DPIA in umetna inteligenca v raziskavah, ki vključujejo osebne podatke

Univerza v Ljubljani, 7. 5. 2026

mag. Andrej Tomšič, Informacijski pooblaščenec

Financira Evropska unija NextGenerationEU

NAČRT ZA OKREVANJE IN ODPORNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO ZNANOST IN INOVACIJE

SPOZNAJ
PODPORA PRI UVAJANJU NAČEL ODPRTE ZNANOSTI V SLOVENIJI

Ocene učinkov na varstvo osebnih podatkov (DPIA)

A. „Kaj gre lahko narobe?“ -> identifikacija tveganj

Verjetnost in resnost!

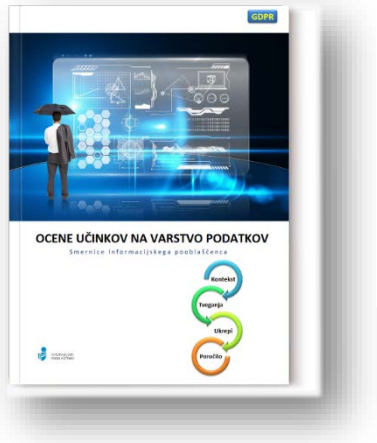
B. „Kaj lahko storimo, da ne bo šlo narobe?“ -> upravljanje tveganj

A. <u>Projektne DPIA</u> (35. člen GDPR, 24(1)., 69., 80., 87. člen ZVOP-2, 49. čl. ZVOPOKD)

- Smernice EDPB
- **Ključno področje**, **smernice**, **priporočila** in **infografika** IP
- 11 prejetih v prvem letu ZVOP-2, 17 v 2024, 11 v 2025

B. <u>Zakonodajne DPIA</u> (24(3) člen ZVOP-2)

- **Ob pripravi predpisov**
- Postopek in metodologija
- Metodologija IP
- 15 prejetih v prvem letu ZVOP-2, 19 v 2024



Kdaj je DPIA obvezna?

35(3) GDPR <--- 69(3) ZVOP-2:

(a) **sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki**, ki temelji na **avtomatizirani obdelavi**, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;

(b) **obsežne** obdelave **posebnih vrst podatkov** iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10, ali

(c) **obsežnega sistematičnega spremljanja javno dostopnega območja.**

Seznam obdelav, ki terjajo izdelavo ocene učinka, je sprejel vsak nadzorni organ (potrdil EDPB)

- IP: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf

Kriterij	Primeri
Evalvacija in razvrščanje posameznikov, vključno s profiliranjem in napovedovanjem (usmeritev na uvodni določbi 71 in 91).	• Odločanje o ustreznosti komitenta glede pridobitve kredita na podlagi podatkov v SISBONU in drugih podatkov • Genetsko testiranje in ugotavljanje verjetnosti za nastanek določene bolezni • Beleženje podatkov o vožnjah in ustvarjanje profilov voznikov za popust pri zavarovanju
Avtomatizirano odločanje s pravnimi ali podobnimi pomembnimi učinki.	• Avtomatizirano odločanje o pridobitvi/zavrnitvi: stanovanjskega ali drugega kredita, denarne socialne omoči, štipendije, usposobljenosti za delo, zdravstvenega zavarovanja …
Sistematični nadzor (zlasti primeri, kjer se posameznik ne more izogniti obdelavi njegovih podatkov ali se obdelave sploh ne zaveda).	• Beleženje registrskih tablic mimo vozečih vozil • Preverjanje uporabnikov bencinskega servisa s seznamom ubežnikov brez plačila • Videonadzor prireditve na javnem prostoru iz brezpilotnika • Videonadzor javnih površin
Posebne vrste osebnih podatkov in drugi podatki bolj občutljive narave.	• Zdravstveni podatki o pacientih v bolnišnici • Kazenske in prekrškovne evidence • Podatki o lokaciji, elektronski komunikaciji posameznika, spletne varnostne kopije podatkov posameznika, pametne naprave, ki beležijo aktivnosti posameznika • Podatki o varovankah v varnih hišah, o pripadnikih določene vere, članih drugih društev, ki zbirajo posebne vrste podatkov
Obdelava, ki omejuje pravice posameznika ali obdelava podatkov, katere cilje je omogočiti ali preprečiti posamezniku dostop do storitev ali pogodbe.	• Obdelava podatkov o uporabi avtocestnega omrežja z elektronskim cestninjenjem • Predhodno preverjanje kreditne sposobnosti komitenta

Množičnost obdelave osebnih podatkov, podkriteriji: **- število (ali delež) zadevnih posameznikov,** **- obseg podatkov,** **- trajanje ali stalnost obdelave,** **- geografski obseg obdelave.**	• Klubi zvestobe pri trgovcih • Podatki o uporabi elektronskih komunikacij pri operaterjih • Podatki o zavarovancih in škodnih primerih pri zavarovalnicah • Registri na državni ravni • Podatki o komitentih in njihovi uporabi bančnih storitev v bankah in hranilnicah
Primerjanje in kombiniranje različnih zbirk podatkov (npr. pridobljenih skozi različne aktivnosti upravljavca) in analitika na osnovi masovnih podatkov.	• Primerjanje podatkov o zavarovancih in podatkov o škodnih primerih pri zavarovalnici z namenom ugotavljanje deležev, trendov, vzročno-posledičnih povezav ipd. • Primerjanje podatkov o absentizmu in podatkov o spolu, starosti in izobrazbi zaposlenih • Primerjanje nakupovalnih navad in podatkov o gibanju kupcev
Obdelava podatkov ranljivih (skupin) posameznikov, kjer obstaja občutno nesorazmerje moči med upravljavcem in posameznikom.	• Obdelava osebnih podatkov zaposlenih, otrok, psihičnih bolnikov, prosilcev za azil, migrantov, starejših, pacientov …
Inovativna uporaba obstoječih in novih tehnologij, katerih osebne in družbene posledice niso nujno dobro raziskane in poznane.	• Biometrijska prepoznava prstnih odtisov, obraza • Testiranje genetskih vzorcev • Določene naprave in senzorji v okviru interneta stvari (npr. »pametne igrače«)

Učinkovito obvladovanje tveganj na področju varstva osebnih podatkov

Kaj je tveganje?

Tveganje za pravice in svoboščine posameznika je posledica **nezakonitega ravnanja z osebnimi podatki**, ki bi lahko posamezniku povzročila **fizično, premoženjsko in ali nepremoženjsko škodo**, kot je npr.: **diskriminacija, kraja ali zloraba identitete, finančna izguba, okrnitev ugleda, izguba zaupnosti osebnih podatkov, odrekanje storitve ali upravičenj**.

Zakaj ocenjevati tveganja?

Ker ne želimo naše organizacije izpostaviti **sankcijam**, okrnitvi **ugleda, negativnemu medijskemu poročanju** ali **izgubi zaupanja** posameznikov.

Ker je to lahko naša formalna dolžnost - ocena tveganj je sestavni del **ocen učinkov na varstvo osebnih podatkov** in **analiz varnosti.**

Slabo opredeljena tveganja lahko vodijo v **spregled dejanskih tveganj** in v **neustrezno oblikovanje ukrepov** za njihovo obvladovanje**.**

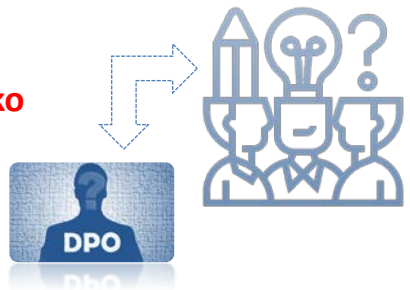
Za obvladovanje tveganj je pomembna:

- **natančna opredelitev tveganj**
- **objektivna ocena verjetnosti in resnosti**
- **strukturiranje** in obravnava tveganj **po temeljnih načelih** varstva osebnih podatkov

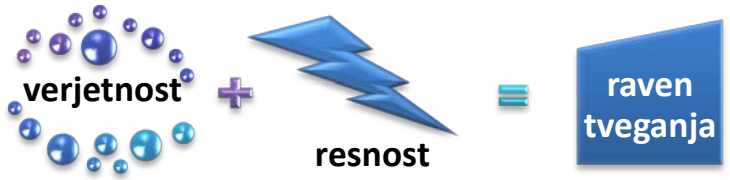
Infografika o temeljnih načelih

Kako popisati tveganja?

Priporočamo **premislek vseh zadevnih oseb**, **kaj vse gre lahko narobe** z vidika osebnih podatkov.



Kako ocenjujemo tveganja?

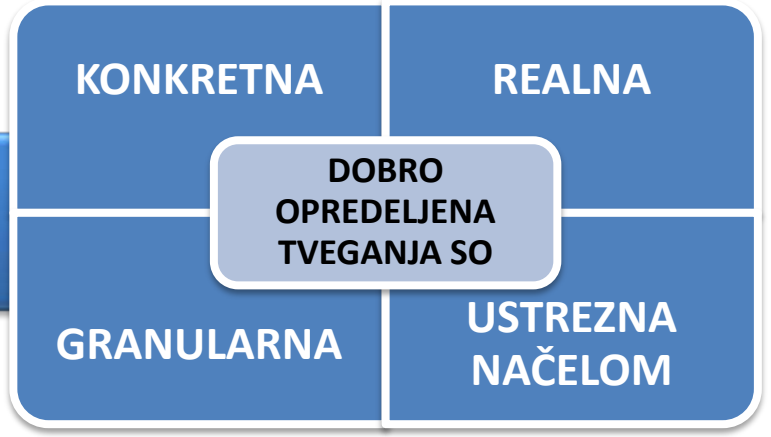


Verjetnost\resnost	visoka (5)	srednja (4)	srednja (3)	srednja (2)	nizka (1)
skoraj gotovo	visoka	visoka	srednja	srednja	nizka
verjetno	visoka	srednja	srednja	nizka	sprejemljiva
možno	srednja	srednja	nizka	sprejemljiva	sprejemljiva
redko	srednja	nizka	sprejemljiva	sprejemljiva	sprejemljiva
izredno redko	nizka	sprejemljiva	sprejemljiva	sprejemljiva	sprejemljiva

Piflarski kotiček Ali veš, kaj na področju ocenjevanja tveganj pomenita izraza „sivi labod“ in „črni labod“??

INFORMACIJSKI POOBLAŠČENEC

Kako ustrezno opredeliti tveganja?



Slabo opredeljena tveganja

„Obdelava podatkov izven namena obdelave.“

⊗ Premalo natančno opredeljeno (kdo je **vir tveganja**, za kakšno nenamensko obdelavo gre…).

„Nejasne informacije o obdelavi osebnih podatkov.“

⊗ Premalo natančno opredeljeno – informacije za posameznike morajo biti celovite in razumljive.

„Posamezniki bodo vložili zahteve glede svojih pravic.“

⊗ To dejansko ni tveganje – tveganje je, da ne vemo, katere pravice jim pripadajo, da na zahtevo ne odgovorimo v roku ipd.

„Neomogočanje uveljavljanja pravic zaposlenega na katerega se nanašajo osebni podatki.“

⊗ Opredelitev tveganja ni jasna.

„Nenamenska uporaba posnetkov videonadzornega sistema.“

⊗ Tveganje je **preveč široko opredeljeno** in zajema **različna možna tveganja glede na različne vzroke in okoliščine**.

Dobro opredeljena tveganja

Zaposleni bodo (v nasprotju z navodili in politikami delodajalca) izkoristili možnost dostopa do osebnih podatkov za uporabo podatkov za neupravičene namene (npr. v zasebne namene, za neupravičeno posredovanje tretjim osebam).

Tveganje, da informacije za posameznike ne bodo podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku in skladno z zahtevami 12. člena Splošne uredbe.
Tveganje, da informacije za posameznike ne bodo celovite skladno z zahtevami 13./14. člena Splošne uredbe.

Zahteve posameznikov za uveljavljanje pravic ne bodo obravnavana pravočasno.
Postopek obravnave zahtev posameznikov ni jasno opredeljen.
Odgovornosti in zadolžitve glede obravnave zahtev niso jasno določene.
Osebe, ki obravnavajo prejete zahteve, niso ustrezno usposobljene.

Uporaba videoposnetkov za zasebne ali druge nedopustne namene s strani pooblaščenih oseb za ravnanje z videonadzornim sistemom (npr. vpogledovanje v posnetke brez utemeljenega in zakonitega razloga).
Nedovoljena razširitev ali preusmeritev območja ali časa snemanja s strani pooblaščenih oseb za ravnanje z videonadzornim sistemom.
Nedovoljena javna objava videoposnetkov.

Izkušnje in priporočila

- **NAMEN DPIA NI UTEMELJEVANJE SMISELNOSTI PROJEKTA**
  - DPIA kot „reklamni material“ projekta
- TVEGANJA **RAZVRSTITE IN OCENITE PO TEMELJNIH NAČELIH** VARSTVA OSEBNIH PODATKOV
- TVEGANJA SE **PODCENJUJEJO**
  - Primer: zakonitost in pravne podlage
- DOLOČITE **METODOLOGIJO** VREDNOTENJA TVEGANJ – KAKO SE IZRAČUNA SKUPNA RAVEN TVEGANJ
- NE POZABITE OCENITI **TVEGANJ IZ NASLOVA PRAVIC POSAMEZNIKA**
- VPRAŠAJMO SE: „*KAJ GRE LAHKO NAROBE*?“ TER TUDI „*NA KATERE OBVEZNOSTI PO SPLOŠNI UREDBI/ZVOP-2 NE SMEMO POZABITI*?“
- **IZVEDENA DPIA NE MORE NADOMESTITI MANJKAJOČE PRAVNE PODLAGE!**
- NI NAVEDBE, ALI JE BILO PRIDOBLJENO **MNENJE DPO** IN KAKŠNO JE
- DPIA **NALOŽENA DPO** (DPO SVETUJE/PREGLEDA DPIA!)
- POGOSTO MANJKA **POSVETOVANJE Z ZAINTERESIRANIMI DELEŽNIKI**
- UPORABITE **KONTROLNI SEZNAM** ZA CELOVITOST DPIA (Priloga 2 smernic EDPB in IP)

Vir: https://www.enforcementtracker.com/

Kazni?

- **58** glob zaradi kršitev Splošne uredbe (35. člen in drugi členi)
- Od tega **7** samostojnih glob zaradi kršitev 35. člena

Država	Datum odločbe	Globa [€]	Upravljavec/ obdelovalec	Člen	Vrsta kršitve
Španija	2023-05-03	200,000	GSMA LTD.	35. člen GDPR	Zbiranje posebnih vrst osebnih podatkov za registracijo na dogodek, brez izvedene ocene učinkov (Neupoštevanje temeljnih načel varstva osebnih podatkov)
Španija	2021-10-26	16,000	SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L.	35. člen GDPR	Preverjanje prstnih odtisov na vhodu, brez izvedene ocene učinkov (Neupoštevanje temeljnih načel varstva osebnih podatkov)
Finska	2020-05-22	16,000	Kymen Vesi Oy	35. člen GDPR	Sledenje lokacij zaposlenih, brez izvedene ocene učinkov (Neupoštevanje temeljnih načel varstva osebnih podatkov)
Španija	2024-12-20	**1,000,000**	LIGA NACIONAL DE FÚTBOL PROFESIONAL	35. člen GDPR	Brez izvedene ocene učinkov (Nezadostni tehnični in organizacijski ukrepi za zagotovitev informacijske varnosti)
Španija	2023-04-28	12,000	ALBERO FORTE COMPOSITE, S.L.	35. člen GDPR	Snemanje zaposlenih na vhodu, brez izvedene ocene učinkov (Nezadostni tehnični in organizacijski ukrepi za zagotovitev informacijske varnosti)
Nizozemska	2024-01-15	150,000	International Card Services B.V.	35. člen GDPR	Množična uporaba osebnih podatkov strank brez predhodno izvedene ocene učinka.
Švedska	2023-11-28	26,500	Östersund Municipality's Department for Children and Education	35. člen GDPR	Brez izvedene ocene učinkov (Nezadostni tehnični in organizacijski ukrepi za zagotovitev informacijske varnosti)

Tveganja glede uporabe UI

- Upravljanje tveganj umetno-inteligenčnega sistemov je kompleksna naloga, saj je **katalogiziranih že več kot 1600 tveganj**, zato je priporočljivo osrediniti se na **tveganja, ki so najbolj relevantna za konkreten sistem** in pri tem uporabiti katerega od **zaupanja vrednih pristopov oziroma okvirov**, kot npr.:
  - **OWASP** AI Security and Privacy Guide (https://owasp.org/www-project-ai-security-and-privacy-guide/);
  - **ENISA**: Multilayer Framework for Good Cybersecurity Practices for AI (https://www.enisa.europa.eu/sites/default/files/publications/Multilayer%20Framework%20for%20Good%20Cybersecurity%20Practices%20for%20AI.pdf);
  - **NIST**: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf).

Tveganja glede uporabe UI

Nekaj relevantnih tveganj:

- Neustrezno človeško preverjanje (ang. *non-meaningful human review*) kot posledica pomanjkanja učenja človeških pregledovalcev za razlago in izpodbijanje rezultatov, ki jih pripravi sistem umetne inteligence.
- Sistemi umetne inteligence, ki ustvarjajo nepravične rezultate za posameznike, so **posledica premalo raznolikih podatkov** na katerih se sistem usposablja, **podatkov, ki niso primerni za namen sistema umetne inteligence**, **podatkov, ki odražajo preteklo diskriminacijo**, oblikovanje **arhitekture izbire** (ang. *choice architecture*) ali drugega podobnega razloga
- Model se premika (ang. *model drift*), ker podatki za razvoj niso več ustrezni ali primerni.
- **Pristanskosti** podatkov in algoritmov.

Uporaba generativne UI pri obdelavi osebnih podatkov v raziskavah

- **VARNA IN ODGOVORNA UPORABA UMETNE INTELIGENCE PRI DELU - Priporočila IP za javne uslužbence**
- Dopustnost uporabe GEN AI orodij v instituciji – interni akt
- V orodja UI ne vnašajte nobenih osebnih, zaupnih in drugih varovanih podatkov – če ni to izrecno dopustno in predvideno za konkretni primer uporabe določenega orodja.
- Ni vsako brisanje osebnih podatkov anonimizacija.
- Vedno preverite pravilnost prejetih odgovorov.
- Ne prenašajte odgovornosti na orodje UI.
- …
- https://www.ip-rs.si/go?u=%2Fumetna-inteligenca%2F

Priporočila

- **Natančno preučite vhodne podatke in namen:** Vprašajte se, ali posamezen podatek resnično služi poslovnemu cilju – ali je lahko proxy za občutljive značilnosti.

- **Revizije pristranskosti:** Zahtevajte, da vaše skupine izvedejo preskuse demografske paritete in enakih možnosti, preden kateri koli model začne delovati.

- **Neprekinjeno spremljanje:** Po uvedbi bodite pozorni na morebitne drifte modela - če se rezultati nekaterih skupin sčasoma poslabšajo, bodite pripravljeni na ponovno učenje ali prilagoditev modela.

Vir: povzeto po dr. Maja Škrjanc: Varna in etična uporaba umetne inteligence, Inštitut Jožef Stefan, 10. marec 2026

SPOZNAJ

PODPORA PRI UVAJANJU NAČEL ODPRTE ZNANOSTI V SLOVENIJI

Hvala za pozornost!