Pravilnik o zavarovanju osebnih podatkov

Društvo za stereologijo in kvantitativno analizo slike, Korytkova ulica 2, 1000 Ljubljana, matična številka: 5669910000, (v nadaljevanju: »**upravljavec**«) na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 s spremembami, v nadaljevanju: »**ZVOP-1**«) ter zlasti 24., 25. in 32. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: »**Splošna uredba o varstvu podatkov**«)

sprejema naslednji

Pravilnik o zavarovanju osebnih podatkov

I. Glede obdelave osebnih podatkov

1.člen

Upravljavec je društvo, ki se ukvarja z glavno dejavnostjo »dejavnost strokovnih združenj«, pri čemer obdelava osebnih podatkov upravljavca predstavlja zgolj postransko dejavnost.

Upravljavec izvaja predvsem naslednja dejanja obdelave osebnih podatkov:

- Obdelava osebnih podatkov, ki jih avtorji sami vnesejo preko spetnega obrazca,
- iskanje in beleženje osebnih podatkov recenzentov preko javno dostopnih informacij (osebnih spletnih strani raziskovalcev, kontaktni podatki objavljeni v znanstvenih objavah).

Upravljavec podatkov ne posreduje in ne iznaša v tretje države in/ali mednarodne organizacije.

Pri izvajanju navedenih dejavnosti upravljavec obdeluje naslednje osebne podatke:

- Ime in priimek,
- naziv,
- elektonski naslov,
- afiliacija,
- področje ekpertize,
- spol.

Upravljavec ne obdeluje posebnih vrst osebnih podatkov (t.i. občutljive osebne podatke), niti ne obdeluje osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

Osebne podatke upravljavec obdeluje na podlagi zakonitega interesa oziroma privolitve in sicer za naslednje namene:

- Uredniški proces (peer review),
- konkatiranje avtorjev in recenzentov,
- obveščanje o objavi prispevka.

2.člen

Za namen identifikacije in popisa vseh vrst osebnih podatkov, katere obdeluje upravljavec, se vodi Seznam evidenc dejavnosti obdelave osebnih podatkov (v nadaljevanju: »**Seznam evidenc**«), katerega namen je omogočiti popoln pregled nad tokom osebnih podatkov. Seznam evidenc je obenem podlaga za sprejem tehničnih, organizacijskih in kadrovskih ukrepov za zavarovanje osebnih podatkov, kot so opisani v tem Pravilniku o zavarovanju osebnih podatkov (v nadaljevanju: »**Pravilnik**«).

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

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

3.člen

Ob upoštevanju opisane narave, obsega, okoliščin in namena obdelave, upravljavec zaključuje, da obdelava podatkov ne predstavlja velikega tveganja za pravice in svoboščine posameznikov, zato priprava predhodne ocene učinka v zvezi z obdelavo podatkov ni potrebna.

Pred vsako novo obdelavo osebnih podatkov, zlasti pa pred uporabo novih tehnologij ter pred vsako spremembo narave, obsega, okoliščin in namenov obdelave, ter vedno, ko se spremeni tveganje, ki ga predstavljajo dejanja obdelave, se upravljavec zaveže ponovno opraviti pregled tveganj in oceniti, ali je v zvezi z obdelavo potrebno pripraviti oceno učinka.

II. Splošne določbe

4.člen

S tem Pravilnikom se določajo tehnični, organizacijski in kadrovski postopki in ukrepi za zavarovanje osebnih podatkov upravljavca, z namenom, da se izpolnijo zakonske zahteve glede varovanja osebnih podatkov in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

Ti ukrepi sestojijo iz zavezujočih pravil, priporočil oziroma načel iz prakse, internih postopkov, organizacijskih struktur in varnosti informacijske tehnologije.

5.člen

Namen tega Pravilnika je zagotoviti zaupnost, celovitost, dostopnost in točnost osebnih podatkov, ki se obdelujejo. Vsi sodelavci se morajo zavedati tveganj, ki so povezana s tehničnimi in informacijskimi sistemi ter komunikacijsko tehnologijo, ter morajo zato izvajati obdelavo osebnih podatkov z zahtevano skrbnostjo.

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

6.člen

Upravljavec se ravna po priznanih pravilih za varnost informacij.

Poleg izkušenj iz prakse, upravljavec pri zagotavljanju varnosti informacijske tehnologije sledi naslednjim standardom:

- Arnes strežnik varna povezava TLS,
- strežnik za prihajajočo pošto, IMAP-strežnik, z varno povezavo SSL.

7.člen

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

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

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

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

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

8.člen

Ta Pravilnik velja za vse člane društva, urednika, recenzente in avtorje prispevkov pri upravljavcu, ne glede na to, ali so še aktivni pri upravljavcu (v nadaljevanju »**sodelavci**«).

9.člen

V tem Pravilniku uporabljeni izrazi imajo pomene kot to izhaja iz veljavnega ZVOP-1 ter Splošne uredbe o varstvu podatkov.

III.Kadrovski ukrepi

10.člen

Naloge in pristojnosti glede obdelave osebnih podatkov, ki so si med seboj v konfliktu, so dodeljene različnim osebam ali oddelkom; vse z namenom, da se v najkrajšem možnem času prepoznajo nepooblaščene ali nenamerne spremembe podatkov.

Velja naslednje ločevanje vlog in nalog:

- namene obdelave osebnih podatkov določa uredniški odbor upravljalca;
- pristojnost za določitev sredstev informacijske tehnologije ali operativne procese je dodeljena tehničnim urednikom,
- za varnost podatkov in za zagotovitev tehničnih, kadrovskih in organizacijskih ukrepov je zadolžen predsednik društva,
- dostop do osebnih podatkov imajo naslednje osebe: predsednik društva in uredniki.

Za pravilno izvajanje tega Pravilnika je dokončno pristojen in odgovoren predsednik društva (upravljavca).

11.člen

Ker obdelava osebnih podatkov pri upravljavcu ne zajema rednega in sistematičnega obsežnega spremljanja posameznikov in ker upravljavec ne obdeluje posebnih vrst osebnih podatkov in/ali podatkov v zvezi s kazenskimi obsodbami in prekrški, upravljavec ne bo imenoval posebne pooblaščene osebe za varstvo podatkov.

12.člen

Vsi delavci, ki ukrepajo pod vodstvom upravljavca in imajo dostop do osebnih podatkov, teh podatkov ne smejo obdelovati brez ali izven navodil upravljavca. Vsi delavci, ki pri svojem delu obdelujejo osebne podatke, so dolžni izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere so zvedeli oziroma bili z njimi seznanjen pri opravljanju svojega dela.

Obveza varovanja podatkov ne preneha s prenehanjem sodelovanja.

Vsi sodelavci, ki pri svojem delu obdelujejo osebne podatke, morajo biti seznanjeni z zakonodajo s področja varstva osebnih podatkov ter z vsebino tega Pravilnika.

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

Za kršitev določil iz tega člena so sodelavci disciplinsko, odškodninsko in kazensko odgovorni.

IV. Fizična in okoljska varnost

13.člen

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

Prostori, kjer se nahajajo osebnih podatki, njihove kopije in informacijski sistemi, morajo biti ognjevarni (gasilni aparati, požarni senzor), zavarovani proti izlitjem vode, poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjeni.

Vsi informacijski sistemi, ki so kritični za upravljavca, se morajo postaviti v varno okolje. To pomeni, da so vsi prostori, v katerih se nahajajo nosilci osebnih podatkov ter strojna in programska oprema, fizično varovani (npr. zaklenjeni, pospravljeni v sef idr.), tako da se nepooblaščenim osebam prepreči dostop do podatkov.

Taki varovani prostori oziroma stavba kot celota, kjer se shranjujejo osebni podatki, so opremljeni z napravo za javljanje vlomov in videonadzorom ali s fizično prisotnostjo varnostnika. Na podlagi takih ukrepov je možno sprožiti alarm in zavarovati dokaze.

14.člen

Osebni podatki se ne smejo hraniti izven varovanih prostorov.

V. Varovanje integritete in zaupnosti podatkov ob sprejemu in prenosu

15.člen

Osebne podatke se prenašajo z informacijskimi, telekomunikacijskimi in drugimi sredstvi ob izvajanju ustreznih postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

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

- Strežnik za prihajajočo pošto, POP3-strežnik z varno povezavo SSL,
- strežnik za odhajajočo pošto, SMTP-strežnik, z varno povezavo SSL (SMTP over SSL) – s SMTP-avtentikacijo,
- strežnik za odhajajočo pošto, SMTP-strežnik, z varno povezavo TLS (mail submission port) – s SMTP-avtentikacijo,
- strežnik za prihajajočo pošto, IMAP-strežnik, z varno povezavo SSL.

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

16.člen

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

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

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

17.člen

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

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

18.člen

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

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

19.člen

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

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

VII.Redno testiranje, ocenjevanje in vrednotenje ukrepov

20.člen

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

Upravljavec bo v ta namen vsaj enkrat letno preveril zakonitost obdelave osebnih podatkov.

VIII.Rok hrambe in brisanje podatkov

21.člen

Upravljavec zagotavlja, da je obdobje hrambe osebnih podatkov omejeno na najkrajše mogoče obdobje.

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

22.člen

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

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

23.člen

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

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

obdelovalce, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

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

X.Poročanje v primeru varnostnega incidenta

24.člen

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

V ta namen upravljavec zagotovi informacijski sistem, ki je sposoben izvajati nadzor za prepoznavanje dogodkov (npr. požarni zid, zaznavanje vdorov, sistem nadzora). Informacijski sistemi nadalje omogočajo dokumentiranje vseh varnostno relevantnih ali sistemsko kritičnih dogodkov.

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

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

25.člen

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

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

XI. Končne določbe

26. člen

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

27. člen

Pravilnik začne veljati osmi (8.) dan potem, ko ga predsednik društva sprejme in objavi.

Pravilnik se objavi na pri upravljavcu običajen način, in sicer se objavi na internetni strani https://www.ias-iss.org/ojs/IAS/about/editorialPolicies#custom-5 tako da se z njegovo vsebino lahko seznanijo vsi sodelavci in avtorji prispevkov pri upravljavcu.

V Ljubljani, dne 20. marec 2023

Marko Kreft, predsednik Društva za stereologijo
in kvantitativno analizo slike