stalnih ukrepov in se izvajajo ob povečani ogroženosti kritične infrastrukture ali izrednem dogodku, če stalni ukrepi, tudi če so stopnjevani, ne zadostujejo. Nosilci stalnih ukrepov za odpornost so kritični subjekti, nosilci dodatnih ukrepov pa so poleg kritičnih subjektov po potrebi tudi nosilci sektorjev kritične infrastrukture. Predlog zakona določa tudi, da lahko nosilec sektorja kritične infrastrukture ob povečani ogroženosti kritične infrastrukture ali izrednem dogodku sprejme dodatne ukrepe za odpornost na ravni sektorja kritične infrastrukture iz svoje pristojnosti ali pripravi predlog dodatnih ukrepov za odpornost, ki ga sprejme vlada. In če morajo te ukrepe izvesti kritični subjekti, lahko sredstva za njihovo izvedbo zagotovi vlada.

Predlog zakona kritičnim subjektom omogoča, da lahko sprejmejo ukrepe za odpornost na podlagi že pripravljenih načrtov ali dokumentov na podlagi sektorskih in drugih pravnih aktov, ki so pomembni za okrepitev odpornosti kritičnih subjektov, ter svojih poslovnih odločitev, da bi se izognili podvajanju (npr. s področja informacijske varnosti, kibernetske varnosti, varstva pred naravnimi in drugimi nesrečami, obrambnega načrtovanja, zasebnega varovanja, tehnološke varnosti, področne zakonodaje, načrtov neprekinjenega poslovanja itd.) (15. člen).

Ocena in ukrepi predstavljajo načrt kritičnega subjekta za odpornost, ki ga morajo kritični subjekti redno posodablјati, najmanj pa enkrat na dve leti. Ob nastanku novih okoliščin, ki lahko pomembno vplivajo na zagotavljanje bistvene storitve in delovanje kritične infrastrukture, mora kritični subjekt

ustrezno spremeniti načrt za odpornost najpozneje v enem mesecu od nastanka takih okoliščin, in k tako spremenjenemu načrtu pridobiti odobritev pristojnega nosila sektorja kritične infrastrukture (16. člen). Predlog zakona daje podlago kritičnemu subjektu, da ta lahko ob upoštevanju nacionalne in svoje ocene tveganja predloži zahtevek za preverjanje preteklosti zaposlenih ter kandidatov za zaposlitev na delovnih mestih, pomembnih za opravljanje bistvenih storitev kritičnega subjekta, ki imajo ali bodo imeli pooblaščen neposredni ali oddaljeni dostop do prostorov, informacij oziroma nadzornih sistemov kritičnega subjekta. Kritični subjekt lahko v skladu z oceno tveganja predloži zahtevek za preverjanje preteklosti tudi za zaposlene pri pogodbenih izvajalcih (17. člen). Za kritične subjekte je pomembna tudi določba o mogoči uporabi evropskih in mednarodnih standardov ter tehničnih specifikacij veljavnih ukrepov za varnost in odpornost kritičnih subjektov (18. člen) ter določba o izvršbi in stečaju kritičnega subjekta (19. člen).

Predlog zakona v okviru V. poglavja določa postopek ugotavljanja kritičnih subjektov posebnega evropskega pomena. Tak status lahko dobi kritični subjekt, ki ga je kot takega določila vlada, če opravlja enake ali podobne bistvene storitve šestim ali več državam članicam oziroma v šestih ali več državah članicah, in ga je Evropska komisija uradno obvestila, da je določen kot kritični subjekt posebnega evropskega pomena (20. člen). Ti so zaradi svojega pomena med drugim pri Evropski komisiji deležni svetovanja in podpore ter tudi ocenjevanja ustreznosti načrtovanih ukrepov za odpornost (21. člen).

Predlog zakona v VI. poglavju podrobneje ureja naloge organov in organizacij na področju kritične infrastrukture, in sicer: vlade, nosilcev sektorjev kritične infrastrukture, kritičnih subjektov, ministrstva, pristojnega za obrambo in koordinacijske skupine. Vlada je najvišji državni organ, ki določa, usmerja in usklajuje politiko na področju kritične infrastrukture (22. člen). Nosilci sektorjev kritične infrastrukture med drugimi nalogami usmerjajo kritične subjekte in zagotavljajo strokovno pomoč pri njihovem načrtovanju ukrepov za odpornost (23. člen). Kritični subjeki so ne glede na lastniško strukturo kritične infrastrukture prvi in najneposredneje pristojni in odgovorni ter tudi poslovno zainteresirani za zagotavljanje neprekinjenega opravljanja bistvenih storitev in delovanje kritične infrastrukture (24. člen). Ministrstvo za obrambo je v vlogi pristojnega nacionalnega organa na področju kritične infrastrukture pristojno za usmerjanje in usklajevanje dejavnosti na področju kritične infrastrukture v Republiki Sloveniji (25. člen). Koordinacijska skupine za usklajevanje upravljanja izrednega dogodka na področju kritične infrastrukture, ki jo imenuje vlada, se aktivira ob izrednih dogodkih, kadar je potreben usklajen in učinkovit odziv na izredne dogodke (26. člen).

VII. poglavje predloga zakona vsebuje glavna sistemska določila glede zagotavljanja podatkovne podpore odločanju, zgodnjega opozarjanja in poročanja na področju kritične infrastrukture. Vzpostavlja podlago za oblikovanje sistema zgodnjega opozarjanja na področju kritične infrastrukture in mehanizma prigrasitve izrednih dogodkov. Namen vzpostavitve sistema zgodnjega opozarjanja sta zaznavanje in analiza razlik v vrednostih kazalnikov po posameznih sektorjih, preden te prerastejo v izredne dogodke ali motnje pri opravljanju bistvenih storitev (27. člen). V povezavi z 29. členom predloga zakona o obveznosti prigrasitve izrednih dogodkov se pričakuje, da bodo kritični subjeki brez odlašanja posredovali razpoložljive informacije, ki jih pristojni organi in organizacije potrebujejo za odločanje. To pristojnim organom, organizacijam in telesom kriznega upravljanja (Svet za nacionalno varnost, sekretariata Sveta za nacionalno varnost, operativna skupina sekretariata Sveta za nacionalno varnost, Nacionalni center za krizno upravljanje in medresorska analitična skupina) omogoča hiter in ustrezen odziv na izredne dogodke ter celovit pregled vpliva, narave, vzroka in morebitnih posledic izrednih dogodkov, s katerimi se spoprijemajo kritični subjeki. Predvideno je, da bodo za ta namen uporabili digitalno platformo, ki jo bo vzpostavil pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost. V letno poročanje o zagotavljanju neprekinjenega delovanja kritične infrastrukture in opravljanju bistvene storitve so po predlogu zakona vključeni vsi trije glavni izvajalci dejavnosti na področju kritične infrastrukture – kritični subjeki, nosilci sektorjev kritične infrastrukture in ministrstvo, pristojno za obrambo. Zadnje bo v skladu s predlogom zakona pristojno za poročanje vladi o zagotavljanju neprekinjenega delovanja vse kritične infrastrukture in opravljanju

bistvenih storitev, medtem ko bodo kritični subjekti in nosilci sektorjev kritične infrastrukture poročali o zagotavljanju neprekinjenega delovanja kritične infrastrukture in opravljanju bistvenih storitev z vidika svoje ravni delovanja. V poročilih se navedejo tudi predlogi ukrepov za izboljšanje stanja na področju kritične infrastrukture, ki morajo biti finančno, materialno in kadrovske utemeljeni (28. člen). 30. člen ZKI predstavlja zakonsko podlago za zbiranje, obdelovanje, uporabo in hrambo podatkov o odgovornih ter kontaktnih osebah nosilcev sektorjev kritične infrastrukture in kritičnih subjektov.

Podatki, ki se nanašajo na ugotavljanje, določanje in odpornost kritičnih subjektov ter kritične infrastrukture in so določeni kot tajni podatki ali poslovna skrivnost, se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost (31. člen).

Nadzor nad izvajanjem določb ZKI bo izvajal inšpektorat, pristojen za obrambo. Čeprav lahko inšpektorat, pristojen za obrambo, v skladu z obstoječimi predpisi in uveljavljenim načinom dela k inšpekcijskemu nadzoru pritegne tudi druge inšpekcijske organe, ki imajo stvarne pristojnosti na področju sektorja kritične infrastrukture, 32. člen predloga zakona v skladu z določbami Direktive 2022/2557 vzpostavlja zakonsko podlago in možnost, da lahko navedeni inšpektorat od bistvenih subjektov, določenih na podlagi zakona, ki ureja informacijsko varnost, zahteva predložitev informacij za oceno, ali ukrepi, ki so jih ti sprejeli za zagotovitev svoje odpornosti, izpolnjujejo zahteve iz 15. člena predloga zakona, in dokazov o učinkovitem izvajanju teh ukrepov. Hkrati vzpostavlja podlago tudi za to, da lahko inšpektorat, pristojen za obrambo, 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 glede tega posreduje informacije. V skladu z določbami Direktive 2022/2555 in predlogom novega zakona, ki bo urejal informacijsko varnost, bodo namreč kritični subjekti, določeni na podlagi tega predloga zakona, tudi zavezanci po zakonu, ki ureja informacijsko varnost, in je tako v tem členu opredeljeno sodelovanje navedenih nadzornih organov smiselno.

V predlogu zakona so naštetih prekrški pri izvajanju zakona, zaradi katerih se kaznujeta kritični subjekt kot pravna oseba in odgovorna oseba kritičnega subjekta (33. člen). 34. člen 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.

V prehodnih določbah predloga zakona je za vlado, ministrstvo in kritične subjekte določen rok, v katerem morajo opraviti glavne oziroma izhodiščne naloge (sprejem izvršilnega predpisa in aktov ter poročanje Evropski komisiji), ki so povezane z ugotavljanjem, določanjem in odpornostjo kritičnih subjektov ter njihove kritične infrastrukture za zagotavljanje neprekinjenega opravljanja bistvenih storitev in so jim naložene s predlogom zakona (35. člen).

Da bi se izognili pravni praznini, se uporaba ZKI in Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije za kritično infrastrukturo Republike Slovenije ter pristojne organe in organizacije, določene na podlagi ZKI, podaljša do določitve kritičnih subjektov na podlagi predloga zakona. Z uveljavitvijo predloga zakona (37. člen) bodo ZKI, Uredba o evropski kritični infrastrukturi in navedeno navodilo prenehali veljati (36. člen).

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

Predlog zakona nima vpliva na državni proračun. Izvajanje ZKI 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 finančna sredstva za izvedbo obravnavanih ukrepov, ki jih naloži državni organ, zagotovila iz državnega proračuna. Višina potrebnih finančnih sredstev in način njihovega zagotavljanja sta v takem primeru odvisna od konkretnih razmer in ju ni mogoče vnaprej oceniti.

Sprejem zakona ne bo imel finančnih posledic na druga javna finančna 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**

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

#### **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. Države članice Evropske unije jo morajo prenesti v svojo zakonodajo do 17. oktobra 2024 (prvi odstavek 26. člena Direktive 2022/2557), kar pomeni, da v državah članicah trenutno še poteka postopek njenega prenosa v nacionalno zakonodajo. Tako ni mogoče prikazati pravne ureditve drugih držav članic zaradi prenosa Direktive 2022/2557 v zakonodajo, temveč je predstavljen prikaz obstoječe ureditve področja kritične infrastrukture v Portugalski, Romuniji, Madžarski in Češki.

Predlog zakona je usklajen s pravnim redom EU.

##### **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 so se določile in prilagodile tudi struktura ter naloge vladnega centra za upravljanje računalniških omrežij (CEGER) za prihodnje izzive, kot so izvajanje načrta za okrevanje in odpornost, strategije za inovacije in posodobitev državne in javne uprave za obdobje 2020–2023 ter akcijskega načrta za digitalni prehod Portugalske. V zakonu so 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 ter evropske kritične infrastrukture v pomembnih sektorjih. Zakon operaterjem kritične infrastrukture in sektorskim subjektom nalaga zagotavljanje zaščite ter odpornosti storitev. V zakonu sta 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 na Portugalskem 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 pripraviti 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 voda, prehrana, zdravstvo, finančne storitve ter sektor obrambe in varnosti.

##### **Romunija**

Romunija je z zakonom o opredelitvi, določitvi in zaščiti kritične infrastrukture iz leta 2010 (Monitorul Oficial nr. 757/12 Noiembrie 2010) v svoj pravni red prenesla direktivo Sveta (ES) št. 114/2008. Zakon ureja nacionalno in evropsko kritično infrastrukturo in določa kriterije 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 se upoštevajo število mrtvih in poškodovanih oseb, posledice prenehanja zagotavljanja dobrin in storitev za gospodarstvo ter prebivalstvo itn. 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 ter sektor kulture. Zakon opredeljuje tudi vlogo Nacionalnega koordinacijskega centra za zaščito kritične infrastrukture, ki deluje v okviru ministrstva, pristojnega za notranje zadeve, in zagotavlja strateško načrtovanje, usklajevanje, nenehno spremljanje ter nadzor nad izvajanjem dejavnosti, opredeljenih v zakonu.

### **Madžarska**

Madžarska je področje kritične infrastrukture uredila z zakonom, ki ga je sprejela leta 2012. Zakon CLXVI o opredelitvi, določitvi in zaščiti kritičnih sistemov in objektov (madž. 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. 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. V skladu z zakonom morajo poročilo o opravljeni identifikacijski oceni predložiti pristojnemu organu za posamezni sektor, ki ga pregleda in oceni ustreznost izpolnjevanja horizontalnih ter sektorskih kriterijev za določitev izvajalcev bistvenih storitev. Če sta izpolnjena vsaj en sektorski kriterij in vsaj en horizontalni kriterij, 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**

Češka je področje kritične infrastrukture uredila z zakonom, sprejetim leta 2000 (Zákon č. 240/2000 Sb), v njem pa je 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 presečne in sektorske kriterije za ugotavljanje ter določanje elementov kritične infrastrukture. Presečni kriteriji za določitev elementa kritične infrastrukture, kot jih opredeljuje zakon, so 250 smrtnih žrtev ali več kot 2500 oseb, ki potrebujejo hospitalizacijo, gospodarski vpliv na bruto domači proizvod v višini več kot 0,5 odstotka in vpliv na zmanjšanje zagotavljanja osnovnih storitev, ki bi prizadelo več kot 125.000 ljudi. Uredba določa devet sektorjev, in sicer energetiko, upravljanje voda, prehrano in kmetijstvo, zdravstvo, promet, komunikacijske in informacijske sisteme, finančne trge, reševalne službe ter javno upravo. 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:**

Na ministrstvih, ki bodo na podlagi predloga zakona določena za nosilce novih sektorjev kritične infrastrukture, bo lahko uresničevanje njihovih pristojnosti in odgovornosti na področju kritične infrastrukture zahtevalo zaposlitev dodatnih javnih uslužbencev, bo pa potrebno tudi 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, javne 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 Ustavno sodišče, sodstvo, Državni zbor Republike Slovenije, Varuha človekovih pravic ter Banko Slovenije izključeni iz njegove uporabe.

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

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

**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 do zdaj na podlagi ZKI niso imeli statusa upravljavca kritične infrastrukture Republike Slovenije in niso bili zavezani k pripravi 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. Glede tega je pomembna določba 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.

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 prekinitve delovanja infrastrukture, ki jo upravlja, naložba subjekta v lastno varnost in zaščito pa dolgoročno navadno pozitivno 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 ter 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, in sicer ministrstvom ter vladnim službam kot nosilcem sektorjev kritične infrastrukture in kritičnim subjektom, na seminarjih oziroma delavnicah, 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:**

Glede predloga zakona ni drugih pomembnih okoliščin.

**7. Prikaz sodelovanja javnosti pri pripravi predloga zakona:**

Javna objava predloga zakona na portalu e-Demokracija, na katerega je bilo mogoče sporočiti mnenja, predloge in pripombe, je trajala od \_\_\_\_ do 2024. Hkrati je bil predlog zakona objavljen na spletnih straneh Ministrstva za obrambo.

**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:**

- dr. Robert Golob, predsednik Vlade RS v funkciji ministra za obrambo,
- dr. Damir Črnčec, državni sekretar, Ministrstvo za obrambo,
- Boštjan Pavlin, mag., generalni direktor Direktorata za obrambne zadeve, Ministrstvo za obrambo,
- Anica Ferlin, vodja Sektorja za civilno obrambo, Direktorat za obrambne zadeve, Ministrstvo za obrambo,
- Igor Nered, sekretar v Kabinetu ministra, Ministrstvo za obrambo.

## II. BESEDILO ČLENOV

### ZAKON

#### o kritični infrastrukturi

#### I. SPLOŠNE DOLOČBE

##### 1. člen

(vsebina zakona)

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

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

##### 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 in razveljavitvi Direktive Sveta 2008/114/ES (UL L št. 333 z dne 27. 12. 2022, str. 164; v nadaljnjem besedilu: Direktiva 2022/2557/EU).

##### 3. člen

(področje uporabe zakona)

(1) Ta zakon se uporablja za javne in 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 IV., V. in IX. poglavje tega zakona ne uporabljajo.

(3) Ta zakon se ne uporablja za subjekte javne uprave ter za organe oblasti, v delu, ko gre za izvajanje svojih dejavnosti na področju nacionalne varnosti, javne 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, ter za Ustavno sodišče, sodstvo, Državni zbor Republike Slovenije, Varuha človekovih pravic in Banko Slovenije.

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

##### 4. 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 je dogodek, ki bi lahko povzročil pomembne motnje ali, ki povzroči motnje v opravljanju bistvene storitve, razen dogodkov, ki jih kot incidente opredeljuje zakon, ki ureja informacijsko varnost;
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. 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);
5. kritični subjekt je javni ali zasebni subjekt, ki ima kritično infrastrukturo, s katero opravlja bistveno storitev;
6. nosilci sektorjev kritične infrastrukture so ministrstva in službe Vlade Republike Slovenije (v nadaljnjem besedilu: vlada), ki so odgovorni za delovna področja, na katera spada kritična infrastruktura;
7. ocena tveganja je postopek ugotavljanja narave in obsega tveganja s prepoznavanjem in analiziranjem morebitnih pomembnih groženj, ranljivosti in nevarnosti, ki bi lahko privedle do izrednega dogodka, ter vrednotenja možnosti izgube sposobnosti opravljanja bistvene storitve ali motenj, ki jih ta izredni dogodek povzroči pri opravljanju bistvene storitve;
8. 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 in po njem okreva;
9. 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);
10. povečana ogroženost kritične infrastrukture je stanje, ki ga zazna pristojni državni organ in za katerega oceni, da bi lahko povzročil izredni dogodek;
11. 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 na podlagi tega zakona (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;
12. pristojni nacionalni organ na področju kritične infrastrukture je ministrstvo, pristojno za obrambo (nadaljnjem besedilu: ministrstvo);
13. sektorji kritične infrastrukture so posamezne vsebinsko zaokrožene celote delovanja kritičnih subjektov, ki opravljajo bistvene storitve;
14. 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.

## II. NACIONALNI OKVIR ZA ODPORNOST KRITIČNIH SUBJEKTOV

### 5. člen

(strategija za odpornost kritičnih subjektov)

(1) Vlada sprejme strategijo za odpornost kritičnih subjektov (v nadaljnjem besedilu: strategija).

(2) V strategiji se določijo cilji in ukrepi za doseganje in ohranjanje visoke ravni odpornosti kritičnih subjektov v vseh sektorjih kritične infrastrukture. 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. ukrepe 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 krepitev sodelovanja med subjekti javne uprave in zasebnimi subjekti;
6. seznam drugih organov in organizacij, ki sodelujejo pri izvajanju strategije;
7. usklajevanje med pristojnimi organi in organizacijami na področju kritične infrastrukture ter pristojnimi organi na podlagi zakona, ki ureja informacijsko varnost za izmenjavo informacij o tveganjih za kibernetično varnost, o kibernetičnih grožnjah in incidentih ter nekibernetičnih tveganjih, grožnjah in izrednih dogodkih ter opravljanju nadzora;
8. veljavne sprejete ukrepe malih in srednjih podjetij za lažje izvajanje obveznosti iz IV. poglavja tega zakona.

(3) Nosilci sektorjev kritične infrastrukture (v nadaljnjem besedilu: nosilci sektorjev) 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.

## **6. člen**

(nacionalna ocena tveganja za opravljanje bistvenih storitev)

(1) Vlada določi bistvene storitve in sprejme nacionalno oceno tveganja za opravljanje bistvenih storitev (v nadaljnjem besedilu: nacionalna ocena tveganja).

(2) V nacionalni oceni tveganja se upoštevajo tveganja za opravljanje bistvenih storitev, vključno s tveganji medsektorske in čezmejne narave.

(3) Pri izdelavi nacionalne ocene tveganja 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) 2017/1938 Evropskega parlamenta in Sveta o ukrepih za zagotavljanje zanesljivosti oskrbe s plinom (UL L 280 z dne 28. 10. 2017, str. 1) in (EU) 2019/941 Evropskega parlamenta in Sveta o pripravljenosti na tveganja v sektorju električne energije (UL L 158 z dne 14. 6. 2019, str. 1) ter z direktivama 2007/60/ES o oceni in obvladovanju poplavne ogroženosti (UL L 288 z dne 6. 11. 2007, str. 27) ter 2012/18/EU Evropskega parlamenta in Sveta o obvladovanju nevarnosti večjih nesreč, v katere so vključene nevarne snovi ES (UL L 197 z dne 24. 7. 2012, str. 1);
3. pomembna tveganja, ki izhajajo iz soodvisnosti sektorjev in odvisnosti sektorjev od drugih subjektov, ki so v državi, drugih državah članicah Evropske unije (v nadaljnjem besedilu: države članice EU) in tretjih državah;
4. vpliv, ki bi ga pomembna motnja v enem sektorju lahko imela v drugih sektorjih, vključno s pomembnimi tveganji za državljane in notranji trg;
5. informacije o izrednih dogodkih, priglašeni v skladu s 29. členom tega zakona.

(4) Nosilci sektorjev kritičnim subjektom posredujejo potrebne informacije o nacionalni oceni tveganja, prepoznanih tveganjih in drugih bistvenih elementih, ki so jim v pomoč pri izdelavi njihove ocene tveganja in sprejemanju ukrepov za odpornost.

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

### III. UGOTAVLJANJE IN DOLOČANJE KRITIČNIH SUBJEKTOV TER KRITIČNE INFRASTRUKTURE

#### **7. člen**

(sektorji kritične infrastrukture)

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

(2) Vlada določi podsektorje in nosilce sektorjev iz prejšnjega odstavka ter sodelujoče organe.

#### **8. člen**

(kriteriji za ugotavljanje kritičnih subjektov)

(1) Vlada določi kategorije subjektov, med katerimi nosilci sektorjev ugotavljajo kritične subjekte.

(2) Nosilci sektorjev pri ugotavljanju kritičnih subjektov upoštevajo strategijo iz 5. člena tega zakona, rezultate nacionalne ocene tveganja in naslednje kriterije:

- subjekt opravlja eno ali več bistvenih storitev;
- subjekt deluje in njegova kritična infrastruktura je 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 od njih 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 imel 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, ki se uporabljajo za določitev enega ali več kriterijev iz prejšnjega odstavka, določi vlada.

#### **9. člen**

(določitev kritičnih subjektov)

(1) Nosilci sektorjev pri pripravi predlogov za določitev kritičnih subjektov in njihove kritične infrastrukture upoštevajo kriterije iz drugega in tretjega odstavka 8. člena tega zakona. Ministrstvo predlog za določitev kritičnih subjektov in kritične infrastrukture posreduje vladi.

(2) Kritične subjekte in njihovo kritično infrastrukturo določi vlada, o čemer ministrstvo obvesti kritične subjekte v enem mesecu od določitve.

(3) Za kritične subjekte se IV. poglavje tega zakona začne uporabljati deset mesecev po njihovi določitvi.

(4) Nosilci sektorjev bančništva, infrastrukture finančnega trga in digitalne infrastrukture v enem mesecu od njihove določitve obvestijo kritične subjekte v teh sektorjih, da nimajo obveznosti iz IV. poglavja tega zakona, ter da se zanje ne uporablja IX. poglavje tega zakona.

(5) Ministrstvo obvesti kritične subjekte o prenehanju statusa kritičnega subjekta in tem, da zanje od datuma tega uradnega obvestila ne veljajo več obveznosti iz IV. poglavja tega zakona.

(6) 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 in ki se lahko predložijo kot take ali v zbirni obliki.

#### **10. člen**

(enotna kontaktna točka)

(1) Ministrstvo je enotna kontaktna točka, ki ima povezovalno vlogo in zagotavlja sodelovanje med pristojnimi organi in organizacijami, čezmejno sodelovanje z enotnimi kontaktnimi točkami držav članic EU in 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 na področju kibernetске varnosti, kibernetских groženj in incidentov ter drugih 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.

#### **11. člen**

(podpora kritičnim subjektom)

(1) Nosilci sektorjev in ministrstvo kritičnim subjektom pri krepitvi njihove odpornosti zagotavljajo podporo z različnimi ukrepi, kot so zlasti strokovna pomoč ter organizacija usposabljanj in vaj za preverjanje njihove odpornosti.

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

(3) Ministrstvo kritičnim subjektom zagotavlja podporo tudi prek komunikacijskega in informacijskega omrežja NCKU, ki omogoča sprejemanje, spremljanje in obdelavo podatkov za vzpostavitev centralne slike delovanja kritične infrastrukture in sistema zgodnjega opozarjanja ter predikcije potencialnih izrednih dogodkov na podlagi obvestil kritičnih subjektov.

(4) Izmenjava informacij o izrednih dogodkih in dogodkih, ki jih kot incidente opredeljuje zakon, ki ureja informacijsko varnost 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.

### **IV. ODPORNOST KRITIČNIH SUBJEKTOV IN KRITIČNE INFRASTRUKTURE**

#### **12. 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 njej vključeni pristojni organi in organizacije ter da se pri tem upoštevajo različne vrste nevarnosti, da izhaja iz ocen tveganja ob upoštevanju soodvisnosti sektorjev kritične infrastrukture ter njihovih medsebojnih vplivov;
2. načelo odgovornosti, v skladu s katerim so za zagotavljanje bistvenih storitev in delovanje kritične infrastrukture neposredno odgovorni kritični subjekti, za krepitev odpornosti kritične infrastrukture in kritičnih subjektov pa 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 in delovanje kritične infrastrukture ter s presojo 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 in 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, oziroma drugimi področnimi predpisi, ki urejajo varovane podatke.

### **13. člen**

(načrt za odpornost)

(1) Načrt za odpornost kritičnih subjektov (v nadaljnjem besedilu: načrt za odpornost) obsega oceno tveganja kritičnega subjekta iz 14. člena tega zakona in ukrepe za odpornost iz 15. člena tega zakona.

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

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

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

### **14. člen**

(ocena tveganja kritičnega subjekta)

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

(2) V oceni tveganja kritičnega subjekta kritični subjekt upošteva tveganja, ki bi lahko povzročila izredni dogodek, vključno s tveganji medsektorske in čezmejne narave. Upošteva tudi 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 kritični subjekti tudi v sosednjih državah članicah EU in tretjih državah.

(3) Za pripravo ocene tveganja kritičnega subjekta lahko kritični subjekt uporabi ocene tveganja ali druge dokumente, pripravljene v skladu z drugimi predpisi, pomembne za izdelavo njegove ocene tveganja, ki jih je pripravil v skladu z drugimi predpisi.

## **15. člen** (ukrepi za odpornost)

(1) Kritični subjekt na podlagi nacionalne ocene tveganja in svoje ocene tveganja kritičnega subjekta sprejme ustrezne ter sorazmerne tehnične, varnostne, organizacijske in druge ukrepe za odpornost, potrebne za:

1. preprečevanje nastanka izrednega dogodka;
2. zagotovitev ustrezne fizične zaščite svojih prostorov in kritične infrastrukture;
3. neprekinjeno zagotavljanje bistvenih storitev in delovanja kritične infrastrukture ob upoštevanju medsebojne soodvisnosti sektorjev kritične infrastrukture;
4. zagotovitev nadomestnih sistemov, ki omogočajo opravljanje bistvenih storitev;
5. zagotovitev ustreznega upravljanja in nadzora primarnih in alternativnih dobavnih verig;
6. zagotovitev zalog sredstev in opreme, potrebnih za opravljanje bistvene storitve;
7. odzivanje na izredne dogodke, za 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 določitvi delovnih mest, pomembnih za opravljanje bistvene storitve, upoštevajo tudi naloge, ki jih opravljajo zunanji ponudniki.

(3) Ukrepi za odpornost so stalni in dodatni. Stalni ukrepi za odpornost se izvajajo v vseh razmerah, ob povečani ogroženosti kritičnega subjekta in kritične infrastrukture ali izrednem dogodku pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi za odpornost se izvajajo ob povečani ogroženosti kritičnega subjekta in 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 kritičnega subjekta načrtujejo in izvajajo kritični subjekti.

(5) Kritični subjekti dodatne ukrepe za odpornost načrtujejo na podlagi ocene tveganja kritičnega subjekta 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 tega člena 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 z navedenimi predpisi.

(9) Kritični subjekt lahko sprejme ukrepe za odpornost na podlagi načrtov ali dokumentov, ki jih je pripravil v skladu z drugimi predpisi.

#### **16. člen**

(posodabljanje načrta za odpornost)

(1) Kritični subjeki 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, mora kritični subjekt ustrezno spremeniti načrt za odpornost najpozneje v enem mesecu od nastanka takih okoliščin. K tako spremenjenemu načrtu za odpornost je treba pridobiti odobritev pristojnega nosilca sektorja.

#### **17. člen**

(preverjanje preteklosti)

(1) Kritični subjekt ob upoštevanju nacionalne ocene tveganja in ocene tveganja kritičnega subjekta lahko predloži zahtevek za preverjanje preteklosti zaposlenih ter kandidatov za zaposlitev na delovnih mestih, pomembnih za opravljanje bistvenih storitev kritičnega subjekta, ki imajo ali bodo imeli pooblastilo za neposredni ali oddaljeni dostop do prostorov, informacij ali nadzornih sistemov kritičnega subjekta. Kritični subjekt lahko v skladu z oceno tveganja predloži zahtevek za preverjanje preteklosti tudi za zaposlene pri pogodbenih izvajalcih.

(2) Preverjanje preteklosti osebe iz prejšnjega odstavka se po njenem predhodnem soglasju opravi, da se:

- potrdi identiteta osebe, katere preteklost se preverja;
- preverijo kazenske evidence Republike Slovenije, držav članic EU in tretjih držav glede zapisov pravnomočnih kazenskih obsodb za kazniva dejanja, ki se preganjajo po uradni dolžnosti, ki so po oceni kritičnega subjekta sporna z vidika opravljanja nalog na določenem delovnem mestu oziroma za izvedbo pogodbenih obveznosti.

(3) Če oseba iz prejšnjega odstavka ne da soglasja za preverjanje preteklosti, se ji delo na delovnih mestih in v prostorih iz prvega odstavka tega člena ne dovoli oziroma pogodba ne sklene.

(4) Preverjanje preteklosti osebe iz prvega odstavka tega člena, ki je državljan Republike Slovenije ali tuje države, po predložitvi zahtevka kritičnega subjekta in soglasja osebe iz prvega odstavka tega člena opravijo zaproseni državni organi, ki pridobijo dokazila iz drugega odstavka tega člena po uradni dolžnosti iz uradnih evidenc, če je to mogoče. Preverjanja preteklosti so sorazmerna in omejena na vrednotenje morebitnega tveganja za opravljanje bistvene storitve kritičnega subjekta.

#### **18. člen**

(standardi)

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

#### **19. 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 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 finančno poslovanje, postopke zaradi insolventnosti in prisilno prenehanje poslovanja, razen če se z izvršbo ali prodajo v postopku stečaja oziroma 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 neprekinjeno delovanje kritične infrastrukture, opravljajo v nezmanjšanem obsegu.

## V. KRITIČNI SUBJEKTI POSEBNEGA EVROPSKEGA POMENA

### 20. 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 oziroma v šestih ali več državah članicah;
- je bil uradno obvešččen 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 oziroma 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) Ministrstvo na podlagi odločitve Evropske komisije, da kritični subjekt iz prejšnjega odstavka tega člena opravlja bistvene storitve za šest ali več držav članic oziroma v šestih ali več državah članicah kritični subjekt, 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.

### 21. člen

(svetovalne misije)

(1) Ministrstvo lahko od Evropske komisije zahteva organiziranje svetovalne misije iz 18. člena Direktive 2022/2557/EU za oceno ukrepov za odpornost kritičnih subjektov posebnega evropskega pomena.

(2) Nosilec sektorja v sodelovanju s kritičnim subjektom posebnega evropskega pomena na pobudo Evropske komisije ali zahtevo ene oziroma več držav članic EU, za katere se oziroma v katerih se opravlja bistvena storitev, Evropski komisiji zagotovi:

- oceno tveganja kritičnega subjekta;
- seznam ukrepov za odpornost kritičnega subjekta iz 15. člena tega zakona;

- informacije o ukrepih za odpornost kritičnega subjekta iz 15. člena tega zakona, 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 iz prvega odstavka tega člena 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 iz prvega odstavka tega člena in mnenje Evropske komisije o svojih ugotovitvah glede ustreznosti ukrepov za odpornost.

## VI. NALOGE NA PODROČJU KRITIČNE INFRASTRUKTURE

### **22. 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 VII. poglavju tega zakona.

### **23. člen**

(nosilci sektorjev kritične infrastrukture)

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

- oblikujejo pobudo in sodelujejo pri pripravi predloga kriterijev za ugotavljanje kritičnih subjektov in njihovih mejnih vrednosti;
- oblikujejo pobudo in sodelujejo pri pripravi predloga za določitev kritičnih subjektov in njihove kritične infrastrukture iz svoje pristojnosti;
- usklajujejo predloge ukrepov za odpornost kritičnih subjektov v sektorju kritične infrastrukture iz svoje pristojnosti;
- usmerjajo kritične subjekte in zagotavljajo strokovno pomoč pri njihovem načrtovanju ukrepov za odpornost;
- 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 in ministrstvom (v nadaljnjem besedilu: kontaktna oseba nosilca sektorja).

### **24. 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).

**25. 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, naslednje naloge:

- na predlog nosilcev sektorjev pripravlja predloge za določitev kriterijev za ugotavljanje kritičnih subjektov in njihovih mejnih vrednosti;
- na predlog nosilcev sektorjev pripravlja predloge za določitev kritičnih subjektov;
- usklajuje predloge ukrepov za odpornost med sektorji kritične infrastrukture.

**26. člen**  
(koordinacijska skupina)

(1) Vlada imenuje koordinacijsko skupino za usklajevanje upravljanja izrednega dogodka, ukrepe za ublažitev posledic izrednega dogodka, zagotovitev čimprejšnjega ponovnega nemotnega delovanja kritične infrastrukture in opravljanje bistvenih storitev, ki jih ministrstvo predloži vladi.

(2) Koordinacijsko skupino iz prejšnjega odstavka, ki jo vodi ministrstvo, 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, in Slovenske obveščevalno-varnostne agencije.

(3) Koordinacijsko skupino iz prvega odstavka tega člena aktivira ministrstvo ob izrednih dogodkih iz 29. člena tega zakona, kadar je potreben usklajen in učinkovit odziv na izredni dogodek.

(4) Ministrstvo skupino skliče najmanj enkrat na leto, po potrebi pa pogosteje.

VII. ZAGOTAVLJANJE PODPORE ODLOČANJU, ZGODNJE OPOZARJANJE IN POROČANJE

**27. člen**

(zagotavljanje podpore odločanju in zgodnje opozarjanje)

(1) Zagotavljanje podpore odločanju temelji na načelu izmenjave podatkov in informacij ter varovanja podatkov iz 12. člena tega zakona.

(2) Za zgodnje opozarjanje na področju kritične infrastrukture nosilci sektorjev in kritični subjekti zagotavljajo 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 soočajo kritični subjekti. Sistem zgodnjega opozarjanja 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 29. člena tega zakona zbira, obdeluje, uporablja ter hrani digitalizirane, avtomatizirane, agregirane in anonimizirane podatke.

(4) NCKU o motnjah in morebitnih grožnjah obvesti Svet za nacionalno varnost, sekretariat Sveta za nacionalno varnost, operativno skupino sekretariata Sveta za nacionalno varnost in medresorsko analitično skupino, 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) V primeru povečane ogroženosti kritične infrastrukture pristojni državni organi z zaznano grožnjo seznanijo nosilca sektorja, ta pa kritični subjekt.

## **28. 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 prekinitve zagotavljanja bistvene storitve z negativnimi materialnimi in drugimi posledicami za delovanje sektorja, glede tega izvedeni ukrepi in rešitve ter 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.

## **29. člen** (priglasitev izrednih dogodkov)

(1) Kritični subjekti morajo pristojnemu nosilcu sektorja, NCKU in ministrstvu takoj priglasiti izredne dogodke, ki povzročijo ali bi lahko povzročili pomembno motnjo pri opravljanju bistvenih storitev, oziroma predložiti priglasitev najpozneje v 24 urah po tem, ko se seznanijo z izrednim dogodkom. Najpozneje v enem mesecu od seznanitve z izrednim dogodkom priglasitvi sledi natančno poročilo o tem izrednem dogodku. Za določitev pomembnosti motnje se upošteva zlasti naslednje:

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

(2) Priglasitev 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 prek 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 EU, ministrstvo tak izredni dogodek priglasijo 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 z 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 prizadetih držav članic EU, kadar izredni dogodek pomembno vpliva ali bi lahko pomembno vplival na kritične subjekte in neprekinjeno opravljanje bistvenih storitev za eno ali več držav članic EU oziroma v eni ali več državah članicah

EU. Enotne kontaktne točke prizadetih držav informacije obravnavajo tako, da spoštujejo njihovo zaupnost in varujejo varnost ter 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 iz prvega odstavka tega člena ter razsežnosti izrednega dogodka, pristojni nosilec sektorja o njem obvesti javnost. Če pristojni nosilec sektorja skupaj z ministrstvom pripravi sporočilo za javnost z navedbo pomembnih dejstev ter izvedenih ukrepov, ga mediji smejo objaviti le v nespremenjeni obliki.

### **30. člen**

(podatki o odgovornih 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 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 in kontaktnih osebah nosilcev sektorjev in kritičnih subjektov zbira, obdeluje, uporablja in hrani ministrstvo.

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

## **VIII. VAROVANJE PODATKOV**

### **31. člen**

(varovanje podatkov)

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.

## **IX. NADZOR**

### **32. člen**

(izvajanje nadzora)

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

(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 15. 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 bistvenega subjekta, identificiranega na podlagi zakona, ki ureja informacijsko varnost, in določenega za kritični subjekt na podlagi tega zakona, ter da mu glede tega posreduje informacije.

## X. KAZENSKÉ DOLOČBE

### 33. člen

(prekrški)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik, če :

1. ne pripravi ali hrani načrta za odpornost (drugi odstavek 13. člena);
2. ne posreduje načrta za odpornost nosilcu sektorja v odobritev (tretji odstavek 13. člena);
3. ne pripravi ocene tveganja (prvi odstavek 14. člena) ali v njej ne upošteva tveganja, ki bi lahko povzročila izredni dogodek, vključno s tveganji medsektorske in čezmejne narave ali stopnjo odvisnosti drugih sektorjev kritične infrastrukture od bistvene storitve, ki jo opravlja kot kritični subjekt ali stopnjo njegove odvisnosti od bistvenih storitev, ki jih opravljajo kritični subjekti drugih sektorjev kritične infrastrukture ali kritični subjekti tudi v sosednjih državah članicah EU in tretjih državah (drugi odstavek 14. člena);
4. na podlagi nacionalne ocene tveganja in svoje ocene tveganja ne sprejme ustreznih ter sorazmernih tehničnih, varnostnih, organizacijskih in drugih ukrepov (prvi odstavek 15. člena), ali ne upošteva nalog, ki jih opravljajo zunanji ponudniki, pri določitvi delovnih mest, pomembnih za opravljanje bistvene storitve (drugi odstavek 15. člena);
5. ne posodablja redno načrta za odpornost (16. člen);
6. ob nastanku novih okoliščin, ki lahko pomembno vplivajo na zagotavljanje bistvene storitve in delovanje kritične infrastrukture v predpisanem roku ne spremeni načrta za odpornost ali k tako spremenjenemu načrtu ne pridobi odobritve pristojnega nosilca sektorja (drugi odstavek 16. člena)
7. nosilca sektorja kritične ne obvesti o dejstvih in okoliščinah, ki kažejo na možnost njegovega prenehanja poslovanja ali stečaja (prvi odstavek 19. člena);
8. ne imenuje kontaktne osebe ali več takih oseb za sodelovanje na področju kritične infrastrukture z drugimi kritičnimi subjekti, nosilci sektorjev in ministrstvom (drugi odstavek 24. člena);
9. ne izdelava vsebinsko ustreznega letnega poročila o zagotavljanju neprekinjenega delovanja kritične infrastrukture in opravljanju bistvene storitve (28. člen);
10. v predpisanem roku ne priglasijo izrednega dogodka, ki je povzročil ali bi lahko povzročil pomembno motnjo pri opravljanju bistvenih storitev (prvi odstavek 29. člen).

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

### 34. 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.

## XI. PREHODNE DOLOČBE

### **35. člen**

(sprejetje aktov in poročanje)

(1) Vlada do 17. januarja 2026 sprejme strategijo iz 5. člena tega zakona in nacionalno oceno tveganja iz 6. člena tega zakona.

(2) Vlada v šestih mesecih od uveljavitve tega zakona določi bistvene storitve iz 6. člena tega zakona, podsektorje sektorjev kritične infrastrukture, nosilce sektorjev kritične infrastrukture in sodelujoče organe iz 7. člena tega 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 tega zakona.

(4) Kritični subjekti pripravijo načrt za odpornost iz 13. člena tega zakona v devetih mesecih po prejemu obvestila o njihovi določitvi.

(5) Ministrstvo v treh mesecih od uveljavitve tega zakona Evropski komisiji sporoči, da je pristojni nacionalni organ in tudi enotna kontaktna točka, pri čemer navede kontaktne podatke.

(6) Ministrstvo Evropski komisiji posreduje strategijo iz 5. člena tega zakona in nacionalno oceno tveganja iz 6. člena tega zakona v treh mesecih od njunega sprejetja.

(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 priglašeni izrednih dogodkov in sprejetimi ukrepi.

(8) 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.

### **36. člen**

(podaljšanje uporabe)

Do določitve kritičnih subjektov iz 9. člena tega zakona se 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) uporabljata 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).

### **37. člen**

(prenehanje veljavnosti)

Z dnem uveljavitve tega zakona prenehajo veljati Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M), 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).

## XII. KONČNA DOLOČBA

### **38. člen**

(začetek veljavnosti)

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

### III. OBRAZLOŽITEV

#### K 1. členu

Člen povzema vsebino predloga zakona tako, da navaja najpomembnejše systemske elemente glede področja kritične infrastrukture, kritične infrastrukture Republike Slovenije ter postopkov ugotavljanja in določanja kritičnih subjektov ter kritične infrastrukture 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 ter organizacij na področju kritične infrastrukture, pristojnega nacionalnega organa in enotne kontaktne točke (to je v skladu z opredelitvijo v 12. točki 4. člena oziroma v 10. členu predloga zakona ministrstvo, pristojno za obrambo, v nadaljnjem besedilu: ministrstvo) ter okvir za zgodnje opozarjanje, zagotavljanje podpore odločanju, poročanje, varovanje podatkov in nadzor na področju kritične infrastrukture.

#### K 2. členu

Člen pojasnjuje namen predloga zakona, ki je prenos Direktive 2022/2557 v pravni red Republike Slovenije.

#### K 3. členu

Člen 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 nekatera poglavja izključena, za posamezne subjekte pa se zakon sploh ne bo uporabljal.

V prvem odstavku člena predloga zakona kot zavezance naslavlja javne 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. Taki subjekti bodo zakon uporabljali v celoti.

V drugem odstavku so navedeni subjekti, ki bodo na podlagi tega zakona sicer lahko določeni kot kritični subjekti, vendar se zanje IV. poglavje Odpornost kritičnih subjektov in kritične infrastrukture, V. poglavje Kritični subjekti posebnega evropskega pomena in IX. poglavje Nadzor 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 razložena 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 kibernetске 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 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 posebnega pomena ne bo uporabljal. Med te subjekte spadajo subjekti javne uprave (subjekt javne uprave po Direktivi 2022/2557 pomeni javni sektor), ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne 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 Ustavno sodišče, sodstvo, Državni zbor Republike Slovenije, Varuh človekovih pravic ter

Banko Slovenije. Zadnje navedeni subjekti so izpostavljeni, ker niso nujno subjekti javne uprave. S to določbo se sledi petemu, šestemu in sedmemu odstavku 1. člena Direktive 2022/2557, pa tudi njeni uvodni izjavi 11, ki med drugim navaja: »Ker so države članice odgovorne za zaščito nacionalne varnosti in obrambe, bi morale imeti možnost odločiti, da se obveznosti za kritične subjekte iz te direktive v celoti ali delno ne uporabljajo, če ti kritični subjekti opravljajo storitve ali izvajajo dejavnosti, ki so povezane predvsem s področjem nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preiskovanjem, odkrivanjem in pregonom kaznivih dejanj.«.

Zadnji odstavek tega 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 kibernetских tveganj Direktiva (EU) 2022/2555 nalaga celovite zahteve za velik sklop subjektov, da se zagotovi njihova kibernetična varnost. Glede na to, da je kibernetična 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 različni izvori, 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

Člen pojasnjuje pomen izrazov, ki so uporabljeni v predlogu zakona. Opredelitve izrazov so večinoma povzete po Direktivi 2022/2557, ki v ospredje pravnega okvira postavlja zagotavljanje bistvenih storitev na notranjem trgu Evropske unije oziroma se zgledujejo po obstoječih opredelitvah pojmov s področja kritične infrastrukture. Slednje so nekoliko preoblikovane v skladu s spremenjenim konceptom zaščite kritične infrastrukture ter prehodom h krepitvi odpornosti kritičnih subjektov in kritične infrastrukture, ki omogoča zagotavljanje bistvenih storitev, s čimer se je terminološko in vsebinsko zadostilo zahtevi 2. člena Direktive 2022/2557, ki je namenjena opredelitvi pojmov.

#### K 5. členu

Člen nalaga pripravo in sprejem strategije za odpornost kritičnih subjektov, ki predstavlja podlago za ugotavljanje kritičnih subjektov. Namen strategije je doseči in ohraniti visoko raven odpornosti kritičnih subjektov v vseh sektorjih kritične infrastrukture ter tako zagotoviti nemoteno opravljanje bistvenih storitev. Predlog zakona s tem členom predstavi minimalna temeljna izhodišča za pripravo strategije, s čimer prispeva k njeni bolj jasni in določni pripravi. Zaradi skladnosti in učinkovitosti je pri pripravi strategije med drugim treba upoštevati sektorske politike in strategije, pripravljene načrte, sprejete ukrepe in podobne dokumente ter tudi hibridno naravo groženj za kritične subjekte. V strategiji je treba opredeliti še sodelovanje in izmenjavo informacij med pristojnim nacionalnim organom na podlagi zakona, ki ureja informacijsko varnost, in drugimi organi in organizacijami. Predlog strategije pripravi ministrstvo v sodelovanju z nosilci sektorjev kritične infrastrukture in ga posreduje vladi v sprejem. Rok za sprejem strategije je določen v 35. členu predloga zakona, tj. do 17. januarja 2026.

#### K 6. členu

Člen določa obveznost vladi določiti bistvene storitve, kot izhodišče za pripravo nacionalne ocene, in sprejeti nacionalno oceno. Priprava nacionalne ocene tveganja pa je naloga ministrstva, 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 tem členu predstavi temeljna izhodišča za pripravo nacionalne ocene tveganja z navedbo elementov, ki jih je treba upoštevati, s čimer se zagotovi ciljno usmerjen in usklajen pristop k njeni pripravi. Pri pripravi nacionalne ocene tveganja je treba upoštevati oceno bistvenih 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 s hibridnimi grožnjami ali drugimi antagonističnimi grožnjami, vključno s terorističnimi kaznivimi dejanji, infiltracijo kriminala in sabotžo. Pri tem je treba upoštevati obstoječe splošne ali sektorske ocene tveganja, pripravljene na podlagi drugih pravnih aktov, koliko so sektorji soodvisni, tudi tisti iz drugih držav članic in tretjih držav, ter še informacije o preteklih priglašeni izrednih dogodkih. Nacionalna ocena tveganja predstavlja podlago za pripravo ocene tveganj kritičnih subjektov. Rok za njen sprejem je določen v 35. členu predloga zakona, tj. do 17. januarja 2026.

#### K 7. členu

Člen določa 11 sektorjev kritične infrastrukture, kot so določeni v prilogi Direktive 2022/2557. Sektorja energetike in prometa imata v skladu s prilogi Direktive 2022/2557 tudi podsektorje. Slednje določi vlada s podzakonskim aktom. 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 pa je usmerjati in podpirati kritični subjekt pri njihovem načrtovanju ukrepov za odpornost.

#### K 8. členu

S tem členom se določajo kriteriji za ugotavljanje kritičnih subjektov. V skladu s prvim odstavkom 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.

V drugem odstavku 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. Sledi ugotavljanje, ali subjektova kritična infrastruktura, ki se uporablja za opravljanje bistvene storitve oziroma omogoča njeno opravljanje, deluje oziroma je v Republiki Sloveniji in ali bi izredni dogodek, kot je opredeljen v 4. členu predloga zakona, imel pomembne moteče učinke oziroma posledice na subjektovo zagotavljanje bistvene storitve ali drugih bistvenih storitev v drugih sektorjih kritične infrastrukture.

V tretjem odstavku tega člena se določajo kriteriji, 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

Člen določa postopek določitve kritičnih subjektov. Prvi odstavek 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. Za kritične subjekte se IV. poglavje predloga zakona o odpornosti kritičnih subjektov in kritične infrastrukture začne uporabljati deset mesecev po njihovi določitvi.

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 rokov za izvedbo teh nalog.

Člen dodatno izpostavlja kritične subjekte, ki bodo določeni kot taki v sektorjih bančništva, infrastrukture finančnega trga in digitalne infrastrukture. Kljub določbi 3. člena predloga zakona, da so kritični subjekti v navedenih treh sektorjih kritične infrastrukture razbremenjeni obveznosti iz poglavja o odpornosti kritičnih subjektov in kritične infrastrukture in da se zanje poglavje o nadzoru ne uporablja, jih je dejansko treba določiti kot kritične subjekte. Kritične subjekte je namreč skladno s prvim odstavkom 6. člena Direktive 2022/2557 določiti v vseh sektorjih in podsektorjih kritične infrastrukture. O statusu kritičnih subjektov v navedenih treh sektorjih jih je, kot vse druge kritične subjekte treba obvestiti, ob tem pa jim sporočiti tudi, da nimajo obveznosti po predlogu zakona.

#### K 10. členu

S členom se 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, čezmejno sodelovanje z enotnimi kontaktnimi točkami drugih držav članic in Evropsko komisijo ter sodelovanje s tretjimi državami. To je ministrstvo, ki je tudi pristojni nacionalni organ na področju kritične infrastrukture, kot je opredeljeno v 4. členu predloga zakona pod zaporedno številko 12. 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 kibernetiko varnost, kibernetične grožnje in incidente ter nekibernetična 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. Tako opredeljuje sodelovanje in izmenjavo informacij s pristojnim nacionalnim organom na podlagi zakona, ki ureja informacijsko varnost.

#### K 11. členu

Člen sledi določbi 10. člena Direktive 2022/2557 o podpori držav članic kritičnim subjektom pri krepitevi njihove odpornosti. V ta namen je predvideno, da se kritičnim subjektom nudi strokovno pomoč, organizira usposabljanje zaposlenega kadra v kritičnih subjektih, izvajata in preverjata njihova pripravljenost ter odpornost, se medsebojno izmenjujejo informacije, izkušnje, dobre prakse itn.

Za izmenjavo 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 nosilci sektorjev kritične infrastrukture in upravljavci kritične infrastrukture, določeni na podlagi ZKI.

S členom se ministrstvu oziroma NCKU nalaga obveznost zagotavljanja podpore kritičnim subjektom v vlogi nacionalnega odzivnega centra, ki ga predstavlja NCKU, ki s svojim zaščitenim komunikacijskim in informacijskim omrežjem ter drugimi v tretjem odstavku navedenimi zmogljivostmi 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 morebitnih izrednih dogodkov na podlagi sporočil kritičnih subjektov.

Predlog zakona tudi določa, da medsebojna izmenjava informacij o izrednih dogodkih in kibernetiskih grožnjah poteka z uporabo namenske digitalne platforme, ki 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 sledi racionalnosti in se izogiba nepotrebному podvajanju.

#### K 12. členu

Člen določa pet temeljnih načel, ki jih morajo kot splošne usmeritve pri svojem delu na področju kritične infrastrukture upoštevati zlasti kritični subjekti, pa tudi vsi drugi pristojni organi in organizacije, kot jih določa predlog zakona.

#### K 13. členu

Člen kritičnim subjektom nalaga obveznost priprave in hrambe načrta za odpornost, ki obsega oceno tveganja kritičnega subjekta ter ukrepe za odpornost. K pripravljenu načrtu morajo pridobiti odobritev pristojnega nosilca sektorja kritične infrastrukture. Četrty odstavek kritičnemu subjektu nalaga obveznost, da pristojnemu nosilcu sektorja oziroma ministrstvu na njegovo zahtevo pošlje načrt za odpornost. Gre za razlikovanje med odobritvijo načrta s strani pristojnega nosilca sektorja kritične infrastrukture in njegov morebiten naknadni vpogled v načrt, in še zlasti vpogled ministrstva, pristojnega za obrambo, v vlogi pristojnega nacionalnega organa in enotne kontaktne točke na področju kritične infrastrukture.

#### K 14. členu

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 pisni rezultat celovitega postopka ugotavljanja narave in obsega tveganja s prepoznavanjem ter 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, da bi se izognili nepotrebному obremenjevanju kritičnih subjektov, tem daje možnost uporabiti že pripravljene ocene tveganja ali druge dokumente na podlagi obveznosti iz drugih pravnih aktov, katerih zavezanci so (npr. s področja zasebnega varovanja, varstva pred naravnimi in drugimi nesrečami, varstva okolja, obrambnega načrtovanja, tehnološke varnosti, načrta za zagotovitev neprekinjenega poslovanja itd.), ki predstavljajo izhodišče tudi za njegovo oceno tveganja oziroma izpolnjevanje obveznosti po tem členu. To lahko ugotovi pristojni nosilec sektorja kritične infrastrukture ob odobritvi načrta za odpornost.

#### K 15. členu

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 ter sorazmerni glede na tveganja, s katerimi se spoprijemajo, 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, posebnosti in obseg takih ukrepov bi morali ustrezno ter sorazmerno izražati tveganja,

ki jih je vsak kritični subjekt prepoznal v okviru svoje ocene tveganja kritičnega subjekta, in posebnosti takega subjekta (npr. zagotovitev nadomestnih sistemov, ki omogočajo opravljanje bistvene storitve, alternativne dobavne verige, rezervne lokacije, zagotovitev zadostnih zalog sredstev, komponent, proizvodov, materiala, surovin, nadomestnih in rezervnih delov, opreme itd. potrebnih za neprekinjeno opravljanje bistvene storitve).

V povezavi z zagotovitvijo ustreznega upravljanja varnosti zaposlenih predlog zakona kritične subjekte obvezuje, da pri določitvi delovnih mest, pomembnih za opravljanje bistvene storitve, upoštevajo tudi naloge, ki jih opravljajo zunanji ponudniki.

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 pa jih sprejme vlada na predlog nosilcev sektorjev kritične infrastrukture za zagotovitev delovanja kritične infrastrukture v obsegu, ki še omogoča opravljanje bistvene storitve. Vlada sprejme predvsem ukrepe, ki presegajo pristojnost posameznega kritičnega subjekta (npr. okrepitev varovanja kritične infrastrukture, sprostitev blagovnih rezerv ali zaprosilo za mednarodno pomoč). Če morajo take dodatne ukrepe za odpornost izvesti kritični subjekti, lahko vlada odloči, da se finančna sredstva za izvedbo teh ukrepov zagotovijo iz državnega proračuna. Za zagotovitev ustrezne fizične zaščite svojih prostorov in kritične infrastrukture (pri čemer se upoštevajo na primer tudi postavitve ograje, izgradnja pregrad, orodja in postopki za nadziranje zavarovanega območja, oprema za odkrivanje in nadzor dostopa itn.) 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 pri oceni tveganj kritičnim subjektom tudi za ukrepe za odpornost daje podlago za uporabo že sprejetih ukrepov na podlagi obveznosti iz drugih aktov, katerih zavezanec so, kot enakovrednih ukrepom iz tega člena, kar lahko ugotovijo nosilci sektorjev kritične infrastrukture ob podaji odobritve k načrtu za odpornost.

#### K 16. členu

Člen določa obveznost kritičnega subjekta, da svoj načrt za odpornost posodobi najmanj enkrat na dve leti. Ob nastanku novih okoliščin, ki lahko pomembno vplivajo na zagotavljanje bistvene storitve in delovanje kritične infrastrukture, pa mora kritični subjekt ustrezno spremeniti načrt najpozneje v enem mesecu od nastanka takih okoliščin, in k tako spremenjenemu načrtu pridobiti odobritev pristojnega nosilca sektorja.

#### K 17. členu

Člen prenaša v slovensko zakonodajo določbo 14. člena Direktive 2022/2557, ki je razložen 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 zahteve za preverjanje preteklosti oseb, ki spadajo v posebne kategorije njihovega osebja. Zagotoviti bi bilo treba, da ustrezni organi zahteve 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<sup>1</sup> in, kadar je ustrezno in potrebno, Uredbe (EU) 2019/816 Evropskega parlamenta in Sveta<sup>2</sup>. Države članice bi se lahko, kadar je smiselno in ustrezno, oprle tudi na Schengenski informacijski sistem druge generacije (SIS II), vzpostavljen z Uredbo (EU) 2018/1862 Evropskega parlamenta in Sveta<sup>3</sup>, 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 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 njihova preteklost. Kritični subjekt lahko v skladu z oceno tveganja predloži zahtevek za preverjanje preteklosti tudi za zaposlene pri pogodbenih izvajalcih.

Ne gre za obveznost, temveč za možnost po predhodni utemeljitvi potrebe po preverjanju preteklosti zaposlenih. Preverjanje preteklosti kot ga opredeljuje predlog zakona, ki sledi določbam Direktive 2022/2557, ne smemo enačiti z varnostim preverjanjem v skladu s drugimi pravnimi akti. Če iz ocene tveganja kritičnega subjekta izhaja potreba po preverjanju preteklosti vseh zaposlenih, mora kritični subjekt, da bi se izognil morebitnemu diskriminatornemu ravnanju kritičnega subjekta, to v svojih aktih tudi ustrezno opredeliti.

Kritični subjekt zahtevkov 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 preverijo preteklost, da se potrdi identiteta osebe, katere preteklost se preverja, in kazenske evidence navedene osebe glede zapisov pravnomočnih kazenskih obsodb za kazniva dejanja, ki se preganjajo po uradni dolžnosti, ki jih kritični subjekt opredeli kot sporna z vidika opravljanja nalog na določenem delovnem mestu. 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 četrtega 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.

Če oseba iz prejšnjega odstavka ne poda soglasja za preverjanje preteklosti, se ji delo na delovnih mestih, ki so pomembna za opravljanje bistvenih storitev kritičnega subjekta in na katerih imajo dostop do prostorov, informacij in nadzornih sistemov, ne dovoli oziroma pogodba ne sklene.

#### K 18. členu

Člen sledi določbi 16. člena Direktive 2022/2557 o uporabi evropskih in mednarodnih standardov ter tehničnih specifikacij veljavnih ukrepov za varnost in odpornost kritičnih subjektov. Standardizacija bi

<sup>1</sup> 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).

<sup>2</sup> 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).

<sup>3</sup> 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 ter Sklepa Komisije 2010/261/EU (UL L 312, 7. 12. 2018, str. 56).

morala ostati predvsem tržno usmerjen proces. V nekaterih okoliščinah in na nekaterih področjih pa je vseeno smiselno zahtevati skladnost s posebnimi standardi, zlasti tistih, ki so pomembni za ukrepe 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 pomeni tehnično specifikacijo, kot je opredeljena v 4. točki 2. člena Uredbe (EU) št. 1025/2012.

#### K 19. členu

Člen 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 ter okoliščinah, ki nakazujejo možnost njihovega prenehanja poslovanja ali stečaja. V skladu s prvim stavkom 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 omejena z njeno družbeno ali ekološko vlogo. Javni interes glede zagotavljanja bistvenih storitev, ki je hkrati tudi splošni interes, zato zahteva posebno ureditev glede stečajev in izvršb kritičnih subjektov, s katero je zagotovljeno neprekinjeno zagotavljanje bistvene storitve 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), da ne prenehajo delovati sistemi, ki omogočajo opravljanje bistvenih storitev, tudi na področju civilnega in gospodarskega prava, ki omogočajo izvajanje človekovih pravic in temeljnih svoboščin.

#### K 20. členu

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 oziroma 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 oziroma 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 deležniki. Če ugotovi, da kritični subjekt dejansko izpolnjuje kriterije, navedene v prvem odstavku tega člena, o tem obvesti ministrstvo. Ministrstvo na podlagi odločitve Evropske komisije konkretni kritični subjekt uradno obvesti o tem, da se šteje za kritični subjekt posebnega evropskega pomena, in o njegovih obveznostih.

#### K 21. členu

Člen ureja organizacijo in izvedbo svetovalnih misij Evropske komisije, ki se izvedejo, da se ocenijo sprejeti ukrepi za odpornost kritičnega subjekta posebnega evropskega pomena, s čimer se sledi določbi 18. člena Direktive 2022/2557. Gre za kritične subjekte, ki so še posebno pomembni za Evropsko unijo in njen notranji trg, zato je pomembno, da se jim svetuje pri izpolnjevanju njihovih obveznosti po tem zakonu ter se oceni, ali dejansko izpolnjujejo obveznosti, ki se nanašajo na njihovo odpornost in zaščito njihove kritične infrastrukture. Člen opredeljuje možnost, da ministrstvo od Evropske komisije zahteva izvedbo svetovalne misije, in nalaga obveznost nosilcu sektorja kritične infrastrukture, da Evropski komisiji zagotovi vse potrebne dokumente in podatke (oceno tveganja, seznam ukrepov, informacije o ukrepih in ugotovitvah o opravljenem nadzoru nad izvajanjem določb

tega zakona), pri čemer se upoštevajo predpisi, 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 22. členu

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 opravljanju nalog, za katere so sicer pristojni, vendar niso zajete v VII. poglavju predloga zakona, ki ureja zagotavljanje podpore odločanju, zgodnje opozarjanje in poročanje.

#### K 23. členu

Člen 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 določitev kritičnih subjektov in njihove kritične infrastrukture, usklajevanja predlogov za odpornost kritičnih subjektov v sektorju, usmerjanja kritičnih subjektov pri njihovem načrtovanju in sprejemanju 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 24. členu

Člen 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 izključene okoliščine, na nastanek katerih subjekt kritične infrastrukture ne more vplivati in se nanje pripraviti. Izhajajoč tudi iz načela odgovornosti, določenega v 12. členu predloga zakona, po katerem so za zagotavljanje bistvenih storitev in delovanje kritične infrastrukture neposredno odgovorni kritični subjekti, morajo ti zagotavljati ustrezne materialne (finančna in materialna sredstva) in tudi organizacijske razmere (npr. usposabljanje vodstvenega kadra in drugih zaposlenih) za neprekinjeno zagotavljanje bistvene storitve in delovanje kritične infrastrukture. Tudi kritični subjekt mora določiti najmanj eno kontaktno osebo za njegovo sodelovanje na področju kritične infrastrukture predvsem s pristojnim nosilcem sektorja kritične infrastrukture, drugimi kritičnimi subjekti, drugimi nosilci sektorjev kritične infrastrukture ter ministrstvom.

#### K 25. členu

Člen 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 (12. točka 4. člena) in za enotno kontaktno točko (10. člen). Kot tako je pristojno za strokovno usmerjanje dejavnosti vseh deležnikov na področju kritične infrastrukture, poleg tega pa je pripravljavec in končni nosilec vseh predlogov, povezanih z ugotavljanjem ter določanjem kritičnih subjektov in njihove kritične infrastrukture, ki bodo predloženi v obravnavo vladi.

#### K 26. členu

Člen narekuje ustanovitev in delovanje koordinacijske skupine. Imenuje jo vlada, sestavljena iz predstavnikov nosilcev sektorjev in ministrstev, pristojnih za obrambo, notranje zadeve, zunanje in evropske zadeve, ter Slovenske obveščevalno-varnostne agencije. Vodi jo ministrstvo, ki tudi vodi in posodablja seznam članov ter nadomestnih članov in skupini zagotavlja administrativno-tehnično podporo. Predvideno je, da se skupina aktivira ob izrednih dogodkih zaradi 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.

#### K 27. členu

Člen podrobneje določa izmenjavo podatkov in informacij v skladu s petim načelom odpornosti kritičnih subjektov in kritične infrastrukture iz 12. člena predloga zakona. Izmenjava podatkov je bistvena za delovanje NCKU, ki je v skladu z 9. členom Uredbe o kriznem upravljanju in vodenju ter Nacionalnem centru za krizno upravljanje (Uradni list RS, št. 28/18, v nadaljnjem besedilu: Uredba) osrednji informacijsko-operativni center kriznega upravljanja, ki opravlja naloge spremljanja in obveščanja v podporo odločanju tudi po tem zakonu. Telesa kriznega upravljanja opredeljujeta 20. člen Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17 in 163/22) in Uredba. To so Svet za nacionalno varnost, sekretariat Sveta za nacionalno varnost, operativna skupina sekretariata Sveta za nacionalno varnost, Nacionalni center za krizno upravljanje in medresorska analitična skupina. Člen se povezuje z 29. členom, s katerim se vzpostavlja mehanizem prigrasitve izrednih dogodkov in obveznost kritičnih subjektov prigrasitve ter poročanja o izrednih dogodkih, pri čemer se pričakuje, da kritični subjekti brez odlašanja posredujejo 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 ter kritični subjekti NCKU zagotavljajo podatke iz svoje pristojnosti. To pristojnim organom in organizacijam omogoča hiter ter ustrezen odziv na izredne dogodke ter celovit pregled vpliva, narave, vzroka in morebitnih posledic izrednih dogodkov, s katerimi se spoprijemajo kritični subjekti. NCKU v skladu s 4. odstavkom 8. člena Uredbe opravlja naloge spremljanja in obveščanja v podporo odločanju ter deluje neprekinjeno. Prav tako NCKU zagotavlja varne komunikacijske in informacijske povezave za izmenjavo podatkov med subjekti, ki so že vključeni v komunikacijski in informacijski sistem NCKU. Med njimi so tudi nosilci sektorjev kritične infrastrukture in upravljavci kritične infrastrukture, določeni na podlagi ZKI. Da pri tem ne bi prihajalo do dodatnih odgovornosti in obremenitev za kritične subjekte, mora izmenjava podatkov potekati digitalizirano in čim bolj avtomatizirano.

Z vidika varovanja osebnih podatkov 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 sta 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 (torej Slovenska obveščevalno-varnostna agencija, Policija in Obveščevalno varnostna služba Ministrstva za obrambo), v primeru povečane ogroženosti kritične infrastrukture, z zaznanim grožnjo seznanijo nosilca sektorja kritične infrastrukture, ta pa nato seznanijo kritični subjekt. S to določbo se želi h krepitvi odpornosti kritičnega subjekta in zaščiti njegove kritične infrastrukture vsaj posredno dejavnije pritegniti tudi nosilce obveščevalno-varnostne dejavnosti v Republiki Sloveniji.

#### K 28. členu

Člen nalaga kritičnim subjektom in nosilcem sektorjev kritične infrastrukture vsakemu za njegovo raven pripravo letnega poročila o zagotavljanju neprekinjenega delovanja kritične infrastrukture ter opravljanju bistvenih storitev, od ministrstva pa zahteva, da na podlagi sektorskih poročil pripravi skupno poročilo o zagotavljanju neprekinjenega delovanja 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 29. člena prigrasiti

takoj, ko je mogoče, ter 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.

#### K 29. členu

Člen nalaga kritičnim subjektom obveznost prigrasitve izrednih dogodkov in v celoti sledi določbi 15. člena Direktive 2022/2557 ter njeni uvodni izjavi 33, ki se glasi: »Vzpostaviti bi bilo treba mehanizem za prigrasitev 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 katerimi se soočajo kritični subjekti. Kritični subjekti bi morali brez nepotrebne odlašanja pristojnim organom prigrasiti incidente, ki povzročijo ali bi lahko povzročili pomembne motnje v opravljanju bistvenih storitev. Kritični subjekti bi morali začetno prigrasitev predložiti najpozneje 24 ur po seznanitvi z incidenti, razen če to operativno ni mogoče. Začetna prigrasitev 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 prigrasitvi bi bilo treba, kadar je mogoče, navesti domnevni vzrok incidenta. Države članice bi morale zagotoviti, da se z zahtevo po predložitvi začetne prigrasitve sredstva kritičnega subjekta ne preusmerijo z dejavnosti, povezanih z obvladovanjem incidenta, ki bi moralo biti prednostna naloga. Začetni prigrasitvi bi moralo, kadar je ustrezno, slediti podrobno poročilo, in sicer najpozneje en mesec po incidentu. Podrobno poročilo bi moralo dopolnjevati začetno prigrasitev in zagotoviti celovitejši pregled incidenta.« Uvodna izjava 24 Direktive 2022/2557 potem določa, da se zahteve iz Direktive 2022/2555 in Direktive 2022/2557 izvajajo na dopolnjujoč način ter da za kritične subjekte ne nastaja upravno breme. Direktivi se v slovenski pravni red prenašata hkrati, 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 o obveznosti medsebojne izmenjave informacij o izrednih dogodkih, kibernetičnih grožnjah in skorajšnjih izrednih dogodkih. Za ta namen pristojni nacionalni organ na podlagi zakona, ki ureja informacijsko varnost, vzpostavi digitalno platformo. Zaradi povezav med navedenima direktivama, predvsem pa da bi se izognili 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 prigrasitve 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, ki jih potrebuje ministrstvo za ugotovitev čezmejnega vpliva izrednega dogodka in prigrasitev izrednega dogodka z vplivom na neprekinjeno opravljanje bistvenih storitev v šestih ali več državah članicah Evropski komisiji ter za obveščanje enotnih kontaktnih točk prizadetih držav članic, in informacije, ki jih potrebuje NCKU za opravljanje 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.

#### K 30. členu

Člen predstavlja podlago za zbiranje, obdelovanje, uporabo in hrambo podatkov o odgovornih ter kontaktnih osebah nosilcev sektorjev kritične infrastrukture in kritičnih subjektov, da se zagotovi podpora odločanju na področju kritične infrastrukture. Nosilec sektorja kritične infrastrukture mora zbirati, obdelovati in hraniti podatke (torej 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 mora zbirati, obdelovati, uporabljati in hraniti iste vrste podatkov o odgovornih ter kontaktnih osebah nosilcev sektorjev kritične infrastrukture in kritičnih subjektih. Obveznost ministrstva in nosilcev

sektorjev kritične infrastrukture glede zbiranja, obdelovanja ter hrambe podatkov o odgovornih in kontaktnih osebah vključuje tudi obveznost posodabljanja ustreznih evidenc podatkov.

#### K 31. členu

Člen ureja varovanje podatkov, ki se nanašajo na ugotavljanje, določanje in odpornost kritičnih subjektov ter kritične infrastrukture v smislu, da od vseh deležnikov na področju kritične infrastrukture zahteva, da zadevne podatke obravnavajo v skladu z nacionalnimi predpisi o varovanju tajnih podatkov ter predpisi EU in Nata, predpisi, ki urejajo poslovno skrivnost (tj. Zakon o gospodarskih družbah). To pomeni, da predlog zakona posebej ne določa dejanskih podatkov s področja kritične infrastrukture, ki so predmet varovanja, ampak to prepušča vsakokratni presoji oseb, ki so pristojne za obravnavanja tovrstnih podatkov od njihovega določanja do arhiviranja.

#### K 32. členu

Člen določa, da nadzor nad izvajanjem določb tega zakona izvaja inšpektorat, ki je pristojen za obrambo. Drugi odstavek tega člena sledi določbam Direktive 2022/2557 in 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, čeprav lahko inšpektorat, pristojen za obrambo, v skladu z že obstoječimi predpisi in uveljavljenim načinom dela k inšpekcijskemu nadzoru 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 ti sprejeli za zagotovitev svoje odpornosti, izpolnjujejo zahteve iz 15. 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 glede tega posreduje informacije. V skladu z določbami Direktive 2022/2555 in predlogom novega zakona, ki bo urejal informacijsko varnost, bodo namreč kritični subjekti, določeni na podlagi tega predloga zakona, tudi zavezanci po predlogu zakona, ki ureja informacijsko varnost, in je v členu opredeljeno sodelovanje navedenih nadzornih organov smiselno.

#### K 33. členu

Člen določa prekrške pri izvajanju tega zakona in višino zagroženih glob, zaradi katerih sta kaznovana kritični subjekt kot pravna oseba ter odgovorna oseba kritičnega subjekta. Ne gre za kaznovanje kritičnega subjekta ali njegove odgovorne osebe zaradi morebitnega nedelovanja kritične

infrastrukture na splošno, temveč 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.

#### K 34. členu

Člen zagotavlja zakonsko podlago, da se lahko v hitrem postopku za prekrške, določene v 33. členu predloga zakona, izreče tudi globa v znesku, ki je višji od najnižje, ki jo predvideva predlog zakona.

#### K 35. členu

Člen določa rok za sprejem strategije in nacionalne ocene tveganja ter 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 ugotavljanje kritičnih subjektov ter kritične subjekte in njihove kritične infrastrukture.

Člen kritičnim subjektom določa rok za pripravo načrta za odpornost iz 13. člena tega zakona, ki obsega oceno tveganja kritičnega subjekta in ukrepe za odpornost kritičnega subjekta.

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

Obveznost ministrstva, ki ga določa člen je tudi Evropski komisiji predložiti zbirno poročilo o prejetih priglasitvah izrednih dogodkov, vključno s številom priglasitev, naravo priglašeni izrednih dogodkov in sprejetimi ukrepi, in sicer prvič do 17. julija 2028 in nato na vsaki dve leti.

Člen ministrstvu nalaga tudi obveznost o prekrških, ki se uporabljajo za kršitve ukrepov, sprejetih na podlagi predloga zakona, obvestiti Evropsko komisijo do 17. oktobra 2024. Evropsko komisijo mora obveščati tudi o njihovih naknadnih spremembah.

#### K 36. členu

S členom se ureja podaljšanje uporabe ZKI in Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije. Navedena predpisa se uporabljata do določitve kritičnih subjektov na podlagi predloga zakona.

#### K 37. členu

Člen določa prenehanje veljavnosti ZKI, Uredbe o evropski kritični infrastrukturi in Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije, in sicer z dnem uveljavitve predloga zakona.

#### K 38. členu

Člen določa petnajstdnevni rok za uveljavitev predloga zakona.

#### **IV. BESEDILO ČLENOV, KI SE SPREMINJAJO**

/

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

/

#### **VI. PRILOGE**

- osnutek Uredbe o ugotavljanju, določanju in odpornosti kritičnih subjektov,
- osnutek Sklepa Vlade Republike Slovenije o določitvi kritičnih subjektov in kritične infrastrukture Republike Slovenije,

Na podlagi drugega odstavka 26.člena Zakona o spremembah in dopolnitvah Zakona o kritični infrastrukturi (Uradni list RS, št. \_\_\_\_\_ ) izdaja Vlada Republike Slovenije

## **U R E D B O**

### **o ugotavljanju, določanju in odpornosti kritičnih subjektov**

#### **1. člen**

Ta uredba določa podsektorje sektorjev kritične infrastrukture, nosilce sektorjev kritične infrastrukture in z njimi sodelujoče organe, bistvene storitve, kategorije subjektov ter mejne vrednosti, ki se uporabljajo za določitev kriterijev za ugotavljanje kritičnih subjektov.

#### **2. člen**

Podsektorji sektorja energetike in sektorja prometa so:

##### **1. SEKTOR ENERGETIKE:**

- 1. 1 elektrika
- 1. 2 daljinsko ogrevanje in hlajenje
- 1. 3 nafta
- 1. 4 plin
- 1. 5 vodik

##### **2. SEKTOR PROMETA:**

- 2. 1 zračni
- 2. 2 železniški
- 2. 3 vodni
- 2. 4 cestni
- 2. 5 javni prevoz

#### **3. člen**

Nosilci sektorjev kritične infrastrukture in z njimi sodelujoči organi so:

##### **1. SEKTOR ENERGETIKE:**

Nosilec: Ministrstvo, pristojno za okolje, podnebje in energijo  
Sodelujoči: Ministrstvo, pristojno za gospodarstvo, turizem in šport

##### **2. SEKTOR PROMETA:**

Nosilec: Ministrstvo, pristojno za infrastrukturo  
Sodelujoči: Ministrstvo, pristojno za gospodarstvo, turizem in šport

### 3. SEKTOR BANČNIŠTVA:

Nosilec: Ministrstvo, pristojno za finance

### 4. SEKTOR INFRASTRUKTURE FINANČNEGA TRGA:

Nosilec: Ministrstvo, pristojno za finance

### 5. SEKTOR ZDRAVJA:

Nosilec: Ministrstvo, pristojno za zdravje

### 6. SEKTOR PITNE VODE:

Nosilec: Ministrstvo, pristojno za naravne vire in prostor

### 7. SEKTOR ODPADNE VODE:

Nosilec: Ministrstvo, pristojno za naravne vire in prostor

### 8. SEKTOR DIGITALNE INFRASTRUKTURE:

Nosilec: Urad Republike Slovenije za informacijsko varnost  
Sodelujoči: Ministrstvo, pristojno za digitalno preobrazbo

### 9. SEKTOR JAVNE UPRAVE:

Nosilec: Ministrstvo, pristojno za javno upravo

### 10. SEKTOR VESOLJA:

Nosilec: Ministrstvo, pristojno za gospodarski razvoj, turizem in šport  
Sodelujoči: Ministrstvo, pristojno za obrambo

### 11. SEKTOR PRIDELAVE, PREDELAVE IN DISTRIBUCIJE ŽIVIL:

Nosilec: Ministrstvo, pristojno za kmetijstvo, gozdarstvo in prehrano  
Sodelujoči: Ministrstvo pristojno za gospodarski razvoj, turizem in šport

## 4. člen

Bistvene storitve v sektorjih in podsektorjih kritične infrastrukture so določene v Prilogi I, ki je sestavni del te uredbe.

## 5. člen

Kategorije subjektov v sektorjih in podsektorjih kritične infrastrukture so določene v Prilogi II, ki je sestavni del te uredbe.

## 6. člen

Mejne vrednosti kriterijev, ki jih nosilci sektorjev kritične infrastrukture uporabljajo za določitev pomembnosti motečega učinka izrednega dogodka na opravljanje bistvenih storitev so naslednje:

- število uporabnikov \_\_\_\_\_, ki so odvisni od bistvene storitve subjekta;
- stopnja odvisnosti drugih sektorjev in podsektorjev od bistvene storitve subjekta;
- tržni delež \_\_\_\_\_ subjekta na trgu te bistvene storitve;
- geografsko razširjenost \_\_\_\_\_, kar zadeva območje, ki bi ga izredni dogodek lahko prizadel;
- pomen subjekta pri ohranjanju zadostne ravni bistvene storitve ob upoštevanju alternativnih načinov za opravljanje te bistvene storitve.

## KONČNA DOLOČBA

## 7. člen

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

Št.  
Ljubljana, dne \_\_\_\_\_  
EVA

Vlada Republike Slovenije  
**dr. Robert Golob**  
predsednik

## Priloga I

### BISTVENE STORITVE

Bistvene storitve so naslednje:

#### 1. SEKTOR ENERGETIKE:

##### 1. 1 elektrika:

- dobava električne energije (elektroenergetska podjetja);
- obratovanje, vzdrževanje in razvoj distribucijskega sistema električne energije (operaterji distribucijskega sistema);
- obratovanje, vzdrževanje in razvoj prenosnega sistema električne energije (operaterji prenosnega sistema);
- proizvodnja električne energije (proizvajalci);
- storitev imenovanega operaterja trga električne energije (imenovani operaterji trga električne energije);
- prilagajanje odjema (udeleženci na trgu električne energije);
- agregiranje električne energije (udeleženci na trgu električne energije);
- shranjevanje energije (udeleženci na trgu električne energije);

##### 1. 2 daljinsko ogrevanje in hlajenje

- sisteme daljinskega ogrevanja in hlajenja: zagotavljanje daljinskega ogrevanja ali daljinskega hlajenja (upravljavci daljinskega ogrevanja ali daljinskega hlajenja);

##### 1. 3 nafta

- transport nafte (upravljavci naftovodov);
- proizvodnja nafte (izvajalci proizvodnje nafte);
- rafiniranje in predelava nafte (upravljavci obratov za rafiniranje in predelavo nafte);
- skladiščenje nafte (upravljavci skladišč nafte);
- upravljanje zalog nafte, vključno z varnostnimi zalogami in posebnimi zalogami nafte (osrednji organi za vzdrževanje zalog);

##### 1. 4 plin

- dobava plina (dobavitelji);
- distribucija plina (operaterji distribucijskega sistema);
- prenos plina (operaterji prenosnega sistema);
- skladiščenje plina (operaterji skladiščnega sistema);
- upravljanje sistema za utekočinjeni zemeljski plin (UZP) (operaterji sistema za UZP);
- proizvodnja zemeljskega plina (podjetja plinskega gospodarstva);
- nabava zemeljskega plina (podjetja plinskega gospodarstva);
- rafiniranje in predelava zemeljskega plina (upravljavci obratov za rafiniranje in predelavo zemeljskega plina);

##### 1. 5 vodik

- proizvodnja vodika (upravljavci proizvodnje vodika);

- shranjevanje vodika (upravljavci shranjevanja vodika);
- prenos vodika (upravljavci prenosa vodika);

## 2. SEKTOR PROMETA:

### 2. 1 zračni

- storitve zračnega prevoza, ki se uporabljajo v komercialne namene (potniškega in tovornega) (letalski prevozniki);
- upravljanje, vodenje in vzdrževanje letališč in infrastrukture letaliških omrežij (upravni organi letališča);
- storitve za kontrolo zračnega prometa (službe za kontrolo zračnega prometa);

### 2. 2 železniški

- storitve železniškega prevoza (potniškega in tovornega) (prevozniki v železniškem prometu);
- upravljanje, vodenje in vzdrževanje železniške infrastrukture, vključno s potniškimi postajami, tovornimi terminali, ranžirnimi postajami in centri za nadzor prometa (upravljavci infrastrukture);
- upravljanje, vodenje in vzdrževanje objektov za izvajanje železniških storitev (upravljavci objektov za izvajanje železniških storitev);
- upravljanje, vodenje in vzdrževanje upravljanja, vodenja-upravljanja in signalizacije železniškega prometa ter telekomunikacijskih naprav in sistemov, ki se uporabljajo za vodenje-upravljanje in signalizacijo (upravljavci infrastrukture);

### 2. 3 vodni

- storitve prevoza po kopenskih vodah, morju in obalnih vodah (potniškega in tovornega) (prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah);
- upravljanje, vodenje in vzdrževanje pristanišč in pristaniških zmogljivosti ter upravljanje opreme in infrastrukture v pristaniščih, vključno z oskrbo z gorivom, pretovarjanjem, privezom, potniškimi storitvami, zbiranjem ladijskih odpadkov in ostankov tovora, pilotažo in vleko (upravni organi pristanišč ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih);
- sistem za nadzor plovbe (upravljavci sistemov za nadzor plovbe);

### 2. 4 cestni

- nadzor upravljanja prometa, vključno z vidiki, povezanimi z načrtovanjem, nadzorom in upravljanjem cestnih omrežij, razen upravljanja prometa ali obratovanja inteligentnih prometnih sistemov, kadar niso bistveni del splošne dejavnosti javnih subjektov (cestni organi);
- storitve inteligentnih prometnih sistemov (upravljavci inteligentnih prometnih sistemov);

### 2. 5 javni prevoz

- storitve javnega potniškega prevoza po železnici in druge vrste prevoza po tirih ter prevoza po cesti (izvajalci javnih prevoznih storitev);

## 3. SEKTOR BANČNIŠTVA:

- sprejemanje vlog (kreditne institucije);

- posojanje (kreditne institucije);

#### 4. SEKTOR INFRASTRUKTURE FINANČNEGA TRGA:

- upravljanje mesta trgovanja (upravljavci mest trgovanja);
- upravljanje klirinških sistemov (centralne nasprotne stranke);

#### 5. SEKTOR ZDRAVJA:

- izvajanje zdravstvenih storitev (izvajalci zdravstvenih storitev);
- analiza, ki jo opravi referenčni laboratorij Evropske unije (referenčni laboratoriji EU);
- raziskave in razvoj zdravil (subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil);
- proizvodnja farmacevtskih surovin in preparatov (subjekti, ki proizvajajo farmacevtske surovine in preparate);
- proizvodnja medicinskih pripomočkov, ki se štejejo za kritične v času izrednih razmer v javnem zdravju (subjekti, ki proizvajajo medicinske pripomočke);
- promet z zdravili (subjekti, ki imajo dovoljenje za promet z zdravili na debelo);

#### 6. SEKTOR PITNE VODE:

- oskrba s pitno vodo in distribucija pitne vode, razen distribucije vode za prehrano ljudi, kadar je ta storitev nebistven del splošne dejavnosti distributerjev, ki distribuirajo druge dobrine in blago (dobavitelji in distributerji vode, namenjene za prehrano ljudi);

#### 7. SEKTOR ODPADNE VODE:

- zbiranje, čiščenje in odvajanje odpadne vode, razen zbiranja, odvajanja ali čiščenja komunalne odpadne vode, odpadne vode iz gospodinjestev ali tehnološke odpadne vode, kadar niso bistveni del splošnih dejavnosti podjetij (podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjestev in tehnološko odpadno vodo);

#### 8. SEKTOR DIGITALNE INFRASTRUKTURE:

- zagotavljanje in opravljanje storitve stičišč omrežij (ponudniki stičišč omrežij);
- zagotavljanje storitve sistema domenskih imen, razen storitev, povezanih s korenskimi imenskimi strežniki (ponudniki storitev sistema domenskih imen);
- zagotavljanje in upravljanje registrov vrhnjih domenskih imen (registri vrhnjih domenskih imen);
- zagotavljanje storitev računalništva v oblaku (ponudniki storitev računalništva v oblaku);
- zagotavljanje storitev podatkovnega centra (ponudniki storitev podatkovnega centra);
- zagotavljanje omrežij za dostavo vsebin (ponudniki omrežij za dostavo vsebin);
- zagotavljanje storitev zaupanja (ponudniki storitev zaupanja);
- zagotavljanje javno dostopnih elektronskih komunikacijskih storitev (ponudniki elektronskih komunikacijskih storitev);
- zagotavljanje javnih elektronskih komunikacijskih omrežij (ponudniki javnih elektronskih komunikacijskih omrežij);

## 9. SEKTOR JAVNE UPRAVE:

- storitve, ki jih opravljajo subjekti javne uprave v smislu člena 2, točka 10, Direktive (EU) 2022/2557, enot centralne ravni države, kot jih opredelijo države članice v skladu z nacionalnim pravom (subjekti javne uprave enot centralne ravni države);

## 10. SEKTOR VESOLJA:

- upravljanje talne infrastrukture, ki jo imajo v lasti, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo zagotavljanje vesoljskih storitev, razen ponudnikov javnih elektronskih komunikacijskih omrežij (upravljavci talne infrastrukture);

## 11. SEKTOR PRIDELAVE, PREDELAVE IN DISTRIBUCIJE ŽIVIL:

(izvajalci živilske dejavnosti, ki se ukvarjajo izključno z logistiko in veleprodajo ter industrijsko proizvodnjo in predelavo v velikem obsegu):

- industrijska proizvodnja in predelava hrane v velikem obsegu;
- storitve verige preskrbe s hrano, vključno s shranjevanjem in logistiko;
- veleprodaja.

**Priloga II**

**SEKTORJI, PODSEKTORJI IN KATEGORIJE SUBJEKTOV**

Sektorji	Podsektorji	Kategorije subjektov
1. energetika	elektrika	<ul style="list-style-type: none"> <li>– elektroenergetska podjetja, kot so opredeljena v členu 2, točka 57, Direktive (EU) 2019/944 Evropskega parlamenta in Sveta<sup>4</sup>, ki opravljajo dejavnosti dobave, kot je opredeljena v členu 2, točka 12, navedene direktive</li> </ul>
		<ul style="list-style-type: none"> <li>– operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 29, Direktive (EU) 2019/944</li> </ul>
		<ul style="list-style-type: none"> <li>– operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 35, Direktive (EU) 2019/944</li> </ul>
		<ul style="list-style-type: none"> <li>– proizvajalci, kot so opredeljeni v členu 2, točka 38, Direktive (EU) 2019/944</li> </ul>
		<ul style="list-style-type: none"> <li>– imenovani operaterji trga električne energije, kot so opredeljeni v členu 2, točka 8, Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta<sup>5</sup></li> </ul>
		<ul style="list-style-type: none"> <li>– subjekti, ki zagotavljajo sistemsko odpornost in redundanco sistemov</li> </ul>

<sup>4</sup> Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14. 6. 2019, str. 125).

<sup>5</sup> Uredba (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije (UL L 158, 14. 6. 2019, str. 54).

Sektorji	Podsektorji	Kategorije subjektov
		– udeleženci na trgu, kot so opredeljeni v členu 2, točka 25, Uredbe (EU) 2019/943, ki zagotavljajo storitve agregiranja, prilagajanja odjema ali shranjevanja energije, kot so opredeljene v členu 2, točke 18, 20 in 59, Direktive (EU) 2019/944
	daljinsko ogrevanje in hlajenje	– upravljavci daljinskega ogrevanja ali daljinskega hlajenja, kot so opredeljeni v členu 2, točka 19, Direktive (EU) 2018/2001 Evropskega parlamenta in Sveta <sup>6</sup>
	nafta	<p>– upravljavci naftovodov</p> <p>– upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in transporta nafte</p> <p>– osrednji organ za vzdrževanje zalog, kot je opredeljen v členu 2, točka (f), Direktive Sveta 2009/119/ES<sup>7</sup></p>

<sup>6</sup> Direktiva (EU) 2018/2001 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spodbujanju uporabe energije iz obnovljivih virov (UL L 328, 21. 12. 2018, str. 82).

<sup>7</sup> Direktiva Sveta 2009/119/ES z dne 14. septembra 2009 o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov (UL L 265, 9. 10. 2009, str. 9).

Sektorji	Podsektorji	Kategorije subjektov
	plin	– dobavitelji, kot so opredeljeni v členu 2, točka 8, Direktive 2009/73/ES Evropskega parlamenta in Sveta <sup>8</sup>
	– operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 6, Direktive 2009/73/ES	
	– operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 4, Direktive 2009/73/ES	
	– operaterji skladiščnega sistema, kot so opredeljeni v členu 2, točka 10, Direktive 2009/73/ES	
	– operaterji sistema za UZP, kot so opredeljeni v členu 2, točka 12, Direktive 2009/73/ES	
	– podjetja plinskega gospodarstva, kot so opredeljena v členu 2, točka 1, Direktive 2009/73/ES	
	– upravljavci obratov za rafiniranje in predelavo zemeljskega plina	
	vodik	– upravljavci proizvodnje, shranjevanja in prenosa vodika

<sup>8</sup> Direktiva 2009/73/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z zemeljskim plinom in o razveljavitvi Direktive 2003/55/ES (UL L 211, 14. 8. 2009, str. 94).

Sektorji	Podsektorji	Kategorije subjektov
2. promet	zračni	– letalski prevozniki, kot so opredeljeni v členu 3, točka 4, Uredbe (ES) št. 300/2008, ki se uporabljajo v komercialne namene
		– upravni organi letališča, kot so opredeljeni v členu 2, točka 2, Direktive 2009/12/ES Evropskega parlamenta in Sveta <sup>9</sup> , letališča, kot so opredeljena v členu 2, točka 1, navedene direktive, vključno z jedrnimi letališči, navedenimi v oddelku 2 Priloge II k Uredbi (EU) št. 1315/2013 Evropskega parlamenta in Sveta <sup>10</sup> , ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih
		– službe za kontrolo zračnega prometa (ATC), kot so opredeljene v členu 2, točka 1, Uredbe (ES) št. 549/2004 Evropskega parlamenta in Sveta <sup>11</sup>

<sup>9</sup> Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14. 3. 2009, str. 11).

<sup>10</sup> Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU (UL L 348, 20. 12. 2013, str. 1).

<sup>11</sup> Uredba (ES) št. 549/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o določitvi okvira za oblikovanje enotnega evropskega neba (okvirna uredba) (UL L 96, 31. 3. 2004, str. 1).

Sektorji	Podsektorji	Kategorije subjektov
	železniški	– upravljavci infrastrukture, kot so opredeljeni v členu 3, točka 2, Direktive 2012/34/EU Evropskega parlamenta in Sveta <sup>12</sup>
		– prevozniki v železniškem prometu, kot so opredeljeni v člen 3, točka 1, Direktive 2012/34/EU, in upravljavci objektov za izvajanje železniških storitev, kot so opredeljeni v členu 3, točka 12, navedene direktive
	vodni	– prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, kot so opredeljena za področje pomorskega prometa v Prilogi I k Uredbi (ES) št. 725/2004, brez posameznih plovil, ki jih upravljajo ta podjetja

<sup>12</sup> Direktiva 2012/34/EU Evropskega parlamenta in Sveta z dne 21. novembra 2012 o vzpostavitvi enotnega evropskega železniškega območja (UL L 343, 14. 12. 2012, str. 32).

Sektorji	Podsektorji	Kategorije subjektov
		<p>– upravni organi pristanišč, kot so opredeljeni v členu 3, točka 1, Direktive 2005/65/ES, vključno z njihovimi pristaniškimi zmogljivostmi, kot so opredeljene v členu 2, točka 11, Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih</p> <p>– upravljavci sistemov za nadzor plovbe (VTS), kot so opredeljeni v členu 3, točka (o), Direktive 2002/59/ES Evropskega parlamenta in Sveta<sup>13</sup></p>

<sup>13</sup> Direktiva 2002/59/ES Evropskega parlamenta in Sveta z dne 27. junija 2002 o vzpostavitvi sistema spremljanja in obveščanja za ladijski promet ter o razveljavitvi Direktive Sveta 93/75/EGS (UL L 208, 5. 8. 2002, str. 10).

Sektorji	Podsektorji	Kategorije subjektov
	cestni	<p>– cestni organi, kot so opredeljeni v členu 2, točka 12, Delegirane uredbe Komisije (EU) 2015/962<sup>14</sup>, odgovorni za nadzor upravljanja prometa, razen javnih subjektov, za katere je upravljanje prometa ali delovanje inteligentnih prometnih sistemov nebistven del splošne dejavnosti</p> <p>– upravljavci inteligentnih prometnih sistemov, kot so opredeljeni v členu 4, točka 1, Direktive 2010/40/EU Evropskega parlamenta in Sveta<sup>15</sup></p>

<sup>14</sup> Delegirana uredba Komisije (EU) 2015/962 z dne 18. decembra 2014 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23. 6. 2015, str. 21).

<sup>15</sup> Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (UL L 207, 6. 8. 2010, str. 1).

Sektorji	Podsektorji	Kategorije subjektov
	javni prevoz	– izvajalci javnih prevoznih storitev, kot so opredeljeni v členu 2, točka (d), Uredbe (ES) št. 1370/2007 Evropskega parlamenta in Sveta <sup>16</sup>
3. bančništvo		– kreditne institucije, kot so opredeljene v členu 4, točka 1, Uredbe (EU) št. 575/2013 – izvajalci prevozov gotovine
4. infrastruktura finančnega trga		– upravljavci mest trgovanja, kot so opredeljeni v členu 4, točka 24, Direktive 2014/65/EU – centralne nasprotne stranke (CNS), kot so opredeljene v členu 2, točka 1, Uredbe (EU) št. 648/2012 – centralne depotne družbe (CDD), kot so opredeljene v členu opredeljene v členu 2(1)(1) Uredbe (EU) št. 909/2014 – upravljavce pomembnih plačilnih sistemov, ki niso v lasti ali upravljanju Evrosistema in so opredeljeni v 200. členu ZPlaSSIED3 ter 4. členu Sklepa o plačilnih sistemih in upravljavcih plačilnih sistemov

<sup>16</sup> Uredba (ES) št. 1370/2007 Evropskega parlamenta in Sveta z dne 23. oktobra 2007 o javnih storitvah železniškega in cestnega potniškega prevoza ter o razveljavitvi uredb Sveta (EGS) št. 1191/69 in št. 1107/70 (UL L 315, 3. 12. 2007, str. 1).

Sektorji	Podsektorji	Kategorije subjektov
5. zdravje		– izvajalci zdravstvenega varstva, kot so opredeljeni v členu 3, točka (g), Direktive 2011/24/EU Evropskega parlamenta in Sveta <sup>17</sup>
		– referenčni laboratoriji EU iz člena 15 Uredbe (EU) 2022/2371 Evropskega parlamenta in Sveta <sup>18+</sup>
		– subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil, kot so opredeljeni v členu 1, točka 2, Direktive 2001/83/ES Evropskega parlamenta in Sveta <sup>19</sup>

<sup>17</sup> Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4. 4. 2011, str. 45).

<sup>18</sup> Uredba (EU) 2022/2371 Evropskega parlamenta in Sveta z dne ... o resnih čezmejnih grožnjah za zdravje in o razveljavitvi Sklepa št. 1082/2013/EU (UL ...).

<sup>19</sup> Direktiva 2001/83/ES Evropskega parlamenta in Sveta z dne 6. novembra 2001 o zakoniku Skupnosti o zdravilih za uporabo v humani medicini (UL L 311, 28. 11. 2001, str. 67).

Sektorji	Podsektorji	Kategorije subjektov
		<p>– subjekti, ki proizvajajo farmacevtske surovine in pripravke iz razdelka C, oddelek 21, NACE Rev. 2</p> <p>– subjekti, ki proizvajajo medicinske pripomočke, ki se štejejo za kritične v izrednih razmerah v javnem zdravju (seznam kritičnih pripomočkov v izrednih razmerah v javnem zdravju) v smislu člena 22 Uredbe (EU) 2022/123 Evropskega parlamenta in Sveta<sup>20</sup></p> <p>– subjekti, ki imajo dovoljenje za promet z zdravili na debelo iz člena 79 Direktive 2001/83/ES</p>

<sup>20</sup> Uredba (EU) 2022/123 Evropskega parlamenta in Sveta z dne 25. januarja 2022 o okrepljeni vlogi Evropske agencije za zdravila pri pripravljenosti na krize in kriznem upravljanju na področju zdravil in medicinskih pripomočkov (UL L 20, 31. 1. 2022, str. 1).

Sektorji	Podsektorji	Kategorije subjektov
6. pitna voda		<p>– dobavitelji in distributerji vode, namenjene za prehrano ljudi, kot so opredeljeni v členu 2, točka 1(a), Direktive (EU) 2020/2184 Evropskega parlamenta in Sveta<sup>21</sup>, razen distributerjev, za katere je distribucija vode za prehrano ljudi nebistven del splošne dejavnosti distribucije drugih dobrin in blaga</p>
7. odpadna voda		<p>– podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjstev in tehnološko odpadno vodo, kot so opredeljena v členu 2, točke 1, 2 in 3, Direktive Sveta 91/271/EGS<sup>22</sup>, razen podjetij, za katere je zbiranje, odvajanje ali čiščenje komunalne odpadne vode, odpadne vode iz gospodinjstev in tehnološke odpadne vode nebistven del splošne dejavnosti</p>

<sup>21</sup> Direktiva (EU) 2020/2184 Evropskega parlamenta in Sveta z dne 16. decembra 2020 o kakovosti vode, namenjene za prehrano ljudi (UL L 435, 23. 12. 2020, str. 1).

<sup>22</sup> Direktiva Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode (UL L 135, 30. 5. 1991, str. 40).

Sektorji	Podsektorji	Kategorije subjektov
8. digitalna infrastruktura		– ponudniki stičišč omrežij, kot so opredeljeni v členu 6, točka 18, Direktive (EU) 2022/2555
		– ponudniki storitev sistema domenskih imen, kot so opredeljeni v členu 6, točka (20), Direktive (EU) .../... <sup>†</sup> , razen upravljavcev korenskih imenskih strežnikov
		– registri vrhnjih domenskih imen, kot so opredeljeni v členu 6, točka 21, Direktive (EU) 2022/2555
		– ponudniki storitev računalništva v oblaku, kot so opredeljeni v členu 46, točka 30, Direktive (EU) 2022/2555
		– ponudniki storitev podatkovnega centra, kot so opredeljeni v členu 6, točka 31, Direktive (EU) 2022/2555

Sektorji	Podsektorji	Kategorije subjektov
		<p>– ponudniki omrežij za dostavo vsebine, kot so opredeljeni v členu 6, točka 32, Direktive (EU) 2022/2555</p>
		<p>– ponudniki storitev zaupanja, kot so opredeljeni v členu 3, točka 19, Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta<sup>23</sup></p>
		<p>– ponudniki javnih elektronskih komunikacijskih omrežij, kot so opredeljeni v členu 2, točka 8, Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta<sup>24</sup></p>
		<p>– ponudniki elektronskih komunikacijskih storitev, kot so opredeljeni v členu 2, točka 4, Direktive (EU) 2018/1972, če so njihove storitve javno dostopne</p>

<sup>23</sup> Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28. 8. 2014, str. 73).

<sup>24</sup> Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L 321, 17. 12. 2018, str. 36).

Sektorji	Podsektorji	Kategorije subjektov
9. javna uprava		– subjekti javne uprave na ravni države, kot jih opredeljuje pravo Republike Slovenije
10. vesolje		– upravljavci talne infrastrukture, ki jo imajo v lasti, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo zagotavljanje vesoljskih storitev, razen ponudnikov javnih elektronskih komunikacijskih omrežij, kot so opredeljeni v členu 2, točka 8, Direktive (EU) 2018/1972
11. pridelava, predelava in distribucija živil		– izvajalci živilske dejavnosti, kot so opredeljeni v členu 3, točka 2, Uredbe (ES) št. 178/2002 Evropskega parlamenta in Sveta <sup>25</sup> , ki se ukvarjajo z industrijsko proizvodnjo in predelavo v velikem obsegu izključno hrane, s tem povezanim shranjevanjem in logistiko ter veleprodajo živil

---

<sup>25</sup> Uredba (ES) št. 178/2002 Evropskega parlamenta in Sveta z dne 28. januarja 2002 o določitvi splošnih načel in zahtevah živilske zakonodaje, ustanovitvi Evropske agencije za varnost hrane in postopkih, ki zadevajo varnost hrane (UL L 31, 1. 2. 2002, str. 1).

Številka:

Ljubljana, dne \_\_\_\_\_

Na podlagi tretjega odstavka 26. člena Zakona o spremembah in dopolnitvah Zakona o kritični infrastrukturi (Uradni list RS, št. \_\_\_\_\_) je Vlada Republike Slovenije na \_\_\_\_\_ seji pod \_\_\_\_\_ točko sprejela

## S K L E P

o določitvi kritičnih subjektov in kritične infrastrukture Republike Slovenije

I

Vlada Republike Slovenije je za kritične subjekte in kritično infrastrukturo Republike Slovenije določila:

### **1. SEKTOR ENERGETIKE:**

#### **1. 1 elektrika**

Kritični subjekt: \_\_\_\_\_

1.1.1 – kritična infrastruktura

#### **1. 2 daljinsko ogrevanje in hlajenje**

Kritični subjekt: \_\_\_\_\_

1.2.1 – kritična infrastruktura

#### **1. 3 nafta**

Kritični subjekt: \_\_\_\_\_

1.3.1 – kritična infrastruktura

#### **1. 4 plin**

Kritični subjekt: \_\_\_\_\_

1.4.1 – kritična infrastruktura

#### **1. 5 vodik**

Kritični subjekt: \_\_\_\_\_

1.5.1 – kritična infrastruktura

### **2. SEKTOR PROMETA:**

#### **2. 1 zračni**

Kritični subjekt: \_\_\_\_\_

2.1.1 – kritična infrastruktura

## **2. 2 železniški**

Kritični subjekt: \_\_\_\_\_

2.2.1 – kritična infrastruktura

## **2. 3 vodni**

Kritični subjekt: \_\_\_\_\_

2.3.1 – kritična infrastruktura

## **2. 4 cestni**

Kritični subjekt: \_\_\_\_\_

2.4.1 – kritična infrastruktura

## **2. 5 javni prevoz**

Kritični subjekt: \_\_\_\_\_

2.5.1 – kritična infrastruktura

## **3. SEKTOR BANČNIŠTVA:**

Kritični subjekt: \_\_\_\_\_

3.1. – kritična infrastruktura

## **4. SEKTOR INFRASTRUKTURE FINANČNEGA TRGA:**

Kritični subjekt: \_\_\_\_\_

4.1. – kritična infrastruktura

## **5. SEKTOR ZDRAVJA:**

Kritični subjekt: \_\_\_\_\_

5.1. – kritična infrastruktura

## **6. SEKTOR PITNE VODE:**

Kritični subjekt: \_\_\_\_\_

6.1. – kritična infrastruktura

## **7. SEKTOR ODPADNE VODE:**

Kritični subjekt: \_\_\_\_\_

7.1. – kritična infrastruktura

## **8. SEKTOR DIGITALNE INFRASTRUKTURE:**

Kritični subjekt: \_\_\_\_\_

8.1. – kritična infrastruktura

**9. SEKTOR JAVNE UPRAVE:**

Kritični subjekt: \_\_\_\_\_

9.1. – kritična infrastruktura

**10. SEKTOR VESOLJA:**

Kritični subjekt: \_\_\_\_\_

10.1. – kritična infrastruktura

**11. SEKTOR PRIDELAVE, PREDELAVE IN DISTRIBUCIJE ŽIVIL:**

Kritični subjekt: \_\_\_\_\_

11.1. – kritična infrastruktura

II

Ta sklep začne veljati naslednji dan po sprejetju.

Ministrstvo za obrambo s tem sklepom seznani kritične subjekte.

Barbara Kolenko Helbl  
generalna sekretarka

Prejmejo:

- nosilci sektorjev kritične infrastrukture
- Služba Vlade Republike Slovenije za zakonodajo