Na podlagi 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 (Splošna uredba o varstvu podatkov; v nadaljnjem besedilu: Splošna uredba) in nacionalne zakonodaje Republike Slovenije s področja varstva osebnih podatkov, predvsem Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 163/2022: v nadaljnjem besedilu: ZVOP-2) ter na podlagi 12. in 14. člena Sklepa o preoblikovanju javnega zavoda Akademska in raziskovalna mreža Slovenije (Ur. l. RS, št. 7/2023) je Upravni odbor Akademske in raziskovalne mreže Slovenije na 144. seji dne 6. 11. 2024 sprejel naslednji

# PRAVILNIK

**o zavarovanju osebnih podatkov**

## I. Splošne določbe

1. člen

(področje uporabe pravilnika)

(1) Pravilnik se uporablja za vsako obdelavo osebnih podatkov v imenu Akademske in raziskovalne mreže Slovenije (v nadaljnjem besedilu: organizacije), ne glede na to, ali obdelava poteka v Evropski uniji ali v tretjih državah.

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

(3) Zaposleni in zunanji sodelavci organizacije, ki pri svojem delu obdelujejo in uporabljajo osebne in/ali zaupne podatke organizacije in/ali se seznanjajo s poslovno skrivnostjo organizacije, so pri svojem delu zavezani spoštovati določbe ZVOP-2, Splošno uredbo, področno zakonodajo, ki ureja posamezno področje njihovega dela in se nanaša na varstvo osebnih podatkov ter ta pravilnik in na njegovi podlagi izdana navodila.

2. člen

(izrazi)

(1) Besede in pojmi v temu pravilniku imajo naslednji pomen:

a. **Osebni podatek:** katerokoli informacija v zvezi z določenim ali določljivim posameznikom (v nadaljevanju: »posameznik, na katerega se nanašajo osebni podatki«);
b. **Pisna zahteva ali vloga**: zahteva ali vloga, ki je podana v pisni obliki in podpisana s strani fizične osebe ali odgovorne osebe pravne osebe z lastnoročnim ali elektronskim podpisom;
c. **Upravljavec**: fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;
d. **Skupni upravljavci**: dva ali več upravljavcev, ki skupaj določijo namene in načine obdelave;
e. **Obdelovalec**: fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
f. **Pooblaščena oseba za varstvo osebnih podatkov (v nadaljevanju DPO)**: imenovana oseba ali skupina oseb, ki upravljavcu na neodvisen način svetuje pri zagotavljanju skladnosti s Splošno uredbo in zakonodajo na področju varstva osebnih podatkov;
g. **Zaposleni**: vsaka fizična oseba, ki je v delovnem razmerju na podlagi sklenjene pogodbe o zaposlitvi. Kot zaposleni se v smislu tega pravilnika šteje tudi oseba, ki na kakršnikoli drugi pravni podlagi opravlja delo za organizacijo;

h. **Zunanji sodelavci organizacije**: pravne in fizične osebe, s katerimi se organizacija dogovori za izvedbo vseh ali posameznega opravila v zvezi z obdelavo osebnih podatkov, zlasti za izvajanje specifičnih dejavnosti obdelave (pogodbeni obdelovalec);
i. **Incident s področja varnosti osebnih podatkov**: vsaka kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

(2) Ostali pojmi, uporabljeni v tem pravilniku, ki jih opredeljuje tudi Splošna uredba, imajo enak pomen, kot ga določa Splošna uredba.

## II. Odgovornosti organizacije

3. člen

(pogoji obdelave osebnih podatkov)

(1) Osebni podatki v organizaciji se smejo obdelovati pod pogoji, ki jih določajo akti iz tretjega odstavka 1. člena tega pravilnika.

(2) Obdelava podatkov o članstvu v sindikatu je dovoljena, če je posameznik za to podal izrecno pisno privolitev (npr. zaradi neposrednega odtegljaja članarine od plače) ali če je potrebna za izvajanje obveznosti in posebnih pravic upravljavca na področju zaposlovanja in v drugih primerih, ki jih določa Splošna uredba.

(3) Pred vnosom v zbirko osebnih podatkov smejo zaposleni preverjati točnost osebnih podatkov z vpogledom v osebni dokument posameznika, na katerega se nanašajo.

(4) Kopiranje osebnih dokumentov in hranjenje kopij osebnih dokumentov ni dovoljeno, razen v primerih, ki jih izrecno določa zakon. Prepovedano je pošiljanje kopij osebnih dokumentov po elektronski pošti.

4. člen

(obveznost vodenja evidence dejavnosti obdelave)

(1) Organizacija vodi evidenco dejavnosti obdelave skladno z določbami 30. člena Splošne uredbe. Poleg podatkov iz 30. člena Splošne uredbe se v evidenci dejavnosti vodi tudi informacija o tem, katera oseba je odgovorna za posamezno obdelavo osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

(2) Za vzpostavitev, vodenje in ažuriranje evidenc dejavnosti obdelave osebnih podatkov in zbirk osebnih podatkov, ki jih evidence dejavnosti obdelave opisujejo, ima organizacija imenovane odgovorne osebe in pooblaščene osebe za obdelavo.

(3) Zaposleni iz prejšnjega odstavka zagotavljajo redno preverjanje ažuriranosti evidenc in njihov vpis v register evidenc.

(4) Vodstvo organizacije se vsaj enkrat letno seznani z ažuriranimi evidencami.

(5) Skupen register evidenc dejavnosti obdelave organizacije zagotavlja pravna služba. DPO ima možnost vpogleda v skupen register evidenc dejavnosti obdelave.

5. člen

(obveznost vključitve DPO in izvajanja ocene učinka)

(1) Posamezni oddelek v organizaciji je dolžan pred uvedbo projekta oz. ob planiranju vsakega projekta, v katerem se bodo ali bi se lahko obdelovali osebni podatki, zlasti pa ob projektih, ki uporabljajo nove tehnologije ali uvajajo nove obdelave osebnih podatkov, obvestiti vodstvo organizacije in pravno službo, ki morata pred izvedbo projekta zaprositi DPO za mnenje, ali je potrebno izdelati oceno učinka v zvezi z varstvom osebnih podatkov. V izjemnih primerih se lahko posamezni oddelek v zvezi s potrebnostjo izdelave ocene učinka obrne direktno na DPO.

(2) DPO mora podati zlasti mnenje o tem:

a. ali je potrebna izvedba ocene učinka v skladu s 35. členom Splošne uredbe oz. 87. členom ZVOP-2;
b. kakšna metodologija bo uporabljena za izvedbo ocene učinka;
c. ali naj se ocena učinka izvede interno ali naj se najame zunanjo strokovno pomoč;
d. katere ukrepe (vključno s tehničnimi in organizacijskimi) implementirati, da se zmanjšajo tveganja za varstvo osebnih podatkov;
e. ali je bila ocena učinka korektno izvedena in
f. ali so rezultati oziroma odločitve ocene učinka (npr. ali nadaljevati z obdelavo osebnih podatkov/projektom, o katerem je ocena učinka izvedena) skladni s Splošno uredbo.

(3) Odgovornost za (pravilno) izvedbo ocene učinka nosi upravljavec.

(4) Če se upravljavec ne strinja z mnenjem DPO, mora pisno utemeljiti, zakaj ni ali ne bo upošteval mnenja DPO.

6. člen

(uresničevanje pravic posameznikov)

(1) Organizacija je dolžna uresničevati pravice posameznikov skladno s poglavjem III Splošne uredbe in v skladu z ZVOP-2.

(2) 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 tako, mu organizacija nudi dostop do osebnih podatkov in informacije iz prvega odstavka 15. člena Splošne uredbe ter zagotavlja naslednje pravice, v kolikor je to v skladu s Splošno uredbo:

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

(3) Posameznik svojo zahtevo v skladu s 15.-21. členom Splošne uredbe vloži pri organizaciji na naslov Tehnološki park 18, SI-1000 Ljubljana, s pripisom »za pooblaščeno osebo za varstvo osebnih podatkov« ali na elektronski naslov: dpo@arnes.si.

(4) Dostop do lastnih osebnih podatkov in uveljavljanje pravic sta za posameznika brezplačna, vendar lahko organizacija zaračuna razumno plačilo, kadar so zahtevki očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo.

(5) V primeru, da iz zahteve ni mogoče identificirati posameznika, organizacija od posameznika zahteva dodatne informacije, ki nedvoumno potrdijo posameznikovo identiteto.

(6) Organizacija po preverjanju upravičenosti zahteve zagotovi odgovor posamezniku najkasneje v enem mesecu po prejemu zahteve. Ta rok se po potrebi podaljša za največ dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. O podaljšanju roka in o razlogih za zamudo organizacija obvesti posameznika. Odločitev organizacije mora vsebovati razloge in informacijo o pravici do pritožbe pri Informacijskem pooblaščencu v roku 15 dni od seznanitve z odločitvijo. Organizacija se po potrebi poveže z DPO, ki svetuje pri pripravi odgovora. Če se organizacija ne strinja z mnenjem DPO, mora pisno utemeljiti, zakaj mnenja DPO ne bo upoštevala.

(7) Zahtevo posameznika za uresničevanje njegovih pravic iz poglavja III Splošne uredbe lahko organizacija zavrne v primeru:

a. če posameznika ne more identificirati kot posameznika, kateremu pripadajo osebni podatki,
b. če niso izpolnjeni osnovni pogoji (npr. ker ne gre za osebne podatke),
c. če je zahteva očitno neutemeljena ali pretirana ali
d. če so v Splošni uredbi, ustavi, mednarodnih aktih ali področnih zakonih določene posebne izjeme.

(8) V primeru, da posameznik meni, da so njegove pravice kršene, se lahko za zaščito ali pomoč obrne na Informacijskega pooblaščenca.

7. člen

(snemanje dogodkov)

(1) Za namene dokumentiranja aktivnosti in obveščanja javnosti o delu in dogodkih v organizaciji, kot so prireditve, srečanja, tekmovanja, izobraževanja in podobno, lahko organizacija tak dogodek delno ali v celoti snema oziroma fotografira in izdelani material objavi na spletnih straneh, tiskovinah in družabnih omrežjih organizacije.

(2) Obvestilo o tem, da bo dogodek sneman oziroma fotografiran, se zapiše na vabilo oziroma na obvestilo o dogodku. Navede se tudi namen snemanja oziroma fotografiranja. Na ta način se šteje, da so udeleženci oziroma obiskovalci obveščeni o snemanju oziroma fotografiranju javnega dogodka.

(3) Kadar je to bolj primerno (ob dogodkih z manjšim številom udeleženih, dogodkih, ki niso odprti za javnost, udeleženci pa utemeljeno pričakujejo večjo stopnjo zasebnosti), se snemanje oziroma fotografiranje ustno napove in udeležencem pusti možnost, da izrazijo svojo voljo glede zajema njihove podobe s kamero.

## III. Pooblaščena oseba

8. člen

(imenovanje in vloga pooblaščene osebe)

(1) Odgovorna oseba organizacije imenuje pooblaščeno osebo za varstvo osebnih podatkov (DPO) s sklepom ali na drug primeren način (npr. s sklenitvijo pogodbe) v skladu s Splošno uredbo in zakonom, ki ureja osebne podatke in poskrbi za objavo informacij o pooblaščeni osebi na spletni strani organizacije.

(2) DPO pomaga izvajati bistvene elemente Splošne uredbe kot so:

a. načela obdelave osebnih podatkov,
b. pravice posameznikov,
c. varnost in evidence obdelave osebnih podatkov,
d. obveščanje o kršitvah obdelave osebnih podatkov.

(3) Organizacija zagotavlja, da je DPO ustrezno in pravočasno vključen v vse zadeve v zvezi z varstvom osebnih podatkov ter da so mu zagotovljena ustrezna sredstva, potrebna za kvalitetno opravljanje njegovih nalog ter da mu je omogočen dostop do osebnih podatkov in dejanj obdelave.

(4) DPO ni odgovoren za zagotavljanje skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter veljavno zakonodajo, ki ureja obdelavo in varstvo osebnih podatkov. Za zagotavljanje navedene skladnosti je na podlagi veljavne zakonodaje odgovorna organizacija oziroma odgovorna oseba organizacije.

9. člen

(naloge pooblaščene osebe)

(1) DPO opravlja zlasti naslednje naloge:

a. obvešča organizacijo o njenih obveznostih glede izvajanja določb Splošne uredbe in ostale veljavne zakonodaje na področju varstva osebnih podatkov ter internih aktov, ki urejajo obdelavo in varstvo osebnih podatkov,
b. spremlja skladnost varstva osebnih podatkov z veljavno zakonodajo ter internimi akti, vključno z dodeljevanjem nalog, svetovanjem zaposlenim v zvezi s pravilno obdelavo osebnih podatkov ter nadzorovanjem varstva osebnih podatkov v organizaciji,
c. svetuje pri izvedbi ocene učinka v zvezi varstvom podatkov in spremlja njeno izvajanje,
d. deluje kot kontaktna točka za Informacijskega pooblaščenca in sodeluje z Informacijskim pooblaščencem predvsem pri vprašanjih v zvezi z obdelavo osebnih podatkov, predhodnim posvetovanjem glede ocene učinka, kadar bi določena obdelava osebnih podatkov povzročila veliko tveganje ali pri katerikoli drugi zadevi v zvezi z varstvom osebnih podatkov,
e. obvešča Informacijskega pooblaščenca o kršitvah obdelav osebnih podatkov in sodeluje z njim glede odprave kršitev.

(2) DPO opravlja zgoraj navedene naloge iz prejšnjega odstavka tega člena v zvezi z vsemi obdelavami osebnih podatkov, ki jih izvaja organizacija.

(3) DPO je pri opravljanju svojih nalog dolžan varovati kot poslovno skrivnost vse podatke, s katerimi se seznani pri opravljanju svojih nalog.

10. člen

(neodvisnost pooblaščene osebe )

Organizacija zagotovi, da DPO pri opravljanju svojih nalog ne prejema nobenih navodil. DPO ne sme biti razrešen ali kaznovan zaradi opravljanja svojih nalog. DPO neposredno poroča odgovorni osebi organizacije.

## IV. Storitve, ki jih za organizacijo opravljajo druge pravne ali fizične osebe

11. člen

(obdelovalci)

(1) Z vsako pravno ali fizično osebo zunaj organizacije, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba ali drug pravni akt, ki vsebuje ali ima kot dodatek vključene navedbe, predvidene v tretjem odstavku 28. člena Splošne uredbe.

(2) Pravila prejšnjega odstavka veljajo tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, če imajo le-te dostop do osebnih podatkov.

(3) Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in določenega obsega vrste osebnih podatkov ter teh ne smejo obdelovati ali drugače uporabljati za noben drug namen. Zunanje pravne ali fizične osebe ne smejo pooblastiti drugega obdelovalca brez predhodnega pisnega dovoljenja organizacije, razen če je možnost prenosa na drugega obdelovalca opredeljena že v pogodbi med upravljavcem in prvotnim obdelovalcem.

(4) Pravna ali fizična oseba, ki za organizacijo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

12. člen

(skupni upravljavci)

(1) Če organizacija z drugimi pravnimi osebami za posamezne obdelave skupaj določi namene in načine obdelave, so v okviru tega pravilnika organizacija in druge pravne osebe skupni upravljavci za te obdelave.

(2) Skupni upravljavci na pregleden način z medsebojno pogodbo določijo dolžnosti vsake od njih z namenom izpolnjevanja obveznosti in skladno s pravili 26. člena Splošne uredbe.

13. člen

(nadzor nad pogodbami)

Vse pogodbe, ki se nanašajo na pogodbeno obdelavo osebnih podatkov in skupno upravljanje osebnih podatkov, ki jih sklene organizacija, se vpišejo v register pogodb, ki ga upravlja pravna služba. DPO ima možnost vpogleda v register pogodb.

## V. Odgovornost za izvajanje varnostnih ukrepov in postopkov

14. člen

(obveznosti organizacije)

(1) Organizacija redno obvešča zaposlene o pomenu in novostih s področja varstva osebnih podatkov in izvaja izobraževanja s tega področja.

15. člen

(določitev skrbnikov obdelav)

(1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov odgovorna oseba organizacije določi odgovorne osebe za posamezno obdelavo osebnih podatkov, ki so poučene in odgovarjajo za vsebino, namen in podlage posamezne obdelave (skrbniki obdelav – kot so navedeni v evidenci dejavnosti obdelav).

16. člen

(obveznost vseh zaposlenih)

(1) Vsak zaposleni, ki v imenu organizacije 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. Z osebnimi podatki, s katerimi se seznani pri svojem delu, mora ravnati vestno in skrbno, na način in po postopkih, ki jih določa ta pravilnik skupaj s povezanimi dokumenti.

(2) Pred nastopom dela mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in ga opozarja na posledice kršitve zaveze.

(3) Zaposleni lahko obdeluje le osebne podatke, ki jih potrebuje v zvezi z izvrševanjem svojih delovnih obveznosti.

(4) Obveznost varovanja osebnih podatkov, s katerimi se zaposleni pri delu seznani, traja tudi po prenehanju razmerja v organizaciji.

17. člen

(disciplinska odgovornost)

(1) Vsako neupoštevanje določil interne dokumentacije o informacijski varnosti ter navodil in postopkov varovanja informacij ali osebnih podatkov se šteje za kršitev delovnih obveznosti v skladu s predpisi in splošnimi akti, ki urejajo kršitve pogodbenih in drugih obveznosti iz delovnega razmerja.

(2) Za hujšo kršitev se šteje zlasti če zaposleni:

- nepooblaščeno sporoča osebne podatke, s katerimi se je seznanil pri svojem delu drugim osebam,
- nepooblaščeno izdela kopije nosilcev osebnih podatkov,
- nepooblaščeno popravlja, spreminja ali dopolnjuje osebne podatke,
- ne obvesti pooblaščene osebe o zlorabi osebnih podatkov ali o vdoru v zbirko osebnih podatkov.

(3) Odgovornost iz prejšnjih odstavkov ne izključuje kazenske, prekrškovne in/ali odškodninske odgovornosti.

18. člen

(vpogled v osebne podatke zaposlenih v izjemnih okoliščinah)

(1) Zaposleni, ki ima upravljavske pravice/dostop do storitve lahko na posebej utemeljeno pisno zahtevo odgovorne osebe organizacije v prisotnosti tričlanske 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 informacijske tehnologije (npr. v računalnik) ali druge elektronske ali komunikacijske storitve (npr. v elektronsko pošto) delavca le, če je to nujno potrebno za izpolnjevanje zakonskih obvez organizacije oziroma za vodenje delovnega procesa.

(2) Vpogled opravi tričlanska 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.

(3) Če se pojavi utemeljen sum, da zaposleni ne spoštuje določil interne dokumentacije o informacijski varnosti , lahko zaposleni, ki ima upravljavske pravice/dostop do storitve, na posebej utemeljeno pisno zahtevo odgovorne osebe organizacije 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.

(4) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je organizacija, lahko organizacija zahteva od operaterjev telekomunikacijskih storitev ali vzdrževalca hišne centrale le takrat, kadar pride med organizacijo in zaposlenim do kakršnegakoli spora glede višine stroškov porabe konkretnega telefonskega priključka.

## VI. Videonadzor

19. člen

(videonadzor)

(1) V organizaciji se sme videonadzor uvesti, če so izpolnjeni pogoji iz Splošne uredbe in 3. poglavja II. dela ZVOP-2.

(2) Podrobnosti o delovanju, upravljanju in nadzoru nad videonadzornim sistemom so urejene v Evidencah dejavnosti obdelave in v Pravilniku o izvajanju videonadzora.

## VII. Sprejem in posredovanje osebnih podatkov

20. člen

(sprejem in evidenca fizične pošte)

(1) Pravila glede sprejema in evidence poštnih pošiljk in pošiljk, ki na drug način prispejo v organizacijo (jih prinesejo stranke ali kurirji), so opredeljena v internem dokumentu, ki ureja postopke pri prejemu in oddaji pisemskih pošiljk.

21. člen

(prenos osebnih podatkov)

(1) 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.

(2) Osebni podatki se pošiljajo na način, da niso dostopni nepooblaščenim osebam. Osebni podatki, ki se posredujejo v fizični obliki, morajo biti posredovani v ovojnici. Ovojnica mora biti izdelana na takšen način, da ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

(3) Osebni podatki se lahko prenašajo po telekomunikacijskih omrežjih, pri čemer se v primeru občutljive narave osebnih podatkov in/ali večje količine osebnih podatkov le-ti zavarujejo s kriptografskimi metodami tako, da je zagotovljena nečitljivost med njihovim prenosom.

22. člen

(prenos posebnih vrst osebnih podatkov)

(1) Posebne vrste osebnih podatkov po 9. členu Splošne uredbe ali osebne podatke v zvezi s kazenskimi obsodbami in prekrški po 10. členu Splošne uredbe se poleg upoštevanja pravil prejšnjega odstavka fizično pošilja naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali priporočeno s povratnico.

(2) Posebne vrste osebnih podatkov se smejo prenašati preko telekomunikacijskih omrežij samo, če so posebej zavarovane s kriptografskimi metodami, tako da je zagotovljena neberljivost med njihovim prenosom.

(3) Za zagotavljanje integritete osebnih podatkov iz prejšnjega odstavka, se po potrebi in v okviru tehničnih možnosti pošiljatelja in prejemnika uporabi elektronski podpis.

23. člen

(posredovanje osebnih podatkov tretjim osebam)

(1) Organizacija posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam (tretja oseba), če je za posredovanje dana ustrezna pravna podlaga v skladu z zakonodajo, razen če drug zakon določa drugače. Osebni podatki se lahko posredujejo tudi tistim tretjim osebam, ki imajo privolitev (pooblastilo) posameznika, na katerega se osebni podatki nanašajo. Tretja oseba sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se ji posredujejo.

(2) Posredovanje osebnih podatkov mora tretja oseba zahtevati pisno. Zahteva mora vsebovati vse sestavine, kot jih določa zakonodaja, ki ureja varstvo osebnih podatkov. V kolikor je tretja oseba za posredovanje osebnih podatkov pridobila soglasje posameznika, mora biti k pisni zahtevi priložena privolitev (pooblastilo) posameznika, na katerega se osebni podatki nanašajo.

(3) Organizacija tretji osebi, če drug zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredovala. Organizacija in tretja oseba se lahko dogovorita za podaljšanje tega roka. Če organizacija v roku 15 dni ne posreduje podatkov oz. se rok ne podaljša, se šteje, da je zahteva zavrnjena.

(4) Za vsako posredovanje osebnih podatkov se zagotovi možnost poznejše ugotovitve kateri osebni podatki so bili posredovani, komu (osebno ime/firma ter naslov/sedež firme), kdaj (datum in ura posredovanja osebnih podatkov) in na kakšni podlagi ter za kateri namen oz. iz katerih razlogov oz. za potrebe katerega postopka.

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

24. člen

(prenos osebnih podatkov v tretje države ali mednarodne organizacije)

(1) Prenos osebnih podatkov v tretje države ali mednarodne organizacije je dovoljen pod pogoji, ki jih predvideva poglavje V Splošne uredbe.

(2) Pred nameravano obdelavo, ki bo ali bi lahko prenašala osebne podatke v tretjo državo ali mednarodno organizacijo, je obvezen posvet z DPO.

## VIII. Varovanje prostorov in računalniške opreme

25. člen

(1) 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.

(2) Varovanje prostorov in računalniške opreme je podrobneje opredeljeno v interni dokumentaciji o informacijski varnosti.

## IX. Varovanje sistemske in aplikativno programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo

26. člen

(1) Varovanje sistemske in aplikativno programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo je opredeljeno v interni dokumentaciji o informacijski varnosti.

## X. Ukrepanje ob sumu nepooblaščenega dostopa in obveščanje

27. člen

(ukrepanje ob sumu incidenta)

(1) Ob vsakem sumu vdora v informacijski sistem organizacije ali kakršnegakoli drugega varnostnega incidenta, ki vključuje ali bi lahko vključeval kršitev varstva osebnih podatkov (nepooblaščena obdelava, izpostavljenost osebnih podatkov…), se mora le-tega začeti preiskovati takoj, ko se zanj izve.

(2) Preiskovanje se izvaja skladno:

a. s tem Pravilnikom;
b. z interno dokumentacijo o informacijski varnosti.

28. člen

(zaznava in obveščanje o kršitvi)

(1) Zaposleni, ki izve ali opazi, da je prišlo do kršitve varstva osebnih podatkov ali do vdora v zbirko osebnih podatkov, mora o tem nemudoma obvestiti osebo, pooblaščeno za informacijsko varnost.

(2) Pooblaščena oseba za informacijsko varnost iz prejšnjega odstavka je po začetni triaži za morebitno kršitev varstva osebnih podatkov dolžna v najkrajšem možnem času sporočiti pravni službi in DPO.

(3) Obvestilo iz prejšnjega odstavka mora vsebovati podatke, potrebne za identifikacijo osebnih podatkov, katerih varstvo je bilo kršeno, kratek opis okoliščin, v katerih je prišlo do kršitve, ali je bil o kršitvi varstva obveščen zaposleni, ki je odgovoren za vodenje zbirke osebnih podatkov ter kateri ukrepi za preprečitev nadaljnjih kršitev varstva osebnih podatkov so bili izvedeni.

(4) V primeru, da je do kršitve varstva osebnih podatkov prišlo pri obdelovalcu, je ta dolžan najkasneje v roku 24 ur od seznanitve s kršitvijo pisno obvestiti organizacijo. Takšno določilo mora biti vključeno v vsako pogodbo o pogodbeni obdelavi, ki jo organizacija sklene z obdelovalcem po uveljavitvi tega pravilnika.

(5) Organizacija je dolžna zagotoviti vse ukrepe za preprečitev nadaljnjih kršitev varstva osebnih podatkov in ustrezno ukrepati zoper tistega, ki je namerno ali iz hude malomarnosti kršil varstvo osebnih podatkov. Obveznost iz tega odstavka veljajo tudi za obdelovalce in skupne upravljavce.

(6) Organizacija mora dokumentirati vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. To dokumentacijo je organizacija na zahtevo dolžna predložiti DPO ali Informacijskemu pooblaščencu.

(7) Vsi zaposleni, ki delajo na raziskavi incidenta ali so kakorkoli povezani z odpravljanjem posledic incidenta, morajo obveščati osebo, pooblaščeno za informacijsko varnost, po interno dogovorjenem postopku, slednja pa po potrebi DPO.

29. člen

(obveščanje nadzornega organa)

(1) V primeru zaznane kršitve varstva osebnih podatkov mora organizacija po posvetu z DPO najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvestiti Informacijskega pooblaščenca, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, skladno z določili 33. člena Splošne uredbe.

(2) Organizacija zagotovi vse potrebne podatke za obveščanje iz prejšnjega odstavka in s pomočjo DPO in drugih deležnikov izpolni obrazec obvestila o kršitvi.

(3) V primeru, ko informacij iz prvega odstavka tega člena Informacijskemu pooblaščencu ni mogoče sporočiti v celoti, se te sporočajo postopoma.

30. člen

(priglasitev incidenta po zakonu, ki ureja informacijsko varnost)

(1) V primeru kršitve varnosti osebnih podatkov, ki se nanaša na informacijski sistem iz prvega odstavka 23. člena ZVOP-2, se glede priglasitve incidenta smiselno uporabljajo določbe iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, v kolikor organizacija glede teh obdelav ni dolžna izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

(2) Organizacija je dolžna upoštevati določbe glede priglasitve incidenta iz zakona, ki ureja informacijsko varnost tudi za ostale kršitve varnosti osebnih podatkov, za katere je v zvezi z njihovo obdelavo dolžna izvajati ukrepe po zakonu, ki ureja informacijsko varnost.

31. člen

(obveščanje posameznikov)

(1) Organizacija mora v sodelovanju z DPO v okviru evalvacije incidenta oceniti, ali je verjetno, da je kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov in so s tem izpolnjeni pogoji za obveščanje posameznikov.

(2) V primeru, da so izpolnjeni pogoji za obveščanje posameznikov iz prejšnjega odstavka, mora organizacija nemudoma in brez nepotrebnega odlašanja sporočiti posameznikom, na katere se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

(3) Vsebino in način obveščanja posameznikov uskladita organizacija in DPO upoštevajoč določila 34. člena Splošne uredbe.

(4) Organizacija mora v dokumentaciji iz šestega odstavka 28. člena tega pravilnika zabeležiti vsa dejstva in razloge v zvezi z odločitvijo za obveščanje ali opustitev obveščanja posameznikov.

## XI. Brisanje podatkov

32. člen

(upoštevanje rokov hrambe)

(1) Po preteku roka hrambe ali namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače. Rok hrambe osebnih podatkov organizacija omeji na najkrajše možno obdobje in le dokler je hramba potrebna za dosego namena obdelave, zaradi katerega so se podatki zbrali ali nadalje obdelovali.

(2) Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz evidenc dejavnosti obdelave.

(3) Kjer so roki za izbris osebnih podatkov določeni v letih, rok za izbris začne teči s potekom koledarskega leta, v katerem je bila zadeva zaključena.

33. člen

(varno in zanesljivo uničevanje medijev)

(1) Za brisanje podatkov iz računalniških medijev ali informacijskih sistemov se uporabi takšna metoda brisanja ali anonimiziranja, da je nemogoča restavracija ali deanonimizacija vseh ali zgolj dela brisanih podatkov.

(2) Podatki na klasičnih medijih (listine, kartoteke, register, seznam ...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov (sežig, razrez ...). Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.). Zaposleni lahko sam uniči fizične dokumente, ki vsebujejo osebne podatke, če ne gre za dokumentarno ali arhivsko gradivo.

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

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

(5) Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje oseba iz oddelka, pooblaščenega s strani direktorja. Ta oseba po uničenju sestavi kratek zapis o načinu in temeljitosti uničenja.

## XII. Končne določbe

34. člen

(veljavnost pravilnika in prenehanje veljave starega)

(1) Konkretni postopki in ukrepi za varovanje osebnih podatkov, vodenih v zbirkah osebnih podatkov, s katerimi upravlja organizacija, so določeni v interni dokumentaciji o informacijski varnosti.

(2) Z dnem, ko je sprejet ta pravilnik, preneha veljati obstoječi Pravilnik o varstvu osebnih podatkov z dne 21.1.2019.

(3) Ta pravilnik stopi v veljavo z dnem sprejetja.