



Na podlagi določb 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) in na podlagi veljavne zakonodaje, ki ureja varstvo osebnih podatkov izdaja direktorica Centra za pomoč na domu Maribor (v nadaljevanju: organizacija oz. upravljavec) naslednji

PRAVILNIK **o varstvu osebnih podatkov**

I. SPLOŠNE DOLOČBE

1. člen

(namen in vsebina pravilnika)

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

Odgovorna oseba, vodstvo, zaposleni, delavci oziroma vse osebe, ki so vključene v delovni proces organizacije na podlagi pogodbe o zaposlitvi ali drugega pogodbenega razmerja, ki pri delu neposredno ali posredno obdelujejo in uporabljajo osebne, zaupne podatke in/ali se seznanjajo s poslovno skrivnostjo organizacije, morajo spoštovati določila Splošne uredbe o varstvu osebnih podatkov, določila veljavne zakonodaje, ki ureja področje varstva osebnih podatkov ter določila drugih predpisov, zavezujočih aktov in pogodb, ki urejajo posamezno področje dela ter z vsebino tega Pravilnika.

Organizacija obdelavo varuje s tehničnimi in organizacijskimi varnostnimi ukrepi, ki temeljijo na oceni tveganj za pravice in svoboščine posameznika, ki jih pomeni obdelava podatkov, ki se nanašajo nanj, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Organizacija s tem pravilnikom ter s politikami, načrti in navodili, ki sestavljajo Sistem upravljanja varstva osebnih podatkov oziroma Sistem za upravljanje in varovanje informacij, določa nosilce, organizacijo in postopke za izvajanje ukrepov iz prejšnjih treh odstavkov tega člena.

Po tem pravilniku se varujejo tudi osebni podatki, ki jih na podlagi pogodbe za organizacijo obdeluje zunanji izvajalec (v nadaljnjem besedilu: obdelovalec) oziroma skupni upravljavec.

2. člen

(pomen izrazov)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

- Analiza varnostnih tveganj je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost osebnih podatkov oz. obdelavo;
- Analiza vpliva na poslovanje je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za neprekinjeno izvajanje obdelave;





- Biometrični podatki pomenijo 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;
- Dokumentiran postopek pomeni, da je postopek zapisan;
- Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, priimek, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- Genetski podatki pomenijo osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;
- Grožnja je možen vzrok za incident, ki lahko povzroči škodo osebnemu podatku, sredstvu za obdelavo ali upravljavcu;
- Incident je eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo ogrozili varnost obdelave osebnih podatkov ali sredstev, s katerimi se obdelava izvaja;
- Informacijski sistem je programska, strojna, komunikacijska in druga oprema organizacije, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi osebnih podatkov;
- Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
- Nosilec podatkov pomeni 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, mikrofili, naprave za prenos podatkov, ipd.);
- 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;
- Obdelovalec pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- Obravnava tveganj je proces izbora in vpeljave ukrepov za zmanjšanje tveganj;
- Odgovorna oseba pomeni fizično osebo, ki je veljavni zakoniti zastopnik oz. direktor organizacije;
- Odgovorna oseba zbirke je zaposleni ali zunanji sodelavec organizacije, odgovoren za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
- Osebni podatek pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki.
- Podatki o organizaciji pomenijo osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
- Posameznik je določena ali določljiva oseba, na katero se nanaša osebni podatek;
- Posebne vrste osebnih podatkov so osebni podatki, ki razkrivajo rasno ali etično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genski podatki, biometrični podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;



- 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 katerimi izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;
- Pseudonimizacija 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;
- Ranljivost je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami;
- Sistemski administrator je oseba, ki skrbi za delovanje sistemske opreme;
- Škodljiva programska oprema so računalniški virusi, črvi, trojanski konji in podobna programska oprema, ki se nepooblaščno namesti v informacijski sistem ali njegov del brez vednosti odgovornih oseb organizacije in posega v integriteto informacijskega sistema;
- Skrbnik informacijskega sistema je oseba, ki skrbi za vsebinsko delovanje informacijskega sistema;
- 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 pooblaščenice za obdelavo osebnih podatkov pod neposrednim vodstvom upravitelja ali obdelovalca;
- 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 proizvodnje 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;
- 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;
- Upravljavec zbirke je zaposleni ali zunanji sodelavec organizacije, zadolžen za obdelavo podatkov iz posamezne zbirke osebnih podatkov;
- Varnostni dogodek je zaznana okoliščina v obdelavi osebnih podatkov, ki kaže na morebitno kršitev varstva osebnih podatkov oziroma odstop od postopkov in ukrepov za zavarovanje osebnih podatkov ali na do tedaj še neznan okoliščino, ki bi lahko bila pomembna za varnost;
- Vodstveni pregled je dokumentiran pregled sistema upravljanja varstva osebnih podatkov, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi skladnost obdelave;
- 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.

II. VARSTVO OSEBNIH PODATKOV

3. člen

(odgovornost vodstva)

Za zagotovitev ustreznih in učinkovitih ukrepov za izvajanje obdelave podatkov v skladu s Splošno uredbo in zakonodajo, ki ureja varstvo osebnih podatkov ter za dokazovanje skladnosti obdelave podatkov, je odgovorno vodstvo organizacije.



Vodstvo odgovornosti iz prvega odstavka tega člena uresničuje zlasti:

- s sprejetjem tega pravilnika ter navodil, politik, načrtov in drugih notranjih aktov, s katerimi se določajo:
 - o postopki za vzpostavitev zakonitih podlag za obdelavo osebnih podatkov, predvsem z vzpostavitvijo evidenc dejavnosti obdelave;
 - o postopki za obravnavanje zahtevkov oziroma ugovorov posameznikov, katerih podatke organizacija obdeluje, vezanih na varstvo njihovih pravic in svoboščin v zvezi z obdelavo osebnih podatkov;
 - o izdelave ocen varnostnih tveganj obdelave;
 - o izdelave ocen učinka v zvezi z varstvom podatkov;
 - o izvajanja ustreznih tehničnih in organizacijskih ukrepov, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščen razkritje, dostop ali drugo nepooblaščen obdelavo;
- z imenovanjem pooblaščenih oseb za varstvo osebnih podatkov;
- z ustreznim vodenjem seznama in ureditvijo pogodbeno obdelave s strani pogodbenih obdelovalcev;
- z imenovanjem delovne oziroma projekte skupine za usklajitev poslovanja organizacije z zakonodajo s področja varstva osebnih podatkov
- z letnim pregledom s strani pooblaščenih oseb za varstvo podatkov, ki vključuje notranjo presojo ter pregled ustreznosti in učinkovitosti ukrepov za zagotavljanje varnosti obdelave ter
- z rednimi izobraževanji zaposlenih na področjih varne obdelave osebnih podatkov.

Vodstvo organizacije mora zagotoviti, da je omogočeno učinkovito izvajanje, spremljanje in nadziranje ukrepov in postopkov za varnost osebnih podatkov, ter njihovo dokazovanje skladnosti obdelave v sodnih, nadzornih in drugih uradnih postopkih.

4. člen

(izjava o varovanju osebnih podatkov)

Pred nastopom dela v organizaciji mora zaposleni podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika, Splošne uredbe in zakonodaja. Izjava mora vsebovati tudi pouk o posledicah kršitve določb.

Izjavo iz prvega odstavka tega člena podpišejo tudi zunanji sodelavci organizacije, ki se v okviru izvajanja pogodbenih del seznani ali bi se lahko seznanili z osebnimi podatki, s katerimi upravlja organizacija.

Izjavo iz prvega odstavka tega člena podpišejo vsi študentje, dijaki, prostovoljci, zunanji pripravniki in specializanti, ki se lahko seznani z osebnimi podatki v okviru sodelovanja z organizacijo.

5. člen

(odgovornost za kršitev)

Kršitev določil pravilnika predstavlja hujšo kršitev delovnih obveznosti po pogodbi o zaposlitvi oziroma bistveno kršitev druge pogodbe, zaradi katere lahko organizacija odpove pogodbo o zaposlitvi oziroma drugo pogodbo, ki je podlaga za opravljanje dela pri ali za organizacijo.



V primeru kršitev določi tega pravilnika, je zaposleni odškodninsko odgovoren organizaciji za škodo, ki bi nastala organizaciji oziroma fizičnim ali pravnim osebam, s katerimi organizacija sodeluje.

Kršitev določi pravilnika ima lahko za posledico kazensko, prekrškovno in/ali odškodninsko odgovornost zaposlenega oziroma osebe, ki krši ta pravilnik.

6. člen **(izvajanje postopkov in ukrepov)**

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi zaposleni v organizaciji, kot tudi zunanji izvajalci, ki imajo s podjetjem podpisan dogovor o sodelovanju.

Vsak zaposleni, 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 razmerja.

7. člen **(nadzor nad izvajanjem postopkov in ukrepov)**

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom opravlja odgovorna oseba organizacije v sodelovanju z delavci zadolženih za informacijsko varnost in pooblaščen osebno za varstvo podatkov.

8. člen **(dokazovanje skladnosti)**

Organizacija za potrebe dokazovanja skladnosti obdelave s predpisanimi zahtevami in tem pravilnikom vodi ustrezno dokumentacijo, s katero je sposobna dokazati, da obdelava poteka v skladu z določbami Splošne uredbe in druge zakonodaje, ki urejajo varstvo osebnih podatkov. V organizaciji se ta dokumentacija vodi v okviru dokumentacije pooblaščen osebno za varstvo podatkov, za katero skrbi s strani odgovorne osebe imenovana služba (npr. pravna služba, kadrovska služba, služba za kakovost oziroma služba za informatiko).

III. POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

9. člen **(imenovanje pooblaščen osebno za varstvo osebnih podatkov)**

Odgovorna oseba organizacije imenuje pooblaščen osebno za varstvo podatkov s sklepom ali na drug primeren način (npr. s sklenitvijo pogodbe) in poskrbi za objavo informacij o pooblaščen osebno na spletni strani organizacije.

Pooblaščen osebno za varstvo podatkov se imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva osebnih podatkov ter zmožnosti za izpolnjevanje nalog iz člena 39 Splošne uredbe oziroma na podlagi veljavne zakonodaje s področja varstva osebnih podatkov.

Organizacija kot pooblaščen osebno za varstvo podatkov imenuje zunanje podjetje DATAINFO.SI, d.o.o., Tržaška cesta 85, 2000 Maribor, dpo@datainfo.si, ki opravlja naloge v skladu z zakonodajo s področja varstva osebnih podatkov in na osnovi sklenjene pogodbe z organizacijo.



O imenovanju ali spremembi funkcije opravljanja pooblaščenice osebe za varstvo osebnih podatkov se obvezno seznani Informacijskega pooblaščenca preko za to predvidenega obrazca.

10. člen **(položaj pooblaščenice osebe za varstvo podatkov)**

Pooblaščenica oseba vodstvu organizacije strokovno in neodvisno pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov z določbami Splošne uredbe in veljavne zakonodaje s področja varstva osebnih podatkov.

Organizacija zagotovi, da je pooblaščenica oseba za varstvo podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov.

Posamezniki, na katere se nanašajo osebni podatki, lahko s pooblaščenico osebo za varstvo podatkov stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic na podlagi te uredbe.

Pooblaščenica oseba za varstvo podatkov je pri opravljanju svojih nalog zavezana varovati skrivnost ali zaupnost v skladu s pravom Unije in veljavno zakonodajo o varstvu osebnih podatkov.

11. člen **(naloge pooblaščenice osebe)**

Pooblaščenica oseba za varstvo podatkov ima naslednje naloge:

- obveščanje organizacije, njegovih pogodbenih obdelovalcev in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno uredbo in veljavno zakonodajo o varstvu osebnih podatkov;
- spremljanje skladnosti s Splošno uredbo in drugo relevantno zakonodajo in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s členom 35 Splošne uredbe;
- aktivno sodeluje pri pripravi ocen učinkov;
- sodelovanje z nadzornim organom;
- sprejem prijav domnevnih kršitev in njihova obravnava;
- sodeluje pri poročanju o kršitvah varstva osebnih podatkov nadzornemu organu;
- predlaga interna navodila za ravnanje in obvešča zaposlene;
- pripravlja mnenja s področja varstva osebnih podatkov;
- deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz člena 36 Splošne uredbe in kjer je ustrezno, izvaja posvetovanje glede katere koli druge zadeve;
- sodeluje s posamezniki, na katere se nanašajo osebni podatki, ki se na organizacijo obračajo glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic.

Pooblaščenica oseba za varstvo podatkov pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave.



IV. OBDELAVA OSEBNIH PODATKOV

12. člen

(pravne podlage obdelave osebnih podatkov)

V organizaciji se lahko na osnovi člena 6 Splošne uredbe obdeluje osebne podatke, v kolikor je izpolnjen vsaj eden od naslednjih pogojev:

- posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- obdelava je potrebna za izvajanje pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
- obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
- obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
- 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 obdelovati 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 ne določa drugače.

13. člen

(namen obdelave osebnih podatkov)

Osebni podatki se smejo obdelovati samo za namene, določene v zakonski podlagi, ali določene v informacijah posredovanih posamezniku, na katerega se nanašajo obdelovani podatki, v okviru pridobivanja privolitve za obdelavo ali sklenitev pogodbe, na podlagi katere se izvaja obdelava.

Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili podatki 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. V primeru, da se načrtuje obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če zakon ne določa drugače.

14. člen

(pogoji za privolitve)

Kadar obdelava temelji na privolitvi, mora biti upravljavec zmožen dokazati, da je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov.

Če je privolitev posameznika, na katerega se nanašajo osebni podatki, dana v pisni izjavi, ki se nanaša tudi na druge zadeve, se zahteva za privolitev predloži na način, ki se jasno razlikuje od drugih zadev, v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Deli take izjave, ki predstavljajo kršitev te uredbe, niso zavezujoči.



Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da svojo privolitve kadar koli prekliče. Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem. O tem se pred privolitvijo obvesti posameznika, na katerega se nanašajo osebni podatki. Privolitev je enako enostavno preklicati kot dati.

Pri ugotavljanju, ali je bila privolitev dana prostovoljno, se med drugim zlasti upošteva, ali je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe.

15. člen **(obdelava posebnih vrst osebnih podatkov)**

Posebne vrste osebnih podatkov se lahko obdelujejo le, če tako določa zakon, ali če je posameznik za to podal izrecno pisno privolitev.

Posebne vrste osebnih podatkov se smejo iz evidenc posredovati osebam iz javnega ali zasebnega sektorja ter tretjim le, če to določa zakon, ali na podlagi pisne zahteve ali pisne privolitve posameznika, na katerega se nanašajo. Privolitev mora biti izrecna in praviloma pisna.

Pri obdelavi posebnih vrst osebnih podatkov morajo biti zaposleni še posebej vestni in skrbni. Posebne vrste osebnih podatkov morajo biti varovane tako, da se nepooblaščenim osebam prepreči dostop do njih.

V. OBVEŠČANJE IN VARSTVO PRAVIC POSAMEZNIKA GLEDE OBDELAVE PODATKOV

16. člen **(obveščanje o obdelavi osebnih podatkov)**

Organizacija posameznika, čigar osebne podatke bo zbiral, obvesti o obstoju izvajanja obdelave in namenih obdelave. Besedila informacij morajo obsegati najmanj naslednje informacije:

- imena in kontaktne podatke upravljavca;
- kontaktne podatke pooblaščenih oseb;
- namene, za katere se osebni podatki obdelujejo;
- obstoju pravice do vložitve prijave pri Informacijskem pooblaščenju in njegove kontaktne podatke;
- obstoju pravice do dostopa do podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo;

Dodatno mora upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih zagotoviti dodatne informacije, da s tem omogoči izvajanje pravic posameznika, na katerega se nanašajo podatki:

- pravno podlago obdelave;
- rok hrambe osebnih podatkov;
- kategorije prejemnikov osebnih podatkov;
- druge informacije, zlasti, če so bili osebni podatki pridobljeni brez vednosti posameznika na katerega se nanašajo.

Predlog besedil informacij iz prejšnjega odstavka pripravi pooblaščen osebja za varstvo osebnih podatkov v sodelovanju z organizacijo.



17. člen

(pravice posameznika, na katerega se nanašajo osebni podatki)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od organizacije dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, mu organizacija nudi dostop do osebnih podatkov in informacije iz 1. odstavka 15. člena Splošne uredbe ter zagotavlja naslednje pravice, v kolikor je to v skladu s Splošno uredbo:

- pravica do popravka;
- pravica do izbrisa („pravica do pozabe“);
- pravica do omejitve obdelave;
- obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave;
- pravica do prenosljivosti podatkov;
- pravica do ugovora in avtomatizirano sprejemanje posameznih odločitev.

Posamezniku, na katerega se nanašajo osebni podatki, se zagotovi vse informacije iz členov 13 in 14 ter sporočila iz členov 15 do 22 in 34 Splošne uredbe, povezana z obdelavo, v jedrnatih, preglednih, razumljivih in lahko dostopnih oblikah ter jasnem in preprostem jeziku, kar velja zlasti za vse informacije, namenjene posebej otroku. Informacije se posredujejo v pisni obliki ali z drugimi sredstvi, vključno, kjer je ustrezno, z elektronskimi sredstvi. Na zahtevo posameznika, na katerega se nanašajo osebni podatki, se lahko informacije predložijo ustno, pod pogojem, da se identiteta posameznika, na katerega se nanašajo osebni podatki, dokaže z drugimi sredstvi.

Za posameznikove zahteve je zadolžen upravljavec/odgovorna oseba posamezne zbirke podatkov, na katere se nanaša zahtevka ali pooblaščen oseba za varstvo osebnih podatkov.

Upravljavec/odgovorna oseba posamezne zbirke podatkov je dolžan prizadetega posameznika obvestiti v najkrajšem možnem času, brez nepotrebnega odlašanja.

18. člen

(pravica dostopa posameznika, na katerega se nanašajo osebni podatki)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije:

- namene obdelave;
- vrste zadevnih osebnih podatkov;
- uporabnike ali kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
- kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahteva popravek ali izbris osebnih podatkov ali omejitev obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora taki obdelavi;
- pravico do vložitve pritožbe pri nadzornem organu;
- kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom.



Kadar se osebni podatki prenesejo v tretjo državo ali mednarodno organizacijo, ima posameznik, na katerega se nanašajo osebni podatki, pravico biti obveščen o ustreznih zaščitnih ukrepih.

Upravljavec zagotovi kopijo osebnih podatkov, ki se obdelujejo. Za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov. 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, se informacije zagotovijo v elektronski obliki, ki je splošno uporabljana.

19. člen **(pravica do popravka)**

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim. Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave, pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave.

20. člen **(pravica do izbrisa („pravica do pozabe“))**

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati, kadar velja eden od naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava in kadar za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito.

Prvi odstavek tega člena se ne uporablja, če je obdelava potrebna:

- za uresničevanje pravice do svobode izražanja in obveščanja;
- za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali prava države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu;
- za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene;
- za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

21. člen **(pravica do omejitve obdelave)**

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec omeji obdelavo, kadar velja en od naslednjih primerov:

- posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki upravljavcu omogoča preveriti točnost osebnih podatkov;



- je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je bila obdelava osebnih podatkov omejena v skladu z odstavkom 1, se taki osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se ti nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa Unije ali države članice.

Upravljavec, ki je dosegel omejitev obdelave v skladu z odstavkom 1, pred preklicem omejitve obdelave o tem obvesti posameznika, na katerega se nanašajo osebni podatki.

22. člen

(obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave)

Upravljavec vsakemu uporabniku, ki so mu bili osebni podatki razkriti, sporoči vse popravke ali izbrise osebnih podatkov ali omejitve obdelave, razen če se to izkaže za nemogoče ali vključuje nesorazmeren napor. Upravljavec o teh uporabnikih obvesti posameznika, na katerega se nanašajo osebni podatki, če ta posameznik tako zahteva.

23. člen

(pravica do prenosljivosti podatkov)

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral, kadar:

- obdelava temelji na privolitvi
- se obdelava izvaja z avtomatiziranimi sredstvi.

Pri uresničevanju pravice do prenosljivosti podatkov v skladu z odstavkom 1 ima posameznik, na katerega se nanašajo osebni podatki, pravico, da se osebni podatki neposredno prenesejo od enega upravljavca k drugemu, kadar je to tehnično izvedljivo.

Ta pravica se ne uporablja za obdelavo, potrebno za opravljanje naloge, ki se izvaja v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu.

24. člen

(pravica do ugovora)

Posameznik, na katerega se nanašajo osebni podatki, ima na podlagi razlogov, povezanih z njegovim posebnim položajem, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim. Upravljavec preneha obdelovati osebne podatke, razen če dokaže nujne legitimne razloge za



obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Posameznika, na katerega se nanašajo osebni podatki, se na pravico izrecno opozori najpozneje ob prvem komuniciranju z njim in se mu to pravico predstavi jasno in ločeno od vseh drugih informacij.

Kadar se osebni podatki obdelujejo v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene ima posameznik, na katerega se ti podatki nanašajo, pravico, da iz razlogov, povezanih z njegovim posebnim položajem, ugovarja obdelavi osebnih podatkov v zvezi z njim, razen če je obdelava potrebna za opravljanje naloge, ki se izvaja zaradi razlogov javnega interesa.

25. člen

(dolžnost obvestitve posameznikov o pravicah)

Odgovorna oseba organizacije je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami Splošne uredbe in zakonodajo o varstvu podatkov, obveščeni o pravicah. Organizacija poskrbi za enotno kontaktno točko, na katero se lahko obrnejo posamezniki pri uveljavljanju svojih pravic.

26. člen

(posredovanje informacij posameznikom, na katere se nanašajo osebni podatki)

Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrežno 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 ustrežno 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 pooblaščenec obdelovalec v primeru dvoma o obstoju zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Posredovanje posebnih vrst osebnih podatkov na osnovi prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz prejšnjega odstavka.

27. člen

(način posredovanja podatkov)

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 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.

Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovnikom v zaprtih ovojnicah.

V primeru, da se posebne vrste osebnih podatkov pošilja v elektronski obliki, mora biti med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

Podrobnosti o načinu pošiljanja posebnih vrst osebnih podatkov predpiše z navodilom odgovorna oseba organizacije po posvetu s pooblaščen osebo za varstvo podatkov.

28. člen **(evidenca posredovanj podatkov)**

Vsakršno koli posredovanje osebnih podatkov se zaznamuje z navedbo naslednjih podatkov:

- osebno ime/firmo in naslov/sedež osebe, kateri so bili posredovani osebni podatki,
- navedba, če je bilo posredovanje opravljeno po uradni dolžnosti,
- pravna podlaga, na podlagi katere so bili posredovani osebni podatki,
- kateri osebni podatki so bili posredovani,
- datum posredovanja podatkov,
- oseba, ki je posredovala podatek.

Seznam iz prejšnjega odstavka se vodi v fizični ali v elektronski obliki.

VI. EVIDENTIRANJE OBDELAVE OSEBNIH PODATKOV

29. člen **(evidenca dejavnosti obdelave)**

Organizacija vodi evidenco dejavnosti obdelave v skladu z določbami 30. člena Splošne uredbe.

Ta evidenca vsebuje vse naslednje informacije:

- naziv evidence;
- 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, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, v primeru prenosov pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

Vsak obdelovalec in predstavnik obdelovalca, kadar ta obstaja, vodita evidenco vseh vrst dejavnosti obdelave, ki jih izvajata v imenu upravljavca, ki vsebuje:

- naziv ali ime in kontaktne podatke obdelovalca ali obdelovalcev in vsakega upravljavca, v imenu katerega deluje obdelovalec, ter, kadar obstajajo, predstavnika upravljavca ali obdelovalca, in pooblaščen osebe za varstvo podatkov;
- vrste obdelave, ki se izvaja v imenu posameznega upravljavca;



- kadar je ustrezno, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo, v primeru prenosov pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

Evidence iz drugega in tretjega odstavka tega člena se vodi v pisni, vključno v elektronski obliki.

Upravljavca, obdelovalec ali predstavnik upravljavca ali obdelovalca, kadar ta obstaja, nadzornemu organu na zahtevo omogočijo dostop do evidenc.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidenco dejavnosti obdelave, vpogled v evidenco dejavnosti obdelave je omogočena vsakemu zaposlenemu na zahtevo.

30. člen **(vloga obdelovalca)**

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za upravljavca, se sklene pisna pogodba o opravljanju storitev, katera vsebuje tudi določila o predmetu obdelave (zlasti vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov in kategorije posameznikov), pravicah in obveznostih pogodbenega obdelovalca in upravljavca ter postopke in ukrepe za zavarovanje osebnih podatkov skladno s Splošno uredbo in zakonom, ki ureja varstvo osebnih podatkov.

Obdelovalci so tudi zunanji sodelavci, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, v kolikor imajo pri svojem delu dostop do osebnih podatkov.

Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil upravljavca in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pooblaščenca pravna ali fizična oseba, ki za upravljavca opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga določa ta pravilnik.

31. člen **(evidenca obdelovalcev)**

Organizacija vodi evidenco obdelovalcev, ki se preverja najmanj enkrat letno. Evidenca vsebuje vsaj naslednje podatke:

- naziv obdelovalca
- interna številka krovne pogodbe z obdelovalcem, če obstaja;
- interna številka pogodbe o pogodbeni obdelavi, če obstaja in datum sklenitve in poteka pogodbe;
- druga oblika zaveze za izpolnjevanje zahtev v skladu z zakonodajo (aneks h krovni pogodbi, enostranska izjava, posebna pogodba ...);
- datum zadnjega preverjanja seznama.



VII. VARNOST OBDELAVE OSEBNIH PODATKOV IN ORGANIZACIJSKI UKREPI

32. člen

(vgrajeno in privzeto varstvo podatkov)

Organizacija v okviru lastnega razvoja oziroma pri naročanju programske opreme za rešitve in storitve obdelave sledi načelu vgrajenega in privzetega varstva osebnih podatkov, ki obsegajo predvsem:

- minimizacijo obdelave osebnih podatkov;
- čimprejšnjo psevdomizacijo osebnih podatkov;
- preglednost pri nalogah in obdelavi osebnih podatkov;
- omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo osebnih podatkov, in
- omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe.

Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi osebnih podatkov ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, se organizacija zavezuje, da bo proizvajalce produktov, storitev in aplikacij spodbujal, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja, zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov. Načeli vgrajenega in privzetega varstva podatkov se morajo upoštevati tudi pri javnih razpisih.

Organizacija se v zvezi z zagotavljanjem vgrajenega in privzetega varstva podatkov iz prvega in drugega odstavka tega člena posvetuje s pooblaščen osebo za varstvo podatkov.

33. člen

(kakovost obdelave podatkov)

Osebni podatki, ki se obdelujejo v organizaciji, morajo biti točni, ažurni, ustrezni in po obsegu primerni glede na namene, za katere se obdelujejo.

VIII. OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV

34. člen

(ocena učinkov na varstvo osebnih podatkov)

Kadar je možno, da bi lahko vrsta obdelave osebnih podatkov, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, je organizacija dolžan pred obdelavo opraviti oceno učinka na varstvo osebnih podatkov.

Po potrebi se v okviru priprave ocene učinkov v zvezi z varstvom podatkov zaprosi za mnenje posameznike, na katere bi se nanašali obdelovani podatki oziroma ponudnika informacijske rešitve oziroma poklicna združenja.

Oceno učinka izdelata odgovorna oseba oddelka, kjer evidenca dejavnosti obdelave nastaja oz. se pojavi potreba po izvedbi ocen učinka. Pri oceni učinka sodeluje tudi pooblaščen oseba za varstvo osebnih podatkov.

IX. BRISANJE PODATKOV

35. člen (rok hrambe podatkov)

Osebni podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz člena 6 Splošne uredbe. Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Osebnostne podatke, ki jih organizacija obdeluje na osnovi pogodbenega odnosa s posameznikom, ta hrani za obdobje, ki je potrebno za izvršitev pogodbe in še 6 let po njenem prenehanju, razen v primerih, ko pride med posameznikom in organizacijo do spora v zvezi s pogodbo. V takem primeru hrani podatke še 6 let po pravnomočnosti sodne odločbe, arbitraže ali poravnave ali, če sodnega spora ni bilo, 6 let od dneva mirne razrešitve spora.

Tiste osebnostne podatke, ki jih organizacija obdeluje na podlagi osebne privolitve posameznika ali zakonitega interesa, bo ta hranil do preklica te privolitve oziroma do zahteve do izbrisa. Po prejemu zahteve za preklic privolitve ali zahteve za izbris se podatki izbrišejo brez nepotrebne odlašanja, v vsakem primeru pa v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev, o čemer se obvesti posameznika. Organizacija lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

36. člen (brisanje podatkov)

Za brisanje podatkov iz nosilcev podatkov 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. Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik oziroma se uničenje preda ustrezni zunanji službi na osnovi sklenjene pogodbe.

Organizacija načine hrambe, arhiviranja in uničenja zdravstvene dokumentacije v fizični ali elektronski obliki sprejme v posebnem dokumentu.

X. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

37. člen (varovanje prostorov)

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



Kot varovani prostor so opredeljeni prostori vodstva oziroma uprave, strežniške sobe, prostori programerske in servisne službe, pisarne, kabineti in drugi prostori, v katere nepooblaščen osebe nimajo vstopa.

Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja odgovorne osebe organizacije.

Ključni varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključni 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.

Zaposleni morajo ob zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zakleniti. Računalniki in druga strojna oprema pa morajo biti izklopljeni oz. fizično ali programsko zaklenjeni.

Obiskovalci se smejo v poslovnih prostorih, v katerih se nahajajo nosilci podatkov, gibati samo v spremstvu zaposlenega. To določilo ne velja za zunanje sodelavce organizacije, katerih vstop in gibanje v prostorih, v katerih se nahajajo nosilci podatkov, je urejeno s pogodbo ter jim je dodeljeno vstopno sredstvo.

38. člen **(vhodna kontrola zaposlenih)**

Za kontrolo vhodov v poslovne prostore in kontrolo vstopov v omaro s ključni uporabnikov se uporablja vstopne kartice/obeske. Vsak zaposleni, ki mu je dodeljena kartica/obesek za vhodno kontrolo je dolžan z njo ravnati z vso skrbnostjo in z zavedanjem, da je namenjena samo njegovi osebni uporabi. Izgubo ali odtujitev kartice mora takoj javiti delodajalcu, ki kartico/obesek nemudoma prekliče.

Vsak zaposleni je bil opozorjen in seznanjen z varnostnimi zahtevami pri ravnanju s kartico/obeskom.

Seznam zaposlenih, ki uporabljajo kartico/obesek za vhodno kontrolo, obsega ime in priimek zaposlenega ter interno številko vstopnega ključka/kartice, ki jo uporablja. Seznam, skupaj z izjavo in datumom ter podpisom prevzema kartice/obeska, hrani kadrovska služba.

39. člen **(videonadzor)**

Na območju organizacije je lahko uveden videonadzor, ki je nujno potreben za varovanje in varnost zaposlenih, uporabnikov, obiskovalcev in poslovnih partnerjev, zaradi varovanja premičnin in opreme, zaradi zagotavljanja varnosti službenih prostorov in nadzora vstopa ali izstopa v službene prostore ali, če zaradi narave dela obstaja možnost ogrožanja zaposlenih, uporabnikov, obiskovalcev in poslovnih partnerjev.

Zaposleni in obiskovalci so z videonadzorom seznanjeni z ustreznimi obvestilnimi napisi.



Podrobnosti o delovanju, upravljanju in nadzoru nad videonadzornim sistemom je urejeno v posebnem pravilniku.

40. člen

(varovanje nosilcev podatkov, ki vsebujejo osebne podatke)

Zaposleni svojega delovnega mesta ne smejo pustiti nenadzorovanega oziroma morajo poskrbeti, da so takrat originalne listine in nosilci osebnih podatkov shranjeni tako, da nepooblaščen osebe do njih nimajo dostopa. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene (politika čiste mize).

Računalniški zasloni morajo biti nameščeni tako, da nepooblaščen osebe nimajo vpogleda v prikazovane podatke.

Računalniki in druga informacijska tehnologija oziroma oprema, ki omogoča dostop do osebnih podatkov morajo biti v času odsotnosti zaposlenega bodisi izklopljeni bodisi fizično ali programsko zaklenjeni (politika čistega zaslona).

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

Nosilci osebnih podatkov, ki se nahajajo izven varovanih prostorov (npr. avla, hodniki, skupni prostori, učilnice, predavalnice, jedilnice) morajo biti zaklenjeni v omarah.

Posebni vrsti osebnih podatkov se ne sme hraniti izven varovanih prostorov. Iznos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov iz prostorov organizacije ni dovoljen, razen v primerih, ko je to nujno potrebno oziroma določeno z zakonom.

V prostorih, ki so namenjeni poslovanju s strankami oziroma nimajo statusa varovanega prostora in je vanje dovoljen dostop nezaposlenim (npr. sprejemna pisarna, tajništvo), morajo biti nosilci podatkov nameščeni tako, da stranke nimajo neposrednega vpogleda vanje. V takih prostorih na oglasnih deskah ali kakorkoli drugače ne smejo biti izpostavljeni taki podatki, na osnovi katerih bi se lahko nepooblaščen osebe seznanile z osebnim podatki posameznika in za katere organizacija nima pravne podlage za njihovo objavo oziroma obdelavo.

Vzdrževalci prostorov, informacijske tehnologije oziroma strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo odgovorne osebe. Delavci, 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).

41. člen

(kopiranje in tiskanje osebnih podatkov s strani zaposlenih)

Zaposleni, ki pri izvajanju svojih delovnih nalog kopirajo ali 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.



Kopiranje in tiskanje dokumentov, ki vsebujejo posebne vrste osebnih podatkov, se lahko opravi samo na napravah, ki so v času kopiranja ali tiskanja pod kontrolo zaposlenega, ki izvaja omenjeni opravili.

V primeru, da se navedeni dokumenti ne shranijo, se trajno uničijo.

42. člen

(vzdrževanje in popravila informacijske tehnologije in elektronskih storitev)

Vzdrževanje in popravila informacijske tehnologije in elektronskih storitev ter druge opreme je dovoljeno samo z vednostjo odgovorne osebe, oziroma ga lahko izvajajo pooblaščenji servisi ali vzdrževalci, ki imajo z organizacijo sklenjeno ustrezno pogodbo.

43. člen

(revizijske sledi)

Organizacija v zvezi z dostopi do podatkov, postopkov obdelave in do sistemov obdelave tvori, beleži in hrani zapise, ki omogočajo ugotavljanje, kdo, kdaj in kje je dostopal do določenega podatka, postopka obdelave oziroma sistema za obdelavo.

Zapisi iz prejšnjega odstavka se hranijo za obdobje 5 let od zaključka leta, v katerem je bil zapis ustvarjen, razen, če za obdelavo posameznih vrst osebnih podatkov drug zakon ne določa drugače.

Za revizijske sledi so odgovorni skrbniki informacijskih sistemov oz. rešitev, ki na podlagi posveta s pooblaščenjo osebo za varstvo osebnih podatkov določijo, kdo in v katerih primerih sme dostopati do zapisov revizijskih sledi. Način zbiranja zapisov, hrambo in uporabo revizijskih sledi organizacija določi v posebnem dokumentu.

44. člen

(mehanizmi za zaščito pred zlonamerno programsko opremo)

Organizacija uporablja ustrezne mehanizme za zaščito pred zlonamerno programsko opremo, da tako zmanjšuje možnost, da bi le-ta ogrozila neoporečnost in zaupnost informacij in programske opreme. Organizacija uporablja programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo (spyware, adware, grayware itd). Omenjena programska oprema mora biti nameščena na vse odjemalce.

Način uporabe mehanizmov za zaščito pred zlonamerno programsko opremo se določi v posebnem dokumentu.

XI. INFORMACIJSKO VARNOSTNA POLITIKA

45. člen

(varovanje dostopa do sistemske in aplikativno programske računalniške opreme)

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

Zaposlenemu oziroma zunanjim sodelavcem se dodeljujejo ali ukinjajo pravice dostopa do informacij, aplikacij in sistemov, ki jih potrebujejo glede na dodeljeno delovno mesto, kar določi in odobri



nadrejena oseba. Način dodeljevanja ali ukinjanja dostopa do sistemske in aplikativne računalniške opreme se določi v posebnem dokumentu.

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve odgovorne osebe ali od nje pooblaščen osebe, izvajajo ga lahko samo pooblaščen servis ali vzdrževalec, ki ima z organizacijo sklenjeno ustrezno pogodbo. Izvajalci morajo izvedene spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati. V primeru, da je potrebno za delo izdelati kopije, morajo biti le-te po prenehanju namena, s katerim so bile izdelane, ustrezno uničene. Enako velja za ostale izpise, izvoze podatkov ali druge pripomočke za izvedbo storitve servisiranja.

Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni podatki, se mora redno preverjati zaradi potencialne prisotnosti računalniških virusov in druge oblike zlonamerne kode. V primeru odkritja virusa, se ta odpravi s strani ustrezne strokovne službe oziroma pristojne osebe, zadolžene za delovanje računalniškega informacijskega sistema, obenem pa se skuša ugotovi tudi vzrok pojava virusa.

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

Zaposleni ne smejo nameščati programske opreme brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz organizacije brez odobritve odgovorne osebe organizacije ali vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

Dostop do podatkov in uporaba sistemske in aplikativno programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programske opreme in podatkov. Vsak uporabnik ima svoje geslo za dostopanje do posameznih elektronskih storitev, ki ga prejme ob nastopu delovnega mesta. Posojanje gesel in uporaba skupinskih gesel je prepovedana.

46. člen

(uporaba naprav za obdelavo osebnih podatkov)

Zaposleni uporabljajo različno informacijsko tehnologijo (računalnik, telefon, tablica in druge elektronske naprave) ter različne elektronske storitve (dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter druga programska oprema oziroma storitve), ki jim jo dodeli delodajalec, izključno za službene namene.

V omejenem obsegu in razumnih mejah se s strani organizacije dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene. Pri tem morajo delavci varovati ugled organizacije, tehnologije in storitev pa se ne sme uporabljati za neprimerne ali žaljive namene. Vodstvo lahko po lastni presoji delavcu kadarkoli prepove uporabo v zasebne namene.

Zasebne naprave iz prejšnjega odstavka morajo biti vključene v popisu informacijskih sredstev ter opremljene z ustreznimi informacijskimi varnostnimi rešitvami (šifriranje, razmejitev obdelave zasebnih podatkov).



47. člen **(uporaba zasebne opreme zaposlenega)**

Delavec lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave (predvsem telefon), če takšno uporabo odobri odgovorna oseba in delavec poda prostovoljno pisno soglasje, da lahko delodajalec za namene izvajanja delovnega procesa pri tem obdeluje njegovo zasebno telefonsko številko oziroma zasebni elektronski naslov.

48. člen **(uporaba svetovnega spleta)**

Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

Zaposleni v organizaciji morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom organa javnega zavoda (IP naslov).

V omrežju organizacije se na zahtevo odgovorne osebe lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja izključno za načrtovanje in varovanje informacijskega sistema.

Vodstvo organizacije lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev s posebno odredbo odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe odgovorne osebe. O blokadi se obvesti vse zaposlene po elektronski pošti.

49. člen **(službena elektronska pošta)**

Službena elektronska pošta se v organizaciji lahko uporablja kot orodje za komunikacijo s posamezniki, uporabniki, strankami, zaposlenimi in zunanjimi izvajalci. Pri tem se morajo delavci držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje organizacije, v katerem je pošiljatelj zaposlen.

Zaposleni po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, zagonske datoteke in skripte ipd.), razen ko to zahtevajo potrebe delovnih procesov.

Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave zaposlenega na določeno storitev (npr. pošte liste, prijava na izobraževanja ipd.) ni dovoljeno, razen če je povezano s poslovnim procesom organizacije.

Zaposleni svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove. Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi organizacije, razen če to ni povezano s potrebami delovnega mesta.



Zaposleni morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi lahko bila škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo pristojno osebo, zadolženo za delovanje računalniškega informacijskega sistema.

Zaposleni nikakor ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih, oziroma mora biti podatkom med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

Uporaba zasebne elektronske pošte (npr. Gmail, Yahoo, ipd.) za službene namene je prepovedana, saj potencialno predstavlja neupravičeno obdelavo osebnih podatkov. Izjemoma je izključno za namene komuniciranja med zaposlenimi na osnovi dovoljenja odgovorne osebe dovoljeno uporabljati zasebno elektronsko pošto.

50. člen (generiranje gesel)

Pri generiranju oziroma določanju gesel je treba spoštovati pravila:

- gesla morajo biti dolžine minimalno 8 znakov ali ustrezno daljša, v kolikor je to določeno za posamezno uporabniško rešitev;
- gesla ne smejo vsebovati smiselnih alfanumeričnih zaporedij znakov;
- gesla morajo biti kvalitetna (priporoča se uporaba ustrezne dolžine, posebni znaki, velike in male črke, številke);
- gesla ne smejo vsebovati besed iz različnih slovarjev;
- gesla naj ne bodo ciklična in naj se ne ponavljajo iz predhodnih obdobj;
- uveljavljeno mora biti obvezno redno spreminjanje gesel (najmanj na 6 mesecev);
- začetna gesla se ob prvi prijavi spremenijo;
- gesla, ki jih je generiral zunanji dobavitelj, je potrebno takoj spremeniti ob prvi uporabi v produkcijskem okolju;
- uporabniško ime ne sme kazati posebnih pooblastil uporabnika.

51. člen (ravljanje z gesli)

Pri ravnanju z gesli je treba obvezno spoštovati napotke:

- pooblaščen oseba, ki dodeljuje gesla, jih mora obravnavati zaupno, preprečiti mora možnost nepooblaščenega vpogleda in jih posredovati na varen način;
- uporabnikom mora biti omogočeno, da kadarkoli spremenijo svoje uporabniško geslo;
- geslo ne sme biti nikdar prikazano na zaslonu;
- gesla, ki se hranijo v elektronski obliki, morajo biti obvezno shranjena v šifrirani obliki;
- vsak uporabnik mora imeti svoje uporabniško ime in geslo izključno za osebno rabo;
- geslo je potrebno hraniti na način, ki drugi osebi popolnoma onemogoči možnost vpogleda;
- vsak uporabnik je odgovoren za zaupnost gesla in ga ne sme v nobenem primeru zaupati drugi osebi;
- v nobenem primeru uporabnik ne sme izdati gesla nadrejenemu, podrejenemu ali osebi, ki ga nadomešča ali IT osebju;
- v primeru razkritja gesla ali suma razkritja gesla mora to nemudoma sporočiti pooblaščen osebi za dodeljevanje gesel.



Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo v sefu v zaprti kuverti ali na drug ustrezen način, tako, da je dostop nepooblaščenih oseb onemogočen. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsako uporabo teh gesel sme dovoliti odgovorna oseba organizacije. Po vsaki takšni uporabi se določi nova vsebina gesel.

52. člen **(varnostno kopiranje podatkov)**

Organizacija zagotovi rezervno kopijo podatkov in omogočiti ponovno vzpostavitev sistema ter uspešno nadaljevanje dela po množici različnih dogodkov oz. varnostnih incidentov, ki povzročijo poškodovanje ali izgubo podatkov. To so problemi s strojno opremo, problemi s programsko opremo, človeške napake, naravne nesreče ipd. Vsi pomembni elektronski podatki se redno shranjujejo na medije daljše trajnosti. Praviloma se enkrat letno izvede test obnove varnostni kopij, kar se ustrezno dokumentira.

Varnostne kopije podatkov se hranijo zaklenjene v zavarovanih ognjevarnih omarah, zaščitene pred nepooblaščenim dostopom ter drugimi vplivi kot so poplave ali elektromagnetne motnje.

Način izvajanja varnostnega kopiranja podatkov se določi v posebnem dokumentu.

53. člen **(oddaljen dostop do sistemov)**

Oddaljen dostop do informacijskega sistema organizacije je dovoljen le na podlagi odobrene metode z ustrezno ravno varnosti, in sicer za tiste delavce, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo na delovni postaji.

Za uveljavitev oddaljenega varnega dostopa je na strojni opremi zagotovljena prepoznavna ustreznega programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami. Za zagotavljanje zaupnosti se šifrira ves promet iz končne točke oddaljenega omrežja do omrežja organizacije.

54. člen **(uporaba naprav za komunikacijo na daljavo)**

Socialnovarstvene, zdravstvene in terapevtske storitve, glede katerih sta lahko ob upoštevanju pravil medicinske doktrine uporabnik storitve in izvajalec ali več izvajalcev socialnovarstvene, zdravstvene ali terapevtske dejavnosti prostorsko ločena, lahko storitve opravijo z uporabo informacijskih in telekomunikacijskih tehnologij (v nadaljnjem besedilu: telestoritve). Dokumentacija se v tem primeru posreduje v skladu s predpisi o varstvu osebnih podatkov, ki se nanašajo na prenos občutljivih osebnih podatkov prek telekomunikacijskih omrežij.

V primeru opravljanja socialnovarstvene, zdravstvene ali terapevtske dejavnosti v obliki telestoritve se šteje, da je socialnovarstveno ali zdravstveno varstvo zagotovljeno v državi, v kateri ima sedež izvajalec socialnovarstvene ali zdravstvene dejavnosti, ki opravlja telestoritev.



Zaposleni lahko za potrebe komunikacije na daljavo uporabljajo storitve telestoritve v skladu z zakonodajo, tem pravilnikom z navodili odgovorne osebe socialnovarstvenega in zdravstvenega zavoda.

55. člen

(vpogled v službeno informacijsko tehnologijo zaposlenega)

Oseba, zadolžena za delovanje informacijskega sistema v organizaciji, lahko na posebej utemeljeno pisno zahtevo odgovorne osebe v prisotnosti tri članske komisije v izrednih primerih (nenadna odpoved delavca, smrt delavca, nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti delavca, odpoved delovnega razmerja s strani zaposlenega brez odpovednega roka, odpoved delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti in podobni izredni primeri) vpogleda v informacijsko tehnologijo (npr. v računalnik) ali druge elektronske storitve (npr. v elektronsko pošto) delavca le, če je to nujno potrebno za izpolnjevanje zakonskih obvez organizacije oziroma za vodenje delovnega procesa.

Vpogled opravi 3 članska komisija, ki jo vsakokrat imenuje odgovorna oseba organizacije. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik, ki vsebuje:

- obrazložitev razloga vpogleda,
- zapisnik o vstopu z morebitnimi pripombami delavca, če je ta navzoč,
- navedbe prisotnih oseb,
- seznam oziroma izpis pridobljenih podatkov.

Če se pojavi utemeljen sum, da zaposleni ne spoštujejo določil informacijsko varnostne politike tega pravilnika, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo odgovorne osebe opravi nadzor uporabe elektronskih storitev, a zgolj z vidika pregleda dnevniških zapisov o količini prometa in shranjenih podatkov, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebin.

O namenu uporabe informacijske tehnologije in elektronskih storitev iz tega člena ter možnosti vpogleda mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje obvestilo skupaj s temi pravili poslano vsem zaposlenim po e-pošti.

56. člen

(ravnanje zaposlenih ob prenehanju delovnega razmerja)

Ob prenehanju delavnega razmerja oziroma po izčrpanju temelja za opravljanje dela je delavec organizacije dolžan vrniti službeno informacijsko tehnologijo, ki jo je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so iz uporabljane informacijske opreme in elektronskih storitev očiščene oziroma izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti.

V primeru prenehanja delovnega razmerja je delavec dolžan z zasebne opreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.



XII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

57. člen (obvestilo o kršitvah)

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščen osebno, sami pa poskušajo takšno aktivnost preprečiti.

Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente ter v skladu s tem pravilnikom ustrezno ravnati.

58. člen (ukrepanje ob varnostnem incidentu)

Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem obvestiti nadrejenega delavca oziroma vodstvo organizacije.

Vodstvo mora najprej izvedeti, kaj se je zgodilo, oceniti, kakšne so potencialne škodljive posledice za pravice in svoboščine posameznikov in sprejeti ustrezne ukrepe za odpravo posledic ali vsaj zmanjšanje tveganj. Priporočljivo je, da se vodstvo za pripravo ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov posvetuje s Pooblaščen osebno za varstvo podatkov.

V primeru, da vodstvo organizacije oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora o tem obvestiti Informacijskega pooblaščenca brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je organizacija v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

Za prijavo se uporabi obrazec, ki ga priporoča Informacijski pooblaščenec in predstavlja del dokumentacije organizacije. Ob prijavi mora Informacijski pooblaščenec pridobiti vsaj naslednje informacije, kot to zahteva Splošna uredba:

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov;
- kontaktne podatke pooblaščen osebno za varstvo podatkov;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

59. člen (obveznost obveščanja Informacijskega pooblaščenca)

Za obveščanje Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov po 33. členu Splošne uredbe je odgovorna oseba organizacije.



Podrobneje so ukrepi ob sumu nepooblaščenega dostopa do osebnih podatkov urejeni v dokumentu: Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.

XIII. KONČNE DOLOČBE

60. člen (seznanitev zaposlenih s pravilnikom)

S pravilnikom so seznanjeni zaposleni in sodelavci v organizaciji, tako da se pravilnik objavi na oglasnih deski in na omrežju organizacije ter se pošlje vsem zaposlenim in sodelavcem preko elektronske pošte.

Zaposleni in ostali pogodbeni sodelavci se redno, praviloma 1 krat letno, udeležijo izobraževanja s področja varstva osebnih podatkov, ki ga izvede pooblaščen osebja za varstvo podatkov.

61. člen (začetek veljavnosti pravilnika)

Ta pravilnik prične veljati z dnem, ko ga podpiše direktorica zavoda in se objavi na interni oglasni deski. Pravilnik se prične uporabljati dne 1.12.2021.

Z dnem, ko je sprejet ta pravilnik, preneha veljati obstoječi Pravilnik o varstvu osebnih podatkov, sprejet dne 25.10.2013.

Maribor, 30.11.2021



direktorica
mag. Barbara Žgajner

Priloge:

- Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov,
- Vzorec obrazca za prijavo kršitve varstva osebnih podatkov.



Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov

V skladu s Pravilnikom o varstvu osebnih podatkov organizacije in v smislu izvajanja 33. in 34. člena Splošne Uredbe (GDPR) pripravljamo navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.¹

Kot upravljavec ali obdelovalec mora organizacija za dokazovanje skladnosti s Splošno Uredbo (GDPR) imeti vzpostavljen učinkovit sistem za zaznavanje in sporočanje v primeru kršitev. Ta navodila predstavljajo del omenjenega sistema. Najpomembnejša obveza iz Splošne Uredbe (GDPR) nalaga, da je organizacija dolžna obvestiti nadzorni organ (Informacijskega pooblaščenca) o zaznanih kršitvah varstva osebnih podatkov, če je (vsaj) verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. **Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah.**

1. Kaj je kršitev varstva osebnih podatkov?

Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev **pomeni varnostni incident**, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Primeri, ki se obravnavajo kot varnostni incident, kot jih navaja Informacijski pooblaščenec, so npr.:

- dostop do osebnih podatkov s strani nepooblaščenih oseb;
- posredovanje osebnih podatkov napačnemu naslovniku;
- izguba ali kraja računalniške opreme (prenosni računalnik, USB ključek, itd., ...), ki vsebuje osebne podatke;
- nepooblaščen uničenje baz z osebnimi podatki;
- sprememba osebnih podatkov brez potrebnega dovoljenja;
- izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščen namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t.i. »izsiljevalski virus«) idr.

Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente in v skladu z pravilnikom in temi navodili ustrezno ravnati.

2. Obveščanje vodstva organizacije

Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem **obvestiti nadrejenega delavca oziroma vodstvo organizacije.**

¹ Pri pripravi navodil smo upoštevali informacije Informacijskega pooblaščenca RS na spletni strani: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/ključna-področja-uredbe/prijava-kršitev/>

Priporočamo, da ima organizacija s strani vodstva določeno **kontaktno osebo**, ki bo v primeru varnostnega incidenta najprej dokumentirala kršitev varstva osebnih podatkov, nato skupaj z vodstvom evidentirala nadaljnje nujne ukrepe, obvestila ali se posvetovala s Pooblaščenno osebo za varstvo podatkov če je ta imenovana, ter izvajala nadaljnje korake vključno s prijavo kršitve Informacijskemu pooblaščenca.

Kontaktna oseba za vse primere kršitve varstva osebnih podatkov v organizaciji je:
Darja Ljubimski, vodja pravne in finančne službe, dosegljiva na darja.ljubimski@pomocnadomu.eu.

3. Obveščanje Pooblaščenno osebe za varstvo podatkov

V primeru, da je organizacija imenovala Pooblaščenno osebo za varstvo podatkov (v nadaljevanju: »pooblaščenno oseba«), jo mora vodstvo o zaznani kršitvi nemudoma obvestiti na dpo@datainfo.si. Vodstvo v primeru, da mora organizacija imeti imenovano Pooblaščenno osebo za varstvo podatkov, nemudoma **Pooblaščenno osebi pošlje obvestilo o zaznani kršitvi**. V skladu s Splošno Uredbo (GDPR) pooblaščenno oseba namreč sodeluje z nadzornim organom (Informacijskim pooblaščencom) ter deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo.

POMEMBNO: Kako pravilno obvestiti pooblaščenno osebo o domnevni kršitvi varstva podatkov?

Informacijski pooblaščenec predlaga dve možnosti:

- prva možnost je, da pooblaščenno osebo obvestite priporočeno po pošti.
- druga možnost pa je obvestitev preko elektronske pošte. V tem primeru je potrebno vsebino/priponko elektronskega sporočila šifrirati in nato posredovati geslo v ločenem elektronskem sporočilu.

Pooblaščenno oseba organizaciji pomaga izdelati **oceno verjetnosti in resnosti** posledic za pravice in svoboščine posameznikov. Verjetnost je povezana z možnostjo nastanka posledic, resnost pa s škodo, ki jo kršitev lahko povzroči posameznikom.

V primeru, da organizacija nima imenovane Pooblaščenno osebe, vseeno priporočamo, da se vodstvo organizacije obrne po strokovno pomoč, predvsem zaradi ustrezne priprave ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov, npr. tako da na dpo@datainfo.si pošlje sporočilo o zaznani kršitvi.

Od ocene je odvisno, ali bo treba o kršitvi obvestiti Informacijskega pooblaščenca. Če je verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, mora organizacija o tem obvestiti Informacijskega pooblaščenca. Če ni verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, obveščanje ni potrebno.

Za **pripravo ocene mora** upravljavec najprej izvedeti, **kaj se je zgodilo**, oceniti kakšne so **potencialne škodljive posledice** za pravice in svoboščine posameznikov in sprejeti **ustrezne ukrepe** za odpravo posledic ali vsaj zmanjšanje tveganj.

4. Obvestilo Informacijskemu pooblaščenccu

Upravlavec mora o kršitvi obvestiti Informacijskega pooblaščenca **brez odlašanja, najkasneje pa v 72 urah** po zaznani kršitvi. V primeru, da ste v organizaciji v vlogi obdelovalca, morate o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

V predvidenem času 72 ur včasih ni mogoče zagotoviti vseh potrebnih informacij o incidentu, kot to zahteva Splošna Uredba (GDPR), zato lahko upravljavec Informacijskemu pooblaščenccu obvestilo o kršitvah posreduje po fazah, vendar brez odlašanja. Od upravljavca se pričakuje, da bo svoje obveznosti

v zvezi s preiskovanjem varnostnih incidentov izvedel prioritarno in hitro. Ne glede na to, je treba v roku 72 ur podati vsaj informacijo o zaznani kršitvi, izsledki notranje preiskave pa se lahko posredujejo kasneje. Upravljavci naj razlog za zamudo pri podaji popolnega obvestila o kršitvah posebej obrazložijo.

Pri Informacijskem pooblaščenцу so pripravili **neobvezen obrazec za podajo obvestila o kršitvi**, ki je dostopen na naslednji povezavi: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev/>

Omenjen obrazec pa je priložen tudi kot priloga temu navodilu.

Obrazec izpolnite v največji možni meri, pomembno je, da ob prijavi Informacijski pooblaščenec pridobi vsaj naslednje informacije, kot to zahteva Splošna Uredba (GDPR):

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov.
- kontaktne podatke pooblaščen osebe za varstvo podatkov.
- opis verjetnih posledic kršitve varstva osebnih podatkov.
- opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

5. Obvestilo posameznikom

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči **veliko tveganje za pravice in svoboščine posameznikov**, Splošna Uredba (GDPR) zahteva, da upravljavec o kršitvi neposredno obvesti zadevne posameznike in da to stori brez odlašanja.

Za obveščanje posameznikov Splošna Uredba (GDPR) postavlja standard '**veliko tveganje**', ki je višja stopnja ogroženosti pravic in svoboščin posameznikov, kot velja za uradno obvestilo nadzornemu organu. Kot je že bilo poudarjeno je treba stopnjo tveganja ocenjevati v vsakem primeru posebej, upošteva verjetnost nastanka posledic in resnost teh posledic. Treba je zlasti upoštevati, da je potreba po obveščanju večja, če obstaja velika verjetnost neugodnih posledic, pri tem pa lahko **ukrep obveščanja zmanjša tveganje** za nastanek teh posledic. Cilj in smoter zahteve po obveščanju posameznikov o kršitvi je prav v možnosti zmanjševanja tveganj za nastanek neugodnih posledic. Na ta način se torej pomaga posameznikom preprečiti neugodne posledice, ki bi sicer lahko pomenile tudi premoženjsko ali nepremoženjsko škodo (upravljavec je lahko odškodninsko odgovoren poleg sankcij, ki jih lahko izreče nadzorni organ).

Informacijski pooblaščenec navaja kot primer, nepooblaščen dostop do zdravstvenih podatkov pacientov določene **bolnišnice**, kjer je že zaradi **narave podatkov** tveganje za pravice in svoboščine pacientov visoko in bo verjetno treba posameznike o kršitvi obvestiti.

V vsakem primeru je smiselno, da se o ukrepu obveščanja posameznikov posvetujete s Pooblaščen osebno..

Samo **obvestilo posameznikom** mora v jasnem in preprostem jeziku vsebovati vsaj:

- kontaktne podatke pooblaščen osebe za varstvo osebnih podatkov (ali druge kontaktne osebe), pri kateri lahko posameznik prejme več informacij oziroma pojasnil o kršitvi,
- informacijo o posledicah,
- informacijo o sprejetih ali predlaganih ukrepih in kjer je to mogoče, dodatna pojasnila posameznikom, kako lahko sami zmanjšajo tveganje za nastanek posledic.

6. Vpis v seznam obvestil o kršitvah

Priporoča se, da organizacija vodi seznam obvestil o kršitvah. Pri Informacijskem pooblaščenju priporočajo vodenje dokumentacije tudi o tistih zaznanih kršitvah, ki niso bile sporočene nadzornemu organu ali posameznikom.

Seznam obvestil o kršitvah naj vsebuje vsaj naslednje podatke:

- datum kršitve
- datum seznanitve s kršitvijo
- datum obvestila Informacijskemu pooblaščenju (v kolikor je bilo uradno obvestilo potrebno)
- interna številka dokumenta / obvestila
- kratek opis kršitve
- opis ukrepov

7. Neukrepanje ob zaznani kršitvi

Informacijski pooblaščenec navaja, da neukrepanje ob zaznavi kršitev varstva osebnih podatkov in neobveščanje nadzornega organa, ko je to potrebno, predstavlja samostojno kršitev po Splošni Uredbi (GDPR), za katero je predpisana globa do 10 milijonov evrov oz. do 2% letnega prometa. Upravljavca lahko doleti kazen za kršitev in kazen, če ni izpolnil zahteve po obveščanju. Temu se dodajo tudi popravljalni ukrepi, ki jih lahko nadzorni organ naloži upravljavcu skladno s členom 58 Splošne Uredbe (GDPR). Zato morate zagotoviti učinkovit interni postopek javljanja kršitev, ki bo omogočil pravočasno zaznavo in sporočanje kršitev z vsemi potrebnimi informacijami o varnostnem incidentu.

V Mariboru, dne 30.11.2021

mag. Barbara Žgajner, direktorica

Podpis _____



URADNO OBVESTILO O KRŠITVI VARNOSTI OSEBNIH PODATKOV

Obvezno preberite!

- ☀ Člen 33 Splošne uredbe o varstvu podatkov (UREDBA (EU) 2016/679) zavezuje upravljavca, da obvesti nadzorni organ o kršitvi varnosti osebnih podatkov.
- ☀ Obrazec izpolni podjetje ali institucija, ki je dolžna obvestiti nadzorni organ. Obrazec ni namenjen posameznikom, ki želijo podati prijavo.
- ☀ Pred izpolnitvijo si preberite ključne informacije glede obveščanja o kršitvah varnosti: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev/>

0. Uradno obvestilo o kršitvi varnosti osebnih podatkov

Vrsta obvestila (Ustrezno označi.)	☐ Obvestilo o kršitvi <i>(s tem obvestilom v celoti obveščate o kršitvi varnosti osebnih podatkov);</i>	☐ Predhodno obvestilo <i>(obvestilo boste kasneje dopolnili);</i>	☒ Dopolnitev / sprememba <i>(s tem obvestilom podajate dopolnitev oziroma spremembo predhodnega obvestila);</i>
Opredelite predhodno obvestilo (številka dokumenta, naslov zadeve / druga oznaka obvestila) <i>(izpolnite le, če ste označili dopolnitev / sprememba).</i>			
Datum predhodnih obvestil <i>(izpolnite le, če ste označili dopolnitev / sprememba.)</i>		Kliknite tukaj, če želite vnesti datum.	

1. O upravljavcu

1.1. Kontaktni podatki upravljavca

Matična številka	
Davčna številka	
Naziv	

Naslov in relevantne kontaktne informacije		
Podatki pooblaščenih osebe za varstvo osebnih podatkov (izpolnite, če ste imenovali pooblaščenca osebo za varstvo osebnih podatkov)	Ime, priimek in funkcija	
	Elektronska pošta	
	Telefonska številka	
	Poštni naslov	
Ime in funkcija osebe, ki podaja obvestilo		
Podatki osebe, ki se jo lahko kontaktira za pridobitev informacij o kršitvi (izpolnite kadar ni osebe, ki je podala obvestilo o kršitvi.)	Ime, priimek in funkcija	
	Elektronska pošta	
	Telefonska številka	
	Poštni naslov	
Sektor dejavnosti organizacije (Ustrezno označi.)	☐ Kmetijstvo, gozdarstvo in ribištvo; ☐ Rudarstvo in kamnoseštvo; ☐ Proizvodnja; ☐ Oskrba z električno energijo, plinom, paro in klimatskimi napravami; ☐ Oskrba z vodo; ravnanje z odpadki in sanacijske dejavnosti; ☐ Gradnja; ☐ Trgovina na debelo in drobno; popravila motornih vozil in motornih koles; ☐ Prevoz in skladiščenje; ☐ Namestitvene storitve in storitve povezane s prehrano; ☐ Informiranje in komuniciranje; ☐ Finančne in zavarovalniške dejavnosti;	☐ Nepremičninske dejavnosti; ☐ Strokovne, znanstvene in tehnične dejavnosti; ☐ Administrativne in podporne storitvene dejavnosti; ☐ Javna uprava in obramba; ☐ Obvezna socialna varnost; ☐ Izobraževanje; ☐ Zdravstvo in socialno delo; ☐ Umetnost, zabava in rekreacija; ☐ Druge storitvene dejavnosti; ☐ Dejavnosti mednarodnih organizacij in teles ☐ Drugo

1.2. Vpletenost drugih organizacij izven upravljalca podatkov v storitve, povezane s kršitvijo

Navedite, kateri subjekti izven upravljalca podatkov so vpleteni v storitve, povezane s kršitvijo (ustrezno označite).		☐ obdelovalci ☐ skupni upravljalci	☐ drugi (navedite kateri v naslednjem okencu)
Ime in kvalifikacija »druge« vpletene organizacije (Izpolnite le, če ste prej označili »druge«. Navesti morate imena in statuse drugih organizacij, ki so vpletene v kršitev, in obrazložiti njihovo vpletenost.)			

2. Časovnica

Datum kršitve v primeru ENKRATNEGA DOGODKA (npr. izguba USB ključka...).		Kliknite tukaj, če želite vnesti datum.
Datum začetka kršitve v primeru TRAJAJOČE KRŠITVE (npr. objava datoteke...).		Kliknite tukaj, če želite vnesti datum.
Datum zaključka kršitve v primeru TRAJAJOČE KRŠITVE.		Kliknite tukaj, če želite vnesti datum.
Ali kršitev še traja?		☐ DA ☐ NE
Datum seznanitve s kršitvijo (če ne poznate natančnega datuma, na črto navedite približno oziroma v razponu).		Kliknite tukaj, če želite vnesti datum.
Opišite, kako oziroma s kakšnim sredstvom ste zaznali kršitev.		

Če vas je o kršitvi obvestil vaš pogodbeni obdelovalec, navedite, kdaj ste prejeli njegovo obvestilo.	Kliknite tukaj, če želite vnesti datum.
Navedite razloge za prepozno podajo obvestila o kršitvi nadzornemu organu <i>(izpolnite le, če je od zaznave kršitve do obvestila preteklo več kot 72 ur).</i>	
Dodatni komentarji o datumu obveščanja <i>(če ne poznate točnega datuma kršitve, lahko v tem polju podate več informacij glede datuma obveščanja).</i>	

3. O kršitvi

Za kakšno vrsto kršitve gre? ☐ Zaupnost (npr. nepooblaščen razkritje podatkov, nepooblaščen dostop do podatkov...) ☐ Celovitost (sprememba podatkov...) ☐ Dostopnost (npr. izguba podatkov, uničenje podatkov...)	
Kakšna je bila narava incidenta? <i>(Ustrezno označite.)</i>	☐ izgubljena ali ukradena naprava; ☐ izgubljen, ukraden ali na ne-varnem mestu puščen dokument; ☐ izgubljena ali odprta pošta; ☐ zlonamern vdor v informacijski sistem; ☐ zlonamerna programska oprema (npr. izsiljevalski virusi);

☐ lažno predstavljanje (t.i. »phishing«); ☐ nepravilno uničenje osebnih podatkov v fizični obliki; ☐ osebni podatki še vedno prisotni na zastareli napravi; ☐ nenamerna objava; ☐ prikazani podatki napačne osebe; ☐ osebni podatki, poslani napačnemu prejemniku; ☐ nepooblaščno verbalno razkritje osebnih podatkov; ☐ drugo (izpolnite spodaj)	
Druga narava incidenta <i>(Izpolnite le, če ste pri prejšnjem vprašanju označili »drugo«.)</i>	
Kakšen je bil vzrok za kršitev?	☐ notranji in <u>ne</u> zlonamerni; ☐ zlonamerni notranji; ☐ zunanji in <u>ne</u> zlonamerni; ☐ zlonamerni zunanji; ☐ neznan ☐ drugi (izpolnite spodaj)
Drugi vzroki za kršitev <i>(Izpolnite le, če ste pri prejšnjem vprašanju označili »drugo«.)</i>	

4. Kršitev varnosti osebnih podatkov – vrste osebnih podatkov

4.1. Običajni osebni podatki

Ustrezno označite, v katere vrste osebnih podatkov je kršitev posegla.

☐ Identiteta posameznikov, na katere se nanašajo podatki (npr. ime, priimek, datum rojstva) ☐ Nacionalna identifikacijska številka (EMŠO) ☐ Kontaktni podatki ☐ Identifikacijski podatki		☐ Finančni in ekonomski podatki ☐ Podatki iz uradnih dokumentov ☐ Lokacijski podatki ☐ Druge vrste podatkov (opišite v naslednjem okencu)	
Opišite vrste osebnih podatkov, v katere je kršitev posegla <i>(izpolnite le, če ste pri prejšnjem vprašanju označili »druge vrste podatkov«).</i>			
Navedite približno število evidenc.			

4.2. Posebne vrste osebnih podatkov (»občutljivi osebni podatki«)

Ustrezno označite, v katere posebne vrste osebnih podatkov je kršitev posegla			
☐ Podatki, ki razkrivajo rasno ali etično poreklo ☐ Podatki o političnem prepričanju ☐ Verska ali filozofska prepričanja ☐ Članstvo v sindikatu ☐ Podatki o spolnem življenju		☐ Podatki o zdravju ☐ Genetski podatki ☐ Biometrični podatki ☐ Vrste podatkov še niso znane ☐ Druge vrste podatkov (opišite v naslednjem okencu)	
Opišite druge posebne vrste osebnih podatkov, v katere je kršitev posegla <i>(izpolnite le, če ste pri prejšnjem vprašanju označili »druge vrste podatkov«).</i>			

Navedite približno število evidenc.	
-------------------------------------	--

5. O posameznikih, na katere se nanašajo podatki

Označite, v čigave osebne podatke je kršitev posegla.	
☐ Zaposleni ☐ Uporabniki ☐ Naročniki ☐ Študenti ☐ Stranke (sedanje in prihodnje)	☐ Pacienti ☐ Mladoletniki ☐ Posamezniki iz ranljivih skupin ☐ Še ne znano ☐ Drugi (opredelite spodaj)
Opredelite kategorijo posameznikov – »drugi« <i>(izpolnite le, če ste prej označili »drugi«).</i>	
Približno število oseb, ki jih zadeva kršitev <i>(navedite približno število).</i>	

6. O ukrepih, sprejetih PRED kršitvijo

Opišite ukrepe, ki ste jih sprejeli pred kršitvijo.	
--	--

7. Posledice

7.1. Kršitev zaupnosti

Ustrezno označite, do kakšnih posledic je prišlo oziroma bi po vašem mnenju lahko prišlo.	
☐ Večje razširjanje podatkov, kot je potrebno oziroma brez privolitve posameznikov;	☐ Podatki se lahko izkoriščajo za druge namene in / ali na nepošten način;
☐ Podatki so lahko povezani z drugimi informacijami o posameznikih;	☐ Drugo (opišite v naslednjem okencu).
Opišite druge posledice glede zaupnosti <i>(izpolnite le, če ste prej označili »drugo«).</i>	

7.2. Kršitev celovitosti

Ustrezno označite, do kakšnih posledic je prišlo oziroma bi po vašem mnenju lahko prišlo.	
☐ Podatki so lahko bili spremenjeni in uporabljeni, četudi niso več veljavni;	☐ Drugo (opišite v naslednjem okencu)
☐ Podatki so lahko bili spremenjeni v sicer veljavne podatke in pozneje uporabljeni v druge namene;	
Opišite druge posledice glede celovitosti <i>(izpolnite le, če ste prej označili »drugo«).</i>	

7.3. Kršitev dostopnosti

Ustrezno označite, do kakšnih posledic je prišlo oziroma bi po vašem mnenju lahko prišlo.	
☐ Izguba sposobnosti zagotavljanja kritične storitve zadevnim posameznikom, na katere se nanašajo podatki;	☐ Drugo (opišite v naslednjem okencu).
☐ Sprememba v sposobnosti zagotavljanja kritične storitve zadevnim posameznikom, na katere se nanašajo podatki;	
Opišite druge posledice glede dostopnosti	

<i>(izpolnite le, če ste prej označili »drugo«).</i>	
--	--

7.4. Fizična, premoženjska ali nepremoženjska škoda ali pomembne posledice za posameznike, na katere se podatki nanašajo

Kakšna je narava potencialnih vplivov na posameznike, na katere se nanašajo podatki? <i>(Ustrezno označite.)</i>	☐ izguba nadzora nad osebnimi podatki; ☐ omejitev pravic posameznikov; ☐ diskriminacija; ☐ kraja identitete; ☐ goljufija; ☐ finančna izguba; ☐ nedovoljena ponovna identifikacija posameznika; ☐ škoda zaradi okrnitve ugleda; ☐ izguba zaupnosti osebnih podatkov, varovanih s poslovno skrivnostjo; ☐ drugo (opišite spodaj)
Opišite druge vplive na posameznika, na katerega se nanašajo podatki <i>(izpolnite le, če ste prej označili »drugo«).</i>	
Kakšna je stopnja resnosti potencialnih vplivov? <i>(Tukaj označite rezultat samoocene glede resnosti vplivov kršitve varnosti podatkov na posameznike.)</i>	☐ zanemarljivo ☐ pomembno ☐ omejeno ☐ maksimalno

8. Ukrepanje

8.1. Sporočilo posameznikom, na katere se nanašajo podatki, o kršitvi varnosti osebnih podatkov

Ali ste o kršitvi obvestili posameznike? (Ustrezno označite.)	☐ DA ☒ NE, ampak bomo obvestili ☒ Ne bomo jih obvestili ☐ Trenutno ni definirano
Kdaj ste obvestili posameznike? (Izpolnite le, če ste označili »DA«.)	Kliknite tukaj, če želite vnesti datum.
Kdaj načrtujete obvestiti posameznike? Navedite datum oziroma ustrezno označite. (Izpolnite le, če ste označili »NE, ampak jim bo sporočeno«.)	Kliknite tukaj, če želite vnesti datum. ☐ datum načrtovanega obveščanja posameznikov še ni znan
Razlog, da posameznikov ne nameravate obvestiti (izpolnite le, če ste označili »NE bomo sporočili«.)	☐ Upravljavec je uvedel ustrezne tehnične in organizacijske zaščitne ukrepe, predvsem ukrepe, s katerimi je nepooblaščenim osebam preprečena seznanitev z osebnimi podatki (npr. ustrezno šifriranje podatkov); ☐ Obveščanje vsakega posameznika, na katerega se nanašajo podatki, bi pomenilo nesorazmerne napore; ☐ Upravljavec je sprejel poznejše ukrepe, ki zagotavljajo, da se večje tveganje za pravice in svoboščine posameznikov, na katere se podatki nanašajo, ne bo uresničilo.
Opišite ukrepe, ki preprečujejo nastanek večjih tveganj in zaradi katerih o kršitvi ni treba obvestiti posameznikov (izpolnite le, če ste označili »NE bomo sporočili«.)	

Navedite približno število posameznikov, ki so bili obveščeni o kršitvi <i>(izpolnite le, če ste označili »DA«).</i>	
Navedite sredstvo komunikacije, ki je bilo uporabljeno za obveščanje posameznikov <i>(izpolnite le, če ste označili »DA«).</i>	
Dodajte obvestilo, ki ste ga poslali posameznikom oziroma navedite sklic ali povezavo do obvestila <i>(izpolnite le, če ste označili »DA«).</i>	
Dodajte javno obvestilo oziroma navedite sklic ali povezavo do obvestila <i>(izpolnite le, če ste označili »DA«).</i>	

8.2. Ukrepi, sprejeti PO KRŠITVI za zmanjšanje posledic kršitve

Navedite ukrepe, ki ste jih sprejeli PO KRŠITVI	
---	--

za zmanjšanje posledic kršitve.	
---	--

8.3. Čezmejna in druga obvestila

Ali s tem obvestilom obveščate VODILNI NADZORNI ORGAN, ker gre za primer kršitve čezmejne narave?		☐ DA ☐ NE																													
Iz seznama držav EU označite, na katere države se nanaša kršitev <i>(iz katerih držav so podatki posameznikov oziroma kje je potekala obdelava, kjer je prišlo do kršitve).</i>	<table border="0"> <tr> <td>☐ Avstrija</td> <td>☐ Finska</td> <td>☐ Litva</td> <td>☐ Portugalska</td> </tr> <tr> <td>☐ Belgija</td> <td>☐ Francija</td> <td>☐ Luksemburg</td> <td>☐ Romunija</td> </tr> <tr> <td>☐ Bolgarija</td> <td>☐ Grčija</td> <td>☐ Madžarska</td> <td>☐ Slovaška</td> </tr> <tr> <td>☐ Ciper</td> <td>☐ Hrvaška</td> <td>☐ Malta</td> <td>☐ Slovenija</td> </tr> <tr> <td>☐ Češka</td> <td>☐ Irska</td> <td>☐ Nemčija</td> <td>☐ Španija</td> </tr> <tr> <td>☐ Danska</td> <td>☐ Italija</td> <td>☐ Nizozemska</td> <td>☐ Švedska</td> </tr> <tr> <td>☐ Estonija</td> <td>☐ Latvija</td> <td>☐ Poljska</td> <td>☐ Združeno kraljestvo</td> </tr> </table>			☐ Avstrija	☐ Finska	☐ Litva	☐ Portugalska	☐ Belgija	☐ Francija	☐ Luksemburg	☐ Romunija	☐ Bolgarija	☐ Grčija	☐ Madžarska	☐ Slovaška	☐ Ciper	☐ Hrvaška	☐ Malta	☐ Slovenija	☐ Češka	☐ Irska	☐ Nemčija	☐ Španija	☐ Danska	☐ Italija	☐ Nizozemska	☐ Švedska	☐ Estonija	☐ Latvija	☐ Poljska	☐ Združeno kraljestvo
☐ Avstrija	☐ Finska	☐ Litva	☐ Portugalska																												
☐ Belgija	☐ Francija	☐ Luksemburg	☐ Romunija																												
☐ Bolgarija	☐ Grčija	☐ Madžarska	☐ Slovaška																												
☐ Ciper	☐ Hrvaška	☐ Malta	☐ Slovenija																												
☐ Češka	☐ Irska	☐ Nemčija	☐ Španija																												
☐ Danska	☐ Italija	☐ Nizozemska	☐ Švedska																												
☐ Estonija	☐ Latvija	☐ Poljska	☐ Združeno kraljestvo																												
Ali ste oziroma ali boste o kršitvi neposredno obvestili tudi druge zadevne EU nadzorne organe, pristojne za varstvo osebnih podatkov?		☐ DA, smo jih že obvestili (izpolnite naslednje okence) ☐ NE ☐ Še bodo obveščeni (izpolnite naslednje okence)																													
Navedite katere nadzorne organe za varstvo osebnih podatkov iz EU ste že		<i>Tukaj navedete, kateri nadzorni organi iz EU so že bili obveščeni o kršitvi.</i>																													

oziroma boste obvestili o kršitvi <i>(izpolnite le, če ste prej označili »DA« ali »Še bodo obveščeni«).</i>	Do kontaktnih nacionalnih nadzornih organov za varstvo osebnih podatkov v EU lahko dostopate na naslednji povezavi: http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm
Ali ste oziroma boste o kršitvi obvestili tudi druge nadzorne organe, pristojne za varstvo osebnih podatkov <u>izven EU</u>?	☐ DA (izpolnite spodaj) ☐ NE ☐ Še bodo obveščeni (izpolnite spodaj)
Navedite katere druge nadzorne organe, pristojne za varstvo osebnih podatkov izven EU, ste oziroma boste obvestili o kršitvi <i>(izpolnite le, če ste prej označili »DA« ali »Še bodo obveščeni«).</i>	<i>Tukaj navedete, kateri drugi nadzorni organi izven EU so že bili obveščeni o kršitvi.</i>
Ali ste oziroma boste o kršitvi obvestili tudi druge nadzorne in regulatorne organe po drugih EU predpisih (Direktiva (EU) 2016/1148 - NIS direktiva; Uredba (EU) št. 910/2014 - Uredba eIDAS)?	☐ DA (izpolnite spodaj) ☐ NE ☐ Še bodo obveščeni (izpolnite spodaj)
Navedite druge nadzorne in regulatorne organe po EU predpisih <i>(izpolnite le, če ste prej označili »DA« ali »Še bodo obveščeni«).</i>	<i>Tukaj navedete, kateri drugi nadzorni organi izven EU so že bili obveščeni o kršitvi.</i>

9. Datum in podpis

Datum:	Podpis:
---------------------	----------------------

☀ To vlogo se naslovi na Informacijskega pooblaščenca, Dunajska 22, 1000 Ljubljana ali na: prijava-krsitev@ip-rs.si. Obrazec obvestila o kršitvi varnosti osebnih podatkov ni predpisan.