



2026-01-1456

Na podlagi tretjega odstavka 4. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25)
Vlada Republike Slovenije izdaja

Uredbo o varovanih podatkih pristojnega nacionalnega organa za informacijsko varnost

**I. POGLAVJE
SPLOŠNE DOLOČBE**

**1. člen
(vsebina uredbe)**

Ta uredba določa organizacijske in logično-tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ) iz zakona, ki ureja informacijsko varnost, ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in ki vsebujejo varovane podatke pristojnega nacionalnega organa (v nadaljnjem besedilu: varovani podatki).

**2. člen
(področje uporabe)**

Organizacijske in logično-tehnične postopke ter ukrepe za varovanje varovanih podatkov pristojnega nacionalnega organa poleg pristojnega nacionalnega organa izvajajo tudi subjekti, ki so prejemniki teh podatkov ali imajo na podlagi zakona, ki ureja informacijsko varnost, pravico do dostopa do posameznih podatkovnih zbirk iz tega zakona, ki vsebujejo varovane podatke pristojnega nacionalnega organa (v nadaljnjem besedilu: zbirke podatkov).

**3. člen
(pomen izrazov)**

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. informacijski sistem pristojnega nacionalnega organa (v nadaljnjem besedilu: IS PNO) je urejena celota programske in strojne opreme, ki se uporablja za obdelavo ali izmenjavo varovanih podatkov;
2. uporabnik IS PNO je uslužbenec pristojnega nacionalnega organa, ki pri svojem delu uporablja IS PNO, ali njegov zunanji uporabnik, ki dostopa do IS PNO ali ima pravico do dostopa do posameznih zbirk podatkov pristojnega nacionalnega organa na podlagi zakona, ki ureja informacijsko varnost;
3. prejemnik varovanega podatka je uporabnik IS PNO ali druga oseba, ki prejme varovani podatek in je del skupnosti;
4. skupnost sestavljajo zavezanici iz 6. člena, subjekti iz 18. člena in državni organi iz 39. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1).

II. POGLAVJE

DOLOČANJE IN OZNAČEVANJE VAROVANIH PODATKOV

4. člen **(pooblastilo za določanje in označevanje)**

(1) Vsak podatek, ki ga ustvari ali prejme pristojni nacionalni organ in za katerega pristojni nacionalni organ oceni, da gre za varovani podatek po zakonu, ki ureja informacijsko varnost, se določi in označi v skladu z določbami te uredbe. Če gre za podatek, ki ga prejme pristojni nacionalni organ, je treba o njegovi določitvi in označitvi iz prejšnjega stavka v petih delovnih dneh obvestiti pošiljatelja.

(2) Predstojnik pristojnega nacionalnega organa, njegov namestnik in pomočnik so pooblaščen za določanje in označevanje varovanih podatkov, spremembo njihovih oznak ali preklic.

(3) Predstojnik pristojnega nacionalnega organa lahko za določanje in označevanje varovanih podatkov, spremembo njihovih oznak ali preklic pooblasti tudi druge uslužbenke, zaposlene v pristojnem nacionalnem organu.

5. člen **(označevanje varovanih podatkov)**

(1) Varovani podatek mora biti jasno in nedvoumno označen v skladu z določbami tega člena, ne glede na nosilec, na katerem je shranjen. Če je varovani podatek na dokumentu v fizični obliki, mora biti predpisana oznaka vsaj na prvi oziroma naslovni strani dokumenta in se mora jasno razlikovati od drugih zapisov. Za zapis oznake se uporabijo poudarjene velike tiskane črke v velikosti pisave 14, ki morajo biti večje od črk drugih zapisov. Če je varovani podatek na drugih nosilcih (na primer zemljevidi, fotografije, CD/DVD, USB-ključ) varovanih podatkov, morata biti oznaki varovanega podatka in njegove stopnje na nosilcu podatkov vidno natiskani, natipkani, napisani, naslikani, nalepljeni ali kako drugače pritrjeni s primernimi sredstvi.

(2) Za označevanje varovanih podatkov se uporablja oznaka »VAROVANI PODATEK URSIV« različnih stopenj.

(3) Oznake varovanih podatkov so naslednje: VAROVANI PODATEK URSIV 1. STOPNJE, VAROVANI PODATEK URSIV 2. STOPNJE in VAROVANI PODATEK URSIV 3. STOPNJE.

(4) Varovani podatek z oznako »VAROVANI PODATEK URSIV 3. STOPNJE« se lahko deli v skupnosti, vendar ne javno. Prejemnik varovanega podatka lahko tega deli z drugim posameznikom, ki je zaposlen v prejemniku in s svojim pogodbenim partnerjem, vendar v obeh primerih le, če je izkazana njuna potreba po seznanitvi.

(5) Varovani podatek z oznako »VAROVANI PODATEK URSIV 2. STOPNJE« se lahko deli le s posamezniki v prejemniku varovanega podatka, če je izkazana njihova potreba po seznanitvi.

(6) Ne glede na določbe prejšnjega odstavka lahko prejemnik varovanega podatka z oznako »VAROVANI PODATEK URSIV 2. STOPNJE« tak podatek v omejenem obsegu deli v skupnosti, ko je to potrebno zaradi odvratanja neposredne nevarnosti za varnost omrežij in informacijskih sistemov zavezancev iz 6. člena ZInfV-1 ter za izvedbo nujnih ukrepov kibernetске obrambe, če nevarnosti ni mogoče odvrniti drugače. Omejeni obseg pomeni, da se ne razkrijejo pošiljatelj podatka in druge informacije, ki niso nujne za odvratanje neposredne nevarnosti za varnost omrežij in informacijskih sistemov zavezancev ter izvedbo nujnih ukrepov kibernetске obrambe. Pri tem mora prejemnik o nadaljnjem deljenju tega varovanega podatka obvestiti pristojni nacionalni organ.

(7) Varovani podatek z oznako »VAROVANI PODATEK URSIV 1. STOPNJE« lahko prejmejo le natančno določeni posamezniki, ki so neposredni naslovniki takega podatka in so zaposleni pri subjektu, ki je del skupnosti iz 4. točke 3. člena te uredbe. Deljenje takega podatka z osebami, ki niso med naslovniki, ni dovoljeno.

(8) Prejemniki varovanega podatka tega ne smejo deliti z drugimi subjekti ali posamezniki zunaj obsega, določenega za posamezne oznake stopenj varovanega podatka v skladu z določbami tega člena.

(9) Če pristojni nacionalni organ oceni, da ne gre več za varovani podatek v skladu z zakonom, ki ureja informacijsko varnost, je treba oznako iz prvega odstavka tega člena prečrtati ali kako drugače označiti, da podatek ne šteje več za varovanega. Ob prečrtani oznaki se navedeta datum označitve, da se podatek ne šteje več za varovanega, in podpis osebe, ki je določila prenehanje statusa varovanega podatka.

(10) Če pristojni nacionalni organ oceni, da je treba označitev varovanega podatka spremeniti, je treba oznako iz tretjega odstavka tega člena prečrtati in varovani podatek označiti s spremenjeno oznako. Ob prečrtani oznaki in novi oznaki se navedeta datum spremembe označitve in podpis osebe, ki je izvedla spremembo.

(11) V primerih iz prejšnjega in devetega odstavka pristojni nacionalni organ v petih delovnih dneh obvesti prejemnike takega podatka.

(12) Oznaka »VAROVANI PODATEK URSIV« ne nadomešča oznake semaforkega protokola. Podatek, označen po navedenem protokolu, to oznako ohrani. Dodatna oznaka podatka z »VAROVANI PODATEK URSIV« ne sme biti nižja od primerljive oznake semaforkega protokola.

III. POGLAVJE UKREPI ZA VAROVANJE VAROVANIH PODATKOV

6. člen **(minimalni nabor varnostnih ukrepov)**

Za varovanje varovanih podatkov se morajo izvajati najmanj ti ukrepi:

1. fizično ali tehnično varovanje dostopov do prostorov, v katerem je IS PNO ali fizična dokumentacija z varovanimi podatki;
2. upravljanje pooblastil za dostop do IS PNO in preverjanje identitete uporabnikov IS PNO;
3. šifriranje varovanih podatkov pri prenosu;
4. ohranjanje dnevniških zapisov o delovanju IS PNO, vključno z evidentiranjem dejavnosti IS PNO, uporabnikov IS PNO in njegovih administratorjev ter vseh obdelav varovanih podatkov v IS PNO;
5. varnostno kopiranje varovanih podatkov in
6. nadzor nad varovanimi podatki, ki se obdelujejo v fizični obliki, preverjanje identitete prejemnikov varovanih podatkov in nadzor nad njihovo hrambo.

7. člen **(varovanje prostorov)**

(1) Prostori pristojnega nacionalnega organa, v katerih je IS PNO, morajo biti varovani najmanj s tehničnimi oziroma logično-tehničnimi ukrepi (na primer senzorji gibanja, alarmni sistemi, nadzor dostopa).

(2) Prejemniki varovanega podatka smiselno izvajajo ukrepe iz prejšnjega odstavka tako, da nepoklicanim osebam onemogočijo dostop do varovanega podatka.

8. člen

(varovanje varovanih podatkov)

Prejemniki varovanih podatkov izvajajo predvsem naslednje ukrepe varovanja varovanih podatkov:

1. nosilec z varovanimi podatki ne smejo puščati na vidnih mestih v prostorih ali na drugih mestih, kjer imajo dostop do njih nepoklicane osebe;

2. strojna oprema z zasloni, ki se uporablja za obdelavo varovanih podatkov, mora imeti zaslone postavljene tako, da je nepoklicanim osebam onemogočen pogled na podatke, če zaslona tako ni mogoče postaviti, pa mora biti ta ob prisotnosti nepoklicane osebe izklopljen ali na njem nastavljen ohranjevalnik zaslona, pri čemer mora biti nastavljeno tudi samodejno zaklepanje zaslona po petih minutah od prenehanja obdelave varovanih podatkov;

3. kadar zapuščajo svoje delovne prostore, morajo zakleniti pisalne mize, omare, blagajne, pisarne in končne naprave, v katerih hranijo oziroma obdelujejo varovane podatke.

9. člen

(upravljanje pravic za dostop do IS PNO in preverjanje identitete uporabnikov)

(1) Pravice za dostop do IS PNO se dodeljujejo po načelu najmanjših pravic, kar pomeni, da se uporabniku dodeli najmanjši mogoči obseg pravic, ki jih potrebuje za opravljanje dela. Pri tem se izvajata tudi periodično preverjanje ustreznosti dodeljenih pravic ter ustrezno dokumentiranje vseh dodelitev, sprememb in ukinitvev pravic.

(2) Vstop v IS PNO je mogoč samo z vnaprejšnjim preverjanjem identitete uporabnika, ki mora temeljiti na večfaktorski avtentikaciji.

(3) Subjekt, ki je del skupnosti iz 4. točke 3. člena te uredbe in ima pravico do dostopa do IS PNO, mora sproti obveščati pristojni nacionalni organ o vsaki spremembi ali ukinitvi pravic posameznikov v tem subjektu glede dostopa do IS PNO.

10. člen

(šifriranje varovanih podatkov)

(1) Varovani podatki v elektronski obliki se lahko prenesejo le v šifrirani obliki ali po kanalih, ki omogočajo šifriranje od pošiljatelja do prejemnika. Izjemoma je mogoče varovani podatek prenesti v nešifrirani obliki ali po drugih kanalih, če drugačen prenos ni mogoč in je to nujno za izvedbo naloge pristojnega nacionalnega organa ali bi lahko nastala škoda zavezancem.

(2) Pri prenosu iz prejšnjega odstavka morajo biti varovani podatki zaščiteni z uporabo kriptografskih mehanizmov na podlagi sodobnih, mednarodno priznanih in kriptografsko močnih algoritmov, ki so v skladu z uveljavljenimi standardi in dobrimi praksami na področju informacijske in kibernetske varnosti, pri čemer se zagotavljajo tudi ustrezno upravljanje kriptografskih ključev, redno posodabljanje uporabljenih algoritmov ter odpornost proti znanim in predvidljivim varnostnim grožnjam.

11. člen **(varnostno kopiranje)**

(1) Za zbirke podatkov, ki vsebujejo varovane podatke, je treba zagotoviti varnostne kopije. Najmanj ena kopija se hrani na drugi lokaciji, ki mora biti od primarne lokacije ustrezno oddaljena v skladu z veljavnimi standardi na področju informacijske oziroma kibernetске varnosti.

(2) Varnostna kopija dnevniških zapisov iz 4. točke 6. člena te uredbe mora biti izdelana in hranjena enako kot zbirke podatkov iz prejšnjega odstavka.

(3) Pristojni nacionalni organ periodično, najmanj pa enkrat letno izvede preizkus obnovitve iz varnostne kopije.

12. člen **(izključitev od pošiljanja varovanih podatkov)**

Če prejemnik varovanih podatkov ne izvaja ukrepov iz tretjega poglavja te uredbe v delu, ki se nanaša na prejemnike varovanih podatkov, mu pristojni nacionalni organ do začetka izvajanja teh ukrepov na podlagi nadzorne odločbe, izdane po zakonu, ki ureja informacijsko varnost, začasno omeji obseg pošiljanja varovanih podatkov ali nekatere pravice glede dostopa.

IV. POGLAVJE **KONČNA DOLOČBA**

13. člen **(začetek veljavnosti)**

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

Št. 00701-5/2026

Ljubljana, dne 28. maja 2026

EVA 2025-1544-0003

Vlada Republike Slovenije
dr. Robert Golob
predsednik