Pravilnik o zavarovanju osebnih podatkov podjetja RAIS d.o.o.

Organizacijski predpis

Verzija 1.0

Lastnosti dokumenta

Številka dokumenta	01710224
Pravice/zaupnost	Interni dokument
Projekt	ISO 9001:2015
Datoteka	Q:\ISO_9001_2015\Pravilniki\OP-01710224 - Pravilnik o zavarovanju osebnih podatkov.doc
Pripravil	Klavdija Vidov
Nastanek	datum: 20.09.2017 08:13:45
Zadnja sprememba	datum: 27.09.2017 10:08, shranil: Klavdija Vidov
Pregledal	datum: 20.09.2017 Klavdija Vidov
Odobril	datum: 27.09.2017 Damjan Cerk

Zgodovina dokumenta

Verzija	Datum	Spreminjal	Opis
1.0	20.09.2017	Klavdija Vidov	Prva verzija dokumenta

PRAVILNIK
o zavarovanju osebnih podatkov podjetja RAIS d.o.o.

I. SPLOŠNE DOLOČBE

1. člen

Pravilnik je sprejet na podlagi sklepa vodstva (vodstvo je opredeljeno v dokumentu Notranja sistemizacija podjetja RAIS d.o.o) ter 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP).

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v podjetju RAIS d.o.o z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.

Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z ZVOP-om, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. ZVOP - Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07).
2. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.
3. Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa.
4. Zbirka osebnih podatkov - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.
5. Obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).
6. Upravljavec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.
7. Pogodbeni obdelovalec – je fizična ali pravna oseba, ki obdeluje posebne podatke v imenu in na račun upravljavca osebnih podatkov.
8. Posredovanje osebnih podatkov – je posredovanje ali razkritje osebnih podatkov.
9. Občutljivi osebni podatki - so podatki o rasnem narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti.
10. Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;

11. Nosilec podatkov so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.).

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

3. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali 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 organizacijske enote.
Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.
Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.
Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.
Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.
Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.
Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

4. člen

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

5. člen

Vzdrževanje in popravila strojne računalniške ter druge opreme je dovoljeno samo z vednostjo in prisotnostjo pooblaščene osebe.

6. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo in prisotnostjo pooblaščene osebe. Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne 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

7. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to vnaprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

8. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe. Izvajalci morajo spremembe in dopolnitve sistemske ter aplikativne programske opreme ustrezno dokumentirati.

9. člen

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

10. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj in vseh ostalih elektronskih medijev, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov.

11. člen

1. Zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.
2. Zaposleni ne smejo odnašati osebnih podatkov iz prostorov podjetja RAIS d.o.o brez odobritve člana vodstva projekta.

12. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Vodstvo podjetja določi režim dodeljevanja hranjenja in spreminjanja gesel.

IV. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

13. člen

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, na katero je ta pošiljka naslovljena.
Zaposleni, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v podjetje - prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega odstavka tega člena.
Zaposleni, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov podjetja.

14. člen

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.

V. BRISANJE PODATKOV

15. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.
Podatki na klasičnih medijih (listine, kartoteke, register, seznam, ...) 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 izpise ipd.).
Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.
Elektronske medije (disketa, CD, DVD, idr.) je potrebno po končani uporabi oz. obdelavi (za katero so bili mediji posredovani) fizično uničiti oziroma vrniti naročniku.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

16. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju, takoj obvestiti pooblaščeno osebo; sami pa poskušajo takšno aktivnost preprečiti.

VII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

17. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren direktor podjetja RAIS d.o.o.
Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, izvaja skrbnik informacijske infrastrukture podjetja RAIS d.o.o.

18. člen

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov ter varovati tajnost podatkov, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.
Pred nastopom dela na delovno mesto mora zaposleni v podjetju RAIS d.o.o. podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.
Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami ZVOP, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

VIII. KRŠITVE

19. člen

Razkrivanje osebnih podatkov - s katerimi se zaposleni pri svojem delu seznani – nepooblaščenim osebam ali zloraba teh podatkov je sankcionirana kot hujša kršitev delovnih obveznosti in kot kaznivo dejanje. Hkrati je to tudi razlog za prenehanje pogodbe o zaposlitvi iz krivdnih razlogov.

IX. SPLOŠNE DOLOČBE

20. člen

Ta pravilnik prične veljati z 20.09.2017.