PRAVILNIK O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV

Izdaja: 1

Revizija: 1

Datum veljavnosti: od 12.3.2019

Pripravil:

infoCenter
www.infocenter.si

Kontaktni podatki:

telefon: 031 692 524
e-pošta: info@infocenter.si
internet: www.infocenter.si

MD SVETOVANJE d.o.o., Dunajska cesta 156, 1000 Ljubljana, Matična št.: 2295750000, ID za DDV: SI97239372

Osnovna šola Simona Jenka, Smlednik 73, 1216 Smlednik, davčna številka: 11413743, matična številka: 5084385000 (v nadaljevanju: upravljavec) na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 s spremembami, v nadaljevanju: ZVOP-1) ter 24., 25. in 32. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov)

sprejema naslednji

Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov

I. Splošne določbe

1. člen

S tem Pravilnikom o postopkih in ukrepih za zavarovanje osebnih podatkov (v nadaljevanju: Pravilnik) se določajo tehnični, organizacijski ter kadrovski postopki in ukrepi za zavarovanje osebnih podatkov upravljavca, z namenom, da se izpolnijo zakonske zahteve glede varovanja osebnih podatkov in zaščitijo pravice posameznikov, na katere se osebni podatki nanašajo.

Ti ukrepi predstavljajo skupek zavezujočih pravil, priporočil in načel iz prakse, internih postopkov, organizacijskih struktur ter varnosti informacijske tehnologije.

2. člen

Namen tega Pravilnika je zagotoviti zaupnost, celovitost, dostopnost in točnost osebnih podatkov, v interesu posameznikov, na katere se osebnih podatki nanašajo, in sicer v vsaki fazi obdelave osebnih podatkov. Vsi delavci se morajo zavedati tveganj, ki so povezana s tehničnimi in informacijskimi sistemi ter komunikacijsko tehnologijo, ter morajo zato izvajati obdelavo osebnih podatkov z zahtevano skrbnostjo.

Ukrepi, opisani v tem Pravilniku, so oblikovani ob upoštevanju najnovejšega tehnološkega razvoja in stroškov, izvajanja ter narave, obsega, okoliščin in namenov obdelave kot tudi tveganj za pravice in svoboščine posameznikov ter zagotavljajo ustrezno varnost podatkov glede na morebitna tveganja, ki jih pomeni obdelava podatkov, zlasti v primeru nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

3. člen

Upravljavec se ravna po priznanih pravilih za varnost informacij.

Pravilnik izhaja iz predpostavke, da absolute varnosti ni in da je zagotavljanje informacijske varnosti živo stanje, ki od upravljavca zahteva stalno izboljševanje in prilagajanje varnosti na spreminjajoče se pogoje. Ukrepi predstavljajo kompromis med tehničnimi zmožnostmi in zmožnostjo realizacije, ki je v danem primeru pogojena s kadrovskimi in ekonomskimi vidiki upravljavca.

4. člen

Upravljavec pri obdelavi osebnih podatkov upošteva splošna načela v zvezi z obdelavo osebnih podatkov.

Upravljavec obdeluje le tiste osebne podatke, za katere ima ustrezno zakonsko podlago na podlagi določb ZVOP-1 in Splošne uredbe o varstvu podatkov.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, razen če relevantna zakonodaja to omogoča.

Pri obdelavi osebnih podatkov upravljavec zagotavlja, da so osebni podatki:

- obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki,
- zbrani za določene, izrecne in zakonite namene ter da se ne obdelujejo dalje na način, ki ni združljiv s temi nameni,
- ustrezni, relevantni in omejeni glede na namene, za katere se obdelujejo,
- točni in - kadar je to potrebno - posodobljeni,
- hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, toliko časa, kolikor je to potrebno za dosego namenov, za katere se obdelujejo, razen če posamezen zakon ne določa drugače,
- obdelujejo na način, ki zagotavlja njihovo celovitost in zaupnost,
- z ustreznimi tehničnimi ali organizacijskimi ukrepi ustrezno varovani pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem, ali poškodbo.

5. člen

Ta Pravilnik velja za vse delavce pri upravljavcu, ne glede na to, ali so v delovnem razmerju pri upravljavcu (v nadaljevanju delavci). Pravilnik je namenjen zlasti tistim delavcem, ki so posredno ali neposredno udeleženi pri obdelavi osebnih podatkov, ter pri zagotavljanju varnosti informacijske tehnologije.

6. člen

Izrazi, ki se uporabljajo v tem Pravilniku, imajo pomene, kot izhajajo iz veljavnega ZVOP-1 ter Splošne uredbe o varstvu podatkov.

II. Seznam evidenc dejavnosti obdelave osebnih podatkov

7. člen

Upravljavec za namen identifikacije in popisa vseh vrst osebnih podatkov, katere obdeluje, vodi Seznam evidenc dejavnosti obdelave osebnih podatkov (v nadaljevanju: Seznam evidenc), v katerem so zapisane vse zbirke osebnih podatkov, ki jih obdeluje, in katerega namen je omogočiti popoln pregled nad tokom osebnih podatkov. Seznam evidenc predstavlja podlago sprejemu tehničnih, organizacijskih in kadrovskih ukrepov za zavarovanje osebnih podatkov, kot so opisani v tem Pravilniku.

Seznam evidenc se vodi na način, da je za vsako evidenco dejavnosti obdelave osebnih podatkov razvidno:

- katere vrste osebnih podatkov se obdelujejo,
- na katere kategorije posameznikov se nanašajo osebnih podatki,
- kaj je namen obdelave osebnih podatkov,
- na kakšni pravni podlagi se osebni podatki obdelujejo,
- kakšen je predviden rok hrambe oz. izbrisa podatkov ter,
- morebitne osebe oz. uporabnike, katerim so osebnih podatki lahko razkriti,
- ali se podatki iznašajo v tretjo državo in/ali mednarodno organizacijo,
- s katerimi tehničnimi, organizacijskimi in kadrovskimi ukrepi se zagotavlja varstvo osebnih podatkov.

Upravljavec skrbi za točnost in ažurnost Seznama evidenc. Upravljavec nadzornemu organu na njegovo zahtevo omogoči dostop do Seznama evidenc.

Delavci, ki pri izvajanju del in nalog za upravljavca obdelujejo osebne podatke, morajo biti seznanjeni s Seznamom evidenc, vpogled vanj pa je potrebno omogočiti tudi vsakomur, ki to zahteva in ima za vpogled zakoniti interes (npr. posameznik, na katerega se nanašajo osebnih podatki, nadzorni organ, policija na podlagi zakonskih pooblastil).

8. člen

Ob upoštevanju narave, obsega, okoliščin in namena obdelave, ki velja za upravljavca in ki je razviden iz Seznama evidenc, upravljavec zaključuje, da obdelava podatkov ne predstavlja velikega tveganja za pravice in svoboščine posameznikov, zato priprava predhodne ocene učinka v zvezi z obdelavo podatkov ni potrebna. V kolikor bo potrebna se izvede kot dodatek k pravilniku.

Upravljavec se zaveže ponovno opraviti pregled tveganj in oceniti, ali je v zvezi z obdelavo potrebna priprava ocene učinka vedno, ko se spremeni tveganje, ki ga predstavljajo dejanja obdelave, ko obdeluje nove osebne podatke, pred uporabo novih tehnologij ali ko se spremenijo narava, obseg, okoliščine in nameni obdelave osebnih podatkov.

III. Kadrovski ukrepi

9. člen

Naloge in pristojnosti glede obdelave osebnih podatkov, ki so si med seboj v konfliktu, so dodeljene različnim osebam ali oddelkom, z namenom, da se v najkrajšem možnem času prepoznajo nepooblaščene ali nenamerne spremembe podatkov.
Vloge in naloge so določene skladno z notranjo organiziranostjo upravljavca, pri čemer je za določanje namenov obdelave osebnih podatkov, pristojnost za določitev sredstev informacijske tehnologije ali operativne procese, varnost podatkov in zagotovitev tehničnih, kadrovskih in organizacijskih ukrepov v prvi vrsti odgovoren direktor upravljavca.

Dostop do osebnih podatkov je opredeljen v Seznamu evidenc.

Za pravilno izvajanje tega Pravilnika je dokončno pristojen in odgovoren direktor upravljavca.

10. člen

Upravljavec v zvezi z pooblaščeno osebo za varstvo podatkov ravna po 37. členu Splošne uredbe o varstvu podatkov.

V kolikor bo imenoval pooblaščeno osebo za varstvo podatkov, jo imenuje s Sklepom o imenovanju pooblaščene osebe za varstvo podatkov.

11. člen

Vsak, ki obdeluje osebne podatke znotraj upravljavca, je dolžan te podatke obdelovati zgolj z dovoljenjem upravljavca in znotraj njegovih navodil, izvajati s tem pravilnikom predpisane postopke in ukrepe za zavarovanje osebnih podatkov ter varovati osebne podatke, za katere je zvedel oz. bil z njimi seznanjen pri opravljanju svojega dela.

Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Vsak, ki pri svojem delu obdeluje osebne podatke, mora biti seznanjeni z zakonodajo s področja varstva osebnih podatkov in z vsebino tega Pravilnika. Upravljavec bo v ta namen poskrbel, da bodo taki delavci podpisali posebno Izjavo o varstvu osebnih podatkov, iz katere bo razvidno, da so seznanjeni z določbami tega Pravilnika in zakonodajo s področja varstva osebnih podatkov.

Upravljavec bo skladno z načelom odgovornosti delavcem, ki rokujejo z osebnimi podatki, po potrebi zagotavljal ustrezna izobraževanja oz. treninge s področja varovanja osebnih podatkov.

Za kršitev določil iz tega člena so delavci disciplinsko, odškodninsko in kazensko odgovorni. Kršitev določil tega Pravilnika se šteje za hujšo kršitev pravic in obveznosti iz delovnega razmerja, kar predstavlja podlago za redno odpoved pogodbe o zaposlitvi iz krivdnih razlogov ali izredno odpoved v primeru hujših kršitev.

IV. Fizična varnost

12. člen

Osebni podatki in informacijski sistemi morajo biti ustrezno zaščiteni pred tatvino, poškodovanjem in negativnimi učinki iz okolja.

Prostori, kjer se nahajajo osebnih podatki, njihove kopije in informacijski sistemi, morajo biti ognjevarni (gasilni aparati, požarni senzor), zavarovani proti izlitjem vode, poplavami in elektromagnetnimi motnjami, v okviru predpisanih klimatskih pogojev.

Vsi informacijski sistemi, ki so kritični za upravljavca, se morajo nahajati v varnem okolju. Vsi prostori, v katerih se nahajajo nosilci osebnih podatkov ter strojna in programska oprema, morajo biti fizično varovani

(npr. zaklenjeni, pospravljeni v predal ali omaro na zaklep ali geslo ipd.), tako da je nepooblaščenim osebam dostop do podatkov preprečen.

Taki varovani prostori oz. stavba kot celota, kjer se shranjujejo osebni podatki, so mehansko ali tehnično varovani.

13. člen

Osebni podatki se ne smejo hraniti izven varovanih prostorov.

Varovani prostori ne smejo ostajajo nenadzorovani, oz. se zaklepajo ob odsotnosti delavcev, ki jih nadzorujejo. Izven delovnega časa se varovani prostori zaklepajo, ključi se morajo hraniti v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih.

14. člen

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.

Delavci v svoji odsotnosti z delovnega mesta upoštevajo t. i. politiko čiste mize in politiko čistega ekrana. Nosilcev osebnih podatkov ne puščajo na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje, računalniške ekrane pa fizično ali programsko zaklepajo.

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

15. člen

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

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo odgovornega delavca upravljavca.

V. Varovanje integritete in zaupnosti podatkov ob sprejemu in prenosu

16. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte:

1) mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je pošiljka naslovljena,
2) odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo k upravljavcu, razen pošiljk iz tretje in četrte točke tega člena,
3) ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki,

4) 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 upravljavca.

17. člen

Osebni podatki se pošiljajo s priporočeno pošto ali osebno preko kurirja.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

18. člen

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

V primeru elektronskega pošiljanja sporočil z osebnimi podatki upravljavec zagotavlja tehnične postopke, ki onemogočijo prestrezanje, kopiranje, spreminjanje, preusmerjanje ali uničenje prenesenih informacij.

19. člen

Obdelava posebnih vrst osebnih podatkov mora biti posebej označena in zavarovana.

Posebne vrste osebnih podatkov se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

VI. Zagotavljanje zaupnosti, celovitosti in odpornosti sistemov in storitev za obdelavo podatkov

20. člen

Dostop do visoko občutljivih informacij upravljavec ureja z različnimi tehničnimi sredstvi in določanjem varnostnih con ter omejevanjem dostopa.

Uporabniki in informacijske storitve in sistemi se v omrežjih ločijo. Prav tako se ločijo razvojna, testna in obratovalna okolja.

Zagotavlja se kontrola dostopa, ki omogoča, da lahko dostop do funkcij, programov in podatkov informacijskega sistema prejmejo le upravičene osebe.

21. člen

Dostop do programske opreme je urejen s t. i. politiko dostopnih pravic. Dostop je dovoljen samo za to vnaprej določenim delavcem ali zunanjim ponudnikom storitev.

Dostop do informacijskih sistemov je omejen na pravice, ki so potrebne za izvajanje določene naloge (npr. pravice do branja, spreminjanja, administratorski dostop). Pri podelitvah pravic dostopa upravljavec sledi načelo »*need-to-know*«, kar pomeni, da uporabniki ne smejo prejeti več pravic, kot bi bile potrebne za izvajanje njihovih nalog ali za dostop do podatkov.

Vsakemu uporabniku se dodeliti jasno (osebno) uporabniško ime (ID oznaka uporabnika). To velja tudi za privilegirane pravice do dostopa (npr. za administratorje).

Za preprečitev morebitnega napada ali varnostnega tveganja se beležijo vsi kritični, zlasti pa neuspeli poskusi dostopa.

Zunanji dostopi, ki so namenjeni vzdrževanju, se aktivirajo le za čas trajanja vzdrževanja po predhodno izvedenem formalnem in dokumentiranem zahtevku. Po prenehanju vzdrževalnih del se ti podeljeni dostopi za vzdrževanje deaktivirajo oz. onemogočijo.

Če določen delavec zamenja delovno mesto, se pravice dostopa ponovno preverja in po potrebi prilagodi. Tudi sicer se morajo pravice do dostopa redno preverjati in ažurirati.

Če delavec preneha opravljati delo za upravljavca, se mora najpozneje ob koncu zadnjega delovnega dne odvzeti vsa izdana dovoljenja za dostop. Enako velja za vse zunanje ponudnike storitev.

22. člen

Strojna oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami, mora biti zaščitena na način, da se zavaruje integriteta in zaupnosti podatkov.

Vsi osebni računalniki, na katerih je možen dostop do osebnih podatkov, so varovani z uporabniškim imenom in geslom.

Programska oprema inštalirana na računalniku, ki omogoča dostop do osebnih podatkov, je varovana z uporabniškim imenom in geslom.

Pooblaščena oseba določi režim dodeljevanja hranjenja in spreminjanja gesel.

23. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oz. ob nujnih primerih.

Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

24. člen

Vzdrževanje, popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve s strani direktorja oz. z njegove strani pooblaščenega delavca (skrbnika), izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z upravljavcem sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Zaposleni ne smejo namestiti programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz poslovnih prostorov brez odobritve vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

25. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja za prisotnost računalniških virusov.

Vse delovne postaje in prenosni računalniki in druga oprema morajo biti opremljeni z aktivirano in posodobljeno protivirusno zaščito. Vsi računalniki na delovnem mestu morajo biti opremljeni s kombinacijo lokalnega požarnega zidu in lokalnega sistema za zaznavanje in preprečevanje vdorov. Vsi prenosni računalniki in druga oprema morajo biti opremljeni z lokalnim požarnim zidom.

Ob pojavu računalniškega virusa se tega čimprej odpravi s pomočjo ustrezne strokovne službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo k upravljavcu na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

26. člen

Če uporabnik ali administrator zapusti delovno mesto ali ne izvaja nobenih vnosov, se mora v določenem časovnem razponu samodejno vključiti zapora zaslona, zaščitena z geslom.

Na sistemih, kjer je to tehnično možno, poteka avtomatska odjava uporabnika, če ni bilo izvedenih vnosov znotraj opredeljenega časovnega razpona.

Pri prenosnih računalnikih se uporablja ustrezno šifriranje trdih diskov. Prav tako se preko kontrole priključka lahko omeji ali onemogoča uporaba zunanjih naprav na odjemalcih.

Poslovne informacije se načeloma ne shranjujejo lokalno na računalnikih na delovnem mestu ali prenosnih računalnikih dlje, kot je treba, in se shranjujejo na centralno upravljane sisteme, ki so predvideni za ta namen.

27. člen

Pred nedovoljenimi dostopi in manipulacijami morajo biti zaščitene tudi pisarniške naprave za komunikacijo kot so tiskalniki, kopirni stroji, faks naprave ipd.

Upravljavec mora prav tako sprejeti ustrezne informacijske varnostne ukrepe, v primeru oddaljenega dostopa.

VII. Zagotavljanje dostopnosti oz. razpoložljivosti podatkov v primeru fizičnega ali tehničnega incidenta

28. člen

Vsaka operacija s podatki se beleži v sistemskih dnevniških datotekah. Beleženje mora izvesti administrator v skladu z zahtevami in možnostmi operacijskih sistemov in aplikacij.

Revizijska sled mora zagotavljati možnost ugotovitve, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani oz. spremenjeni ter kdo je to storil. Vsi dogodki se morajo opremiti s časovnim žigom.

29. člen

Osebni podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oz. privolitvijo posameznika, na katerega se podatki nanašajo.

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakonska podlaga, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora biti k vlogi priložena pisna zahteva oz. privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, kam oz. komu, kdaj in na kakšni podlagi. Evidenca sledljivosti posredovanj podatkov se vodi po kronološkem vrstnem redu.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

30. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki tam nahajajo (tj. izdelava varnostnih kopij podatkov).

Za podatke, za katere velja visoka zahteva po razpoložljivosti, se mora varnostna kopija vzpostaviti redno, tako da se lahko v primeru izpada ene ali več komponent ponovno vzpostavi pripravljenost za obratovanje celotnega sistema.

31. člen

Ob izpadu sistema mora biti zagotovljeno, da se ne izgubijo nobene kritične informacije.

Mediji za varnostno shranjevanje se morajo hraniti na krajih, ki izpolnjujejo zahteve zaupnosti, integritete in razpoložljivosti zadevnih informacij. To vključuje tudi zadostno prostorsko ločevanje med mediji za varnostno shranjevanje in varnostnim virom (npr. skladiščenje v drugih prostorih).

Zagotoviti se mora, da ima administracijsko osebje v nujnem primeru dostop do varnostnih medijev.

Določiti se morajo roki za shranjevanje in roki za izbris varnostnih kopij.

32. člen

Informacije se arhivirajo v skladu z zakonskimi, pogodbenimi in poslovnimi zahtevami.

Določiti se mora trajanje shranjevanja za bistvene poslovne informacije in arhivske kopije.

Arhivski podatki se morajo skladiščiti ali shranjevati na krajih, ki izpolnjujejo zahteve razpoložljivosti, integritete in zaupnosti.

VIII. Redno testiranje, ocenjevanje in vrednotenje ukrepov

33. člen

Upravljavec se zaveže, da bo redno testiral, ocenjeval in vrednotil učinkovitost tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

Upravljavec bo v ta namen vsaj enkrat letno preveril zakonitost obdelave osebnih podatkov. Za namen oprave notranje kontrole bo upravljavec pregledal dnevnike v zvezi z delovanji obdelav osebnih podatkov (dnevniške datoteke) in se posvetoval z ustreznimi strokovnjaki za informacijsko varnost.

IX. Rok hrambe in brisanje podatkov

34. člen

Upravljavec zagotavlja, da je obdobje hrambe osebnih podatkov omejeno na najkrajše mogoče obdobje. V ta namen upravljavec v Seznam evidenc predpiše roke za izbris osebnih podatkov.

Po preteku roka hranjenja se osebni podatki zbrišejo oz. trajno uničijo ali anonimizirajo, razen če zakon ali drug akt določa drugače.

35. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov. Brisanje mora biti popolno in nepovratno. Poleg nosilca takih podatkov je potrebno uničiti tudi podatke v mapi »Izbrisano« ali »Koš« oz. drugi ustrezni mapi/direktoriju, tako da vsebine ni več moč obnoviti.

Podatki na klasičnih medijih (listine, kartoteke, register, seznam ipd.) 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 oz. neuspešne izpise ipd.).

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

X. Storitve, ki jih opravljajo zunanje pravne ali fizične osebe

36. člen

Upravljavec lahko posamezna dejanja obdelave podatkov zaupa tudi zunanji pravni ali fizični osebi (v nadaljevanju: obdelovalec), ki zagotavlja zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov za varstvo osebnih podatkov. Obdelovalec, ki opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta Pravilnik.

V takem primeru bo upravljavec z obdelovalcem sklenil ustrezne pisne dogovore o pogodbeni obdelavi osebnih podatkov, v katerih bo določil pravice in obveznosti obeh strank. V takšnem dogovoru morajo biti obvezno predpisani pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja ter obveznosti obdelovalca napram upravljavcu. Omenjeno velja tudi za obdelovalce, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

Obdelovalec lahko na podlagi takega dogovora v imenu in za račun upravljavca opravlja samo dogovorjena opravila v zvezi z obdelavo osebnih podatkov upravljavca. Obdelovalec podatkov ne sme obdelovati ali drugače uporabljati za noben drug namen.

XI. Poročanje v primeru varnostnega incidenta

37. člen

Upravljavec zagotavlja dosleden in učinkovit sistem za ravnanje z varnostnimi incidenti, vključno z dokumentiranjem in obveščanjem o varnostnih dogodkih.

V ta namen upravljavec zagotovi informacijski sistem, ki je sposoben izvajati nadzor za prepoznavanje dogodkov (npr. požarni zid, zaznavanje vdorov, sistem nadzora). Informacijski sistemi nadalje omogočajo dokumentiranje vseh varnostno relevantnih ali sistemsko kritičnih dogodkov. Za spremljanje teh beleženj je odgovorna pooblaščena oseba (skrbnik) informacijskega sistema, ki mora v primeru varnostno pomembnih incidentov poročati vodstvu upravljavca.

Vsi delavci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, nedostopnosti, spreminjanju ali poškodovanju podatkov, takoj obvestiti vodstvo upravljavca, sami pa poskušajo takšno aktivnost preprečiti.

Upravljavec v evidenco varnostnih incidentov beleži vsako kršitev varstva osebnih podatkov, iz katere morajo biti razvidna dejstva v zvezi s kršitvijo varstva osebnih podatkov, učinki take kršitve in sprejeti popravni ukrepi.

V evidenco varnostnih incidentov se po kronološkem vrstnem redu vpisujejo vsi varnostni incidenti, ne glede na stopnjo in vrsto tveganja za pravice in svoboščine posameznikov. Upravljavec zlasti beleži kršitve zaupnosti podatkov (npr. nepooblaščeno razkritje podatkov), kršitve v zvezi z možnostjo dostopa do podatkov in kršitve integritete podatkov (npr. nepooblaščena sprememba podatkov).

38. člen

Če je verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, mora upravljavec nemudoma, najkasneje pa v roku 72 ur po seznanitvi s kršitvijo, o njej uradno obvestiti pristojni nadzorni organ, skladno s 33. členom Splošne uredbe o varstvu podatkov.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikom, mora upravljavec skladno z določbo 34. člena Splošne uredbe o varstvu podatkov brez nepotrebnega odlašanja obvestiti tudi posameznike, na katere se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

XII. Končne določbe

39. člen

Vse spremembe in dopolnitve tega Pravilnika se sprejmejo na enak način kot Pravilnik in v pisni obliki.

40. člen

Pravilnik začne veljati na dan objave.

Pravilnik se objavi na pri upravljavcu običajen način, tako da se z njegovo vsebino lahko seznanijo vsi delavci pri upravljavcu.

41. člen

Ta Pravilnik je na razpolago in vpogled vsem delavcem v kadrovski službi upravljavca v času delovnika. Delavcem je omogočeno, da se brez nadzora seznanijo z vsebino tega Pravilnika.

V/Na Smledniku, dne 12.3.2019

Marko Valenčič, ravnatelj

_____