Na podlagi 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07) in ob upoštevanju vsebine Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov (v nadaljevanju Splošna uredba) je skupščina ZVEZE ANITE OGULIN IN ZPM, Proletarska 1, 1000 Ljubljana, dne 26. 11. 2024 sprejela naslednji

P R A VIL N I K
O ZAVAROVANJU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen
(Vsebina in namen pravilnika)

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v humanitarni organizaciji Zveza Anita Ogulin in ZPM (v nadaljevanju: ZAO), vodenih v zbirkah osebnih podatkov, s katerimi upravlja, z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba, nepooblaščen dostop, obdelava, uporaba ter posredovanje osebnih podatkov.

Zaposleni v ZAO in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s Splošno uredbo, s področno zakonodajo, ki ureja posamezno področje njihovega dela, ter z vsebino tega Pravilnika.

S tem Pravilnikom se določijo osebe, ki so odgovorne za posamezne zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo posamezne osebne podatke, s katerimi upravlja ZAO in jih obdeluje.

Ta Pravilnik določa ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov pri ZAO. Določbe tega Pravilnika veljajo za vse vodene zbirke podatkov pri ZAO, ne glede na obliko, v kateri je osebni podatek izražen.

Varstvo osebnih podatkov se zagotavlja vsaki posameznici ali posamezniku, ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, ali katerokoli drugo osebno okoliščino.

V zadevah, ki jih ne ureja ta Pravilnik, se neposredno uporabljajo določbe Zakona o varstvu osebnih podatkov in Splošna uredba.

2. člen
(Varovani osebni podatki)

Za varovane osebne podatke štejejo tisti podatki, ki predstavljajo katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, ne glede na obliko, v kateri so izraženi. 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 posameznika.

V smislu določbe 1. odstavka tega člena štejejo za osebne podatke o posamezniku zlasti:

- identifikacijski podatki o posamezniku,

- podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti,
- podatki, ki se nanašajo na družinska razmerja,
- podatki, ki se nanašajo na stanovanjske in bivalne pogoje posameznika,
- podatki o zaposlitvi,
- podatki o socialnem in ekonomskem stanju posameznika,
- podatki o izobrazbi in pridobljenih znanjih,
- slikovni (in glasovni) podatki nadzornih video sistemov,
- podatki o uporabi komunikacijskih sredstev,
- podatki o aktivnostih v prostem času,
- podatki o zdravstvenem stanju posameznika,
- podatki o ideoloških in verskih prepričanjih,
- podatki o posamezniku na področju notranjih zadev,
- podatki o navadah posameznika.

3. člen

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov, s katerimi se:

- varujejo prostori, strojna in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do računalniških sistemov, na katerih se
- obdelujejo osebni podatki in dostop do podatkovnih zbirk;
- omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki vneseni v podatkovne
- zbirke, oziroma računalniške sisteme, kdaj in kdo je dostopal do njih in to v obdobju, za katero se posamezni podatki shranjujejo.

4. člen

Obdelava in zavarovanje posebnih vrst osebnih podatkov, med katere sodijo podatki o rasnem ali etničnem poreklu, 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, morata biti izvajana posebno vestno in skrbno.

5. člen
(Pomen izrazov)

V tem Pravilniku uporabljeni izrazi imajo naslednji pomen:
Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
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;
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;
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, priklic, 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);
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; v konkretnem primeru ZAO;
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;
Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
Nosilec podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
Poslovna skrivnost - so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah.
ZVOP-1 - Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

II. OBDELAVA OSEBNIH PODATKOV

6. člen

(Vzpostavitev zbirke osebnih podatkov)

Vsi zaposleni in zunanji sodelavci pri upravljavcu, ki pri svojem delu uporabljajo osebne podatke, ki jih obdeluje upravljalec ali podatke, ki predstavljajo poslovno oziroma poklicno skrivnost ali imajo iz kakršnihkoli razlogov možnost dostopa do teh podatkov, morajo biti seznanjeni z zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki jim dovoljuje obdelavo osebnih podatkov, s tem Pravilnikom in s splošnimi akti, ki opredeljujejo poslovno oziroma poklicno skrivnost.

Posamezno zbirko osebnih podatkov na posameznem delovnem področju ZAO vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi sekretar.

7. člen

(Obdelava osebnih podatkov)
V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah ZVOP-1 in Splošne uredbe.

Obdelava osebnih podatkov je zakonita, če je izpolnjen vsaj eden od naslednjih pogojev:

a. posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
b. obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
c. obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
d. obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;

e. obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

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, če zakon ali Splošna uredba ne določata drugače.

Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani, tako da se nepooblaščenim osebam onemogoči dostop do njih.

Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (v nadaljevanju: pooblaščeni obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami zakona, Splošne uredbe ter z vsebino tega Pravilnika.

8. člen

(Katalog zbirk osebnih podatkov)

Opis zbirk osebnih podatkov, katerih upravljavec je ZAO, se vodi v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami 26. člena zakona. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni s katalogom zbirk osebnih podatkov. Vpogled v katalog zbirk osebnih podatkov je potrebno omogočiti tudi vsakomur, ki to zahteva.

ZAO je dolžan voditi ažuren seznam, evidenco, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

V seznam se vpisujejo naslednji podatki: naziv zbirke osebnih podatkov, osebno ime in delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

9. člen

(Sprejem osebnih podatkov, pregledovanje pošte)

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na ZAO, ki jih prinesejo uporabniki ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drugega naslovnika in so pomotoma dostavljene ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na poseben namen.

Delavec, 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 ZAO.

10. člen
(Posredovanje osebnih podatkov)

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

Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.

Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Upravljalec mora uporabniku ali upravljavcu, če zakon ne določa drugače, zahtevane osebne podatke posredovati najpozneje v 15 dneh od dne prejema popolne zahteve, ali pa ga v tem roku pisno obvestiti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

Posredovanje občutljivih osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz 3. Odstavka tega člena.
Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice. Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Občutljive osebne podatke je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

11. člen
(Evidenca posredovanj)

Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje z uradnim zaznamkom, ki vsebuje navedbo naslednjih podatkov:
- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum in ura posredovanja osebnih podatkov ter

- pravna podlaga, na kateri so bili posredovani osebni podatki.

Oblika uradnega zaznamka je odvisna od nosilca podatkov, ki vsebuje posredovani osebni podatek in se evidentira neposredno v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek.

Uradni zaznamek iz prvega odstavka tega člena zapiše odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

12. člen
(Posredovanje osebnih podatkov znotraj ZAO)

Dokumenti, ki vsebujejo osebne podatke zaposlenega, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu s tretjim odstavkom 10. člena tega Pravilnika.

Osebni podatki zaposlenih in ostalih oseb se lahko posredujejo znotraj ZAO tudi tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

Oseba iz tretjega odstavka prejšnjega člena mora zaznamovati vsako posredovanje občutljivih osebnih podatkov znotraj ZAO, v skladu s prejšnjim členom.

13. člen
(Pregledovanje, prepisovanje in kopiranjeosebnih podatkov s strani upravičencev)

Pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, je potrebno preveriti identiteto upravičenca oziroma vsakega drugega, ki verjetno izkaže, da ima od pregledovanja, prepisovanja in preslikovanja pravno korist (v nadaljevanju: upravičenec) z vpogledom v njegovo osebno izkaznico ali drug dokument, ki nedvoumno izkazuje njegovo istovetnost.

Pri vsakem posameznem pregledovanju, prepisovanju in kopiranju dokumentov po tem členu, ki vsebujejo osebne podatke, se zapiše uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi upravičenec, mora biti razviden datum in ura pregleda, vrsta dokumenta, katerega kopija se je posredovala upravičencu, osebno ime upravičenca, njegov naslov, številka in vrsta dokumenta, iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bil opravljen pregled, prepis oziroma kopiranje dokumenta.

Upravičenca je pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, potrebno opozoriti na dolžnost varovanja takšnih podatkov. Opozorilo mora biti sestavni del uradnega zaznamka iz prejšnjega odstavka.

Kopiranje vsebin zbirk osebnih podatkov se vpiše tudi v Evidenco izdelave kopij.

14. člen
(Kopiranje in tiskanje osebnih podatkov s strani zaposlenih)

Zaposleni v ZAO, ki pri izvajanju svojih delovnih nalog kopirajo, na drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo osebne podatke, na napravah, ki jih uporablja večje število zaposlenih, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

15. člen
(Hramba osebnih podatkov)

Osebni podatek lahko upravljalec vodi v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se podatki obdelujejo. Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe razviden kataloga zbirke osebnih podatkov.

Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov. Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).

Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

Pri prenosu nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja, je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov. O uničenju se sestavi ustrezen zapis.

III. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

16. člen

Upravljalec mora posamezniku na njegovo zahtevo:

- omogočiti vpogled v katalog zbirke osebnih podatkov;
- potrditi, ali se podatki v zvezi z njim obdelujejo ali ne in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje (pravica do dostopa);
- dopolniti, popraviti, izbrisati ali omejiti uporabo osebnih podatkov, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom ali Splošno uredbo (pravica do popravka, do izbrisa, do omejitve obdelave),
- posredovati osebne podatke, ki jih je posameznik posedoval upravljalcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in ima posameznik pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljalec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral (pravica do prenosljivosti podatkov).

Upravljalec na zahtevo posameznika do seznanitve z osebnimi podatki zagotovi kopijo osebnih podatkov, ki se obdelujejo. Kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, in če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače, upravljalec informacije zagotovi v elektronski obliki, ki je splošno uporabljana in je skladna s pravili posredovanja osebnih podatkov s tem Pravilnikom.

17. člen

Upravljalec osebnih podatkov mora posamezniku na njegovo zahtevo tudi:

- posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj;
- posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen;

- dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave;
- dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
- pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.
-

IV. PODROČNE UREDITVE VARSTVA OSEBNIH PODATKOV

18. člen
(Dostop do programske opreme)

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.

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 upravljalcem sklenjeno ustrezno pogodbo. Upravljalec mora spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

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

Spremembe in dopolnitev sistemske in aplikativne programske opreme se vpisujejo v Evidenco.

19. člen

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 čim prej odpravi s pomočjo ustrezne strokovne službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu ZAO.

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

20. člen

Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov ZAO brez odobritve predpostavljenega in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

21. 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.

Pooblaščena oseba določi režim dodeljevanja hranjenja in spreminjanja gesel.

22. člen
(Gesla in njihova uporaba)

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 oziroma ob nujnih primerih.

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

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.

23. člen
(Elektronska pošta in uporaba druge programske opreme na računalniku)

Elektronska pošta in računalnik se uporabljata v službene namene.

24. člen
(Internet)

Internet se uporablja v službene namene.

V. VAROVANJE PROSTOROV, NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME

25. člen
(Varovanje prostorov)

Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, tajne podatke in druge varovane podatke, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven njega pa samo na podlagi dovoljenja sekretarja.

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.

26. člen
(Varovanje nosilcev)

Nosilci podatkov, ki vsebujejo občutljive osebne podatke ali druge osebne podatke, se ne smejo hraniti izven varovanih prostorov, zaposleni pa jih lahko odnašajo izven prostorov ZAO samo z dovoljenjem sekretarja in če je to nujno potrebno za reševanje zadeve, ki vsebuje te občutljive osebne podatke.

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.

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

27. člen
(Vzdrževanje in popravila)

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z ZAO sklenjeno ustrezno pogodbo. Upravljalec mora spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

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

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

29. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se tedensko preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo na ZAO na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov.

30. člen
(Prepovedi)

Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov ZAO brez odobritve in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

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

Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

VI. BRISANJE PODATKOV

31. člen

Po prenehanju potrebe po vodenju in zakonske podlage za obdelavo osebnih podatkov, se podatki zbrišejo oziroma nosilci podatkov uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Roki, po katerih se osebni podatkov izbrišejo iz zbirke podatkov, so razvidni iz kataloga zbirke osebnih podatkov.

32. 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.

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

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

33. člen

Upravljalec mora zagotoviti ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti odgovorno osebo, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.
Ob navedenih ukrepih mora upravljalec ozaveščati osebe, udeležene v postopkih obdelave podatkov o varnostnih politikah ter postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov (kot npr.: odjavljanje iz sistema po zaključku dela, uporaba programskega zaklepanja računalnika ob odsotnosti od računalnika, zaklepanje prostorov ali stalni nadzor, načelo čiste in urejene delovne mize in delovnega prostora, pomen zagotavljanja sledljivosti obdelave, vsak uporabnik uporablja svoje uporabniško ime in geslo, fizično varovanje gesel, previdnost pri izbiri gesel, občasno spreminjanje gesel, varno pošiljanje podatkov po elektronskih medijih, pazljivost in skrbnost pri posredovanju podatkov po telefonu, takojšnje obveščanje o incidentu, posvetovanje s pooblaščeno osebo za varstvo osebnih podatkov, upoštevanje notranjih pravil in aktov,…).

VIII. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV

34. člen
(Izvajanje postopkov in ukrepov)

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

35. člen
(Odgovornost za izvajanje in nadzor nad izvajanjem)

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s tem Pravilnikom, so odgovorne pooblaščene osebe, ki jih imenuje sekretar.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem Pravilnikom, opravlja sekretar, skupaj z osebo, zadolženo za delovanje računalniškega informacijskega sistema.

36. člen
(Izjava)

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in drugih zaupnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami zakona, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega Pravilnika in zakona.

37. člen
(Odgovornost za kršitev)

Zaposleni, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti zakonitega zastopnika upravljalca.

Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu, na podlagi katerega se zbirajo ali nameni, določenimi v katalogu zbirk osebnih podatkov. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

Kršitev določil tega Pravilnika s strani zaposlenih pomeni hujše kršenje obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

38. člen

V primeru, da upravljalec ugotovi, da je v procesu obdelave osebnih podatkov prišlo do slučajnega, namernega ali drugačnega nezakonitega uničenja, spremembe, izgube, nepooblaščenega razkritja, dostopa ali druge oblike nepooblaščene obdelave, je dolžan brez nepotrebnega odlašanja, oziroma najpozneje v 72 urah po seznanitvi s kršitvijo, o kršitvi uradno obvesti pristojni nadzorni organ (Informacijskega pooblaščenca).

Ta obveznost upravljalca ni podana, če ni izkazana verjetnost, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, na katere se kršitev nanaša.

Uradno obvestilo iz 1. odstavka tega člena Pravilnika nadzornemu organu mora vsebovati vsaj naslednje podatke:

- opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih upravljalec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učiinkov kršitve.

IX. POOBLAŠČENA OSEBA ZA VARSTVO OSEBNIH PODATKOV

39. člen

Upravljalec določi in imenuje pooblaščeno osebo za varstvo osebnih podatkov, ki upravljavcu pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami zakona, ki ureja varstvo osebnih podatkov.

Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:

- obveščanje upravljalca in pri njem zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno Uredbo in drugimi določbami prava Unije ali nacionalne zakonodaje iz področja varstvu osebnih podatkov;
- spremljanje skladnosti s Splošno Uredbo, drugimi določbami prava Unije ali nacionalne zakonodaje iz področja varstva osebnih podatkov in politikami upravljalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- svetovanje pri izvajanju ocene učinka tveganja;
- sodelovanje z nadzornim organom (Informacijskim pooblaščencem) in drugo.

Pooblaščena oseba je lahko zaposlena oseba pri upravljavcu ali druga oseba, ki sklene z upravljavcem ustrezno pogodbo. Imeti pa ima poklicne odlike, tovrstna znanje, izkušnje.

X. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

40. člen
(Pogodbena obdelava)

Upravljalec lahko zaupa posamezna opravila v zvezi z obdelavo osebnih podatkov zunanji pravni ali fizični osebi (pogodbeni obdelovalec), pri tem pa si mora upravljalec prizadevati, da pogodbeni obdelovalec zagotavlja zadostna jamstva o tem, da bo izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave s Splošno uredbo, zakonom, ki ureja področje varstva osebnih podatkov in tem Pravilnikom.

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov (v nadaljevanju: pogodbeni obdelovalec), se sklene pisna pogodba. Pogodba mora obvezno vsebovati tudi pogoje in ukrepe za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

Navedeno velja tudi za pogodbene obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in inštalirajo novo strojno ali programsko opremo.

Pogodbeni obdelovalci (zunanje pravne oz. fizične osebe) lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pogodbeni obdelovalci, ki za ZAO opravljajo pogodbeno dogovorjene storitve izven prostorov ZAO, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta Pravilnik.

ZAO vodi seznam zunanjih izvajalcev, ki vsebuje: naziv in sedež pravne osebe, ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka).

XI . POSEBNE UREDITVE ZA ZBIRKE OSEBNIH PODATKOV, VODENIH PRI UPRAVLJALCU

41. člen

(Videonadzor)
V primeru izvajanega videonadzora mora upravljavec osebnih podatkov o izvajanju videonadzora objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:
- da se izvaja videonadzor;
- naziv upravljavca osebnih podatkov ter
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

42. člen

Videonadzor dostopa v poslovne prostore se lahko izvaja, če je to potrebno za varnost ljudi in premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja delavcev.

O izvajanju videonadzora je potrebno pisno obvestiti vse zaposlene, ki opravljajo delo v nadzorovanem prostoru.

Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

43. člen

Videonadzor znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi in premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.
Videonadzor se lahko izvaja le glede tistih delovnih prostorov, kjer je potrebno varovati interese iz prejšnjega odstavka.

Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

Zaposleni morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

XII. DRUGE DOLOČBE

44. člen
(Začetek veljavnosti)

Tapravilnik prične veljati naslednji dan po sprejetju.

VLjubljani, 26.11. 2024

Zveza Anita Ogulin in ZPM

Predsednica Alenka Petkovšek

Zveza Anita Ogulin