Na podlagi Zakona o varstvu osebnih podatkov 1 (Uradni list RS št. 86/04, 113/05), Zakona o tajnih podatkih (Uradni list RS št. 50/06) ter določil 29. člena Statuta Elektro Primorske, javnega podjetja za distribucijo električne energije, d.d., Nova Gorica, Erjavčeva 22 je direktor družbe dne ...15.1.2007.... sprejel

PRAVILNIK
O VAROVANJU ZAUPNIH IN OSEBNIH PODATKOV TER DOKUMENTARNEGA GRADIVA

I. SPLOŠNE DOLOČBE

1. člen

Ta pravilnik določa načine varovanja zaupnih in osebnih podatkov v Elektro Primorski, d.d. (v nadaljevanju: družba) ter fizične, organizacijsko tehnične ukrepe ter obvezne sestavine postopkov za varovanje podatkov, ki jih mora pri vzpostavitvi sistema ukrepov in postopkov varovanja podatkov upoštevati in zagotoviti družba, da bi preprečila nezakonito in neupravičeno poseganje v informacijsko zasebnost posameznika ter v zaupne podatke družbe . V skladu s tem pravilnikom morajo ravnati tudi osebe, ki imajo dostop do teh podatkov.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. zaupni podatek: podatek, ki je razglašen za tajnost, ker je tako pomemben, da bi z njegovim razkritjem lahko nastale škodljive posledice za delovanje družbe;
2. osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
3. zbirka podatkov je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov
4. obdelava podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi s podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke podatkov oziroma so namenjeni vključitvi v zbirko podatkov
5. avtomatizirana obdelava je obdelava podatkov s sredstvi informacijske tehnologije
6. dokument: vsak napisan, narisan, natisnjen, razmnožen, fotografiran, fotokopiran, fonografiran ali optično ali kako drugače zapisan podatek
7. obravnavanje podatkov postopki in ukrepi pri sprejemu, pošiljanju, obdelavi, hrambi, razkritju, uporabi in uničenju podatkov
8. nosilec podatkov: vse vrste sredstev, na katerih so zapisani ali posneti podatki;
9. varovani prostori: vsi prostori v katerih se nahajajo nosilci zaupnih ali osebnih podatkov ali prostori v katerih je oprema, preko katere je mogoč dostop do teh podatkov.

II. VRSTE TAJNOSTI IN STOPNJE ZAUPNOSTI PODATKOV

3. člen

Vrste tajnosti zaupnih podatkov so:

1. strogo tajno podatki, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese družbe ali jim nepopravljivo škodovalo;
2. tajno: podatki, ki so tako pomembni, da bi z njihovo izdajo nastale ali bi lahko nastale hujše škodljive posledice za delovanje družbe.
3. zaupno: podatki, katerih razkritje bi škodovalo interesom družbe
4. interno: podatki, katerih razkritje bi škodovalo izvajanju nalog družbe

Podatkom, ki so določeni za tajnost, se glede na njihov pomen določi stopnja zaupnosti: strogo zaupno, zaupno ali interno:

a) tajno: določi direktor družbe;
b) zaupno: določi direktor sektorja, kjer se podatki nahajajo;
c) interno: strokovna navodila za opravljanje delovnih nalog, delovni materiali za zakonske in podzakonske predpise, analitična - statistična in druga gradiva o delu družbe, interno informiranje in interni imeniki;

Osebni podatki se lahko obdelujejo samo v skladu z zakonom ali na podlagi pisne privolitve posameznika. Z osebnimi podatki se, glede na njihovo vsebino, ravna kot s podatki »strogo tajno«. »tajno« ali »zaupno« (npr. interni telefonski imenik, seznam zaposlenih, ki so na dopustu). Stopnjo zaupnosti zbirk osebnih podatkov določi pooblaščena oseba. Zbirke osebnih podatkov, ki se obdelujejo v skladu z zakonom, se varujejo s stopnjo zaupnosti, ki je višja ali enaka kot »tajno »

III. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

Prostori, v katerih se nahajajo nosilci zaupnih ali osebnih podatkov, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja vodje pristojne organizacijske enote.

Za prostore, kjer se hranijo nosilci podatkov z oznako »strogo tajno« morajo varnostni ukrepi omogočiti popoln nadzor nad delom in gibanjem v teh prostorih.

Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključe se ne sme puščati v ključavnici v vratih z zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma jih je treba zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Izven delovnega časa morajo biti omare in pisalne mize z nosilci zaupnih in osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni. Izjema so centralni računalniki.

Zaposleni ne smejo puščati nosilcev zaupnih ali osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilce zaupnih ali osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

5. člen

Za prostore, v katerih je nameščena informacijska in telekomunikacijska oprema za obravnavanje podatkov, pa poleg ostalih pravil, določenih s tem pravilnikom, veljajo še naslednja pravila:

1. zadrževanje delavcev družbe v teh prostorih, razen tistih, ki so v njih zaposleni, ali je njihova prisotnost nujno potrebna za nemoteno opravljanje delovnih nalog, ni dovoljeno;
2. obiski strank so dovoljeni samo v spremstvu najmanj enega delavca družbe, če ni s tem pravilnikom drugače določeno.;
3. servisiranje informacijske ali telekomunikacijske opreme lahko izvajajo delavci družb, s katerimi ima Elektro Primorska d.d. sklenjeno ustrezno vzdrževalno pogodbo. Obiski morajo biti dogovorjeni z odgovorno osebo. V primeru, da s serviserjem družba nima sklenjene pogodbe, mora serviser pred pričetkom del podpisati izjavo o svoji odgovornosti v zvezi s podatki in opremo ali pa ga mora ves čas nadzorovati delavec družbe.
4. omare oziroma pisalne mize, v katerih so shranjeni mediji, morajo biti vedno zaprte.

6. člen

S štampiljkami in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki.

7. člen

Nosilcev podatkov z oznako »strogo tajno » in »tajno« zaposleni ne smejo odnašati izven prostorov družbe, ostale nosilce podatkov, ki vsebujejo zaupne podatke, pa samo z dovoljenjem pooblaščene osebe.

8. člen

Dokumente, ki vsebujejo tajne podatke, se hrani in arhivira v ustreznih prostorih in opremi, kot določajo predpisi o arhivski dejavnosti, ter tako, da imajo dostop zgolj pooblaščeni uporabniki .

9. člen

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

10. člen

Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

III. VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

11. člen

Strojno in programsko opremo, ki je v družbi namenjena za informacijsko in telekomunikacijsko obravnavanje podatkov, je dovoljeno uporabljati le za izvajanje nalog družbe.

Opremo iz predhodnega odstavka lahko uporablja le delavec družbe in to za izvajanje nalog za katere je odgovoren. Pravila uporabe strojne in programske opreme so natančno določena v aktu Varnostna politika uporabe računalniške opreme, ki ga sprejme direktor družbe.

12. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to

vnaprej določenim zaposlenim in pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

13. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z družbo sklenjeno ustrezno pogodbo.Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

14. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila, kot za ostale podatke iz tega pravilnika.

15. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo pomembni podatki, se vsakodnevno preveri glede na prisotnost računalniških virusov. Za odpravo morebitnega računalniškega virusa poskrbi ustrezna strokovna služba, ki ugotovi tudi vzrok pojava virusa.

Pred uporabo vseh podatkov in programske opreme, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v družbo na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, je treba preveriti morebitno prisotnost računalniških virusov.

16. člen

Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, ki je zadolžena za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz družbe brez odobritve vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

17. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

18. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (nadzorniška gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo v zapečatenih ovojnicah in se jih varuje kot »strogo tajno« na sedežu družbe pri vodji informacijskega sistema. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

19. člen

Za potrebe ponovne vzpostavitve računalniškega sistema ob okvarah in ob drugih izjemnih

situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj.

Te kopije se hranijo v zato določenih mestih, ki morajo biti zavarovana pred ognjem, proti poplavam in elektromagnetnim motnjam v okviru predpisanih klimatskih pogojev ter zaklenjena (praviloma so ta mesta kovinske blagajne).

20. člen

Za fizične, organizacijske in tehnične ukrepe ter postopke varovanja podatkov po tem pravilniku, ki se obdelujejo, prenašajo ali hranijo v komunikacijskih, informacijskih in drugih elektronskih sistemih, se smiselno uporablja določbe predpisa, ki ureja te ukrepe in postopke na podlagi zakona, ki ureja tajne podatke.

21. člen

V primeru izvajanja videonadzora, mora družba objaviti vidno in razločno obvestilo, ki mora vsebovati naslednje elemente:

- da se izvaja videonadzor;
- naziv osebe javnega ali zasebnega sektorja, ki ga izvaja;
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo podatki ter kdo ima dostop do teh podatkov.

Videonadzor mora biti zavarovan pred dostopom nepooblaščenih oseb.

Odločitev o videonadzoru sprejme direktor družbe ali pooblaščena oseba. O uvedbi videonadzora pristojna oseba obvesti vse zaposlene, ki delajo v nadzorovanem prostoru, pred uvedbo pa se posvetuje z reprezentativnim sindikatom.

IV. SPREJEM IN POSREDOVANJE ZAUPNIH IN OSEBNIH PODATKOV

22. člen

Zaupne in osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

23. člen

Podatke, ki so strogo tajni, tajni ali zaupni je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo obravnavanje teh podatkov.

Fizično se take podatke prenaša v zaprti ovojnici iz neprosojnega materiala, ki mora imeti v levem zgornjem kotu navedbo pošiljatelja ter datum dokumenta, v desnem zgornjem kotu pa oznako o stopnji zaupnosti.

24. člen

Zbirajo in obdelujejo se lahko samo tisti osebni podatki, ki imajo ustrezno zakonsko osnovo. Za vse ostale osebne podatke je potrebno pridobiti pisno privolitev posameznika, na katerega se nanašajo.

Družba za vsako zbirko osebnih podatkov, ki jo vodi in vzdržuje, v skladu s 26. členom zakona o varstvu osebnih podatkov zagotovi katalog zbirke osebnih podatkov, ki je dejansko opis posamezne zbirke in vsebuje:

1. naziv zbirke osebnih podatkov;

2. podatke o upravljavcu osebnih podatkov (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča, za samostojnega podjetnika posameznika pa še firmo, sedež in matično številko; za pravno osebo: naziv oziroma firmo in naslov oziroma sedež upravljavca osebnih podatkov in matično številko);
3. pravno podlago za obdelavo osebnih podatkov;
4. kategorije posameznikov, na katere se nanašajo osebni podatki;
5. vrste osebnih podatkov v zbirki osebnih podatkov;
6. namen obdelave;
7. rok hrambe osebnih podatkov;
8. omejitve pravic posameznikov glede osebnih podatkov v zbirki osebnih podatkov in pravno podlago omejitev;
9. uporabnike ali kategorije uporabnikov osebnih podatkov, vsebovanih v zbirki osebnih podatkov;
10. dejstvo, ali se osebni podatki iznašajo v tretjo državo, kam, komu in pravno podlago iznosa;
11. splošen opis zavarovanja osebnih podatkov;
12. podatke o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig;
13. podatke o zastopniku iz tretjega odstavka 5. člena tega zakona (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča, za samostojnega podjetnika posameznika pa še firmo, sedež in matično številko; za pravno osebo: naziv oziroma firmo in naslov oziroma sedež upravljavca osebnih podatkov in matično številko).

Podatke 1., 2., 4., 5., 6., 9., 10.., 11. 12. in 13. točke kataloga zbirke osebnih podatkov mora posredovati državnemu nadzornemu organu za varstvo osebnih podatkov – informacijskemu pooblaščencu – najmanj 15 dni pred vzpostavitvijo zbirke osebnih podatkov ali pred vnosom nove vrste osebnih podatkov. Prav tako mu mora posredovati spremembe teh podatkov najkasneje v osmih dneh od dneva spremembe.

25. člen

Zaupni in osebni podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko osnovo ali pisno privolitvijo posameznika, na katerega se nanašajo.

Za vsako posredovanje zaupnih in osebnih podatkov mora upravičenec vložiti pisno vlogo, na kateri mora biti navedena zakonska osnova za pridobitev osebnih podatkov, ali predložiti pisno privolitev posameznika. Vsako posredovanje zaupnih in osebnih podatkov se beleži v evidenco posredovanj, ki mora vsebovati pregled zahtevkov, kateri podatki so bili posredovani, komu in kdaj (7. in 10. člen Zakona o varstvu osebnih podatkov).

V. BRISANJE PODATKOV

26. člen

Čas hranjenja zbirk zaupnih in osebnih podatkov je določen z namenom, zaradi katerega so podatki zbrani.

Po preteku roka hranjenja se podatki brišejo ali uničijo, seveda če ne gre za zbirko, v kateri se zbrani podatki shranjujejo za časovno neomejeno obdobje.

27. člen

Podatki na klasičnih medijih (listine, kartoteke, registri, seznami ..) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov.

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izbrise ...). Prepovedano je odmetavati odpadne nosilce podatkov z zaupno vsebino v koše za smeti.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

28. člen

Zaposleni so dolžni takoj obvestiti pooblaščeno osebo ali predstojnika o aktivnostih, za katere obstaja upravičen sum, da so povezane z razkrivanjem ali nepooblaščenim uničevanjem zaupnih podatkov, zlonamerno ali nepooblaščeno uporabo, prilaščanjem, spreminjanjem ali poškodovanjem. Ob tem tudi sami poskušajo takšno aktivnost preprečiti.

VII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

29. člen

Za izvajanje postopkov in ukrepov za varovanje zaupnih in osebnih podatkov so odgovorni direktorji sektorjev, vodje distribucijskih enot, vodje organizacijskih enot in pooblaščene osebe, ki jih imenuje direktor družbe.

Osebe iz prejšnjega odstavka morajo poslovanje organizacijskih enot, ki jih vodijo, organizirati tako, da zagotovijo spoštovanje določb tega pravilnika in drugih predpisov o varovanju podatkov, in seznanijo delavce v svoji enoti z dolžnostjo varovanja podatkov.

30. člen

Vsak, ki obdeluje zaupne in osebne podatke ali se z njimi v okviru opravljanja svojega dela seznani, je dolžan izvajati predpisane postopke in ukrepe za varstvo in zavarovanje podatkov teh podatkov. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Pred nastopom dela na delovnem mestu, kjer se obdelujejo podatki s stopnjo zaupnosti, ki je višja ali enaka od »uradna tajnost - zaupno« , mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju poklicne skrivnosti in vsebuje pouk o posledicah kršitve.

31. člen

Za kršitev prejšnjega člena so zaposleni disciplinsko odgovorni.

32. člen

Zunanji sodelavci smejo opravljati samo storitve obdelave zaupnih in osebnih podatkov v okviru naročnikovih pooblastil in jih ne smejo obdelovati ali drugače uporabljati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora vsebovati tudi pogoje in ukrepe za zagotovitev varstva zaupnih ali osebnih podatkov.

Za kršitev določil predhodnega odstavka so zunanji sodelavci odgovorni na temelju pogodbenih obveznosti.

VIII. KONČNE DOLOČBE

33. člen

Vsi, ki obravnavajo zaupne in osebne podatke, morajo prilagoditi prostore in sprejeti ustrezne ukrepe za izvajanje tega pravilnika najkasneje v šestih mesecih od uveljavitve tega pravilnika

34. člen

Ta pravilnik prične veljati osmi dan po objavi na oglasih deskah družbe.

35. člen

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varovanju zaupnih in osebnih podatkov ter dokumentarnega gradiva, ki ga je direktor družbe sprejel 20. 2. 2000.

Direktor:

David Valentinčič, univ.dipl.inž.

Št. 1/1

ELEKTRO PRIMORSKA
JAVNO PODJETJE ZA DISTRIBUCIJO
ELEKTRIČNE ENERGIJE d.d.
NOVA GORICA, Erjavčeva 22