REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
Twitter: @URSIV_Slovenia

Številka: 007-35/2023/46
Ljubljana, 10. november 2023
EVA: 2023-1544-0003
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE

ZADEVA: Predlog Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov – predlog za obravnavo

1. Predlog sklepov vlade:

Na podlagi drugega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21 in 130/22 – ZEKom-2, 18/23-ZDU-1O in 49/23) je Vlada Republike Slovenije na … seji … sprejela

SKLEP

Vlada Republike Slovenije je izdala Uredbo o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov ter jo objavi v Uradnem listu Republike Slovenije.

Barbara Kolenko Helbl
generalna sekretarka

Sklep prejmejo:
- Urad Vlade Republike Slovenije za informacijsko varnost,
- vsa ministrstva in vladne službe.

Prilogi:

– predlog Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov,
– obrazložitev uredbe.

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

/

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- Dr. Uroš Svete, direktor urada, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
- Kory Golob, pomočnik direktorja urada, URSIV

- Mag. Melita Šinkovec, sekretarka, vodja Sektorja za informacijsko in kibernetsko varnost,URSIV
- Barbara Pernuš Grošelj, sekretarka, Sektor za informacijsko in kibernetsko varnost, URSIV

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

/

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

/

5. Kratek povzetek gradiva:

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pripravil predlog uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (v nadaljnjem besedilu: predlog uredbe), pri čemer gre za podzakonski predpis, ki ga izda Vlada Republike Slovenije (v nadaljnjem besedilu: vlada) na podlagi drugega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23-ZDU-1O in 49/23; v nadaljnjem besedilu ZInfV).

Področje urejanja predloga uredbe je doslej urejala Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 in 131/20; v nadaljnjem besedilu: Uredba o informacijski varnosti), ki je bila izdana na podlagi zakona, ki ureja državno upravo in je urejala minimalne skupne zahteve glede informacijske varnosti državnih organov, organov lokalnih skupnosti, javnih agencij in nosilcev javnih pooblastil ter drugih subjektov, ki se povezujejo s centralnim informacijsko-komunikacijskim sistemom. Uredba o informacijski varnosti je bila v neskladju s sistemskim zakonom s področja informacijske varnosti (ZInfV), ob tem praktično ni bilo mogoče nadzirati njenega izvajanja (razen v postopkih notranjih revizij), kar je bilo ocenjeno za veliko tveganje in izpostavljenost državnega centralnega informacijsko-komunikacijskega sistema kibernetskim grožnjam. Zato je bil sprejet Zakon o spremembah in dopolnitvah Zakona o informacijski varnosti (Uradni list RS, št. 49/23; v nadaljnjem besedilu ZInfV-B), ki je že na zakonski ravni v novem 18.a členu ZInfV uredil osnovne obveznosti povezanih subjektov glede informacijske varnosti, za podrobnejše urejanje tega področja pa je pooblastil vlado (gre za predmetni predlog uredbe). Hkrati je ZInfV-B tudi še za te njegove zavezance (povezane subjekte) na zakonski ravni uredil nadzor in sankcije za morebitne kršitve obveznosti. Po prehodni določbi 14. člena ZInfV-B je z dnem uveljavitve tega zakona prenehala veljati Uredba o informacijski varnosti, ki pa se uporablja do pričetka uporabe podzakonskega predpisa iz novega 18.a člena ZInfV.

Sicer bi morali povezani subjekti že sedaj izpolnjevati pogoje določene iz Uredbe o informacijski varnosti v državni upravi, ki je bistveno bolj obširna od predloga uredbe, zato prilagoditev predlagani uredbi za njih ne bi smela povzročiti težav, osnovne obveznosti povezanih subjektov je ob tem predvidel že ZInfV-B, predlagana uredba jih le podrobneje ureja.

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	NE
c)	administrativne posledice	NE
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	NE
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna	NE

	– razvojne dokumente Evropske unije in mednarodnih organizacij	

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

/

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva				

II. Finančne posledice za državni proračun

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1

SKUPAJ				

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ		

OBRAZLOŽITEV:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

/

II. Finančne posledice za državni proračun

/

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

/

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

/

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

/

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

/

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na: - pristojnosti občin, - delovanje občin, - financiranje občin.	DA (le v kolikor gre za povezane subjekte)

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: DA
- Združenju občin Slovenije ZOS: DA
- Združenju mestnih občin Slovenije (ZMOS): DA

Bistveni predlogi in pripombe, ki niso bili upoštevani.
Odzvala ta se ZOS in ZMOS.

SOS je v dopisu št. 007-62/2023-3 z dne 16. 8. 2023 sporočil, da do poteka roka za oddajo mnenja na predlagano uredbo niso prejeli pripomb občin članic SOS, bodo pa URSIV seznanili, če jih bodo prejeli naknadno, kar pa se doslej ni zgodilo.

ZMOS pa je v dopisu št. 007-17/2023-2 z dne 17. 8. 2023 navedla, da nimajo vsebinskih pripomb. V zvezi s (takratnim) 7. in 8. členom (sedaj 6. in 7. člen) predlagane uredbe pa menijo, da bi bilo smotrno pripraviti vzorec metodologije oziroma analize obvladovanja tveganj ter navodil, kar bi prispevalo k bolj poenoteni praksi. Zato predlagajo, da se uredbi doda prilogi v obliki vzorca metodologije in navodil. Hkrati predlagajo, da se občinam prek združenj pošljejo primere dokumentov, ki bi jim bili v pomoč.
Predlog ZMOS je bil upoštevan na način, da je v sedanjem 4. členu (vsebina in struktura varnostne dokumentacije) predloga uredbe dodan nov četrti odstavek, po katerem pristojni nacionalni organ na svoji spletni strani objavi priporočila za pripravo varnostne dokumentacije in jih po potrebi posodablja. Glede na prehodno določbo prvega odstavka 9. člena predlagane uredbe pristojni nacionalni organ prva takšna priporočila objavi v šestdesetih dneh od njene uveljavitve. Rešitev s priporočili hkrati upošteva tudi potrebo po določeni fleksibilnosti, saj so posamezni povezani subjekti lahko v različnih situacijah, kar lahko primerno upoštevajo.

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	DA
Gradivo ni takšne narave, da bi ga bilo treba objaviti na spletni strani predlagatelja.	

(Če je odgovor DA, navedite:)

Datum objave: objava na spletnih straneh e-demokracija dne 14. 7. 2023 z rokom za komentiranje oz. odziv javnosti do 14. 8. 2023.

Upoštevani so bili:
- ***v celoti,***
- *večinoma,*
- *delno,*
- *niso bili upoštevani.*

Bistvena mnenja, predlogi in pripombe, ki niso bili upoštevani, ter razlogi za neupoštevanje:
Na objavo osnutka predloga te uredbe na spletnih straneh e-demokracija se je odzvala Agencija Republike Slovenije za javnopravne evidence in storitve (AJPES) z dopisom št. 007-25/2023 z dne 1. 8. 2023 in podala pripombe, ki so bile v celoti upoštevane.
Na predlog AJPES:
- *sta bila med pomeni izrazov v 2. členu predlagane uredbe dodana izraza »sredstvo« in »uporabnik«;*
- *v tretjem odstavku (sedaj) 7. člena predlagane uredbe, je bila izvedena ustrezna korekcija številčenja točk;*
- *v 10. členu (prenehanje uporabe) je bila pri navedbi objave Uredbe o informacijski varnosti v državni upravi v Uradnem listu Republike Slovenija dodana še številka objave 49/23.*

Poročilo je bilo dano ……...

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA

11. Gradivo je uvrščeno v delovni program vlade:	NE
Dr. Uroš Svete direktor urada	

PRILOGA

Na podlagi drugega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21 in 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) Vlada Republike Slovenije izdaja

U R E D B O

o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov

I. SPLOŠNE DOLOČBE

1. člen
(namen in področja uporabe)

Ta uredba podrobneje določa vsebino in strukturo predpisane dokumentacije povezanih subjektov, metodologijo za pripravo analize obvladovanja tveganj informacijske varnosti z oceno sprejemljive ravni tveganj, način izvajanja obveznosti povezanega subjekta na področju informacijske varnosti, minimalni obseg varnostnih ukrepov glede informacijske varnosti ter pripravo navodil in postopkov za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave.

2. člen
(pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. analiza obvladovanja tveganj je proces ugotavljanja narave tveganja, ocenitve tveganja in ovrednotenje tveganja ter določitve ravni tveganja;

2. celovitost je lastnost informacij in informacijskih sistemov, da so točne in popolne;

3. centralizirani organi državne uprave (v nadaljnjem besedilu: centralizirani organi) so subjekti, za katere v skladu s prvim odstavkom 74.a člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23) upravljanje informacijsko-komunikacijske infrastrukture, razvoj skupnih informacijskih rešitev ter njihovo tehnološko, procesno in organizacijsko skladnost s centralnim informacijsko-komunikacijskim sistemom ter načrtovanje in upravljanje vseh proračunskih virov na teh področjih izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov;

4. CSIRT organov državne uprave je organizacijska enota Urada Vlade Republike Slovenije za informacijsko varnost, ki se odziva na incidente na področju informacijske varnosti organov državne uprave, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov ter od povezanih subjektov sprejema priglasitve incidentov z možnim vplivom na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem;

5. ocenitev tveganja je celotni proces ugotavljanja tveganja, analize tveganja in ovrednotenja tveganja;

6. ovrednotenje tveganja je proces primerjanja rezultatov analize tveganja z merili tveganja, da bi ugotovili, ali je tveganje oziroma njegova velikost sprejemljiva oziroma znosna;

7. razpoložljivost je lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo;

8. sistem upravljanja varovanja informacij je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov;

9. sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za povezani subjekt in zato zahteva zaščito;

10. ugotavljanje tveganja je proces odkrivanja, prepoznavanja in opisovanja tveganj;

11. uporabnik je fizična ali pravna oseba, ki uporablja posamezno storitev povezanega subjekta neposredno, posredno ali s posredovanjem oziroma je odvisna od nje;

12. zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom.

II. UPRAVLJANJE INFORMACIJSKE VARNOSTI

3. člen
(odgovorne osebe povezanega subjekta)

(1) Za informacijsko varnost povezanega subjekta je odgovoren predstojnik organa oziroma odgovorna oseba pravne osebe (v nadaljnjem besedilu: odgovorna oseba povezanega subjekta).

(2) Odgovorna oseba povezanega subjekta v skladu s prvo alinejo prvega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV) določi kontaktno osebo za informacijsko varnost in njenega namestnika. Za izvajanje posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta iz druge, tretje in četrte alineje prvega odstavka 18.a člena ZInfV odgovorna oseba povezanega subjekta lahko določi tudi drugo fizično ali pravno osebo.

III. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

4. člen
(vsebina in struktura varnostne dokumentacije)

(1) Povezani subjekti izdelajo varnostno dokumentacijo, ki vsebuje najmanj elemente iz prvega odstavka 18.a člena ZInfV.

(2) Varnostno dokumentacijo iz prejšnjega odstavka tega člena podpiše odgovorna oseba povezanega subjekta.

(3) Če ima povezani subjekt za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni v skladu s to uredbo.

(4) Pristojni nacionalni organ na svoji spletni strani objavi priporočila za pripravo varnostne dokumentacije.

5. člen
(analiza obvladovanja tveganj)

(1) Povezani subjekt pripravi analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj na način iz 6. člena te uredbe.

(2) Povezani subjekt na podlagi analize obvladovanja tveganj z oceno sprejemljive ravni tveganj navede ustrezne ukrepe za preprečitev ali omilitev neželenih učinkov in zagotovi nenehno izboljševanje.

(3) Povezani subjekt izvaja analizo obvladovanja tveganj informacijske varnosti najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe v informacijskih sistemih in delovnih procesih, pri čemer upošteva splošna merila za sprejemljivo raven tveganj in merila za izvajanje ocenitve tveganj informacijske varnosti.

(4) Povezani subjekt dokumentira in hrani informacije o ugotovitvah ocene sprejemljive ravni tveganj in obravnave tveganj informacijske varnosti.

6. člen
(metodologija za pripravo analize obvladovanja tveganj informacijske varnosti)

(1) Povezani subjekt pripravi analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj tako, da:

1. navede metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedel analizo obvladovanja tveganj v skladu s to uredbo;

2. izvede popis informacijskih sredstev znotraj sistema upravljanja varovanja informacij oziroma omrežja, iz katerega se povezuje v centralno državno informacijsko-komunikacijsko omrežje oziroma sistem, in določi njihove upravljavce ter v analizo obvladovanja tveganj vključi navedena sredstva. Centralizirani organi izvedejo ta popis v sodelovanju z ministrstvom, pristojnim za upravljanje informacijsko-komunikacijskih sistemov, ki jim mora na zahtevo poslati ustrezne podatke, s katerimi razpolaga, in sicer v 15 dneh od prejema posamičnega zahtevka;

3. prepozna in v analizi obvladovanja tveganj navede možne grožnje za izgubo celovitosti, razpoložljivosti in zaupnosti sredstev iz prejšnje točke;

4. prepozna in v analizi obvladovanja tveganj navede ranljivosti sredstev iz 2. točke tega odstavka, ki bi jih grožnje iz prejšnje točke lahko prizadele;

5. oceni stopnjo vpliva uresničitve groženj iz 2. točke tega odstavka na razpoložljivost, celovitost in zaupnost sredstev iz 1. točke tega odstavka zaradi ranljivosti iz prejšnje točke ter v analizi obvladovanja tveganj navede ocenjeno stopnjo vpliva uresničitve groženj;

6. oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi ter v analizi obvladovanja tveganj navede oceno o primernosti obstoječih ukrepov;

7. v analizi obvladovanja tveganj ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev;

8. glede na vrednotenje ugotovljenih tveganj in posebnosti delovnega področja, na katerem deluje povezani subjekt, določi in obrazloži oceno sprejemljive ravni tveganj ter

9. navede ukrepe za odpravo ali zmanjšanje tveganj nad sprejemljivo ravnjo tveganj.

(2) Povezani subjekt v sistem upravljanja varovanja informacij vključi najmanj tista informacijska sredstva, ki podpirajo njegove glavne oziroma pomembne storitve in procese za zagotovitev povezave s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom. Centralizirani organi izvedejo to nalogo v sodelovanju z ministrstvom, pristojnim za

upravljanje informacijsko-komunikacijskih sistemov, ki jim mora na zahtevo poslati ustrezne podatke, s katerimi razpolaga, in sicer v 15 dneh od prejema posamičnega zahtevka.

(3) Povezani subjekt izvede popis informacijskih sredstev iz druge točke prvega odstavka tega člena tako, da za vsako informacijsko sredstvo določi oziroma navede najmanj:

1. kratko identifikacijsko oznako, s katero se to informacijsko sredstvo edinstveno identificira;

2. naziv oziroma ime informacijskega sredstva;

3. opis glavnih funkcionalnosti informacijskega sredstva;

4. ime in priimek ali naziv delovnega mesta osebe, ki je skrbnik informacijskega sredstva. Centralizirani organi te podatke navedejo v sodelovanju z ministrstvom, pristojnim za upravljanje informacijsko-komunikacijskih sistemov, ki jim mora na zahtevo poslati ustrezne podatke o skrbništvu posameznega dodeljenega informacijskega sredstva, in sicer v 15 dneh od prejema posamičnega zahtevka, ter

5. opis glavnih komponent strojne oziroma programske opreme.

(4) Povezani subjekt izvede analizo obvladovanja tveganj z določitvijo sprejemljive ravni tveganj tako, da so rezultati teh postopkov dosledni, primerljivi in verodostojni.

IV. OBVLADOVANJE INCIDENTOV INFORMACIJSKE VARNOSTI

7. člen
(navodila in postopki za obvladovanje incidentov informacijske varnosti)

(1) Povezani subjekt izdela in vzdržuje navodila in postopke za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave, ki mu priglaša incidente z možnim pomembnim vplivom na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem.

(2) Navodila in postopki za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave morajo vsebovati najmanj:

1. opis sistema in postopkov za zaznavo incidentov informacijske varnosti v informacijskem sistemu in delovnem okolju;

2. opis sistema in postopkov za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo;

3. opis postopkov za odziv, obravnavo in analizo incidentov informacijske varnosti, vključno z evidentiranjem vseh odzivnih aktivnosti;

4. opis odgovornosti oseb oziroma organizacijskih enot ali pogodbenih izvajalcev, ki jih je treba vključiti v aktivnosti iz prejšnje točke;

5. opis postopkov in odgovornosti za poročanje o incidentih znotraj in zunaj povezanega subjekta;

6. opis protokola obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave.

(3) Obvestilo, ki mora biti zajeto s protokolom obveščanja iz 6. točke prejšnjega odstavka, se pošlje CSIRT organov državne uprave in zajema najmanj:

1. identifikacijsko oznako dogodka oziroma zadeve;

2. ime povezanega subjekta, ki poroča;

3. podatke o osebi, ki poroča, in

4. opis dogodka, ki vsebuje podatke o tem, kdaj, kako in zakaj se je incident zgodil, kdaj je bil odkrit, katera informacijska sredstva so bila prizadeta in kakšni so možni negativni vplivi na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem.

V. MINIMALNI VARNOSTNI UKREPI

8. člen
(sprejetje in izvajanje minimalnih varnostnih ukrepov informacijske varnosti)

(1) Povezani subjekt za zagotavljanje celovitosti, zaupnosti, razpoložljivosti omrežij in informacijskih sistemov sprejme in izvaja organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki izhajajo iz analize obvladovanja tveganj informacijske varnosti in zahtev upravljavca centralnega informacijsko-komunikacijskega sistema, ki jih ta objavi na svoji spletni strani.

(2) Varnostni ukrepi iz prejšnjega odstavka morajo biti:

1. učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje, ki izhajajo iz analize obvladovanja tveganj z oceno sprejemljive ravni tveganj;

2. prilagojeni tako, da se prizadevanja povezanega subjekta usmerijo v ukrepe, ki najbolj vplivajo na njegovo informacijsko varnost, povezano s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom, in se izogibajo podvajanjem;

3. skladni tako, da se primarno obravnavajo osnovne in skupne varnostne ranljivosti povezanega subjekta, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna delovna področja;

4. sorazmerni s tveganji tako, da se izogiba čezmerni obremenitvi povezanega subjekta;

5. konkretni tako, da povezani subjekt te varnostne ukrepe izvaja in da ti ukrepi prispevajo h krepitvi njegove informacijske varnosti;

6. preverljivi tako, da povezani subjekt lahko na zahtevo pristojnega organa predloži dokazila o njihovem izvajanju, in

7. vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sredstev.

(3) Organizacijski, logično-tehnični in tehnični varnostni ukrepi morajo obsegati najmanj:

1. upravljanje pooblastil za dostop;

2. varovanje dostopa do glavnih komponent strojne opreme;

3. preverjanje identitete uporabnikov;

4. zaščito pred zlonamerno programsko kodo;

5. zaznavanje poskusov vdorov in preprečevanje incidentov ter

6. upravljanje in preprečevanje izrab tehničnih ranljivosti.

(4) Ukrepe iz 4. do 6. točke prejšnjega odstavka za centralizirane organe izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov.

(5) Pri načrtovanju in izvajanju varnostnih ukrepov povezani subjekti upoštevajo mednarodne standarde in dobre prakse na področju informacijske varnosti, posebne potrebe delovnega področja povezanega subjekta ter varnostne zahteve upravljavca centralnega informacijsko-komunikacijskega sistema. Informacijski sistem mora izpolnjevati minimalne varnostne zahteve, kar pomeni, da mora imeti nameščeno programsko opremo zadnje (stabilne) verzije oziroma verzije, za katero se zagotavlja podpora proizvajalca programske opreme.

(6) V primerih oziroma delih, kjer varnostne ukrepe izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, mora le-to o izvedenih ukrepih redno obveščati povezani subjekt, za katerega izvaja te ukrepe.

(7) Upravljavec centralnega informacijsko-komunikacijskega sistema varnostne zahteve iz petega odstavka tega člena objavi na svoji spletni strani.

VI. PREHODNI IN KONČNA DOLOČBA

9. člen
(objava na spletnih straneh)

(1) Pristojni nacionalni organ na svoji spletni strani objavi prva priporočila za pripravo varnostne dokumentacije iz četrtega odstavka 4. člena te uredbe v 60 dneh od njene uveljavitve.

(2) Upravljavec centralnega informacijsko-komunikacijskega sistema na svoji spletni strani prvič objavi zahteve iz prvega in iz sedmega odstavka 8. člena te uredbe v 60 dneh od njene uveljavitve.

10. člen
(prenehanje uporabe)

Z dnem začetka uporabe te uredbe se preneha uporabljati Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20 in 49/23 – ZInfV-B).

11. člen
(začetek veljavnosti in uporabe)

Ta uredba začne veljati 1. januarja 2024, uporabljati pa se začne 1. maja 2024.

OBRAZLOŽITEV

I. UVOD

1. Pravna podlaga (besedilo, vsebina zakonske določbe, ki je podlaga za izdajo predpisa):

Zakonodaja Republike Slovenije: drugi odstavek 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV).

2. Rok za izdajo uredbe, določen z zakonom:

Rok za izdajo te uredbe je šestdeset dni od uveljavitve Zakona o spremembah in dopolnitvi Zakona o informacijski varnosti (Uradni list RS, št. 49/23; v nadaljnjem besedilu: ZInfV-B), kar je določeno v prehodni določbi prvega odstavka 13. člena (izdaja podzakonskih predpisov) ZInfV-B, in sicer do 27. julija 2023.

3. Splošna obrazložitev predloga uredbe, če je potrebna:

Po prehodni določbi 14. člena ZInfV-B je z dnem uveljavitve tega zakona prenehala veljati Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 in 131/20), ki pa se uporablja do začetka uporabe te predlagane uredbe.

Uredba o informacijski varnosti v državni upravi je določala minimalne skupne zahteve glede informacijske varnosti, ki vključujejo enotne okvire upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi. Navedena uredba je veljala za organe državne uprave in za druge državne organe, organe lokalnih skupnosti, javne agencije in nosilce javnih pooblastil ter druge subjekte, ki se povezujejo s centralnim informacijsko-komunikacijskim sistemom, ter se po prehodni določbi 14. člena za te subjekte še vedno uporablja.

Predlagana uredba bo z začetkom njene uporabe nadomestila uporabo Uredbe o informacijski varnosti v državni upravi in sledi ciljem Uredbe o informacijski varnosti v državni upravi, ki pa ni imela podlage za izvajanje nadzora nad izvajanjem uredbe razen v morebitnih notranjerevizijskih postopkih. Z izdajo predlagane uredbe v skladu z določbo drugega odstavka 18.a člena ZInfV se torej upošteva načelo pravne države.

4. Predstavitev presoje posledic za posamezna področja, če te niso mogle biti celovito predstavljene v predlogu zakona: /

5. Izjava o skladnosti predloga s pravnimi akti Evropske unije in korelacijska tabela, če gre za prenos direktive: /

II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

Obrazložitev k posameznim členom

K 1. členu
Predlagani 1. člen uredbe določa vsebino uredbe, ki se nanaša na vsebine iz prvega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV).

K 2. členu
Predlagana določba vsebinsko opredeljuje pomen izrazov, uporabljenih v tej uredbi, in sicer gre le za tiste izraze, ki niso že opredeljeni oziroma pojasnjeni v ZInfV, kar je v skladu z načelom pravne države.

K 3. členu

Predlagana določba ureja odgovornost za informacijsko varnost v povezani osebi, za kar je odgovoren predstojnik organa oziroma odgovorna oseba pravne osebe (v nadaljnjem besedilu: odgovorna oseba povezanega subjekta), torej je to odvisno od statusne ureditve posameznega povezanega subjekta. Odgovorna oseba povezanega subjekta mora v skladu s prvo alinejo prvega odstavka 18.a člena ZInfV določiti kontaktno osebo za informacijsko varnost in njenega namestnika, kar olajša sodelovanje med povezanim subjektom in pristojnim nacionalnim organom, ki mu povezani subjekt roku iz ZInfV s tem namenom sporoči tudi njune kontaktne podatke in vsakokratno spremembo teh podatkov. Za izvajanje posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta iz druge, tretje in četrte alineje prvega odstavka 18.a člena ZInfV pa odgovorna oseba povezanega subjekta lahko določi tudi drugo fizično ali pravno osebo (ki ni kontaktna oseba), ki je s tem pooblaščena za izvajanje posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta. Gre za avtonomno odločitev posameznega povezanega subjekta, kako bo organiziral svoje delovne procese, vendar pa komunikacija med pristojnim nacionalnim organom in povezanim subjektom poteka po kontaktni osebi in njenem namestniku, in sicer zaradi zagotovitve hitrosti komunikacije in da ne bi bilo zmede. Če se povezani subjekt odloči, da posamezne ali vse naloge iz prvega odstavka 18.a člena ZInfV zanj izvaja druga fizična ali pravna oseba, mora to pogodbeno urediti ter zagotoviti izvajanje dolžnega nadzorstva.

K 4. členu

Predlagana določba določa vsebino in strukturo varnostne dokumentacije, ki jo mora podpisati odgovorna oseba povezanega subjekta, ter določa tudi uskladitev morebitne že obstoječe varnostne dokumentacije, izdelane na podlagi drugih predpisov, s predlagano uredbo. V pomoč povezanim subjektom pristojni nacionalni organ na svoji spletni strani objavi tudi priporočila za pripravo varnostne dokumentacije. Pri tem se je upoštevalo, da so okoliščine pri različnih povezanih subjektih lahko zelo različne in mora biti posledično zagotovljena določena mera prilagodljivosti za povezane subjekte. Zato so v tem primeru na mestu zgolj nezavezujoča priporočila, ki pa so povezanim subjektom lahko v pomoč. Pristojni nacionalni organ, ki je pristojen za objavo priporočil na svoji spletni strani, lahko le-ta po potrebi tudi posodablja.

K 5. členu

Predlagana določba določa izvedbo analize obvladovanja tveganj z oceno sprejemljive ravni tveganj na način iz 6. člena predlagane uredbe, pri čemer jo je treba izvajati najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe v informacijskih sistemih in delovnih procesih. Na podlagi rezultatov analize obvladovanja tveganj in ocene sprejemljive ravni tveganj povezani subjekti sprejmejo ustrezne varnostne ukrepe (pojasnjujemo, da gre najmanj za ukrepe iz 8. člena te uredbe). Iz razloga preglednosti in sledljivosti je predpisano tudi dokumentiranje in hranjenje informacij o ugotovitvah ocene sprejemljive ravni tveganj ter o obravnavi tveganj informacijske varnosti.

K 6. členu

Predlagana določba v prvem odstavku navaja predpisane korake oziroma metodologijo za pripravo in izvedbo analize obvladovanja tveganj informacijske varnosti. V drugem in tretjem odstavku navaja korake za izvedbo popisa sredstev oziroma virov, ki podpirajo tiste glavne oziroma pomembne storitve in procese, ki zagotavljajo povezavo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom. Pri tem določbe prvega, drugega in tretjega odstavka upoštevajo, da tisti povezani subjekti, ki so hkrati tudi centralizirani organi državne uprave (v nadaljnjem besedilu: centralizirani organi), nimajo v lasti oziroma upravljanju posameznih informacijskih sredstev (delovne postaje, prenosniki, strežniki, stikala in drugo), ki jih uporabljajo za povezovanje v centralno državno informacijsko-komunikacijsko omrežje oziroma sistem, saj so ta sredstva v lasti oziroma upravljanju ministrstva, pristojnega za upravljanje informacijsko-komunikacijskih sistemov. Zato centralizirani organi določene naloge, in sicer tiste iz 2. točke prvega odstavka, iz drugega odstavka in iz 4. točke tretjega odstavka tega člena, lahko izvedejo le ob sodelovanju z ministrstvom, pristojnim za upravljanje informacijsko-komunikacijskih sistemov, ki jim mora zato na zahtevo poslati ustrezne podatke, s katerimi razpolaga, in sicer v 15 dneh od prejema posamičnega zahtevka.

Četrti odstavek v skladu s pravili (informacijskovarnostne) stroke določa, da povezani subjekt izvede analizo obvladovanja tveganj z določitvijo sprejemljive ravni tveganj tako, da so rezultati teh postopkov dosledni, primerljivi in verodostojni.

K 7. členu

Predlagana določba opredeljuje najmanjši obseg načrta odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave in določa način obveščanja CSIRT organov državne uprave ter obvezne vsebine oziroma elemente, ki jih mora to obvestilo zajemati.

K 8. členu
Predlagana določba določa obveznosti povezanih subjektov glede sprejetja in izvajanja minimalnih varnostnih ukrepov informacijske varnosti, in sicer izvajanje organizacijskih, logično-tehničnih in tehničnih varnostnih ukrepov, ki izhajajo iz izvedene analize obvladovanja tveganj informacijske varnosti in predloženih zahtev upravljavca centralnega informacijsko-komunikacijskega sistema, ki jih ta objavi na svoji spletni strani. Takšna objava je potrebna tudi glede morebitne posodobitve prej navedenih zahtev.

Kot minimalni oziroma obvezni varnostni ukrepi so določeni ukrepi oziroma varnostne kontrole za: preverjanje identitete uporabnikov, upravljanje pooblastil za dostop, varovanje dostopa do glavnih komponent strojne opreme, zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov ter upravljanje in preprečevanje izrab tehničnih ranljivosti. Zaradi upoštevanja položaja centraliziranih organov zadnje tri navedene ukrepe za takšne povezane organe izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov.

Pri izvajanju drugega in tretjega odstavka 8. člena uredbe morajo zavezanci v skladu s petim odstavkom tega člena predlagane uredbe upoštevati mednarodne standarde in dobre prakse na področju informacijske varnosti, posebne potrebe delovnega področja posameznega povezanega subjekta ter predložene varnostne zahteve upravljavca centralnega informacijsko-komunikacijskega sistema. Informacijski sistem mora izpolnjevati minimalne varnostne zahteve, kar pomeni, da mora imeti nameščeno programsko opremo zadnje (stabilne) verzije oziroma verzije, za katero se zagotavlja podpora proizvajalca programske opreme.

V primerih oziroma delih, kjer varnostne ukrepe izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, mora le-to o izvedenih ukrepih redno obveščati povezani subjekt, za katerega izvaja te ukrepe.

Upravljavec centralnega informacijsko-komunikacijskega sistema varnostne zahteve iz petega odstavka tega člena objavi na svoji spletni strani. Navedeno vključuje možnost, da takšne zahteva lahko po potrebi na isti način tudi posodablja.

K 9. členu
Prehodna določba določa rok šestdesetih dni po uveljavitvi te uredbe za prve objave pristojnih organov na njihovih spletnih straneh. Pri tem gre v prvem odstavku za objavo priporočil pristojnega nacionalnega organa iz četrtega odstavka 4. člena, v drugem odstavku pa gre za objavi zahtev upravljavca centralnega informacijsko-komunikacijskega sistema iz prvega in sedmega odstavka 8. člena te uredbe.

K 10. členu
Z dnem začetka uporabe te uredbe se preneha uporabljati Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20 in 49/23 – ZInfV-B).

K 11. členu
Predlagana končna določba določa uveljavitev uredbe z dnem 1. januarja 2024. Določa se tudi začetek uporabe te uredbe z dnem 1. maja 2024. Navedena določba torej daje povezanim subjektom ustrezen čas po uveljavitvi predlagane uredbe in po predvidenih objavah v skladu z 9. členom predlagane uredbe za njihovo prilagoditev predlagani uredbi. Sicer bi morali povezani subjekti že zdaj izpolnjevati določene pogoje iz Uredbe o informacijski varnosti v državni upravi, ki je bistveno bolj obširna, zato prilagoditev predlagani uredbi ne bi smela obremenjevati zavezancev.