PREDLOG

Na podlagi 165. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/2012) izdaja direktor Agencije za pošto in elektronske komunikacije Republike Slovenije

SPLOŠNI AKT

o zavarovanju hranjenih podatkov

I. SPLOŠNE DOLOČBE

1. člen
(vsebina)

Ta splošni akt določa organizacijske ukrepe, ki jih operaterji morajo sprejeti, za zaščito hranjenih podatkov pred uničenjem, izgubo, spremembo ter nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja.

2. člen
(pomen izrazov)

(1) Izrazi uporabljeni v tem splošnem aktu imajo naslednji pomen:

1. Agencija je neodvisen regulativni organ, katere pristojnosti, organizacija in delovanje določa Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/2012, v nadaljevanju: ZEKom-1).
2. Sistem upravljanja varovanja informacij (v nadaljevanju: SUVI) je tisti del celotnega sistema upravljanja, ki temelji na pristopu poslovnega tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij.
3. Varnost omrežja in storitev je zmožnost javnega komunikacijskega omrežja, da z določeno stopnjo gotovosti prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo zaupnost, verodostojnost, celovitost ali razpoložljivost shranjenih ali prenesenih podatkov ter s tem povezanih javno dostopnih komunikacijskih storitev, ki jih ponujajo ta omrežja in ali so prek njih dostopne.
4. Sredstvo je vse, kar ima določeno vrednost za operaterja, za njegovo dejavnost ali izvajanje storitev.
5. Incident je eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo ogrozili varnost omrežij in storitev ali celovitost omrežja.
6. Grožnja je možen vzrok za incident, ki lahko povzroči škodo sredstvu, omrežju ali operaterju.
7. Ranljivost je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami.
8. Analiza varnostnih tveganj je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost omrežij in storitev.
9. Obravnava tveganj je proces izbora in vpeljave ukrepov za zmanjševanje tveganj.
10. Preostalo tveganje je tveganje, ki ostane po obravnavi tveganj.
11. Dokumentiran postopek pomeni, da je postopek zapisan.
12. Vodstveni pregled je dokumentiran pregled, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi ustreznost in učinkovitost SUVI.
13. Hranjeni podatki so podatki, ki so določeni v 164. členu ZEKom-1.
14. Obdelava podatkov je obdelava osebnih podatkov skladno z zakonom, ki ureja varstvo osebnih podatkov.

(2) Ostali pojmi uporabljeni v tem splošnem aktu imajo enak pomen, kot so določeni v ZEKom-1.

3. člen

(sistem upravljanja varovanja informacij)

(1) Operater mora sprejeti in izvajati postopke in ukrepe za zavarovanje hranjenih podatkov, ki morajo hranjene podatke zaščititi pred slučajnim ali namernim uničenjem, izgubo ali spremembo in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja.

(2) Operater mora postopke in ukrepe iz 1. odstavka tega člena obravnavati v okviru enotnega SUVI, s smiselno uporabo I. poglavja splošnega akta o varnosti omrežij in storitev, sprejetega na podlagi 86. člena ZEKom-1.

II. HRAMBA PODATKOV

4. člen

(splošno o hranjenih podatkih)

(1) Hranjeni podatki morajo biti enake kakovosti kot podatki, ki so biti zajeti v omrežju. Vse določbe tega splošnega akta, ki veljajo za hranjene podatke, veljajo tudi za prenos podatkov od zajetja v omrežju do informacijskega sistema za hrambo podatkov.

(2) Hranjeni podatki morajo biti dosegljivi in primerni za kasnejšo uporabo za namene iz prvega odstavka 163. člena ZEKom.

5. člen

(zavarovanje hranjenih podatkov)

(1) Postopki in tehnologija za hrambo podatkov morajo zagotavljati nadzor dostopa do hranjenih podatkov in popolno sledljivost obdelave hranjenih podatkov z zagotavljanjem celovitosti, zaupnosti in razpoložljivosti hranjenih podatkov. Vsak zajem, dostop, spreminjanje ali druga oblika obdelave hranjenih podatkov mora biti evidentirana z revizijsko sledjo.

(2) Dostop do hranjenih podatkov mora biti omejen na posameznike z ustreznimi pooblastili. Operater mora sprejeti in vzdrževati ažuren seznam pooblastil, ki omogočajo dostop do hranjenih podatkov in revizijske sledi.

(3) Informacijski sistem za hrambo podatkov mora biti ločen in neodvisen od drugih informacijskih sistemov operaterja ter mora zagotavljati fizično in logično varnost. Oprema za hrambo podatkov mora biti nameščena v varnem prostoru, ki onemogoča neavtoriziran dostop. Zagotovljena mora biti zaščita pred vplivi okolja.

(4) Informacijski sistem za hrambo podatkov mora zagotavljati zaščito zoper izgubo podatkov z rednim izdelovanjem, preverjanjem kakovosti in varnim hranjenjem varnostnih kopij. Za zavarovanje varnostnih kopij hranjenih podatkov veljajo iste zahteve kot za zavarovanje hranjenih podatkov.

(5) Pri prenosu podatkov v hrambo drugemu operaterju ali tretjim strankam preko elektronskih komunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod, tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

6. člen

(avtentičnost in celovitost)

(1) Postopki in tehnologija za hrambo podatkov morajo onemogočiti spremembo (avtentičnost) ali izbris podatkov (celovitost) med potjo podatkov od izvirnih naprav do sistema za hrambo ter v času hrambe in zagotavljati povezanost reproducirane vsebine z vsebino izvirnih podatkov iz omrežja ter zagotavljati nespremenljivost in neokrnjenost podatkov ter revizijsko sled.

(2) Avtentičnost in celovitost hranjenih podatkov se mora zagotoviti z dodajanjem varnostnih vsebin (npr. elektronski podpis, časovni žig in podobno), z drugimi sorodnimi tehnološkimi sredstvi in postopki, ki omogočajo dokazovanje avtentičnosti in celovitosti hranjenih podatkov (npr. tehnološka sredstva, ki omogočajo enkratno zapisovanje in večkratno branje.) ali z zagotavljanjem dodatnih organizacijskih ukrepov.

(3) Avtentičnost in celovitost hranjenih podatkov ter revizijske sledi v digitalni obliki morata biti zagotovljeni ves čas hrambe podatkov.

(4) Operater nosi breme dokazovanja avtentičnosti, celovitosti in preprečevanja tajenja obdelave hranjenih podatkov in revizijske sledi.

7. člen

(uničenje hranjenih podatkov)

Uničenje hranjenih podatkov na elektronskih pomnilnih medijih mora biti izvedeno tako, da jih ni mogoče delno ali v celoti obnoviti ali prebrati s pomočjo posebnih tehničnih sredstev oziroma postopkov.

III. KONČNE DOLOČBE

8. člen

(začetek veljavnosti)

(1) Ta splošni akt začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

(2) Z dnem uveljavitve tega splošnega akta se preneha uporabljati Splošni akt o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov (Uradni list RS št. 126/08).