REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 83 30
F: 01 478 83 31
E: gp.mju@gov.si
www.mju.gov.si

GENERALNI SEKRETARIAT
VLADE REPUBLIKE SLOVENIJE
gp.gs@gov.si

Številka: 007-7/2017/106
Ljubljana, 10. 4. 2018

ZADEVA: Uredba o informacijski varnosti v državni upravi (EVA 2016-3130-0001) – predlog za obravnavo – novo gradivo št. 2
1. Predlog sklepov vlade:
Na podlagi sedmega odstavka 21. člena 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 in 65/14) je Vlada Republike Slovenije na … seji dne… sprejela naslednji sklep: Vlada Republike Slovenije je sprejela Uredbo o informacijski varnosti v državni upravi (EVA 2016-3130-0001) in jo objavi v Uradnem listu Republike Slovenije. mag. Lilijana Kozlovič GENERALNA SEKRETARKA Sklep prejmejo: – Ministrstvo za javno upravo, – Ministrstvo za pravosodje, – Ministrstvo za finance, – Služba Vlade RS za zakonodajo. Priloge: – predlog Uredbe o informacijski varnosti v državni upravi
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:
- Boris Koprivnikar, minister, Ministrstvo za javno upravo - mag. Jurij Bertok, generalni direktor Direktorata za informatiko - Damjan Križman, vodja Sektorja za informacijsko varnost, Direktorat za informatiko - mag. Matjaž Jevševar, sekretar, Direktorat za informatiko - mag. Damijan Marinšek, sekretar, Direktorat za informatiko
3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:
Pri pripravi gradiva niso sodelovali zunanji strokovnjaki.

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:		
/		
5. Kratek povzetek gradiva:		
V 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 in 51/16), ki ureja upravljanje informacijsko komunikacijskih sistemov državne uprave, je četrtem odstavku zapisano, da »vlada določi podatkovne in tehnološke standarde, smernice za skupne informacijske rešitve in skupno varnostno politiko.« Uredba o informacijski varnosti v državni upravi določa skupno varnostno politiko oziroma skupno politiko informacijske varnosti organov državne uprave in velja tudi za druge državne organe, organe lokalnih skupnosti, javne agencije in nosilce javnih pooblastil ter druge subjekte, ki se povezujejo s centralnim informacijsko komunikacijskim sistemom. S to uredbo so določeni enotni okviri upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi.		
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	**DA**
c)	administrativne posledice	**DA**
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 – razvojne dokumente Evropske unije in mednarodnih organizacij	**NE**
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

V zvezi s predlaganim vladnim gradivom se navedejo predvidene spremembe (povečanje, zmanjšanje):

- prihodkov državnega proračuna in občinskih proračunov,
- odhodkov državnega proračuna, ki niso načrtovani na ukrepih oziroma projektih sprejetih proračunov,
- obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana na ukrepih oziroma projektih sprejetih proračunov.

II. Finančne posledice za državni proračun

Prikazane morajo biti finančne posledice za državni proračun, ki so na proračunskih postavkah načrtovane v dinamiki projektov oziroma ukrepov:

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

Navedejo se proračunski uporabnik, ki financira projekt oziroma ukrep; projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in proračunske postavke (kot proračunski vir financiranja), na katerih so v celoti ali delno zagotovljene pravice porabe (v tem primeru je nujna povezava s točko II.b). Pri uvrstitvi novega projekta oziroma ukrepa v načrt razvojnih programov se navedejo:

- proračunski uporabnik, ki bo financiral novi projekt oziroma ukrep,
- projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in
- proračunske postavke.

Za zagotovitev pravic porabe na proračunskih postavkah, s katerih se bo financiral novi projekt oziroma ukrep, je treba izpolniti tudi točko II.b, saj je za novi projekt oziroma ukrep mogoče zagotoviti pravice porabe le s prerazporeditvijo s proračunskih postavk, s katerih se financirajo že sprejeti oziroma veljavni projekti in ukrepi.

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Navedejo se proračunski uporabniki, sprejeti (veljavni) ukrepi oziroma projekti, ki jih proračunski uporabnik izvaja, in proračunske postavke tega proračunskega uporabnika, ki so v dinamiki teh projektov oziroma ukrepov ter s katerih se bodo s prerazporeditvijo zagotovile pravice porabe za dodatne aktivnosti pri obstoječih projektih oziroma ukrepih ali novih projektih oziroma ukrepih, navedenih v točki II.a.

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

Če se povečani odhodki (pravice porabe) ne bodo zagotovili tako, kot je določeno v točkah II.a in II.b, je povečanje odhodkov in izdatkov proračuna mogoče na podlagi zakona, ki ureja izvrševanje državnega proračuna (npr. priliv namenskih sredstev EU). Ukrepanje ob zmanjšanju prihodkov in prejemkov proračuna je določeno z zakonom, ki ureja javne finance, in zakonom, ki ureja izvrševanje državnega proračuna.

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

Kratka obrazložitev

Ocenjujemo, da posledice za javnofinančna sredstva ne presegajo 40.000 EUR v tekočem in naslednjih treh letih, saj uredba ureja področje informacijske varnosti v skladu z uveljavljeno dobro poslovno prakso, ki se je v veliki meri v organih državne uprave in pri drugih zavezancih že izvajala. Uvedbo oziroma uporabo posameznih tehničnih nadzorstev že sedaj predpisujejo številni predpisi, kot so: Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih, Uredba o upravnem poslovanju, Priporočila informacijske varnostne politike… Uredba nalaga zavezancem tudi uvedbo nekaterih specifičnih nadzorstev na podlagi predhodno opravljene ocene tveganja. Neposrednih finančnih posledic uvedbe teh nadzorstev ni mogoče vnaprej predvideti. Vendar pa morajo biti morebitne naložbe v dodatna nadzorstva uravnotežene tako, da bodo stroški uvedbe posameznega nadzorstva sorazmerni s škodo, ki bi lahko nastala, če nadzorstva ne bi uvedli.

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na: - pristojnosti občin, - delovanje občin, - financiranje občin.	**NE**

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: DA/ **NE**
- Združenju občin Slovenije ZOS: DA/ **NE**

– Združenju mestnih občin Slovenije ZMOS: DA/ **NE** Predlogi in pripombe združenj so bili upoštevani: – v celoti, – večinoma, – delno, – niso bili upoštevani. Bistveni predlogi in pripombe, ki niso bili upoštevani.
9. Predstavitev sodelovanja javnosti:
Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja: **NE**
Gradivo se nanaša na interno poslovanje državne uprave.
(Če je odgovor DA, navedite: Datum objave: …… V razpravo so bili vključeni: – nevladne organizacije, – predstavniki zainteresirane javnosti, – predstavniki strokovne javnosti. – . Mnenja, predlogi in pripombe z navedbo predlagateljev (imen in priimkov fizičnih oseb, ki niso poslovni subjekti, ne navajajte): Upoštevani so bili: – v celoti, – večinoma, – delno, – niso bili upoštevani. Bistvena mnenja, predlogi in pripombe, ki niso bili upoštevani, ter razlogi za neupoštevanje: Poročilo je bilo dano …….. Javnost je bila vključena v pripravo gradiva v skladu z Zakonom o …, kar je navedeno v predlogu predpisa.)
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti: DA
11. Gradivo je uvrščeno v delovni program vlade: DA
Boris Koprivnikar minister

BESEDILO PREDLOGA UREDBE – Priloga 1 (ločen dokument)

Besedilo predloga uredbe je glede na besedilo iz prvotnega gradiva nekoliko spremenjeno v 4., 6., 22., 27. in 64. členu. Manjše spremembe so posledica upoštevanja pripomb / nasprotovanj obravnavi objavljenega vladnega gradiva Ministrstva za notranje zadeve, Ministrstva za kulturo in Ministrstva za obrambo.

Novo gradivo št.2

Besedilo predloga uredbe je glede na besedilo iz predhodnega gradiva, po uskladitvah z MK, MNZ, MZZ, KPV in SVZ spremenjeno:

Naslov uredbe je spremenjen v »Uredba o informacijski varnosti v državni upravi«

2. člen (pomen izrazov)
Brisan je izraz »katastrofičen dogodek«, ki se v besedilu ne pojavlja več v besedni zvezi obnovitev (okrevanje) po katastrofičnem dogodku (angl. disaster recovery), »disaster recovery« je v besedilu sedaj opisan kot »okrevanja po nenadnem dogodku, ki povzroči škodo večjih razsežnosti«;
Dodan je izraz »okrevanje«;
Brisani sta izraza »kibernetski napad« in »kibernetski prostor«, ker se v besedilu uredbe ne pojavljata več;
Nov je izraz »storitve računalništva v javno dostopnem oblaku«, ki je v veliki meri usklajen z definicijo pojma v direktivi NIS; nadomestil je izraza »računalništvo v oblaku« in »javni oblak«;

3. člen (odbor za upravljanje informacijske varnosti)
Zaradi jasnosti, da k delu odbora ne sodi reševanje incidentov, je v tretji alineji 4. odstavka (naloge odbora) sedaj zapisano »obravnava poročil o dogodkih in incidentih…«;
Predlagano spremembo 4. alineje 4. odstavka (KPV), da naj odbor poroča nacionalnemu organu, pristojnemu za informacijsko varnost in ne vladi, smo morali po ponovnem pregledu SVZ umakniti. Pojasnilo je v priloženem mnenju SVZ.

4. člen (naloge ministrstva)
Manjše spremembe v dikciji 2. odstavka.

13. člen (obvezni dokumenti)
2. alineja 1. odstavka (v izogib izrazu katastrofičen dogodek / katastrofa) sedaj glasi: »načrt neprekinjenosti poslovanja in okrevanja po nenadnem dogodku, ki povzroči škodo večjih razsežnosti«.

14. člen (operativna navodila)
V prvem odstavku je brisano »za vsak informacijski sistem«; drugi odstavek je skrajšan in poenostavljen; dodan je 4. odstavek: »Operativna navodila se redno posodablja.«;

15. člen (načrt neprekinjenosti poslovanja in okrevanja po nenadnem dogodku, ki povzroči škodo večjih razsežnosti)
Besedilo tega člena je v 1. odstavku usklajeno tako, da se ne uporablja izraz »katastrofičen dogodek«;

19. člen (obveščanje in priglasitev dogodkov informacijske varnosti)
Namesto »poročanja o« se uporablja izraz »priglasitev« (kot v direktivi NIS);
Predlagan nov 5. odstavek (KPV): »Če dogodek informacijske varnosti izpolnjuje kriterije za priglasitev incidentov po drugih predpisih, ga organ, ki je zavezanec po teh predpisih, priglasi tudi v skladu s temi predpisi« smo morali po ponovnem pregledu SVZ umakniti. S tem se ne spreminja vsebina določb tega člena. Pojasnilo je v priloženem mnenju SVZ.

20. člen (evidentiranje incidentov informacijske varnosti)

Nadomeščena je beseda »poročanje« z besedo »evidentiranje«; Dodana sta nov prvi odstavek: »Ministrstvo vodi evidenco incidentov informacijske varnosti« in 3. odstavek: »Evidenco incidentov informacijske varnosti se sprotno posodablja«;

23. člen (varnostna presoja informacijskih sistemov)
1. odstavek sedaj glasi: »Skrbnik informacijskega sistema zagotovi izvedbo neodvisne varnostne presoje informacijskega sistema vsaj pred prvim prenosom v obratovalno okolje in po vsaki večji spremembi, ki ima oziroma bi lahko imela vpliv na varnost v informacijskem sistemu obravnavanega informacijskega premoženja.« (omiljena je določba, ki predpisuje, kdaj je treba izvesti varnostno presojo);
Dodan je nov 2. odstavek (prej 3.), ki pojasnjuje, kaj je »neodvisna varnostna presoja«;
3. odstavek: izraz »katastrofičen dogodek« nadomeščen z opisom;
Novo besedilo 4. odstavka: »Postopek varnostne presoje se dokumentira«;

37. člen (uporaba zasebnih informacijskih naprav)
4. odstavek sedaj glasi: »Če se v omrežju zazna nedovoljena naprava, se naprava odstrani ali onemogoči, zadeva pa se obravnava kot varnostni incident v skladu z določbami o dogodkih in incidentih informacijske varnosti iz te uredbe.« (določba tega odstavka sedaj več ne predpisuje uvedbo naprav za odkrivanje nedovoljenih naprav v omrežju);

41. člen (uporaba storitev računalništva v javno dostopnem oblaku)
Člen je usklajen s spremembami v pomenih izrazov; sedaj se uporablja izraz »storitev računalništva v javno dostopnem oblaku«;

44. člen (nadzor nad prenosno kodo)
Manjše spremembe, brisana 1. alineja;

54. člen (varnost gesel)
Manjše spremembe v 1. in 2. odstavku (določba tega odstavka sedaj več ne predpisuje uvedbo sistemov za upravljanje z gesli);

62. člen (prenosne informacijske naprave)
Brisan 6. odstavek.

Dodan nov 64. člen (obstoječi dokumenti): »Šteje se, da organi, ki imajo lastne informacijske sisteme in ki že imajo sprejete dokumente, ki so po vsebini skladni z določbami 14. in 15. člena te uredbe, izpolnjujejo določbe 13. člena te uredbe«.

65. člen (prej 64.) (roki za izvedbo ukrepov in posredovanje podatkov)
Lektorski popravki;
Manjše korekcije rokov in prilagoditve zaradi drugih sprememb.

Novo gradivo št.3

39. člen (uporaba sistema elektronske pošte), odstavek (6): brisano »ki ga je odobril organ, pristojen za kriptografsko zaščito podatkov«.
45. člen (upravljanje izmenljivih nosilcev podatkov), odstavek (3): brisano »ki ga je odobril organ, pristojen za kriptografsko zaščito podatkov«.
52. člen (postopki avtentikacije): brisano »kjer se zagotovi, da informacijski sistemi uporabljajo mehanizme, ki izpolnjujejo zahteve glede kakovosti varnostnih žetonov. Ki jih predpiše organ, pristojen za kriptografsko zaščito podatkov«.
53. člen (večfaktorska avtentikacija), odstavek (3): brisano »in ta naprava izpolnjuje zahteve, ki jih predpiše organ, pristojen za kriptografsko zaščito podatkov«.
54. člen (varnost gesel): brisan odstavek (1).
59. člen (primerne kriptografske rešitve): brisano »ki jih odobri organ, pristojen za kriptografsko zaščito podatkov, in tisti«.

OBRAZLOŽITEV

I. UVOD

1. Pravna podlaga:

Zakonodaja RS: Četrti odstavek 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 in 51/16)

2. Rok za izdajo uredbe z zakonom ni določen.

3. Splošna obrazložitev predloga uredbe, če je potrebna:

Informacijska varnost (varovanje oziroma ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij) je v današnji družbi, ki je v veliki meri odvisna od delovanja informacijskih sistemov oziroma razpoložljivosti informacijskih storitev, izjemnega pomena. Skrb za informacijsko varnost v konkurenčnem tržnem okolju informacijske družbe je poslovna nuja, v državni upravi pa obveznost do državljanov in drugih uporabnikov njenih storitev.

Organi državne uprave morajo na področju informacijske varnosti upoštevati določbe Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05 z dne 3. 3. 2005 in spremembe), ki se nanašajo na informacijsko varnost. Uredba o upravnem poslovanju je večino določb o informacijski varnosti zajela v 4. podpoglavju (Informacijska varnost) V. poglavja, nekaj določb s to tematiko pa najdemo tudi v 1. (Zgradbe in prostori) in 2. podpoglavju (Oprema) tega poglavja. Določbe iz zgoraj omenjene uredbe področja informacijske varnosti ne urejajo celovito.

Na podlagi 80. člena Uredbe o upravnem poslovanju je Ministrstvo za javno upravo izdalo Priporočila informacijske varnostne politike javne uprave (št: 386-2/2008/23, z dne 28. 10. 2010) in jih objavilo na svojih spletnih straneh. Ta dokument celoviteje ureja področje informacijske varnosti v javni upravi, vendar gre za nezavezujoča priporočila.

Zakon 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 in 51/16) v 74. a členu ureja upravljanje informacijsko komunikacijskih sistemov državne uprave. V četrtem odstavku tega člena je zapisano, da »Vlada določi podatkovne in tehnološke standarde, smernice za skupne informacijske rešitve in **skupno varnostno politiko**.« Namen Uredbe o informacijski varnosti v državni upravi je določiti skupno varnostno politiko oziroma skupno politiko informacijske varnosti organov državne uprave. Ta uredba bo veljala tudi za druge državne organe, organe lokalnih skupnosti, javne agencije in nosilce javnih pooblastil ter druge subjekte, ki se povezujejo s centralnim informacijsko komunikacijskim sistemom. S to uredbo se določa minimalne skupne zahteve informacijske varnosti, ki vključujejo enotne okvire upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi.

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

5. Izjava o skladnosti predloga predpisa s pravnimi akti EU:

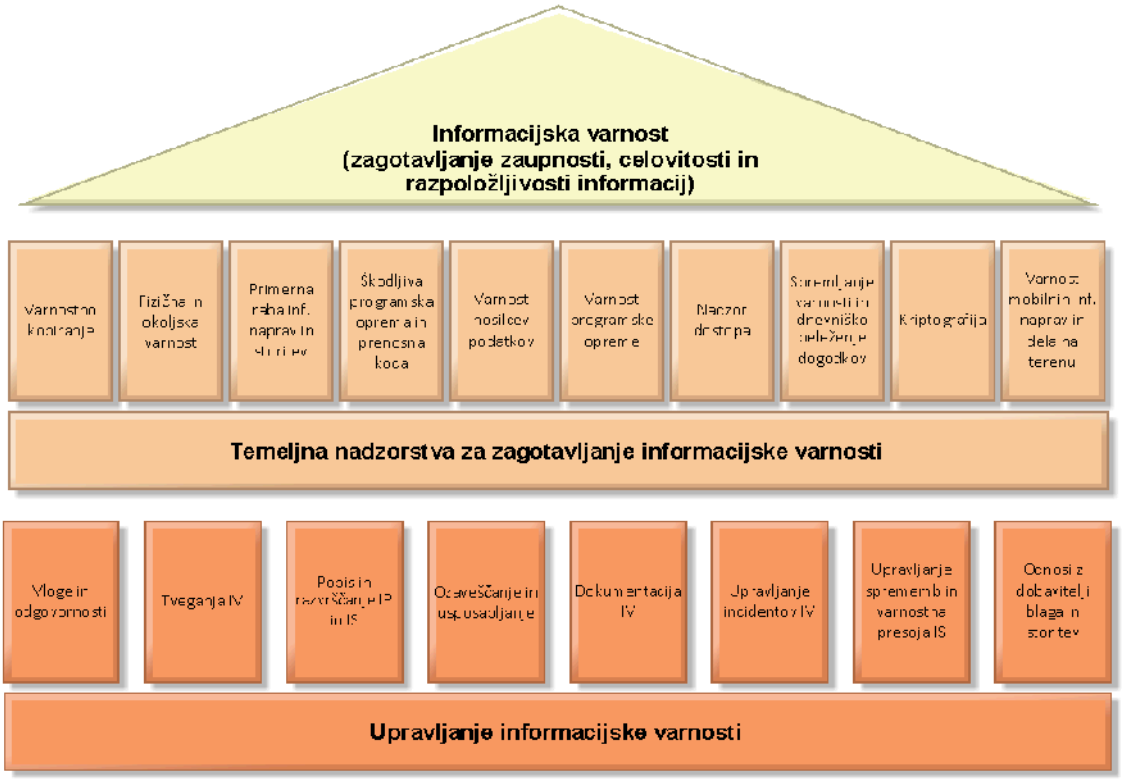
-

II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

Struktura uredbe

Uredba je razdeljena na 4 poglavja. I. poglavje (Splošne določbe) vsebuje določbe o namenu uredbe in področju njene uporabe ter določa pomen uporabljenih izrazov v tej uredbi. II. (Upravljanje informacijske varnosti) in III. (Temeljna nadzorstva za zagotavljanje informacijske varnosti) poglavje sta osrednji poglavji uredbe, v katerih so določene ključne prvine sistema informacijske varnosti organov državne uprave ter drugih subjektov, ki se povezujejo s centralnim informacijsko komunikacijskim sistemom državne uprave. Zadnje, IV. poglavje (Prehodne in končne določbe) vsebuje določbe o prehodnem obdobju za izvajanje posameznih določb, razveljavlja tiste člene Uredbe o upravnem poslovanju, ki se nanašajo na informacijsko varnost ter določa začetek veljavnosti te uredbe.

Sistem informacijske varnosti temelji na učinkovitem upravljanju informacijske varnosti in na uvedbi temeljnih nadzorstev za zagotavljanje informacijske varnosti. *Model tega sistema, ki se odraža v strukturi uredbe, je prikazan na spodnji sliki.*



Obrazložitev

I. SPLOŠNE DOLOČBE

Namen uredbe je določiti skupno politiko informacijske varnosti za organe državne uprave ter druge subjekte, ki se povezujejo s centralnim informacijsko komunikacijskim sistemom državne uprave. Določa enotne okvire upravljanja informacijske varnosti v državni upravi in temeljna nadzorstva za zagotavljanje informacijske varnosti (1. člen).

Izrazi, ki so uporabljeni v tej uredbi (2. člen), so, kjer je to mogoče, usklajeni s standardom ISO/IEC 27000:2014.

II. UPRAVLJANJE INFORMACIJSKE VARNOSTI

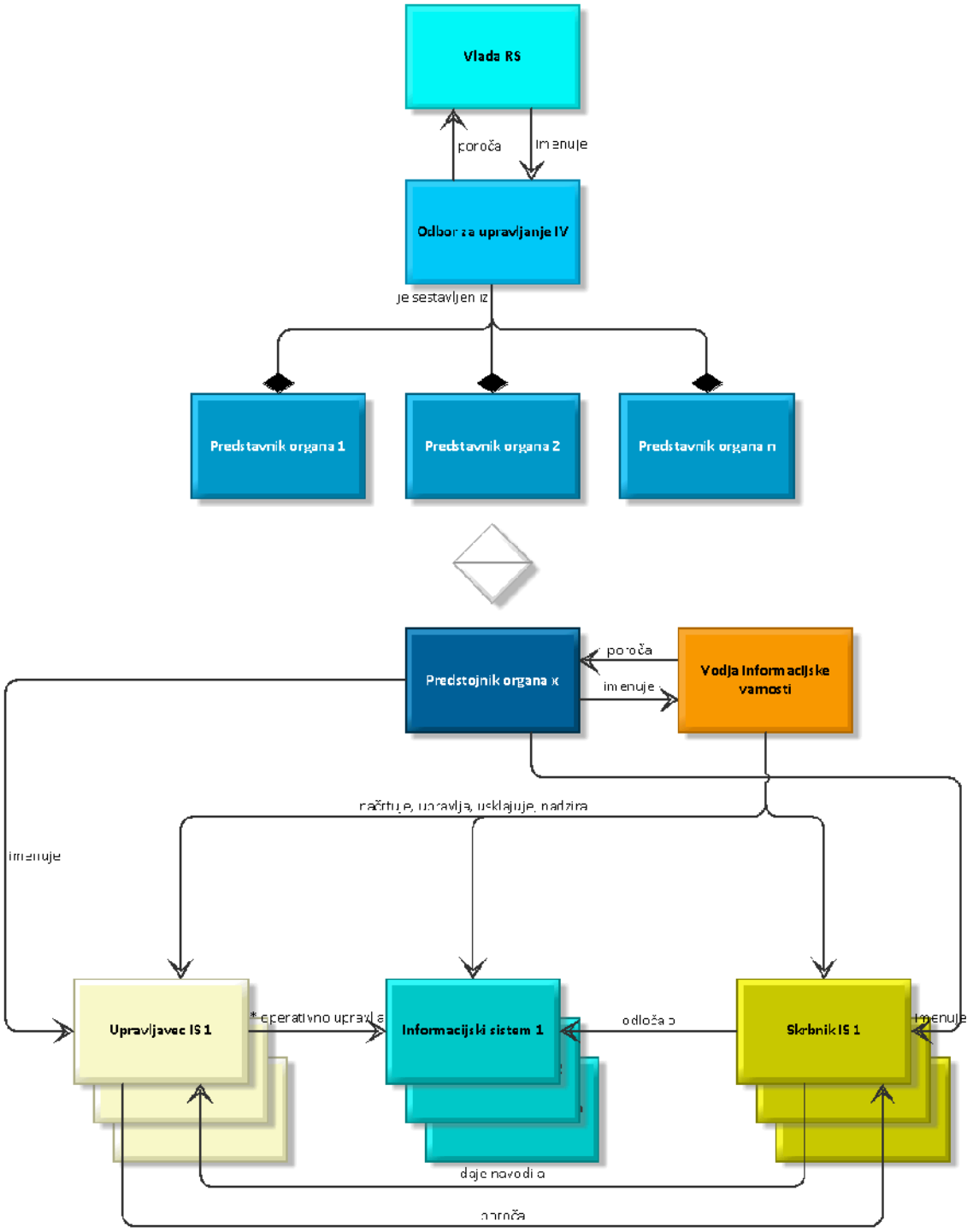
V poglavju Upravljanje informacijske varnosti je določena enotna upravljavska struktura informacijske varnosti v državni upravi.

1. Vloge in odgovornosti

Na ravni celotne državne uprave se ustanovi odbor za upravljanje informacijske varnosti, ki koordinira aktivnosti na področju informacijske varnosti v državni upravi. Odbor, ki ga imenuje vlada, je sestavljen iz predstavnikov tistih organov, ki opravljajo ključne naloge na področju varnosti in informatike v državni upravi. Naloge odbora so upravljavske in ne operativne. Način dela odbora se uredi s poslovnikom (3. člen).

Ministrstvo, pristojno za javno upravo, je, v skladu z določbami Zakona o državni upravi (74.a člen), pristojno za izvajanje enotne informacijske varnostne politike. V okviru izvajanja enotne varnostne politike izvaja naloge in pristojnosti, kot so: spremljanje izvajanja določb te uredbe, odzivanje na incidente informacijske varnosti v organih in pri drugih zavezancih po tej uredbi in druge specifične naloge s področja informacijske varnosti, katerih namen je vzdrževati visoko raven informacijske varnosti v državni upravi (4. člen).

Za zagotavljanje informacijske varnosti so odgovorni vsi uslužbenci, vodje in funkcionarji na vseh ravneh v državni upravi, vendar morajo biti ključne odgovornosti in zadolžitve na področju informacijske varnosti formalno dodeljene konkretnim osebam. Za informacijsko varnost znotraj posameznega organa je odgovoren predstojnik tega organa, ki za izvajanje posameznih ključnih nalog na področju informacijske varnosti imenuje: vodjo informacijske varnosti, če ima organ lastne informacijske sisteme, pa še skrbnike informacijskih sistemov in upravljavce informacijskih sistemov. Vodja informacijske varnosti je oseba, ki je zadolžena za upravljanje sistema informacijske varnosti organa in predstavlja kontaktno točko na področju informacijske varnosti. Skrbnik (v strokovni literaturi se običajno uporablja izraz »lastnik«) informacijskega sistema je oseba, odgovorna za dobavo, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe posameznega informacijskega sistema ter varovanje informacijskih premoženj, ki jih ta informacijski sistem obravnava. Skrbnik je praviloma poslovni uporabnik tega sistema in ne oseba s področja IT. Upravljavec informacijskega sistema po navodilih lastnika skrbi za upravljanje oziroma izvajanje nadzorstev. To so ključne osebe v organizacijski strukturi upravljanja informacijske varnosti posameznega organa. Povezani subjekti morajo določiti koordinatorja informacijske varnosti, ki predstavlja kontaktno točko za vprašanja informacijske varnosti v povezanem subjektu (5. člen). Uredba podrobneje opredeli njihove odgovornosti in zadolžitve v členih od 6 do 8. *Ključni deležniki v organizacijski strukturi informacijske varnosti v državni upravi, njihova medsebojna razmerja, sestava in vloga pri upravljanju informacijskih sistemov so prikazani na spodnji sliki.*



2. Tveganja informacijske varnosti

Pomembno je, da organ prepozna svoje varnostne zahteve. Eden glavnih virov za identifikacijo varnostnih zahtev je ocenjevanje tveganj, ob upoštevanju celovite poslovne strategije in ciljev organa. Z oceno tveganj se prepoznajo grožnje informacijskemu premoženju, ovrednotita se ranljivost in verjetnost pojava ter oceni potencialni vpliv. Organi morajo varovati svoje informacije in informacijske sisteme sorazmerno z ocenjenimi ravnmi tveganja, ki jih določijo v postopku ocene tveganja (9. člen).

3. Popis in razvrščanje informacijskega premoženja in informacijskih sistemov

Vse informacije in informacijski sistemi nimajo enakega pomena za poslovanje organa. Njihovo razkritje, izguba ali nerazpoložljivost imajo različen vpliv na njegovo poslovanje. Zato je treba vsa informacijska premoženja in informacijske sisteme organa identificirati, popisati in razvrstiti v razrede glede na vrednost, pomembnost in občutljivost na nepooblaščeno razkritje, spreminjanje ali razpoložljivost. Vsakemu prepoznanemu informacijskemu premoženju in sistemu se mora dodeliti skrbnika (10. in 11. člen). Skrbnik informacijskega sistema je namreč odgovoren za vse vidike njegove varnosti in varnosti informacijskega premoženja, ki ga obravnava. Skrbnik uvršča informacijska premoženja in sisteme v varnostne razrede (7. člen).

4. Ozaveščanje in usposabljanje

Nizka raven zavedanja o pomenu informacijske varnosti in neznanje na tem področju sodita med najpomembnejše dejavnike tveganja. 12. člen predpisuje vsem uslužbencem organa obvezno vključevanje v programe usposabljanja in ozaveščanja s področja informacijske varnosti.

5. Dokumentacija informacijske varnosti

Sistem upravljanja informacijske varnosti mora biti ustrezno dokumentiran. Uredba v 13. členu zavezuje vse organe, ki imajo lastne informacijske sisteme, da pripravijo in vzdržujejo ključne dokumente informacijske varnosti (operativna navodila in načrt neprekinjenosti poslovanja in okrevanja po nenadnem dogodku, ki povzroči škodo večjih razsežnosti). Z besedno zvezo »okrevanja po nenadnem dogodku, ki povzroči škodo večjih razsežnosti« smo opisali to, kar se v angleški strokovni literaturi označuje z »disaster recovery«. S tem smo se izognili uporabi izraza »okrevanje po katastrofi /katastrofičnem dogodku«. Organ lahko sprejme tudi dodatna pravila na področju informacijske varnosti, s katerimi podrobneje opiše izvajanje določb te uredbe in dopolni njene minimalne zahteve (pravila informacijske varnosti). Ti dokumenti so opisani v členih od 14 do 16.

6. Obvladovanje incidentov informacijske varnosti

Obvladovanje incidentov informacijske varnosti, kot pomemben del preventivnih in popravljalnih aktivnosti, obsega dosledno zaznavo dogodkov in incidentov informacijske varnosti, sprotna priglasitev za to pooblaščenim osebam oziroma organom in hiter ter učinkovit odziv nanje. To področje je urejeno v podpoglavju »Obvladovanje incidentov informacijske varnosti« (členi od 17 do 21).

7. Upravljanje sprememb in varnostna presoja informacijskih sistemov

Uvajanje novih sistemov in spreminjanje obstoječih sta pomembna dejavnika tveganja informacijske varnosti, zato mora biti vzpostavljen ustrezen proces upravljanja sprememb, ki bo zagotavljal varno uvedbo novih funkcionalnosti in storitev ter predvidljivost učinkov načrtovanih sprememb (22. člen). Varno delovanje novih in spremenjenih informacijskih sistemov je treba zagotoviti tudi z rednim izvajanjem varnostnih presoj (23. člen).

8. Odnosi z dobavitelji blaga in storitev

Posebno pozornost je treba posvetiti varnosti tistih informacijskih sistemov, premoženj in storitev, ki jih dobavljajo ali upravljajo zunanji dobavitelji in so dostopni zunanjim dobaviteljem blaga in storitev. Zahteve za zagotavljanje informacijske varnosti morajo biti opredeljene v pogodbah z dobavitelji, določeni morajo biti postopki dobave in zagotovljen učinkovit nadzor (členi od 24 do 28).

III. TEMELJNA NADZORSTVA ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

V tem poglavju so določbe, ki urejajo ključna področja informacijske varnosti in določajo temeljna nadzorstva za zagotavljanje informacijske varnosti.

1. Varnostno kopiranje

Varnostno kopiranje podatkov predstavlja osnovno zaščito pred njihovo izgubo. Načrt varnostnega kopiranja mora zagotoviti, da ne bo prišlo do izgube informacij, ki so pomembne za poslovanje organa in uporabnike njegovih storitev (29. člen).

2. Fizična in okoljska varnost

Zahteve za zagotavljanje fizične in okoljske varnosti informacijskih premoženj in sistemov, obravnavane v tem podpoglavju, urejajo področje varnega okolja, fizičnega dostopa, ravnanje s sredstvi za dostop, varno namestitev informacijskih naprav in hrambo tistih podatkov, za katere je treba zaščititi njihovo zaupnost (členi od 30 do 35).

3. Primerna raba informacijskih naprav in storitev

Veliko škode lahko povzročijo uslužbenci, ki pri svojem delu uporabljajo informacijske naprave in storitve na neustrezen, nestrokoven ali neprimeren način, zato je posebno podpoglavje posvečeno primerni rabi informacijskih naprav in storitev: uporabi informacijskih naprav organa, zasebnih informacijskih naprav, elektronske pošte, interneta in storitev računalništva v javnem oblaku (členi od 36 do 41).

4. Škodljiva programska oprema in prenosna koda

Zlonamerna oziroma škodljiva programska koda lahko povzroči nerazpoložljivost sistemov in storitev ter razkritje ali uničenje podatkov. To podpoglavje obravnava zaščito pred škodljivo programsko kodo, ukrepanje ob okužbi s škodljivo programsko opremo in nadzor prenosne kode, katere nenadzorovana uporaba lahko prav tako povzroči veliko škode (členi od 42 do 44).

5. Varnost nosilcev podatkov

To podpoglavje obravnava upravljanje izmenljivih nosilcev podatkov, njihov varen izbris in uničenje (45. in 46. člen).

6. Varnost programske opreme

Varnosti programske opreme, kot enega temeljnih elementov informacijskega sistema, je treba posvetiti posebno pozornost. Informacijsko varnost je treba upoštevati v vseh fazah razvojnega cikla programske opreme in mora biti sestavni del vseh projektov njenega razvoja in uvedbe. To podpoglavje obravnava varnostne vidike razvoja in dobave programske opreme, prenosa v obratovanje, njenega nameščanja in uporabe (členi od 47 do 50).

7. Nadzor dostopa

Nepooblaščen dostop do informacijskih sistemov oziroma informacij in storitev, ki jih zagotavljajo, lahko privede do nepooblaščenega razkritja informacij, do krnitve njihove celovitosti ali njihovega uničenja. Nadzor dostopa je eden ključnih ukrepov varovanja informacijskih sistemov in informacij. V členih od 51 do 55 so obravnavane pravice dostopa, metode avtentikacije, varnost gesel in nadzor dostopa do državnega komunikacijskega omrežja.

8. Spremljanje varnosti in dnevniško beleženje dogodkov

Nadzorni sistemi, ki nadzirajo delovanje poslovnih informacijskih sistemov, omogočajo hiter odziv na nepravilnosti in grožnje, ki jih zaznavajo. Zapisovanje in hramba informacij v dnevnikih

dogodkov o spremembah, posegih ter rabi informacijskega sistema zagotavlja revizijsko sled, ki omogoča naknadno analizo in ugotavljanje vzrokov za varnostne kršitve in incidente. Dnevnike dogodkov, ki pogosto vsebujejo tudi osebne podatke, se sme uporabljati izključno z namenom ugotavljanja ranljivosti in napak, nadziranja ustreznosti nadzorstev, reševanja incidentov in ugotavljanja zlorab. Njihova hramba je časovno omejena (podpoglavje: »Spremljanje varnosti in dnevniki dogodkov«; členi od 56 do 58).

9. Kriptografija

Podpoglavje o kriptografiji, vedi, ki se ukvarja s skrivanjem vsebine sporočila z uporabo šifriranja in dešifriranja in je izredno pomembno sredstvo za zagotavljanje zaupnosti in celovitosti informacij ter za identifikacijo in avtentikacijo uporabnikov, obravnava primerne kriptografske rešitve, uporabo šifriranja in potrdil za elektronski podpis (členi od 59 do 61).

10. Varnost prenosnih informacijskih naprav in dela na terenu

Uslužbenci pri svojem delu uporabljajo poleg pisarniške informacijske opreme tudi številne prenosne informacijske naprave izven varovanega pisarniškega okolja, kjer so izpostavljene dodatnim tveganjem. Uporabniki prenosnih naprav morajo ta tveganja poznati in jih upoštevati. Uporabo prenosnih informacijskih naprav in delo izven pisarne ureja poglavje »Varnost prenosnih informacijskih naprav in dela na terenu« (člena 62 in 63).

IV. PREHODNE IN KONČNA DOLOČBA

V prehodnih in končnih določbah so določeni roki, v katerih morajo posamezni zavezanci po tej uredbi izpolniti zahteve, ki jim jih nalaga ta uredba, razveljavljajo se tisti členi Uredbe o upravnem poslovanju, ki se nanašajo na informacijsko varnost in določi se začetek veljavnosti te uredbe. 64. člen določa, da organom, ki že imajo sprejete dokumente, ki so po vsebini skladni z določbami te uredbe, ni treba pripraviti novih dokumentov.