Podjetje A1 INFORMATIKA d.o.o. (podjetje), ki ga vodi Primorac Ivan (direktor) sprejema

PRAVILNIK
o varovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen
(vsebina)

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

Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z zakonom, ki ureja varstvo osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika. Pri svojem delu morajo ravnati skladno s temi predpisi.

V zadevah varstva osebnih podatkov, ki jih ne ureja ta pravilnik se neposredno uporabljajo določbe 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[1] (v nadaljevanju Splošna uredba).

Določila tega pravilnika veljajo in se smiselno uporabljajo tudi za zunanje sodelavce, štipendiste podjetja in kandidate za sklenitev delovnega razmerja.

2. člen
(varovanje osebnih podatkov)

Varovanje osebnih podatkov zajema pravne, organizacijske in ustrezno logistično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori in informacijska tehnologija,
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- zagotavlja varnost posredovanja in prenosa osebnih podatkov,
- preprečuje nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki, in do njihovih zbirk,
- omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki vpisani in uporabljeni v zbirki podatkov in kdo je to storil - za obdobje, za katero se posamezni podatki shranjujejo.

3. člen
(pomen izrazov)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

[1] Uradni list Evropske unije, L 119, 4. maj 2016

1. Splošna uredba – Uredba (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;
2. relevantni predpisi - Splošno uredba, zakon, ki ureja varstvo osebnih podatkov in drugi predpisi, ki urejajo varstvo osebnih podatkov;
3. osebni podatek pomeni: katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
4. obdelava pomeni: vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;
5. omejitev obdelave pomeni: označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;
6. oblikovanje profilov pomeni: vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;
7. psevdonimizacija pomeni: obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;
8. zbirka pomeni: vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
9. upravljavec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;
10. obdelovalec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
11. uporabnik pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru

posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;

12. tretja oseba pomeni: fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
13. privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;
14. kršitev varstva osebnih podatkov pomeni: kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
15. genski podatki pomeni: osebne podatke v zvezi s podedovanimi ali pridobljenimi genskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;
16. biometrični podatki pomeni: osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;
17. podatki o zdravstvenem stanju pomeni: osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
18. glavni sedež pomeni:

    a) v zvezi z upravljavcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugem sedežu upravljavca v Uniji in ima ta sedež pooblastila za izvajanje takih odločitev, sedež, ki sprejema take odločitve;

    b) v zvezi z obdelovalcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, če obdelovalec nima osrednje uprave v Uniji, sedež obdelovalca v Uniji, kjer se izvajajo glavne dejavnosti obdelave v okviru dejavnosti sedeža obdelovalca, kolikor za obdelovalca veljajo posebne obveznosti iz te uredbe;
19. predstavnik pomeni: fizično ali pravno osebo s sedežem v Uniji, ki jo pisno imenuje upravljavec ali obdelovalec v skladu s členom 27 Splošne uredbe in ki predstavlja upravljavca ali obdelovalca v zvezi z njegovimi obveznostmi iz te uredbe;

20. podjetje pomeni: fizično ali pravno osebo, ki opravlja gospodarsko dejavnost, ne glede na njeno pravno obliko, vključno s partnerstvi ali združenji, ki redno opravljajo gospodarsko dejavnost;
21. povezana družba pomeni: obvladujočo družbo in njene odvisne družbe;
22. zavezujoča poslovna pravila pomeni: politike na področju varstva osebnih podatkov, ki jih upravljavec ali obdelovalec s sedežem na ozemlju Republike Slovenije spoštuje pri prenosih ali nizih prenosov osebnih podatkov upravljavcu ali obdelovalcu povezane družbe ali skupine podjetij, ki opravljajo skupno gospodarsko dejavnost, v eni ali več tretjih državah;
23. nadzorni organ pomeni: Informacijskega pooblaščenca, določenega s tem zakonom ter zakonom, ki ureja informacijskega pooblaščenca;
24. zadevni nadzorni organ pomeni: nadzorni organ, ki ga obdelava osebnih podatkov zadeva, ker:
    a) ima upravljavec ali obdelovalec sedež na ozemlju države članice tega nadzornega organa;
    b) obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, s prebivališčem v državi članici tega nadzornega organa, ali
    c) je bila vložena pritožba pri tem nadzornem organu;
25. čezmejna obdelava osebnih podatkov pomeni bodisi:
    a) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti sedežev upravljavca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec sedež v več kot eni državi članici, bodisi
    b) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljavca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;
26. ustrezen in utemeljen ugovor pomeni: ugovor osnutku odločitve glede tega, ali je bila uredba kršena, oziroma glede tega, ali je predvideno ukrepanje v zvezi z upravljavcem ali obdelovalcem v skladu s to uredbo, kar jasno navede pomen tveganja, ki ga predstavlja osnutek odločitve, kar zadeva temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in – kjer je to ustrezno – prosti pretok osebnih podatkov v Uniji;
27. storitev informacijske družbe pomeni: storitev, kakor je opredeljena v točki (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta (Uradni list EU, L 241, 17. 9. 2015, str. 1);
28. mednarodna organizacija pomeni: organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo ali kateri koli drugo telo, ustanovljeno s sporazumom med dvema ali več državami ali na podlagi takega sporazuma ali za sodelovanje na področju mednarodnega javnega prava tudi organizacija in njena podrejena telesa, ki jih ureja mednarodno javno pravo, ali katera koli druga telesa, ustanovljene z mednarodno pogodbo med Republiko Slovenijo in drugo državo ali med Republiko Slovenijo in več državami ali na podlagi take mednarodne pogodbe.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen (prostori)

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

Dostop zaposlenim, strankam in obiskovalcem je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja.

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.

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

Ključi varovanih prostorov se uporabljajo in hranijo v skladu z navodilom direktorja.

Posebne vrste osebnih podatkov se ne smejo hraniti izven varovanih prostorov.

5. člen (varovanje prostorov)

V varovane prostore osebe, ki ne delajo v prostorih in ki niso zaposlene v podjetju, ne smejo vstopati brez spremstva ali prisotnosti zaposlenega. Zaposleni, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ga ob zapustitvi zakleniti.

Zaposleni, ki pri svojem delu uporabljajo osebne podatke, ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na vidnem mestu ali jih kako drugače izpostavljati nevarnostim vpogleda nepooblaščenim osebam vanje.

V prostorih, ki so namenjeni poslovanju s strankami oz. z osebami, ki niso zaposlene v podjetju, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

6. člen (ravnanje z osebnimi podatki)

Nosilcev osebnih podatkov zaposleni ne smejo odnašati iz podjetja brez izrecnega pisnega dovoljenja direktorja, in sicer le za potrebe podjetja.

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktor.

7. člen (vzdrževanje in popravilo)

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo direktorja, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki

imajo s podjetjem sklenjeno ustrezno pogodbo o servisiranju računalniške oziroma strojne opreme.

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

8. člen (dostop)

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

9. člen (spreminjanje programske opreme)

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

Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

10. člen (shranjevanje in varovanje)

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

11. člen (dolžnosti zaposlenega)

Zaposleni, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se pri servisiranju, popravilu, spreminjanju ali dopolnjevanju sistemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov po prenehanju potrebe po kopiji ta uniči.

Zaposleni, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti ves čas servisiranja računalnika in programske opreme prisoten in mora nadzirati, da ni nedopustnega ravnanja z osebnimi podatki.

Ob izkazani potrebi po popravilu računalnika, na katerega disku so osebni podatki, zunaj podjetja in brez nadzora pooblaščenega zaposlenega podjetja se morajo podatki z diska računalnika izbrisati tako, da je onemogočena restavracija. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih podjetja v prisotnosti pooblaščenega zaposlenega.

12. člen (virusi)

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

Ob pojavu računalniškega virusa se tega v čim krajšem času odpravi s pomočjo s pomočjo zunanjih strokovnjakov, 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 v podjetje na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

13. člen (prepovedi glede programske opreme)

Zaposleni ne smejo namestiti nobene programske opreme brez vednosti oseb, zadolženih za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov podjetja brez odobritve direktorja in vednosti oseb, zadolženih za delovanje računalniškega informacijskega sistema.

14. člen (gesla)

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 vnešeni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Direktor določi režim dodeljevanja hranjenja in spreminjanja gesel.

15. člen (hramba gesel)

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

Varovana gesla se smejo uporabiti v izjemnih in nujnih primerih. Vsaka taka uporaba se dokumentira. Po taki uporabi se določi nova gesla.

16. člen (kopije)

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.

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

IV. OBDELAVA OSEBNIH PODATKOV

17. člen (podlaga za obdelavo)

Osebni podatki v zasebnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana privolitev posameznika.

Ne glede na prejšnji odstavek se lahko obdelujejo osebni podatki posameznika, ki je sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

Ne glede na prvi odstavek tega člena se lahko v obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe.

Ne glede na prvi odstavek tega člena se lahko obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonitih upravičenih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

18. člen (drug namen)

Obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani, je dovoljena izjemoma, kadar je združljiva z nameni, za katere so bili osebni podatki prvotno zbrani ali kadar to določa zakon. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec, med drugim upoštevati:

- povezavo med nameni za katere so bili podatki zbrani in nameni nadaljnje uporabe,
- okoliščine, v katerih so bili osebni podatki zbrani,
- naravo osebnih podatkov, zlasti če gre za obdelavo posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški,
- morebitne posledice nadaljnje obdelave za Posameznika,
- obstoj ustreznih zaščitnih ukrepov, med katere sodijo šifriranje ali psevdonimizacija.

Presoja mora biti opravljena pred začetkom obdelave za druge namene v pisni obliki.

Obdelava osebnih podatkov v podjetju za drug namen kot za tistega, za katerega so bili zbrani ni dopustna na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več delovanj obdelave v skladu z določenim namenom.

Če je načrtovana obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga ne določa drugače.

19. člen (obdelava posebnih vrst osebnih podatkov)

Obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov,

biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo, je prepovedana.

Ne glede na določbo prejšnjega odstavka je obdelava posebnih vrst osebnih podatkov dovoljena če:

- če posameznik za to podal izrecno pisno privolitev,
- je nujno potrebna za varovanje življenja ali telesa posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svojo privolitev,
- je posameznik, na katerega se nanašajo osebni podatki posebne vrste, te javno objavil, brez očitnega ali izrecnega namena, da omeji namen njihove obdelave,
- tako določa drug zakon zaradi izvrševanja bistvenega javnega interesa, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki.
- je potrebna zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca na področju zaposlovanja ali je potrebna za izvajanje pravic, ki izhajajo iz zakonov s področja s socialno varstvene dejavnosti, ter za izpolnjevanje obveznosti v zvezi s tem, v skladu z zakonom, ki določa tudi ustrezna jamstva pravic posameznika,
- jih za namene zakonitih dejavnosti obdelujejo ustanove, društva, verske skupnosti, sindikati, politične stranke ali druge nepridobitne organizacije s političnim, filozofskim, verskim ali sindikalnim ciljem, vendar le, če se obdelava nanaša na njihove člane ali na posameznike, ki so v zvezi s temi cilji z njimi v rednem stiku, ter če se ti podatki ne posredujejo drugim posameznikom ali osebam javnega ali zasebnega sektorja brez pisne privolitve posameznika, na katerega se nanašajo,
- jih za namene zdravstvenega varstva prebivalstva in posameznikov ter vodenja ali opravljanja zdravstvenih služb obdelujejo zdravstveni delavci in zdravstveni sodelavci v skladu z zakonom,
- je potrebna iz razlogov javnega interesa na področju javnega zdravja, kot je zaščita pred velikimi nevarnostmi za zdravje ljudi s področja nalezljivih bolezni, zlasti epidemij, ki so lahko tudi čezmejne narave ali za zagotavljanje visokih standardov kakovosti in varnosti pri zdravstvenem varstvu ter zdravilih in medicinskih izdelkih in te podatke obdelujejo zdravstveno osebje ali druge osebe, ki je zavezano k ustreznemu varovanju tajnosti in se ti podatki obdelujejo v okviru njihovih nalog.

20. člen (ravnanje s posebnimi vrstami osebnih podatkov)

Obdelava in zavarovanje posebne vrste osebnih podatkov, mora biti izvajana posebno vestno in skrbno. Osebni podatki posebne vrste morajo biti pri obdelavi

posebej označeni in varovani tako, da se nepooblaščenim osebam prepreči dostop do njih.

21. člen (zbirke osebnih podatkov)

Opis zbirk osebnih podatkov, katerih upravljavec je podjetje, se vodi v evidenci dejavnosti obdelave.

Evidenca dejavnosti obdelave osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave osebnih podatkov, vpogled pa je potrebno omogočiti tudi Informacijskemu pooblaščencu kot nadzornemu organu, če to zahteva.

22. člen (evidenca dejavnosti obdelave)

Podjetje vodi evidenco dejavnosti obdelav, in skrbi za točnost in ažurnost te evidence.

Ta evidenca vsebuje:

- naziv ali ime in kontaktne podatke podjetja in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki;
- informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije in dokumentacijo o ustreznih zaščitnih ukrepih;
- predvidene roke za izbris različnih vrst podatkov;
- opis tehničnih in organizacijskih varnostnih ukrepov.

Evidenca dejavnosti obdelav se dopolnjuje v primeru sprememb poslovanja z osebnimi podatki.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

23. člen (pošta)

Zaposleni, ki so zadolženi za sprejem in evidenco pošte, odpirajo in pregledujejo vse poštne pošiljke in pošiljke, ki na drug način prispejo v podjetje, razen pošiljk iz drugega in tretjega odstavka tega člena.

Zaposleni, ki je zadolžen za sprejem pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot

osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo osebno na zaposlenega.

Zaposleni, ki je zadolžen za sprejem pošte, ne sme odpirati pošiljk, naslovljenih na zaposlenega, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime zaposlenega brez označbe njegovega uradnega položaja in šele nato naslov podjetja.

24. člen (prenos)

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. Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen 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.

25. člen (posebna vrsta osebnih podatkov)

Obdelava posebne vrste osebnih podatkov mora biti posebej označena in zavarovana.

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.

Osebni podatki posebne vrste se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

26. člen (zahteva za posredovanje podatkov)

Upravljavec osebnih podatkov mora brezplačno posredovati osebne podatke uporabnikom ali upravljavcem, ki izkažejo pravno podlago za pridobivanje zahtevanih osebnih podatkov.

Zahteva mora vsebovati:

- podatke o uporabniku (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščene osebe,
- pravno podlago,
- namen obdelave osebnih podatkov in razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve,
- predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni,
- vrste osebnih podatkov, ki naj se mu posredujejo,
- obliko in način pridobitve zahtevanih osebnih podatkov.

Podjetje mora podatke posredovati v 15 dneh od prejema zahteve ali pa posameznika v tem roku obvestiti o razlogih za zavrnitev.

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

27. člen (pravice posameznikov)

Posameznik na katerega se nanašajo osebni podatki, ima skladno z relevantnimi predpisi pravico od podjetja zahtevati informacije, kateri podatki se obdelujejo v zvezi z njim.

Posameznik na katerega se nanašajo osebni podatki, ima skladno z relevantnimi predpisi pravico od podjetja pridobiti potrdilo o tem, ali so v obdelavi njegovi osebni podatki.

Posameznik na katerega se nanašajo osebni podatki, ima skladno z relevantnimi predpisi pravico doseči, da podjetje brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim.

Posameznik na katerega se nanašajo osebni podatki, ima skladno z relevantnimi predpisi pravico doseči, da podjetje brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim.

Posameznik na katerega se nanašajo osebni podatki, ima skladno z relevantnimi predpisi pravico doseči, da podjetje omeji obdelavo osebnih podatkov, če so zato podani pogoji po členu 18 Splošne uredbe o varstvu osebnih podatkov.

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval podjetju, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu.

Posameznik, na katerega se nanašajo podatki, ima pravico, da kadarkoli ugovarja obdelavi osebnih podatkov v zvezi z njim, če so podani pogoji po 21. členu Splošne uredbe.

Posameznik, na katerega se nanašajo podatki, ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva, če so izpolnjeni pogoji po 22. členu Splošne uredbe.

28. člen (uveljavljanje pravic)

Posameznik uresničuje pravice iz prejšnjih odstavkov tega člena z vložitvijo zahteve pri podjetju. Posameznik navedene pravice uveljavlja brezplačno. Podjetje lahko zaradi potrditve identitete posameznika zahteva njegove podatke. Upravljavec mora o zahtevi posameznika odločiti brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju zapletenosti in števila zahtev. O podaljšanju je potrebno obvestiti posameznika.

Pri očitno neutemeljenih ali pretiranih zahtevah posameznika, na katerega se podatki nanašajo, zlasti če se zahteve pogosto ponavljajo, lahko podjetje s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka.

Če posameznik po prejeti odločitvi upravljavca meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe pri upravljavcu vloži obrazložen ugovor v roku 15 dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh.

Če upravljavec ne odloči o zahtevi posameznika v roku, lahko posameznik pri Informacijskem pooblaščencu vloži pritožbo zaradi molka.

29. člen (osebni podatki umrlih)

Podjetje podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščeni z zakonom in tistim, ki izkažejo pravni interes za uveljavljanje pravic pred osebami javnega sektorja.

Izjemoma se podatki o umrlem posamezniku lahko posredujejo tudi drugim osebam kot to določa zakon, ki ureja varstvo osebnih podatkov.

VI. HRAMBA OSEBNIH PODATKOV

30. člen (hramba)

Za hrambo so odgovorni zaposleni, ki so pooblaščeni za obdelovanje osebnih podatkov.

Zbirke osebnih podatkov zaposlenih v podjetju (kadrovske evidence) in druge zbirke osebnih podatkov, vodene v podjetju, se hranijo v zaklenjeni vodotesni in ognjevarni omari podjetja.

Roki hranjenja zbirk osebnih podatkov se določijo za vsako zbirko osebnih podatkov.

VII. BRISANJE PODATKOV IN UNIČENJE NOSILCEV

31. člen (brisanje)

Osebni podatki se lahko zbirajo in hranijo le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se vodijo in zbirajo. Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Osebni podatki se izbrišejo tudi če:

- posameznik privolitev prekliče,
- posameznik obdelavi ugovarja,
- so bili osebni podatki obdelani nezakonito,
- je potrebno osebne podatke izbrisati za izpolnitev EU-zakonodajne ali zakonske obveznosti,
- so bili osebni podatki zbrani v zvezi s ponudbo storitev informacijske družbe iz člena 8(1) Splošne uredbe.

32. člen (način brisanja)

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, to je s fizičnim uničenjem nosilcev.

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.

VIII. ODGOVORNOST UPRAVLJAVCA IN OBDELOVALCA

33. člen (odgovornost upravljavca)

Podjetje izvaja ustrezne tehnične in organizacijske ukrepe za zagotovitev skladnosti obdelave z določbami Splošne uredbe, zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov. Ukrepi morajo biti primerni glede na naravo, obseg, okoliščine in namene obdelave ter tveganja za poseg v človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi. Ukrepe je treba tudi pregledovati in dopolnjevati, kadar je to potrebno.

Upravljavec mora biti sposoben dokazati, da obdelava poteka v skladu z določbami Splošne uredbe, tega zakona oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov. To dokazuje še zlasti z vodenjem ustrezne dokumentacije glede izvajanja obveznosti po tem poglavju.

34. člen (odgovornost obdelovalca)

Podjetje lahko posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa obdelovalcu. Pogodba mora določati predmet, trajanje, vrsto in namen obdelave, vrsto osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki ter pravice in obveznosti podjetja. Pogodba mora biti skladna z zahtevami relevantnih predpisov. Pogodba mora biti sestavljena pisno ali v enakovredni elektronski obliki.

Podjetje sme sodelovati samo s tistimi obdelovalci, ki zagotovijo zadostna jamstva o tem, da bodo izvajali ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave z relevantnimi predpisi.

Obdelovalec brez predhodnega posebnega ali splošnega pisnega dovoljenja podjetja v obdelavo ne sme vključiti drugih obdelovalcev, pri čemer mora podjetje posebej presoditi ali vključitev dodatnega obdelovalca lahko vpliva na tveganost obdelave osebnih podatkov. Za drugega obdelovalca veljajo enake dolžnosti varstva osebnih podatkov kot za prvega obdelovalca. Če drugi obdelovalec ne izpolnjuje svojih obveznosti glede varstva osebnih podatkov, za izpolnjevanje obveznosti drugega obdelovalca v odnosu do podjetja odgovarja prvi obdelovalec.

V primeru spora ali prenehanja sodelovanja med podjetjem in pogodbenim obdelovalcem je dolžan pogodbeni obdelovalec osebne podatke, ki jih je pogodbeno

obdeloval, na podlagi zahteve podjetja, nemudoma vrniti podjetju, morebitne kopije teh podatkov pa takoj uničiti oziroma z njimi ravnati skladno z navodili upravljavca.

IX. UKREPANJE V PRIMERU KRŠITVE VARSTVA OSEBNIH PODATKOV

35. člen (obvestilo Informacijskemu pooblaščencu)

Zaposleni podjetja so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.

Podjetje oziroma obdelovalec morata v brez nepotrebnega odlašanja najpozneje pa v 72 urah, obvestiti Informacijskega pooblaščenca o vsaki kršitvi varstva osebnih podatkov, ki jo zaznata, če je verjetno, da bo povzročila tveganje za posege v človekove pravice in temeljne svoboščine posameznikov. Vsebino obvestila določa obrazec Uradno obvestilo o kršitvi.

Če je podjetje ali obdelovalcev podatke prejel ali posredoval upravljavcu ali obdelovalcu v tujino mora podjetje ali obdelovalec o kršitvi obvestiti tudi upravljavca ali obdelovalca v tujini.

Zapise in druge podatke na podlagi katerih bi se dalo ugotoviti dejstva v s kršitvijo mora podjetje ali obdelovalec zavarovati ter jih na poziv predložiti informacijskemu pooblaščencu, ki lahko naloži določene ukrepe.

36. člen (obvestilo posamezniku)

Kadar je verjetno, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, podjetje brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov. Vsebino obvestila določa obrazec Uradno obvestilo o kršitvi.

Posameznika pa ni potrebno obvestiti o kršitvi, če bi to zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

37. člen (odgovornost)

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren direktor.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor.

38. člen (dolžnost varovanja)

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega ali drugega pogodbenega razmerja.

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni 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 relevantnimi predpisi, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

Za že zaposlene pri podjetju se šteje, da so se seznanili z določbami tega pravilnika s podpisom izjave o varovanju zaupnih podatkov.

XI. ODGOVORNOST ZA KRŠITVE

39. člen (kršitev obveznosti)

Za kršitev določil iz tega pravilnika so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

XII. KONČNE DOLOČBE

40. člen

Ta pravilnik sprejema direktor podjetja in začne veljati naslednji dan po podpisu.

Pravilnik se hrani v tajništvu podjetja.

Kraj Ljubljana, datum 20.5.2018

Direktor:

Primorac Ivan

PRILOGA:
- Izjava o varovanju zaupnih podatkov