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, določitev kontaktne osebe za informacijsko varnost in njenega namestnika ter posredovanje njunih podatkov pristojnemu nacionalnemu organu, minimalni obseg varnostnih ukrepov glede informacijske varnosti in pripravo navodil ter 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. 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 incidente z možnim vplivom na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem.
4. ocenitev tveganja je celotni proces ugotavljanja tveganja, analize tveganja in ovrednotenja tveganja;
5. ovrednotenje tveganja je proces primerjanja rezultatov analize tveganja z merili tveganja, da bi ugotovili, ali je tveganje oziroma njegova velikost sprejemljiva oziroma znosna;
6. razpoložljivost je lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo;
7. 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;
8. ugotavljanje tveganja je proces odkrivanja, prepoznavanja in opisovanja tveganj;
9. 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) Za izvajanje posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta odgovorna oseba povezanega subjekta določi kontaktno osebo za informacijsko varnost in njenega namestnika ter posreduje njune kontaktne podatke pristojnemu nacionalnemu organu.

4. člen
(kontaktna oseba za informacijsko varnost)

Kontaktna oseba za informacijsko varnost in njen namestnik sta v povezanem subjektu zadolžena za izvajanje posameznih ključnih nalog na področju informacijske varnosti, ki so povezane s sistemom upravljanja varovanja informacij, ki zagotavlja povezovanje s centralnim informacijsko-komunikacijskim sistemom.

III. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

5. člen
(vsebina in struktura varnostne dokumentacije)

(1) Povezani subjekti izdelajo varnostno dokumentacijo, ki vsebuje najmanj elemente iz prvega 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).

(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.

6. člen
(analiza obvladovanja tveganj)

(1) Povezani subjekt pripravi analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj na način iz 7. 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 sprejem tveganj in merila za izvajanje ocenitve tveganj informacijske varnosti.

(4) Povezan subjekt hrani dokumentirane informacije o ugotovitvah ocenitev tveganj in obravnave tveganj informacijske varnosti.

7. 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;

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

4. prepozna in v analizo obvladovanja tveganj navede ranljivosti sredstev iz 2. točke tega odstavka, ki bi jih lahko grožnje iz prejšnje točke 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 in v analizo obvladovanja tveganj navede ocenjeno stopnjo vpliva uresničitve groženj;

6. oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi ter v analizo 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 raven tveganj in

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, ki zagotavljajo povezavo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom.

(3) Povezani subjekt izvede popis informacijskih sredstev iz druge točke prvega odstavka tega člena na način, da vsakemu informacijskemu sredstvu določi oziroma navede najmanj:

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

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 in

5. opis glavnih komponent strojne oziroma programske opreme.

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

IV. OBVLADOVANJE INCIDENTOV INFORMACIJSKE VARNOSTI

8. 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 beleženjem 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 izven povezanega subjekta;

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

(3) Obvestilo iz 6. točke prejšnjega odstavka se pošlje CSIRT organov državne uprave in zajema najmanj:

1. identifikacijsko oznako dogodka oziroma zadeve;

2. naziv povezanega subjekta, ki poroča

2. podatke o osebi, ki poroča in

3. 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 potencialni ali možni negativni vplivi na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem.

V. MINIMALNI VARNOSTNI UKREPI

9. člen
(sprejem 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 upravljalca centralnega državno informacijsko-komunikacijskega sistema.

(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 njihovo 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 prekomernemu bremenu za povezani subjekt;

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

6. preverljivi tako, da lahko na zahtevo pristojnega organa predloži dokazila o njihovi implementaciji 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. preverjanje identitete uporabnikov;

2. upravljanje s pooblastil za dostop;

3. varovanje dostopa do glavnih komponent strojne opreme;

4. zaščito pred zlonamerno programsko kodo;

5. zaznavanje poskusov vdorov in preprečevanje incidentov in

6. upravljanje in preprečevanje izrab tehničnih ranljivosti.

(4) Pri načrtovanju in izvajanju varnostih ukrepov povezani subjekti upoštevajo mednarodne standarde in dobre prakse na področju informacijske varnosti, posebne potrebe delovnega

področja povezanega subjekta ter varnostne zahteve upravljalca centralnega državno informacijsko-komunikacijskega sistema.

VI. PREHODNA IN KONČNA DOLOČBA

10. člen
(pričetek in prenehanje uporabe)

(1) Ta uredba se prične uporabljati šestdeseti dan po njeni uveljavitvi.

(2) Z dnem pričetka uporabe te uredbe se preneha uporabljati Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 in 131/20).

11. člen

(začetek veljavnosti)

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

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. 7. 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 pričetka 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 in se po prehodni 14. člena za te subjekte še vedno uporablja

Predlagana uredba bo s pričetkom njene uporabe nadomestila uporabo Uredbo o informacijski varnosti v državni upravi in sledi ciljem Uredbe o informacijski varnosti v državni upravi, ki pa ni imela podlage za izvajanja nadzora nad izvajanjem uredbe razen v morebitnih notranje revizijskih postopkih. Z izdajo predlagane uredbe skladno 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
Predlagan 1. člen uredbe določa vsebino uredbe, ki se nanaša na prvi odstavek 18.a člena Zakona o informacijski varnosti.

K 2. členu
Predlagana določba vsebinsko opredeljuje pomen izrazov uporabljenih v tej uredbi.

K 3. členu
Predlagana določba ureja odgovornost za informacijsko varnost povezane osebe, za kar je odgovoren predstojnik organa oziroma odgovorna oseba pravne osebe (v nadaljnjem besedilu: odgovorna oseba povezanega subjekta), kar je torej odvisno od statusne ureditve posameznega povezanega subjekta. Odgovorna oseba povezanega subjekta mora za izvajanje posameznih ključnih nalog informacijske varnosti določiti kontaktno osebo za informacijsko varnost in njenega namestnika, ki sta s tem torej pooblaščena za izvajanje posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta. Njune kontaktne podatke je treba tudi sporočiti pristojnemu nacionalnemu organu, kar olajša potrebno sodelovanje s povezanim subjektom ter doprinese k hitrosti reševanja zadev informacijske varnosti med njima.

K 4. členu
Predlagana določba natančneje opredeljuje naloge kontaktne osebe za informacijsko varnost in njenega namestnika v povezanem subjektu in sicer naloge na področju informacijske varnosti, ki so povezane s sistemom upravljanja varovanja informacij, ki zagotavlja povezovanje s centralnim informacijsko-komunikacijskim sistemom.

K 5. členu
Predlagana določba določa vsebino in strukturo varnostne dokumentacije, katero mora podpisati odgovorna oseba povezanega subjekta ter določa tudi uskladitev morebitne že obstoječe varnostne dokumentacije, izdelane na podlagi drugih predpisov, s predlagano uredbo.

K 6. členu
Predlagana določba določa izvedbo analize obvladovanja tveganj z oceno sprejemljive ravni tveganj, na način iz 7. člen predlagane uredbe, pri čemer jo je trebno 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 ukrepe iz 9. člena te uredbe) in določa obveznost hrambe dokumentiranih informacij v izvezi s tveganji informacijske varnosti.

K 7. 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 predlagana določba 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. Četrti odstavek v skladu s pravili (informacijsko-varnostne) stroke določa, da povezani subjekt izvede analizo obvladovanja tveganj z določitvijo sprejemljive ravni tveganj tako, da bodo rezultati teh postopkov dosledni, primerljivi in verodostojni.

K 8. členu
Predlagana določba opredeljuje najmanjši obseg načrta odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave ter določa način obveščanja CSIRT organov državne uprave ter vsebine oziroma elemente, ki jih mora to obvestilo najmanj zajemati.

K 9. členu
Predlagana določba določa obveznosti povezanih subjektov glede sprejema 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 podanih zahtev upravljalca centralnega državno informacijsko-komunikacijskega sistema. Kot minimalni oziroma obvezni varnostni ukrepi so določeni ukrepi oziroma varnostne kontrole za: preverjanje identitete uporabnikov, upravljanje s pooblastil za dostop, varovanje dostopa do glavnih komponent strojne opreme, zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov in upravljanje in preprečevanje izrab tehničnih ranljivosti.
Pri izvajanju drugega in tretjega odstavka 9. člena uredbe morajo zavezanci upoštevati mednarodne standarde in dobre prakse na področju informacijske varnosti, posebne potrebe delovnega področja posameznega povezanega subjekta ter podane varnostne zahteve upravljalca centralnega državno informacijsko-komunikacijskega sistema.

K 10. členu
Predlagana prehodna določba določa pričetek uporabe predlagane uredbe, ki je šestdeseti dan po objavi v Uradnem listu Republike Slovenije. Prav tako določa tudi prenehanje uporabe Uredbe o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 in 131/20) in sicer s pričetkom uporabe predlagane uredbe. Navedena določba torej daje povezanim subjektom ustrezen čas po uveljavitvi predlagane uredbe za njihovo prilagoditev predlagani uredbi. Sicer bi morali povezani subjekti že sedaj izpolnjevati določene pogoje iz Uredbe o informacijski varnosti v državni upravi, ki pa je bistveno bolj obširna zato prilagoditev predlagani uredbi ne bi smela povzročati bremena za zavezance.

K 11. členu
Predlagana končna določba določa uveljavitev uredbe, ki je naslednji dan po objavi v Uradnem listu Republike Slovenije.