OSNUTEK PREDLOGA 13. 6. 2025

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

UREDBO

O VAROVANJU VAROVANIH PODATKOV PRISTOJNEGA NACIONALNEGA ORGANA ZA INFORMACIJSKO VARNOST

I. 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 nadaljevanju: varovani podatki).

2. člen

(področje uporabe)

Organizacijske in logično-tehnične postopke in ukrepe za varovanje varovanih podatkov morajo poleg pristojnega nacionalnega organa izvajati tudi subjekti, ki so prejemniki teh podatkov ali ki imajo na podlagi zakona, ki ureja informacijsko varnost, pravico dostopa do evidenc iz zakona, ki ureja informacijsko varnost, ki vsebujejo varovane podatke pristojnega nacionalnega organa.

3. člen

(pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. evidenca je skupni izraz za evidenco, zbirko podatkov ali seznam iz zakona, ki ureja informacijsko varnost, ki jo upravlja pristojni nacionalni organ in ki vsebuje varovane podatke pristojnega nacionalnega organa ali varovane podatke varnostne skupnosti;

2. 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 pristojnega nacionalnega organa ter varovanih podatkov varnostne skupnosti;

3. semaforski protokol (TLP protokol) je skupek pravil in dogovorov o omejitvah v zvezi z nadaljnjim širjenjem prejetih ali deljenih informacij, kot ga uporabljajo pri izmenjavi informacij skupine CSIRT, ki je namenjen varni in nadzorovani izmenjavi teh podatkov znotraj varnostne skupnosti, katerega namen je vzpostaviti matriko oznak, pomenov oznak in vrste prejemnikov varovanih podatkov pristojnega nacionalnega organa ali varovanih podatkov varnostne skupnosti;

4. uporabnik IS PNO je uslužbenec pristojnega nacionalnega organa, ki pri svojem delu uporablja IS PNO ali zunanji uporabnik, ki je na podlagi zakona, ki ureja informacijsko varnost, prejemnik varovanih podatkov pristojnega nacionalnega organa ali varovanih podatkov varnostne skupnosti oziroma ima pravico dostopa do njegovih evidenc;

5. varnostna skupnost je skupek subjektov, ki so zavezanci in subjektov, ki sodelujejo pri kibernetski obrambi iz zakona, ki ureja informacijsko varnost, vključno s subjekti drugih držav članic Evropske unije oziroma institucijami, organi, uradi, agencijami in mrežami Evropske unije in subjekti tretjih držav ali mednarodnih organizacij, s katerimi ima Republika Slovenija sklenjen mednarodni sporazum;

6. zavezanec je bistveni ali pomembni subjekt, ki je zavezanec iz zakona, ki ureja področje informacijske varnosti.

II. DOLOČANJE IN OZNAČEVANJE VAROVANIH PODATKOV

4. člen

(določitev varovanih podatkov)

(1) Varovani podatek je vsak podatek, katerega je ustvaril ali prejel pristojni nacionalni organ in je označen v skladu z določbami te uredbe.

(2) Predstojnik pristojnega nacionalnega organa, njegov pomočnik oziroma namestnik in vodje notranje organizacijskih enot pristojnega nacionalnega organa so pristojni za določitev varovanih podatkov ali spremembo njihovih oznak.

(3) Predstojnik pristojnega nacionalnega organa lahko za določanje varovanih podatkov pooblasti tudi druge uslužbence, 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 medij, na katerem je zapisan. Če je varovani podatek na fizičnem dokumentu, mora biti predpisana oznaka vsaj na prvi oziroma naslovni strani dokumenta.

(2) Za označevanje varovanih podatkov se uporablja semaforski protokol, oznaka je lahko napisana v slovenskem ali v angleškem jeziku ali v obeh jezikih. Za večjo preglednost se lahko ta oznaka tudi ustrezno barvno označi.

(3) Oznake varovanih podatkov so naslednje: TLP: ZELENO/GREEN, TLP: JANTAR/AMBER, TLP: JANTAR+STROGO/AMBER+STRICT IN TLP: RDEČE/RED.

(4) Varovani podatki označeni z oznako TLP: ZELENO/GREEN se lahko delijo znotraj varnostne skupnosti, vendar ne javno. Prejemniki takega podatka so lahko subjekti iz 5. točke 3. člena te uredbe in njihovi pogodbeni partnerji.

(5) Varovani podatki označeni z oznako TLP: JANTAR/AMBER se lahko delijo le znotraj posameznega subjekta, ki je naslovnik oziroma prejemnik varovanega podatka in z njegovimi pogodbenimi partnerji. Prejemniki takega podatka so lahko subjekti iz 5. točke 3. člena te uredbe in njegovi pogodbeni partnerji.

(6) Varovani podatki označeni z oznako TLP: JANTAR+STROGO/AMBER+STRICT se lahko delijo le znotraj posameznega subjekta, ki je naslovnik oziroma prejemnik varovanega podatka. Prejemniki takega podatka so lahko subjekti iz 5. točke 3. člena te uredbe.

(7) Ne glede na določbe prejšnjega odstavka je prejemnik varovanega podatka z oznako TLP: JANTAR+STROGO/AMBER+STRICT tak podatek dolžan v omejenem obsegu deliti s pristojnim nacionalnim organom, z zavezanci ali s subjekti, ki sodelujejo pri kibernetski obrambi iz zakona, ki ureja informacijsko varnost, ko je to potrebno zaradi odvračanja neposredne nevarnosti za varnost omrežij in informacijskih sistemov zavezancev in izvedbo nujnih ukrepov kibernetske obrambe, če nevarnosti ni mogoče odvrniti na drug način. Omejen obseg pomeni, da se ne razkrije pošiljatelja podatka in drugih informacij, ki niso nujno potrebne za odvračanje neposredne nevarnosti za varnost omrežij in informacijskih sistemov zavezancev in izvedbo nujnih ukrepov kibernetske obrambe.

(8) Varovani podatki označeni z oznako TLP: RDEČE/RED lahko prejmejo samo točno določeni posamezniki, ki so neposredni naslovniki takega podatka. Deljenje takega podatka z osebami, ki niso med naslovniki ni dovoljeno.

(9) Ne glede na določbe tega člena pristojni nacionalni organ dokumente in podatke, ki so nastali v postopkih inšpekcijskega nadzora in vsebujejo podatke oziroma informacije, ki bi lahko ob razkritju imele negativni vpliv na varnost omrežij in informacijskih sistemov zavezanca, označi z oznako TLP: JANTAR+STROGO/AMBER+STRICT. Izvod zapisnika o inšpekcijskem nadzoru oziroma pregledu, ki se izroči zavezancu, se z navedenimi oznakami ne označi.

(10) Če prenehajo razlogi, da se podatek šteje za varovani podatek, je treba označbo iz prvega odstavka tega člena prečrtati ali na drug način označiti, da podatek ne šteje več za varovanega. Poleg prečrtane oznake se napiše datum označitve, da se podatek ne šteje več za varovanega in navede podpis osebe, ki je določila prenehanje statusa varovanega podatka.

(11) Če nastanejo razlogi za spremembo označitve varovanega podatka, je treba označbo iz tretjega odstavka tega člena prečrtati in ga označiti s spremenjeno oznako. Poleg prečrtane oznake in nove oznake se napiše datum spremembe označitve in navede podpis osebe, ki je izvedla spremembo.

(12) V primerih iz prejšnjega in devetega odstavka pristojni nacionalni organ obvesti prejemnike takega podatka.

III. UKREPI ZA VAROVANJE VAROVANIH PODATKOV

6. člen

(minimalni nabor varnostnih ukrepov)

Za varovanje varovanih podatkov v IS PNO se morajo izvajati najmanj naslednji ukrepi:

1. fizično ali tehnično varovanje dostopov do prostorov, kjer se nahaja IS PNO ali fizična dokumentacija, ki vsebuje varovane podatke;
2. upravljanje pooblastil za dostop in preverjanje identitete uporabnikov;
3. šifriranje varovanih podatkov;
4. ohranjanje dnevniških zapisov o delovanju IS PNO, vključno z evidentiranjem dejavnosti IS PNO, uporabnikov in administratorjev IS PNO 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 ter nadzor nad njihovo hrambo.

7. člen

(varovanje prostorov)

(1) Prostori, v katerih se nahaja IS PNO ali varovani podatki v fizični obliki, morajo biti varovani najmanj s tehničnimi oziroma logično-tehničnimi ukrepi (npr. senzorji gibanja, alarmni sistemi, kontrole pristopa).

(2) Prejemniki varovanega podatka smiselno izvajajo ukrepe iz prejšnjega odstavka na način, da nepoklicanim osebam onemogočijo dostop do varovanega podatka pristojnega nacionalnega organa.

8. člen

(varovanje varovanih podatkov)

(1) Uporabniki IS PNO izvajajo predvsem naslednje ukrepe varovanja varovanih podatkov:

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

2. medijev z varovanimi podatki ne smejo puščati na vidnih mestih v prostorih ali drugih mestih, kjer so dostopni nepoklicanim osebam;

3. strojna oprema z zasloni, ki se uporablja za obdelavo varovanih podatkov, mora imeti zaslone nameščene tako, da je nepoklicanim osebam onemogočen pogled na podatke, če zaslona tako ni mogoče namestiti, pa mora biti ta v času prisotnosti nepoklicane osebe ugasnjen ali v fazi ohranjevalnika zaslona.

(2) Ukrepe iz prejšnjega odstavka morajo izvajati tudi prejemniki varovanega podatka.

9. člen

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

(1) Pravice za dostop do IS PNO se podeljujejo po načelu najmanjših pravic, kar pomeni, da se uporabniku dodeli najmanjši možen nabor pravic, ki jih potrebuje za opravljanje svojega dela.

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

(3) Subjekt iz 5. točke 3. člena te uredbe, ki ima pravico dostopa do IS PNO, mora redno in ažurno obveščati pristojni nacionalni organ o vseh okoliščinah, ki imajo za posledico spremembo ali ukinitev pravic posameznika v IS PNO.

10. člen

(šifriranje varovanih podatkov)

(1) Evidence, ki vsebujejo varovane podatke morajo biti šifrirane z algoritmi, ki veljajo za močne v skladu z veljavnimi standardi na področju informacijske oziroma kibernetske varnosti.

(2) Na enak način morajo biti šifrirane tudi varnostne kopije evidenc iz prejšnjega odstavka.

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

11. člen

(varnostno kopiranje)

(1) Evidence, ki vsebujejo varovane podatke morajo biti varnostno kopirane. Najmanj ena kopija mora biti hranjena na sekundarni lokaciji, ki mora biti od primarne lokacije ustrezno oddaljena v skladu z veljavnimi standardi na področju informacijske oziroma kibernetske varnosti.

(2) Varnostna kopija dnevniških zapisov iz 10. člena te uredbe mora biti izdelana in hranjena na enak način kot evidence iz prejšnjega odstavka.

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

12. člen

(nadzor)

(1) Za izvajanje notranjega nadzora nad določbami te uredbe je pristojen predstojnik pristojnega nacionalnega organa, ki lahko za to pooblasti tudi druge osebe, zaposlene v pristojnem nacionalnem organu.

(2) Pristojni nacionalni organ sme izvesti preverjanje izvajanja ukrepov iz tretjega poglavja te uredbe tudi pri prejemnikih varovanih podatkov v delu, ki k izvajanju varnostnih ukrepov zavezuje te prejemnike. V kolikor prejemnik varovanih podatkov tega ne omogoči, mu pristojni nacionalni organ varovanih podatkov več ne posreduje.

IV. KONČNA DOLOČBA

13. člen

(začetek veljavnosti)

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

OBRAZLOŽITEV

I. UVOD

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

Predlagana uredba se izdaja na podlagi tretjega odstavka 4. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1).

Tretji odstavek 4. člena ZInfV-1 določa:
»(3) Izmenjava varovanih podatkov pristojnega nacionalnega organa mora biti za potrebe izvajanja tega zakona omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij in podatkov ter se zaščitita varnost in poslovni interes zadevnih subjektov. Podrobnejše organizacijske in logično-tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in vsebujejo varovane podatke pristojnega nacionalnega organa, določi vlada.«.

2. Rok za izdajo uredbe, določen z zakonom

Prvi odstavek 64. člena ZInfV-1 določa, da se Vlada izda predpisa iz tretjega odstavka 4. člena in šestega odstavka 20. člena tega zakona v šestih mesecih od uveljavitve tega zakona.

ZInfV-1 je bil v Državnem zboru Republike Slovenije sprejet po nujnem postopku zato se predvideva sprejetje podzakonskih predpisov v najkrajšem možnem času.

3. Splošna obrazložitev predloga uredbe, če je potrebna

Direktiva 2022/2555/EU Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L št. 333 z dne 27. 12. 2022, str. 80), zadnjič popravljeno s Popravkom (UL L št. 90348 z dne 12. 6. 2024, str. 139), (v nadaljnjem besedilu: Direktiva 2022/2555/EU) v devetem odstavku uvodne izjave pojasnjuje, da se od nobene države članice ne bi smelo zahtevati, da daje informacije, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene nacionalne varnosti, javne varnosti ali obrambe. V tem okviru bi bilo potrebno upoštevati pravila Unije ali nacionalna pravila za varovanje tajnih podatkov, sporazume o nerazkritju informacij in neuradne sporazume o nerazkritju informacij, kot je semaforski protokol (*Traffic Light Protocol*). V tem smislu se torej napotuje na nacionalne določbe posameznih držav članic, saj Direktiva 2022/2555/EU sama te materije ne ureja. V zadevni uvodni določbi se hkrati še pojasnjuje, da je semaforski protokol treba razumeti kot način oziroma sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij. Uporablja se v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT) ter v nekaterih centrih za analizo in izmenjavo informacij.

ZInfV-1 je sistemski zakon, ki ureja področje informacijske in kibernetske varnosti, določa nacionalni sistem informacijske varnosti v Republiki Sloveniji in je v naš pravni red prenesel Direktivo 2022/2555/EU v celoti.

Za učinkovito izvajanje ZInfV-1, bo Vlada Republike Slovenije s predlagano uredbo, ki se izdaja na podlagi tretjega odstavka 4. člena ZInfV-1, ki je nacionalna določba, določila še organizacijske in logično-tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa za informacijsko varnost iz zakona, ki ureja informacijsko varnost, ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in ki vsebujejo varovane podatke pristojnega nacionalnega organa.

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

Presoja posledic in učinkovito izvajanje ZInfV-1 za posamezna področja je bila celovito predstavljena v predlogu ZInfV-1 in se nanaša tudi na predlagano Uredbo o varovanju varovanih podatkov pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: uredba).

II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

SPLOŠNE DOLOČBE

Namen predloga uredbe je določitev načina obravnavanja varovanih podatkov pristojnega nacionalnega organa za informacijsko varnost (v nadaljevanju: pristojni nacionalni organ), določitev organizacijskih in logično-tehničnih postopkov in ukrepov za varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in vsebujejo varovane podatke, z namenom zagotavljanja visoke ravni varnosti omrežij in informacijskih sistemov ter zaščite pred kibernetskimi grožnjami.

ZInfV-1 v drugem odstavku 4. člena določa, da se podatki in informacije, ki se obdelujejo na podlagi ZInfV-1 in so opredeljeni kot tajni, poslovna skrivnost ali varovani podatki, obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje.

Tretji odstavek 4. člena ZInfV-1 določa, da mora biti izmenjava varovanih podatkov pristojnega nacionalnega organa za potrebe izvajanja ZInfV-1 omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij in podatkov ter se zaščitita varnost in poslovni interes zadevnih subjektov. Podrobnejše organizacijske in logično-tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in vsebujejo varovane podatke pristojnega nacionalnega organa, določi vlada.

Četrti odstavek 4. člena ZInfV-1 določa, da se pri pošiljanju ali izmenjavi podatkov in informacij na podlagi ZInfV-1 upoštevajo tudi (neformalni) sporazumi o nerazkritju informacij, kot je semaforski protokol.

Uredba velja za vse subjekte varnostne skupnosti, ki so prejemniki varovanih podatkov pristojnega nacionalnega organa.

DOLOČANJE IN OZNAČEVANJE VAROVANIH PODATKOV

Varovani podatek pristojnega nacionalnega organa je vsak podatek, katerega je ustvaril ali prejel pristojni nacionalni organ in je označen v skladu z določbami predlagane uredbe.

V pristojnem nacionalnem organu so za določanje varovanih podatkov in spreminjanje njihovih oznak pristojni predstojnik pristojnega nacionalnega organa, njegov pomočnik oziroma namestnik in vodje notranje organizacijskih enot. Predstojnik pristojnega nacionalnega organa pa lahko v skladu z delovnimi potrebami za določanje in spreminjanje oznak varovanih podatkov pooblasti tudi druge uslužbence, zaposlene v pristojnem nacionalnem organu.

Vsak varovani podatek mora biti jasno označen s predpisanimi oznakami ne glede na medij na katerem je zapisan. V primeru, ko je varovani podatek v obliki fizičnega dokumenta, mora biti predpisana oznaka navedena vsaj na prvi oziroma naslovni strani dokumenta.

Za predpisano označevanje varovanih podatkov je uporabljajo oznake semaforskega protokola (ang. *Traffic Light Protocol*), ki je neuraden mednaroden sporazum o nerazkritju informacij in se uporablja v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT). Oznake so lahko zapisne v slovenskem ali v angleškem jeziku ali v obeh jezikih. Oznake, dovoljeno deljenje in dovoljene postopke s primeri pojasnjuje naslednja preglednica:

TLP oznaka	Dovoljeno deljenje	Dovoljeni postopki (primeri)
TLP:RDEČE/RED	samo neposredni prejemnik (naslovnik)	- brez deljenja - izključno za odzivanje in zaščito informacijske infrastrukture
TLP:JANTAR+STROGO/ AMBER+STRICT	samo znotraj organizacije	- interna uporaba v organizaciji (potreba po vedenju) - brez deljenja s podružnicami ali pogodbenimi partnerji - odzivanje in zaščita informacijske infrastrukture
TLP:JANTAR/AMBER	znotraj organizacije in z zaupanja vrednimi pogodbenimi partnerji	- interna uporaba v organizaciji (potreba po vedenju) - možna delitev z izbranimi pogodenimi partnerji ali izvajalci - dokumentacija o incidentu ali o ukrepih za odzivanje in obrabo
TLP:ZELENO/GREEN	znotraj varnostne skupnosti (ne pa tudi javno)	- deljenje z drugimi člani varnostne skupnosti - uporaba za kolektivna opozorila in obvestila

Kadar prejemnik prejme varovan podatek, ki je označen z oznako TLP:JANTAR+STROGO/ AMBER+STRICT, pa obstaja neposredna nevarnost za varnost omrežij in informacijskih sistemov zavezancev ali izvedbo nujnih ukrepov kibernetske obrambe, mora tak podatek v omejenem obsegu deliti s pristojnim nacionalnim organom, z zavezanci ali s subjekti, ki sodelujejo pri kibernetski obrambi iz ZInfV-1, če take nevarnosti ni mogoče odvrniti drugače. V takem premeru se ne razkrije pošiljatelja podatka in drugih informacij, ki niso nujno potrebne za odvračanje neposredne nevarnosti za varnost omrežij in informacijskih sistemov zavezancev in izvedbo nujnih ukrepov kibernetske obrambe.

Pristojni nacionalni organ lahko z oznako TLP:JANTAR+STROGO/ AMBER+STRICT označi tudi zapisnik o inšpekcijskem nadzoru in druge dokumente nastale v postopku inšpekcijskega nadzora po ZInfV-1, kadar taki dokumenti vsebujejo podatke ali informacije o tehničnih ranljivostih ali varnostnih tveganjih za varnost omrežij in informacijskih sistemov zavezancev in bi razkritje takih podatkov javnosti ali drugim osebam lahko imelo negativni vpliv na varnost oziroma izpostavljenost dejanskim grožnjam omrežij in informacijskih sistemov zavezanca. Izvod zapisnika o inšpekcijskem nadzoru oziroma pregledu, ki se izroči zavezancu, se z navedenimi oznakami ne označi.

V primeru, ko nastopijo razlogi za prenehanje statusa varovanega podatka ali spremembi oznake je treba to ustrezno označiti na dokumentu, napisati datum spremembe in dodati podpis osebe, ki je spremembo izvedla. V teh primerih pristojni nacionalni organ obvesti vse prejemnike takega podatka.

UKREPI ZA VAROVANJE VAROVANIH PODATKOV

Uredba predpisuje minimalni nabor varnostnih ukrepov, ki jih je potrebno izvajati ob obravnavanju varovanih podatkov. Izvajanje predpisanih ukrepov je obvezno tako za pristojni nacionalni organ kot za vse prejemnike varovanih podatkov. Predpisani ukrepi se nanašajo na fizično ali tehnično varovanje dostopov do prostorov kjer se nahajajo varovani podatki, upravljanje pooblastil za dostop in preverjanje identitete uporabnikov, šifriranje varovanih podatkov, ohranjanje dnevniških zapisov o delovanju informacijskega sistema pristojnega nacionalnega organa, varnostno kopiranje in nadzor nad varovanimi podatki.

Pristojni nacionalni organ sme izvesti preverjanje izvajanja predpisanih varnostnih ukrepov iz tretjega poglavja uredbe tudi pri prejemnikih varovanih podatkov v delu, ki k izvajanju varnostnih ukrepov zavezuje te prejemnike. V kolikor prejemnik varovanih podatkov izvedbe preverjanja izvajanja predpisanih varnostnih ukrepov ne omogoči, mu pristojni nacionalni organ varovanih podatkov več ne posreduje.

KONČNA DOLOČBA

Uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije, kar je običajen rok za uveljavitev predpisov.

.