



ZDRUŽENJE EPEKA, SO. P.

PRAVILNIK O VARSTVU OSEBNIH PODATKOV IN INFORMACIJSKI VARNOSTI

Na podlagi Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta (Splošna uredba o varstvu podatkov – GDPR), Zakona o varstvu osebnih podatkov (ZVOP-2) in drugih veljavnih predpisov s področja varstva osebnih podatkov Znanstveno-raziskovalno združenje za umetnost, kulturne in izobraževalne programe in tehnologijo EPEKA, socialno podjetje (v nadaljevanju: združenje ali EPEKA), sprejema naslednji pravilnik.





I. SPLOŠNE DOLOČBE

1. člen

(predmet in namen)

- (1) Ta pravilnik določa načela, odgovornosti, organizacijske in tehnične ukrepe ter postopke za zakonito, pošteno, pregledno in varno obdelavo osebnih podatkov pri EPEKI.
- (2) Pravilnik zajema zbiranje, evidentiranje, uporabo, vpogled, posredovanje, shranjevanje, popravljanje, izbris in drugo obdelavo osebnih podatkov v fizični ali elektronski obliki ter zagotavljanje informacijske varnosti.
- (3) Namen pravilnika je varovati pravice in svoboščine posameznikov, zlasti uporabnikov programov, beguncev, prosilcev za mednarodno zaščito, oseb z začasno zaščito, otrok, drugih oseb s posebnimi potrebami, zaposlenih, prostovoljcev, članov in pogodbenih sodelavcev.

2. člen

(pravni okvir in razmerje do drugih pravil)

- (1) EPEKA pri obdelavi osebnih podatkov upošteva GDPR, ZVOP-2 v vsakokrat veljavnem besedilu, veljavno področno zakonodajo ter posebne zahteve financerjev in pogodbenih partnerjev, če so skladne z zakonodajo.
- (2) V primeru neskladja določb tega pravilnika s prisilnimi predpisi se uporabljajo veljavni predpisi. Posebni projektni postopki lahko določijo strožje varovalke, ne smejo pa zmanjšati zakonsko zagotovljenega varstva.
- (3) Pravilnik ne nadomešča obvestil posameznikom, pogodb o obdelavi, evidenc dejavnosti obdelave, varnostnih ocen ali dokumentov, ki jih predpisujejo posamezni financerji.

3. člen

(uporaba in zavezanost)

- (1) Pravilnik zavezuje zaposlene, organe združenja, prostovoljce, praktikante, zunanje sodelavce in druge osebe, ki za EPEKO dostopajo do osebnih podatkov.
- (2) Osebe iz prejšnjega odstavka obdelujejo osebne podatke samo v okviru nalog, pooblastil in dokumentiranih navodil; zaveza zaupnosti traja tudi po prenehanju sodelovanja.
- (3) Zunanji pogodbeni obdelovalci morajo izpolnjevati pogodbeno dogovorjene zahteve, ki so skladne z GDPR in tem pravilnikom.

4. člen

(pomen izrazov)

- (1) Izrazi osebni podatek, obdelava, upravljavec, obdelovalec, posameznik, privolitev, posebne vrste osebnih podatkov, kršitev varnosti osebnih podatkov in drugi izrazi imajo pomen iz GDPR ter ZVOP-2.
- (2) Za posebne vrste podatkov se štejejo podatki iz člena 9 GDPR; podatki o kazenskih obsodbah in prekrških se obravnavajo posebej v skladu s členom 10 GDPR in nacionalnimi predpisi.
- (3) Informacijski incident pomeni dogodek, ki lahko ogrozi zaupnost, celovitost ali razpoložljivost informacij; ni vsak informacijski incident tudi kršitev varnosti osebnih podatkov.



II. NAČELA IN ZAKONITE PODLAGE OBDELAVE

5. člen (temeljna načela)

- (1) Osebni podatki se obdelujejo zakonito, pošteno in pregledno, za določene, izrecne in zakonite namene ter v najmanjšem obsegu, ki je potreben za doseg teh namenov.
- (2) EPEKA skrbi za točnost podatkov, omejitev hrambe, celovitost in zaupnost ter za dokazljivost skladnosti z načeli iz člena 5 GDPR.
- (3) Pri načrtovanju dejavnosti se uporabljata načeli vgrajenega in privzetega varstva podatkov (člen 25 GDPR).

6. člen (ugotavljanje pravne podlage)

- (1) Za vsako dejavnost obdelave mora biti pred začetkom določena in dokumentirana ustrezna pravna podlaga iz člena 6(1) GDPR. Pravna podlaga se določi glede na konkretni namen in ni nujno enaka za vse aktivnosti istega programa.
- (2) Kadar se obdelujejo posebne vrste osebnih podatkov, se poleg ustrezne podlage iz člena 6 GDPR zagotovi tudi veljavna izjema iz člena 9(2) GDPR oziroma druga zahtevana pravna podlaga. Obdelava podatkov iz člena 10 GDPR je dovoljena le pod pogoji, določenimi z zakonodajo.
- (3) Privolitev se uporablja le, če je prostovoljna, konkretna, informirana in nedvoumna, pri posebnih vrstah podatkov pa izrecna, kadar jo zahteva zakon. Zavrnitev ali preklic privolitve ne smeta povzročiti neupravičene izgube storitev, ki niso odvisne od te privolitve.
- (4) Če obdelava temelji na zakonitem interesu, EPEKA po potrebi pripravi in hrani dokumentirano presojo tehtanja interesov; pri projektih z ranljivimi posamezniki je potrebna posebna previdnost.

7. člen (obdelava pri programih in projektih)

- (1) EPEKA obdeluje osebne podatke samo v obsegu, ki je potreben za organiziranje in izvajanje programov, svetovanje, pomoč pri vključevanju, projektno spremljanje, izpolnjevanje zakonitih obveznosti, dokazovanje upravičenih stroškov ter druge dokumentirane namene.
- (2) Pri programih za begunce, osebe z mednarodno ali začasno zaščito in druge osebe s posebnimi potrebami se podatki o statusu, zdravju, družinskih razmerah, izkušnjah nasilja ali drugih tveganjih zbirajo zgolj, kadar so nujni, sorazmerni in zakonito utemeljeni.
- (3) Kjer je mogoče, se za statistiko in poročanje uporabljajo agregirani ali nepovratno anonimizirani podatki; psevdonimizirani podatki se še vedno obravnavajo kot osebni podatki.

8. člen (otroci in druge ranljive osebe)

- (1) Pri podatkih otrok ter oseb, ki zaradi starosti, jezika, invalidnosti, položaja ali drugih okoliščin težje uveljavljajo pravice, EPEKA zagotovi dodatna pojasnila in primerne varovalke.
- (2) Obvestila se po potrebi prilagodijo jeziku, stopnji razumevanja in dostopnosti. Obdelava podatkov otrok temelji na ustrezni pravni podlagi; kadar je potrebna privolitev starša ali zakonitega zastopnika, se pridobi v zakonsko zahtevanem obsegu.

(3) Občutljivi zapisi o posameznih primerih se obravnavajo ločeno od splošnih evidenc udeležbe in so dostopni samo posebej pooblaščenim osebam.

9. člen

(fotografije, posnetki in objave)

(1) Pred fotografiranjem, snemanjem, objavo ali drugo prepoznavno uporabo podobe posameznika se preveri namen in ustrezna pravna podlaga; za promocijske objave se po potrebi pridobi ločena, informirana privolitev.

(2) Pri otrocih, prosilcih za mednarodno zaščito, žrtvah nasilja in drugih ogroženih posameznikih je treba pred objavo izvesti dodatno presojo tveganj; privolitev sama po sebi ne odpravlja potrebe po zaščiti oseb in varovanju njihove identitete.

(3) Za gradiva, namenjena javnosti, se prednostno uporabljajo neprepoznavne ali ustrezno anonimizirane upodobitve, kadar bi prepoznavnost lahko povečala tveganje za posameznika.

III. ODGOVORNOSTI IN ORGANIZACIJSKO UPRAVLJANJE

10. člen

(odgovornost upravljavca)

(1) EPEKA je upravljavec osebnih podatkov, kadar sama določa namene in sredstva obdelave; kadar skupaj z drugim subjektom določa namene in sredstva, se razmerje med skupnimi upravljavci uredi v skladu s členom 26 GDPR.

(2) Pristojni organ združenja zagotavlja potrebna sredstva, jasno razdelitev nalog, spremljanje izvajanja ukrepov in sprejem ustreznih odločitev ob tveganjih ter varnostnih incidentih.

(3) Projektni vodje odgovarjajo za to, da se pri projektih pred zbiranjem podatkov preverijo nameni, pravne podlage, potrebni podatki, roki hrambe, prejemniki in dostopi.

11. člen

(pooblaščenca oseba za varstvo podatkov)

(1) EPEKA ima imenovano pooblaščenca osebo za varstvo podatkov (DPO). Imenovanje, pristojnosti in kontaktni podatki so razvidni iz ločenega sklepa o imenovanju, ki se hrani v notranji dokumentaciji združenja.

(2) DPO neodvisno svetuje, spremlja skladnost, sodeluje pri ozaveščanju ter svetuje o ocenah učinka; v primerih, določenih s predpisi, nastopa kot kontaktna točka posameznikov in Informacijskega pooblaščenca.

(3) EPEKA zagotavlja ustrezen položaj DPO in preprečuje nasprotje interesov. Kontaktne podatke DPO javno objavi ter jih skupaj z zahtevanimi podatki sporoči Informacijskemu pooblaščenca najpozneje v osmih dneh od imenovanja skladno s 45. členom ZVOP-2.

12. člen

(odgovorna oseba za informacijsko varnost)

(1) Za koordinacijo informacijske varnosti EPEKA določi notranjo odgovorno osebo oziroma sodelavca, ki organizira izvedbo tehničnih ukrepov, koordinira odpravo ranljivosti in vodi ustrezne evidence incidentov.

(2) Naloge odgovorne osebe za informacijsko varnost in njeni kontaktni podatki se opredelijo z internim sklepom ali pooblastilom; pristojnosti DPO in operativne odgovornosti za informacijsko varnost morajo biti jasno razmejene.

(3) Pri večjih incidentih odgovorna oseba za informacijsko varnost nemudoma obvesti odgovorno osebo združenja in DPO.

13. člen

(usposabljanje, pooblastila in zaupnost)

(1) EPEKA zaposlene, prostovoljce in sodelavce pred prvim dostopom do osebnih podatkov seznani z njihovimi obveznostmi ter jim zagotovi ustrezno uvaljalno usposabljanje s področja varstva podatkov in informacijske varnosti.

(2) Znanje se ob pomembnih spremembah nalog, sistema ali pravil osveži; izvedena usposabljanja se v primernem obsegu evidentirajo.

(3) Vsaka oseba z dostopom do osebnih podatkov podpiše izjavo o **zaupnosti** (Priloga 1) oziroma enakovredno pogodbeno zavezo.

14. člen

(evidenca dejavnosti obdelave)

(1) EPEKA vodi in **redno** posodablja evidenco dejavnosti obdelave v skladu s členom 30 GDPR za obdelave, za katere velja obveznost evidentiranja; zaradi odgovornosti in raznolikosti projektov jo vodi tudi kot notranje orodje za pregled najpomembnejših obdelav.

(2) Evidenca vključuje zahtevane podatke iz člena 30 GDPR, zlasti namene obdelave, kategorije posameznikov in osebnih podatkov, prejemnike, morebitne prenose v tretje države, predvidene roke hrambe in splošen opis varnostnih ukrepov. Vodi se v pregledni elektronski ali drugi ustrezni obliki, ki omogoča posodabljanje.

(3) Za ažurnost posameznih projektnih vnosov skrbi vodja projekta, za skupno evidenco pa imenovana oseba po posvetovanju z DPO.

IV. OBVEŠČANJE POSAMEZNIKOV IN NJIHOVE PRAVICE

15. člen

(pregledne informacije posameznikom)

(1) Ob zbiranju podatkov EPEKA posamezniku zagotovi informacije po členih 13 oziroma 14 GDPR, zlasti identiteto upravljavca, kontakt DPO, namen in pravno podlago, uporabnike, morebitne prenose v tretje države, rok hrambe, pravice posameznika in način vložitve pritožbe.

(2) Obvestila se pripravijo jasno, razumljivo in dostopno, po potrebi v drugih jezikih, ustno s tolmačenjem ali v primerni prilagojeni obliki. EPEKA za posamezne programe pripravi kratka, vsebinsko prilagojena obvestila, ki vsebujejo informacije iz členov 13 oziroma 14 GDPR.

(3) Obvestilo o obdelavi osebnih podatkov ni enakovredno izjavi o privolitvi; kadar je podlaga drugačna od privolitve, se tega ne predstavlja kot soglasje, ki ga mora posameznik podpisati.



16. člen
(pravice posameznika)

- (1) Posameznik lahko pod pogoji GDPR zahteva dostop do podatkov, njihov popravek ali izbris, omejitev obdelave, prenosljivost podatkov, ugovarja obdelavi ter ne želi biti predmet odločitve, ki temelji izključno na avtomatizirani obdelavi, kadar GDPR zagotavlja ustrezne pravice.
- (2) Posameznik lahko kadarkoli prekliče privolitev za prihodnjo obdelavo, ne da bi to vplivalo na zakonitost obdelave pred preklicem.
- (3) Posameznik ima pravico vložiti pritožbo pri Informacijskem pooblaščenцу Republike Slovenije; informacije o možnosti pritožbe se navedejo v obvestilu o obdelavi.

17. člen
(postopek obravnave zahtev)

- (1) Zahteve se sprejemajo osebno, pisno ali po elektronski poti na uradnem kontaktnem naslovu združenja oziroma DPO. Prejemnik zahtevo brez odlašanja posreduje DPO ali pristojni osebi ter jo evidentira.
- (2) EPEKA na zahtevo odgovori brez nepotrebnega odlašanja in praviloma najpozneje v enem mesecu od njenega prejema; kadar je glede na zapletenost ali število zahtev to potrebno, se rok lahko podaljša za največ dva dodatna meseca ob pravočasnem obvestilu posamezniku.
- (3) Identiteta vlagatelja se preverja sorazmerno in samo v potrebnem obsegu. Če EPEKA zahteve ne izpolni, pojasni razloge in pravna sredstva; obravnava praviloma poteka brezplačno, razen zakonsko dovoljenih izjem.
- (4) O prejetih zahtevah se vodi preprosta varovana evidenca, ki vsebuje najmanj datum prejema, vrsto zahteve, odgovorno osebo, datum in način odgovora ter izid obravnave. Poseben predpisan obrazec ni potreben.

V. POSREDOVANJE PODATKOV IN POGODBENA RAZMERJA

18. člen
(notranje in zunanje razkritje podatkov)

- (1) Podatki se v združenju posredujejo samo osebam, ki jih zaradi konkretnih nalog potrebujejo in imajo odobren dostop. Razkritje zunanjim prejemnikom se izvede samo na dokumentirani pravni podlagi in v najmanjšem potrebnem obsegu.
- (2) Pred razkritjem se preverijo identiteta prejemnika, njegov pravni položaj in namen, pravna podlaga, obseg podatkov in ustreznost varnega načina prenosa; po potrebi se vodi zapis o posredovanju.
- (3) Podatkov se ne pošilja na osebne elektronske naslove ali račune za shranjevanje, če za to ni odobritve in ustreznih varoval.

19. člen
(poročanje financerjem in nadzor)

- (1) Pri poročanju financerjem, javnim organom in nadzornim institucijam EPEKA pred vsakim razkritjem preveri, ali obveznost izhaja iz zakona, zakonitega postopka, veljavne projektne oziroma pogodbene podlage ali drugega ustreznega razloga po GDPR.



(2) Če pogodba zahteva liste prisotnosti ali druge podatke o udeležencih, vodja projekta skupaj z DPO preveri konkretni obseg zahteve in v evidenci obdelav zabeleži ustrezno pravno podlago; pogodba sama po sebi ne ustvari pravne podlage po členu 6(1)(c) GDPR.

(3) Prednost imajo zbirni in anonimizirani podatki, kjer ti zadoščajo za izkazovanje rezultatov. Če je nujno posredovanje imen, podpisov ali drugih podatkov, se posameznike o takem posredovanju pravočasno in razumljivo obvesti.

20. člen (pogodbeni obdelovalci)

(1) Pri uporabi zunanjih ponudnikov IT-storitev, oblaka, računovodstva ali drugih izvajalcev, ki obdelujejo osebne podatke v imenu EPEKE, se pred začetkom obdelave preverijo varovalke in sklene pogodba oziroma drug pravni akt iz člena 28(3) GDPR.

(2) Pogodba uredi predmet, trajanje, naravo in namen obdelave, vrste podatkov, kategorije posameznikov, dokumentirana navodila, zaupnost, varnostne ukrepe, pod-obdelovalce, sodelovanje pri pravicah in incidentih, revizije ter vrnitev ali izbris podatkov.

(3) Za obdelavo zunaj EGP se poleg člena 28 GDPR preverijo tudi pogoji mednarodnih prenosov po poglavju V GDPR.

21. člen (partnerstva in razmerja med upravljavci)

(1) Pri sodelovanju v projektih se za vsakega partnerja preveri, ali nastopa kot samostojni upravljavec, skupni upravljavec ali obdelovalec; odgovornosti se dokumentirajo pred izmenjavo osebnih podatkov.

(2) Kadar EPEKA z drugimi organizacijami izmenjuje podatke kot samostojni upravljavec (controller-to-controller; C2C), samostojno odgovarja za zakonitost svojih obdelav, ustrezno obveščanje posameznikov in varnost osebnih podatkov.

(3) Pri izmenjavi podatkov z organizacijami ali službami zunaj EGP se preverijo pravne podlage, morebitni mednarodni prenos in ustrezni zaščitni ukrepi; enako velja za projektne digitalne platforme.

VI. ZAVAROVANJE FIZIČNIH DOKUMENTOV IN PROSTOROV

22. člen (varovani prostori)

(1) Prostori, omare in druga mesta, kjer se hranijo osebni podatki, so varovani pred dostopom nepooblaščenih oseb. Dokumentacija se hrani v zaklenjenih omarah oziroma ustrezno zaščiteneh prostorih.

(2) Obiskovalci se v prostorih z dostopom do osebnih podatkov ne zadržujejo brez spremljanja; dokumenti in zasloni morajo biti nameščeni tako, da vsebina ni vidna nepooblaščenim.

(3) Uporablja se načelo čiste mize in zaklenjenega zaslona, zlasti v prostorih, kjer potekajo individualna svetovanja, obravnave primerov ali delo z občutljivimi osebnimi podatki.

23. člen

(papirna dokumentacija in delo na terenu)

- (1) Liste prisotnosti, prijavne obrazce, osebne dosjeje in drugo papirno dokumentacijo lahko na terenu prevzame samo pooblaščen oseb, ki skrbi za njihovo varno hrambo in prenos.
- (2) Pri prevozu in začasni hrambi dokumentov se uporabljajo zaprte mape, varovane torbe ali primerljivi ukrepi; dokumentov se ne pušča brez nadzora v vozilih, javnih prostorih ali na delovnih mizah.
- (3) Zapisniki svetovanj se oblikujejo s čim manj identificirajočimi podatki, kadar polna identifikacija ni potrebna.

24. člen

(uničevanje papirnih nosilcev)

- (1) Po izteku roka hrambe, če ni druge zakonite podlage za hrambo, se papirna dokumentacija varno uniči tako, da podatkov ni mogoče obnoviti ali razbrati.
- (2) Zaupna dokumentacija se ne odlaga v običajne koše za odpadni papir; za organizirano uničenje pri zunanjem izvajalcu je treba zagotoviti ustrezno pogodbeno zavezo in dokazljivost izvajanja.

VII. INFORMACIJSKA VARNOST IN DIGITALNA OBDELAVA

25. člen

(varnostni ukrepi glede na tveganja)

- (1) EPEKA na podlagi ocene tveganj izvaja ustrezne tehnične in organizacijske ukrepe iz člena 32 GDPR za zaščito zaupnosti, celovitosti, razpoložljivosti in odpornosti informacijskih sistemov ter za sposobnost obnovitve podatkov po incidentu.
- (2) Ukrepi med drugim vključujejo upravljanje dostopa, protivirusno zaščito, posodobitve, varnostne kopije, po potrebi šifriranje in psevdonimizacijo, obvladovanje incidentov in periodično preverjanje učinkovitosti.
- (3) Varnostne zahteve veljajo tudi za delo na daljavo, uporabo prenosnih naprav in projektne platforme.

26. člen

(dostopne pravice in uporabniški računi)

- (1) Vsaka oseba uporablja lasten, njej dodeljen uporabniški račun; skupni računi so dovoljeni le izjemoma, kadar jih ni mogoče nadomestiti in so uvedeni dodatni ukrepi sledljivosti.
- (2) Pravice dostopa se dodelijo po načelu najmanjših privilegijev, ob nastopu dela in ob spremembi nalog pa se dokumentirano odobrijo oziroma prilagodijo.
- (3) Ob prenehanju sodelovanja se dostopi nemudoma oziroma najpozneje do zaključka zadnjega delovnega dne onemogočijo, službene naprave, ključi in nosilci vrnejo, pooblastila pa pregledajo.

27. člen

(gesla in večfaktorska avtentikacija)

- (1) Uporabljajo se unikatna, dovolj dolga in varna gesla; gesel ni dovoljeno deliti ali hraniti v nezaščiteni obliki. Ob sumu razkritja je potrebna takojšnja zamenjava.

(2) Za oblačne storitve, elektronsko pošto, oddaljene dostope in račune z večjimi privilegiji se kjer je mogoče uvede večfaktorska avtentikacija (MFA), kjer jo storitev omogoča oziroma kjer je glede na tveganje potrebna. Odstopanja morajo biti ocenjena, dokumentirana in ustrezno zavarovana.

(3) Priporoča se uporaba odobrenega upravljalnika gesel. Privilegirani dostopi se dodelijo posebej in se uporabljajo le za administrativne naloge.

28. člen

(posodobitve in zaščita naprav)

(1) Na delovnih napravah se uporabljajo podprti operacijski sistemi in aplikacije; varnostne posodobitve se nameščajo pravočasno glede na oceno tveganja.

(2) Na napravah se uporablja ustrezna protivirusna oziroma druga zaščita pred škodljivo programsko opremo ter požarni zid. Nameščanje neodobrene ali nelicencirane programske opreme ni dovoljeno.

(3) Prenosne naprave, na katerih se hranijo občutljivi osebni podatki, morajo biti dodatno zaščitene; uporabi se šifriranje diska ali enakovreden ukrep, kjer je to ustrezno in tehnično izvedljivo, ob tveganjih pa se uvedejo strožje omejitve lokalnega shranjevanja.

29. člen

(oblačne storitve in shranjevanje)

(1) Oblačne storitve za hranjenje osebnih podatkov se uporabljajo le po predhodni odobritvi odgovorne osebe in pregledu pogodbenih, varnostnih ter čezmejnih vidikov.

(2) EPEKA dokumentira uporabljene ponudnike, lokacije shranjevanja oziroma prenosa podatkov, uporabniške dostopne pravice, varnostne funkcije in roke hrambe; osebnih podatkov projektov ni dovoljeno samovoljno kopirati v osebne oblačne račune.

(3) Za posebej občutljive projektne podatke se določi varna struktura map in pravice dostopa; deljenje prek javnih povezav se privzeto onemogoči, razen če je izrecno odobreno z ustreznimi omejitvami.

30. člen

(elektronska pošta in komunikacija)

(1) Elektronska sporočila z osebnimi podatki se pošiljajo samo preverjenim naslovnikom in v najmanjšem potrebnem obsegu; pred pošiljanjem več prejemnikom se preveri uporaba skrite kopije, kadar je potrebna za varovanje identitete prejemnikov.

(2) Za dokumente z večjim tveganjem se uporabljajo odobreni varni načini izmenjave, po potrebi zaščitene datoteke z ločeno posredovanim geslom ali enakovredni ukrepi.

(3) Komunikacijske aplikacije in zasebne naprave se smejo uporabljati za obdelavo osebnih podatkov samo v skladu z odobrenimi pravili, z nadzorom dostopa, omejitvami hrambe in varnostnimi nastavitvami; posebni podatki o primerih se ne pošiljajo v nezaščitene skupinske pogovore.

31. člen

(varnostne kopije in obnovitev)

(1) EPEKA zagotavlja periodično izdelavo varnostnih kopij bistvenih podatkov in storitev glede na poslovno potrebo, projektne obveznosti ter oceno tveganj.

(2) Varnostne kopije se zaščitijo pred nepooblaščenim dostopom, nenamernimi spremembami in izgubo; najmanj občasno se preveri možnost obnovitve.

(3) Roki hrambe varnostnih kopij, odgovornosti za izdelavo in postopek obnove se zapišejo v ustrezna interna IT-navodila.

32. člen

(evidentiranje in redno preverjanje)

(1) Kjer je tehnično mogoče in sorazmerno, se vzpostavi beleženje varnostno pomembnih dogodkov, kot so administrativni dostopi, neuspešni poskusi prijave in pomembnejše spremembe dovoljenj.

(2) EPEKA najmanj enkrat letno in ob večjih spremembah sistemov oziroma ob večjih incidentih pregleda dodeljene pravice, osnovne varnostne ukrepe, stanje pogodbenih ponudnikov in potrebo po dodatnem usposabljanju.

VIII. KRŠITVE VARNOSTI OSEBNIH PODATKOV

33. člen

(prepoznavanje in notranja prijava)

(1) Vsak, ki zazna ali utemeljeno sumi izgubo dokumentacije, napačno posredovanje podatkov, krajo naprave, nepooblaščen dostop, okužbo sistema ali drugo kršitev, mora o tem nemudoma obvestiti pristojno kontaktno osebo za informacijsko varnost in DPO oziroma odgovorno osebo združenja.

(2) Prijavitelj ne sme samovoljno prikrivati incidenta ali brisati dokazov; opravi lahko nujne ukrepe za zmanjšanje škode, če s tem ne poveča tveganja.

(3) O zaznanih incidentih se vodi varovana evidenca, ki vsebuje najmanj datum in opis dogodka, prizadete podatke oziroma sisteme, oceno tveganja, sprejete ukrepe, odločitve o obveščanju pristojnih in datum zaključka. Poseben predpisan obrazec ni potreben.

34. člen

(obravnavna, dokumentiranje in ukrepi)

(1) Po prejemu prijave pristojna oseba koordinira zaježitev in odpravo incidenta, ugotovi okoliščine in kategorije prizadetih podatkov ter z DPO oceni tveganje za pravice in svoboščine posameznikov.

(2) EPEKA dokumentira vsako kršitev varnosti osebnih podatkov, dejstva, posledice in izvedene popravne ukrepe, ne glede na to, ali je prijava nadzornemu organu obvezna.

(3) Po zaključku se sprejmejo sorazmerni preventivni ukrepi in preveri njihova učinkovitost.

35. člen

(prijava nadzornemu organu in obvestitev posameznikov)

(1) Če je verjetno, da kršitev pomeni tveganje za pravice in svoboščine posameznikov, se o njej skladno s členom 33 GDPR brez nepotrebnega odlašanja, po možnosti najpozneje v 72 urah po seznanitvi, obvesti Informacijskega pooblaščenca; kadar prijava ni opravljena v roku, se navedejo razlogi za zamudo.

(2) Kadar je verjetno veliko tveganje za pravice in svoboščine posameznikov, se prizadete posameznike brez nepotrebnega odlašanja obvesti skladno s členom 34 GDPR, razen če velja predpisana izjema.

(3) Če projektna pogodba določa še ločeno obveščanje financerja ali partnerja, se ta obveznost preveri in izvede brez poseganja v zakonske obveznosti ali nepotrebnega razkritja podatkov.

IX. OCENA TVEGANJ IN OCENA UČINKA

36. člen

(preverjanje tveganj pred obdelavo)

- (1) Pred uvedbo nove obdelave ali pomembno spremembo obstoječe obdelave vodja dejavnosti skupaj z odgovorno osebo in DPO dokumentira namen, podatke, pravno podlago, prejemnike, uporabo tehnologij in tveganja.
- (2) Posebna pozornost se nameni obsežnim podatkom o ranljivih osebah, obdelavi posebnih vrst osebnih podatkov, spremljanju posameznikov, uporabi novih tehnologij in morebitnim mednarodnim prenosom.

37. člen

(DPIA in predhodno posvetovanje)

- (1) Kadar je verjetno, da bo predvidena obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov, se pred začetkom obdelave izvede ocena učinka v zvezi z varstvom podatkov (DPIA) po členu 35 GDPR.
- (2) Predhodna presoja potrebe po DPIA se kratko dokumentira tudi takrat, ko je ugotovljeno, da DPIA ni potrebna. Zapis vsebuje opis obdelave, ugotovljena tveganja, odločitve in razloge zanjo ter datum in pristojno osebo; zanj ni predpisan poseben obrazec.
- (3) Če po sprejetih ukrepih ostane veliko tveganje, ki ga ni mogoče ustrezno zmanjšati, EPEKA pred začetkom obdelave preveri obveznost predhodnega posvetovanja z Informacijskim pooblaščencom po členu 36 GDPR.

X. ROKI HRAMBE IN PRENEHANJE OBDELAVE

38. člen

(določanje rokov hrambe)

- (1) Rok hrambe za vsako kategorijo osebnih podatkov se določi v evidenci dejavnosti obdelave na podlagi namena, zakonskih ali pogodbenih zahtev, obveznosti revizijske sledljivosti in zastaranja relevantnih zahtevkov.
- (2) Projektna dokumentacija in osebni podatki uporabnikov se ne hranijo samodejno neomejeno dolgo. Za vsak projekt se preverijo posebna pravila financerja ter pogoji za minimalno potrebno hrambo.
- (3) Če po izteku roka obstaja druga zakonita podlaga za nadaljnjo hrambo posameznega dela dokumentacije, se obseg in razlog dokumentirata.

39. člen

(izbris, arhiviranje in anonimizacija)

- (1) Ko namen in pravna podlaga za hrambo prenehata, se podatki izbrišejo, anonimizirajo ali varno uničijo, razen če je nadaljnja hramba potrebna po veljavnih predpisih ali za uveljavljanje pravnih zahtevkov.
- (2) Digitalni nosilci se izbrišejo z ustreznimi tehničnimi postopki, ki upoštevajo vrsto naprave; pred odtujitvijo oziroma odstranitvijo naprave se preveri, da osebni podatki niso več dostopni.

(3) Za arhivirane podatke se omejijo dostopi in nadaljnja uporaba; posameznikovih podatkov se ne hrani »za vsak primer« brez določenega namena.

XI. NADZOR, ODGOVORNOST IN IZVAJANJE

40. člen

(notranji nadzor)

(1) DPO in pristojne operativne osebe v okviru svojih vlog sodelujejo pri rednem preverjanju izvajanja pravilnika, vključno z evidencami obdelave, varnostjo sistemov, pogodbenimi ponudniki in obravnavo zahtev posameznikov.

(2) Za ugotovljene pomanjkljivosti se opredelijo nosilec, rok in ukrep; ugotovitve in izvedeni popravki se v ustreznem obsegu dokumentirajo.

(3) EPEKA sodeluje z nadzornim organom ter pristojnimi revizijskimi in pogodbenimi organi v obsegu svojih zakonskih in pogodbenih obveznosti.

41. člen

(kršitve obveznosti oseb)

(1) Kršitve obveznosti iz tega pravilnika se obravnavajo skladno z veljavnimi predpisi, pogodbami in internimi akti; pri ukrepanju se upoštevajo teža kršitve, okoliščine in sorazmernost.

(2) Vsaka oseba, ki obdeluje osebne podatke, je odgovorna za upoštevanje odobrenih postopkov in za pravočasno opozarjanje na tveganja ter incidente.

42. člen

(izvajanje pravilnika in vodenje evidenc)

(1) Sestavni del pravilnika je Priloga 1 – Izjava o zaupnosti in varovanju osebnih podatkov. Evidence obdelav, zahtev posameznikov, varnostnih incidentov, preverjanj tveganj, odgovornosti in tehničnih ukrepov se vodijo kot samostojni delovni zapisi oziroma preglednice in niso priloge pravilnika.

(2) Evidence in druge delovne zapise se vodi v obsegu, ki zagotavlja zakonsko zahtevano vsebino, preglednost in sledljivost. EPEKA lahko uporabi obstoječe projektne evidence, če vsebujejo potrebne podatke in so ustrezno zavarovane; ni treba uvajati novih obrazcev, kadar enakovredna evidenca že obstaja.

(3) Ob začetku uporabe pravilnika se preveri dejanska uvedba predpisanih varnostnih ukrepov, določijo odgovorne osebe in evidentira načrt odprave ugotovljenih vrzeli. Podrobnejša operativna navodila za posamezne projekte, informacijske sisteme ali lokacije se po potrebi sprejmejo posebej.



XII. KONČNE DOLOČBE

43. člen

(uveljavitev in prenehanje starega pravilnika)

(1) Ta pravilnik sprejme pristojna oseba oziroma organ združenja v skladu s statutom in začne veljati z dnem sprejema oziroma z datumom, določenim v sklepu o sprejemu.

(2) Z uveljavitvijo tega pravilnika preneha veljati Pravilnik o varovanju osebnih podatkov EPEKA z dne 5. 8. 2014.

(3) Z besedilom pravilnika morajo biti seznanjene vse osebe, ki jih zavezuje; pravilnik je dostopen v notranjem sistemu dokumentacije združenja.

Sprejeto v Mariboru, dne: 21. 11. 2025

Za Združenje EPEKA, so. p.
Štefan Simončič, predsednik

Podpis in žig:





PRILOGA 1

IZJAVA O ZAUPNOSTI IN VAROVANJU OSEBNIH PODATKOV

Izjavo podpiše zaposleni, prostovoljec, praktikant ali drug sodelavec pred pridobitvijo dostopa do osebnih podatkov.

Ime in priimek: _____

Delovno mesto / vloga / projekt: _____

Podpisani/-a potrjujem, da:

- sem seznanjen/-a s Pravilnikom o varstvu osebnih podatkov in informacijski varnosti EPEKA ter z navodili, pomembnimi za moje delo;
- bom osebne podatke obdeloval/-a samo v okviru svojih nalog in dodeljenih pooblastil ter jih ne bom posredoval/-a nepooblaščenim osebam;
- bom uporabljal/-a odobrene informacijske sisteme, varoval/-a gesla in naprave ter osebnih podatkov brez odobritve ne bom prenašal/-a v zasebne račune ali na nezaščitene nosilce;
- bom ob vsaki izgubi, napačnem posredovanju, sumu vdora ali drugi varnostni kršitvi nemudoma obvestil/-a pristojno osebo;
- bom obveznost zaupnosti spoštoval/-a tudi po koncu zaposlitve oziroma sodelovanja.

Kraj in datum: _____ Podpis: _____

