



Zakonodajne ocene učinka na varstvo osebnih podatkov

mag. Andrej Tomšič
Informacijski pooblaščenec

7. april 2025



Ocene učinkov na varstvo osebnih podatkov (DPIA)

A. „Kaj gre lahko narobe?“

Verjetnost in resnost!

-> **identifikacija tveganj**

B. „Kaj lahko storimo, da ne bo šlo narobe?“

-> **upravljanje tveganj**

A. Projektne DPIA (35. člen GDPR, 24(1)., 69., 80., 87. člen ZVOP-2)

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



B. Zakonodajne DPIA (24. člen ZVOP-2)

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



Izkušnje z zakonodajnimi ocenami učinka

24. člen ZVOP-2 (ocena učinka in predhodno posvetovanje)

(3) Kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj **predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe**. Po proučitvi ocene učinka **nadzorni organ poda mnenje glede obdelave osebnih podatkov, glede katerega se mora predlagatelj zakona opredeliti**. Kadar ocene učinka ni treba izdelati, predlagatelj zakona opravi samo predhodno posvetovanje z nadzornim organom v skladu s 36. členom Splošne uredbe.



PRIMERI

- digitalizacija zdravstva
- povezovanje zbirk
- uvajanje novih informacijskih sistemov
- avtomatizirano odločanje
- obdelava posebnih vrst osebnih podatkov

problematika,
ki terja
zakonsko
urejanje

Ocene učinkov na varstvo osebnih podatkov pri pripravi predpisov (zakonodajne ocene učinka)

Ocena učinkov je orodje za pravočasno **identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki**. 24. člen **ZVOP-2** določa zahtevo po ocenah učinka pri pripravi zakonov: kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe (»zakonodajne ocene učinka«). Prav tako ZVOPOKD v 49. členu za določene primere zahteva izvedbo takšne zakonodajne ocene učinkov.

Namen **zakonodajnih ocen učinka** je, da se še pred oblikovanjem dokončnega besedila členov opravi **pravočasne razmisleke** o tem, kako **ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona**. Te razmisleke (npr. ali je za doseg ciljev zakona resnično treba obdelovati osebne podatke, kakšne namene zasledujemo, kateri nabor osebnih podatkov je potreben, katere ukrepe je treba vključiti za zagotovitev zakonite in poštene obdelave, kakšne varovalke moramo vključiti v zakon, ali bo šlo za povezovanje zbirk podatkov, določitev rokov hrambe ipd.) se **opiše v oceni učinkov**, jo pošlje IP v mnenje (v t.i. **predhodno posvetovanje**) in na podlagi mnenja IP oblikuje (bolj) dokončno besedilo členov, ki gre lahko nato v medresorsko usklajevanje.

PREDLAGATELJ

idejna zasnova
in ocena učinka
(analiza rešitev
in tveganj z
vidika varstva
osebnih
podatkov)

predlog
predpisa

javna razprava
medresorsko
usklajevanje

potrditev in
posredovanje v
obravnavo v
Državni zbor RS



INFORMACIJSKI
POOBlašČENEC

mnenje IP na
oceno učinka
(predhodno
posvetovanje)

mnenje IP na
predlog
predpisa
(po potrebi več
iteracij)

Več informacij o ocenah učinka:

<https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/ključna-področja-uredbe/ocena-účinka-v-zvezi-z-varstvom-podatkov/>

IP je pripravil osnutek metodologije za pripravo zakonodajnih ocen učinka:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2022/MJU_metodologija_ocene_účinkov_jul2022.docx



Izkušnje z zakonodajnimi ocenami učinka

Vladna metodologija

- Težave z izpolnjevanjem / učinkovitost metodologije glede na zasledovane cilje?
- Verjetno zaradi enotnega modela za ocene učinka, ki pokriva tudi druga področja, in ga je težko aplicirati na področje varstva osebnih podatkov. Primer:

12. Ali ima predpis učinek na makroekonomijo kot npr. inflacija, gospodarska rast, javno-finančni prihodki, zadolžitev ali širše (mednarodno)? DA / NE	12.1. Kakšen učinek ima predpis na posamezne sektorje in v kakšnem obsegu? POZITIVEN / NEGATIVEN / NIMA UČINKA. Obrazložitev:
	12.2. Kakšen učinek ima predpis na posamezne regije in v kakšnem obsegu? POZITIVEN / NEGATIVEN / NIMA UČINKA. Obrazložitev:



Izkušnje z zakonodajnimi ocenami učinka

6. Ali ima predpis učinek, s katerim se posega v osebne podatke (določa obdelava novih ali spremenjenih osebnih podatkov)? DA / NE	6.1. Kakšen učinek ima predpis glede posega v osebne podatke – utemeljenost posega? POZITIVEN / NEGATIVEN / NIMA UČINKA. Obrazložitev:
---	--



38. člen Ustave RS
in poseg v
informacijsko
zasebnost
posameznika?

Priporočamo uporabo metodologije IP:

<https://www.ip->

[rs.si/fileadmin/user_upload/RAZNO/Metodologija%20zakonodajne%20ocene%20u%C4%8Dinkov_jul202.docx](https://www.ip-rs.si/fileadmin/user_upload/RAZNO/Metodologija%20zakonodajne%20ocene%20u%C4%8Dinkov_jul202.docx)



Cilji, nameni, pomen

- Glede na to, da mora obdelavo osebnih podatkov določati zakon (kakor tudi upravljavce, namene, roke hrambe, evidence, morebitno povezovanje zbirk ipd.), je **bistveno, da se tveganja glede varstva osebnih podatkov analizirajo že v času priprave predpisa**, saj jih upravljavci kasneje, ko so bistveni elementi že določeni v predpisu, ne morejo spremeniti in njihove ocene učinka nimajo več takšnega pomena.
- Ocena učinka v zvezi z varstvom osebnih podatkov **lahko v fazi snovanja predpisa zagotovi upoštevanje temeljnih načel varstva osebnih podatkov**: poštenosti, preglednosti in zakonitosti, minimizacije obdelave, namenskosti, ažurnosti, rokov hrambe ter **določitev ustreznih zaščitnih ukrepov in varovalk – njen cilj je celovit premislek** o tem, katere podatke se bo zbiral in za katere namene, kakšne so možnosti minimizacije nabora in obsega obdelave, katere evidence bodo vsebovale katere podatke in kdo bo z njimi upravljal, ali gre pri tem morda za skupno upravljanje, ali je predvideno povezovanje evidenc, kakšne so relevantne pravice posameznika, kateri so najkrajši možni roki hrambe, komu se bodo določeni podatki posredovali, ali prihaja do prenosa osebnih podatkov v tretje države ipd.
- Izjemnega pomena so zlasti pri **uvajanju sistematičnih novih obsežnih nacionalnih zbirk osebnih podatkov, novih policijskih pooblastil in pristojnosti, na področju obdelave posebej občutljivih podatkov** (kot npr. podatki o zdravstvenem stanju, podatki o kazenskih in prekrškovnih postopkih, genski, biometrijski podatki ipd.), **pri opredeljevanju ukrepov, ki zadevajo široko populacijo ali specifične družbene segmente**, saj z analizo tveganj in učinkov na posameznika in družbo **omogočajo javni diskurz o sprejemljivosti, primernosti, učinkovitosti ter nujnosti določenih ukrepov v demokratični družbi**.



Kaj si želimo videti v zakonodajnih ocenah učinka?

- **Kako so upoštevana temeljna načela varstva osebnih podatkov?**
 - **Zakonitost:** jasne, primerne in določene pravne podlage
 - **Preglednost:** kaj moramo na ravni zakona določiti glede informiranja posameznikov?
 - **Namenskost:** so nameni jasni in določeni, kakšna so tveganja za nenamenske, druge uporabe?
 - **Minimizacija:** kateri podatki so res potrebni? Od koga/od kod in kdaj? Ali je možno cilje izpolniti z anonimiziranimi podatki? S psevdonimizirani? Z manj „govorečimi“ podatki?
 - **Točnost:** tveganja, da bo bodo zbrani oz. obdelovani podatki netočni, pomanjkljivi, nepopolni, napačni, zastareli
 - **Omejitev shranjevanja** – ali so roki hrambe določeni, minimizirani glede na namene in kako jih utemeljimo?
 - **Varnost podatkov** – kaj je smiselno določiti že na ravni zakona?



Kaj si želimo videti v zakonodajnih ocenah učinka?

- Ali so v zakonu jasno in ustrezno opredeljene **obdelave** osebnih podatkov, **upravljavci/skupni upravljavci/uporabniki**, **nabor** podatkov, **roki** hrambe, **nameni** obdelave?
- Je **tok podatkov** (zbiranje, hrambe, prenosi, dostopi) dovolj jasen, predvidljiv?
- **Katera tveganja za upoštevanje temeljnih načel varstva osebnih podatkov smo zaznali in kako jih naslavljamo, katere varovalke bodo uporabljene?**
 - npr. nova centralizirana državna zbirka
- Ali smo preverili **druge možnosti – milejše ukrepe?**
- Kakšne so **izkušnje drugih držav** na tem področju, kako smo jih upoštevali?
- Ali in kako so upoštevani možni **učinki na pravice posameznika** v primeru nezakonitega dostopa, spremembe ali izgube podatkov?
 - Upoštevanje „teže“ podatkov, njihove občutljivosti in **resnosti** posledic za posameznike (upravljavce, državo)
- Če je predvideno **povezovanje zbirk, ali je ustrezno definirano** (katere zbirke se povezujejo katerih upravljavcev, povezovalni znak in nameni)?
- Katere **pravice posameznika** so možne? Ali so kakšne **omejitve**, so jasno opredeljene in nujne? Argumenti?

Pri izdelavi zakonodajne ocene učinka so sodelovali javni uslužbenci _____

Mnenje pooblaščenih oseb za varstvo podatkov je bilo pridobljeno _____.

In česa ne?

1.3 Ali je bila izvedena primerjava z ureditvami v tujini?

DA. Izvedena je bila s štirimi državami, in sicer s Finsko, Estonijo, Portugalsko in Avstrijo.

5.1. Ali je podana ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84 Splošne uredbe)?

Ne, takšna ocena (še) ni narejena. Ocena učinka na varstvo osebnih podatkov po določbah 35. člena Splošne uredbe bo narejena, ko bodo definirani ukrepi za varnost, ki jih bo zagotavljala družba.

6. Ali so bile v pripravo predpisa vključene zainteresirane strani?

6.1. Ali je bilo pridobljeno mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov?

Predlagatelj se je dne _____ posvetoval z Informacijskim pooblaščencom z namenom pridobitve usmeritev.

2.2. Ali je opredeljen nabor podatkov, upravljavci in uporabniki ter roki hrambe?

DA.

2. Ali ima predpis učinek na temeljna načela varstva osebnih podatkov?

DA / **NE** (ustrezno označi)

1. Ali ima predpis učinek s katerim se posega v osebne podatke (predpis predvideva nove ali spremenjene obdelave osebnih podatkov)?

DA / **NE** (ustrezno označi)



Primeri varovalk

Različne varovalke/kavtele so uporabne pri različnih načelih/tveganjih – pomembnost konteksta:

1. izrecne zakonske prepovedi (npr. nadaljnje uporabe, uporabe za druge namene)
2. sorazmerno kratki roke hrambe
3. omejenost dostopov na nujno potrebne
4. tehnični in organizacijski ukrepe za preprečevanje uporabe v druge namene
5. psevdonimizacija
6. anonimizacija
7. sledljivost obdelave
8. obvezno informiranje posameznikov
9. logične kontrole pri vnosu podatkov (npr. pri EMŠO ali davčnih številkah)
10. sistem štirih oči, kjer je ustrezno
11. naknadne kontrole kakovosti vnesenih, prejetih, posredovanih podatkov
12. odobritveni mehanizmi
13. enotni kanali za posredovanje/prejem podatkov (npr. 220. člen ZEKom-2)
14. sodna avtorizacija
15. višji dokazni standard
16. vodenje statistik ter redno letno poročanje o rabi ukrepa,
17. notranji (DPO!) in zunanji nadzori,
18. obveščanje posameznika, katerega podatki so bili obdelani (npr. 220. člen ZEKom-2)

...



220. člen ZEKom-2

(posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa)

- (1) Operater mora zaradi varstva posameznikovih življenjskih interesov policiji na podlagi njene **pisne zahteve, če je to glede na okoliščine konkretnega primera** nujno, posredovati podatke, potrebne za ugotovitev zadnje lokacije opreme za mobilno komunikacijo oziroma več zadnjih lokacij opreme, če je to tehnično mogoče, če:
- (2) **Obrazloženo zahtevo** za posredovanje podatkov, potrebnih za ugotovitev zadnje lokacije opreme za mobilno komunikacijo, policija **pošlje operaterju pisno**. Zahteva **mora biti podpisana lastnoročno ali elektronsko s kvalificiranim elektronskim podpisom**. Izjemoma se po elektronski poti lahko pošlje tudi sken lastnoročno...
- (4) **Policija vso dokumentacijo in ugotovitve, ki so podlaga za podajo zahteve, in samo zahtevo iz prvega odstavka tega člena hrani na način in pod pogoji iz prvega odstavka 221. člena tega zakona ter zagotavlja neizbrisno registracijo izvedenih ukrepov** in posegov v skladu z drugim odstavkom 221. člena tega zakona.
- (5) **Operater podatke**, poslane na podlagi zahteve iz prvega odstavka tega člena, izvedenih ukrepov in posegov v skladu z drugim odstavkom 221. člena **hrani na način in pod pogoji iz prvega odstavka 221. člena tega zakona ter zagotavlja neizbrisno registracijo**.
- (6) **Minister**, pristojen za notranje zadeve, **po predhodnem mnenju Informacijskega pooblaščenca** podrobneje **predpiše način posredovanja zahteve, obdelave posredovanih podatkov, notranjega nadzora glede načina oziroma tehničnih vprašanj obdelave osebnih podatkov ter tehnične značilnosti informacijskega sistema za izvajanje nalog iz prvega odstavka tega člena**.



7) Na podlagi prejete zahteve iz prvega odstavka tega člena mora operater zahtevane podatke poslati vlagatelju zahteve v najkrajšem možnem času oziroma takoj, ko je to tehnično mogoče. **Operater nosi breme dokazovanja tehnične nezmožnosti.**

(8) **Policija mora osebo, za katero je zahtevala in pridobila podatke o lokaciji** v skladu s tem členom, o tem takoj, ko je to mogoče, **pisno seznaniti**, razen če bi to škodovalo interesom samega posameznika ali interesom drugih, njemu bližnjih posameznikov v primerih iz prvega odstavka tega člena, dokler traja takšno stanje, vendar ne več kot eno leto.

(9) **Policija ne sme posredovati pridobljenih podatkov po tem členu prijaviteljem pogrešanih oseb in otrok iz 2. ali 3. točke prvega odstavka tega člena**, če bi bila s posredovanjem teh podatkov ogrožena...

(10) **Inšpekcijski nadzor nad obdelavo podatkov iz prvega odstavka tega člena opravlja Informacijski pooblaščenec najmanj enkrat letno.**

+ **Pravilnik o načinu izvajanja 220. člena Zakona o elektronskih komunikacijah:**

- Preverjanje drugih možnosti pred naslovitvijo zahteve za podatke
- Ena vstopna točka pri operaterju
- Ena vstopna točka pri OKC
- Točno določen e-naslov za posredovanje podatkov
- Točno določen obseg in formati podatkov, način prikaza podatkov, obrazci za izmenjavo podatkov, tehnični skrbniki
- Omejitev dopustne uporabe podatkov znotraj organa
- Redni letni notranji nadzor GPU



O vrednotenju resnosti tveganj

- V prejetih ocenah učinka se v grobem posplošuje vidik resnosti tveganja kot »**kršitev varstva osebnih podatkov**«.
- Pogosto le z **opredelitvijo ravni brez podrobnejše obrazložitve** (npr. majhna/srednja/visoka).
- **Primerno bi bilo vidik resnosti natančneje analizirati.**
- Pri ocenjevanju resnosti je koristno upoštevati tako:
 - **posledice za posameznike**, katerih osebni podatkov bodo obdelovani,
 - kot **posledice za upravljavca/obdelovalca/državo**, ki ima dolžnosti zagotavljanja ustreznega varstva osebnih podatkov.



Resnost tveganj in načelo točnosti

- Ocena, ali bi uresničitev tveganja predstavljala kršitev, za katere so po Splošni uredbi predvidene **nižje** (4. odstavek 83. člena Splošne uredbe) ali **višje kazni** (5. odstavek 83. člena Splošne uredbe).

Nižje kazni so predvidene za kršitve:

- a) **obveznosti upravljavca in obdelovalca** v skladu s **členi 8, 11, 25 do 39 ter 42 in 43**;
- b) obveznosti organa za potrjevanje v skladu s členoma 42 in 43;
- c) obveznosti organa za spremljanje v skladu s četrnim odstavkom členom 41. člena Splošne uredbe.

Višje kazni pa so predvidene za kršitve:

- a) **osnovnih načel** obdelave, vključno s pogoji za privolitev, v skladu s **členi 5, 6, 7 in 9**;
- b) **pravic posameznika**, na katerega se nanašajo podatki, v skladu s **členi 12 do 22**;
- c) **prenosi** osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji,;
- d) katere koli **obveznosti v skladu s pravom države članice**, sprejete na podlagi poglavja IX;
- e) ki pomenijo neupoštevanje odredbe ali začasne ali dokončne omejitve obdelave ali prekinitve prenosa podatkov, ki jo izda nadzorni organ v skladu z drugim odstavkom 58. člena ali nezagotovitev dostopa, s čimer se krši prvi odstavek 58. člena Splošne uredbe.

Smiselno upoštevati tudi možne višine kazni, kot jih določa ZVOP-2, ZVOPOKD oz. obstoječa področna zakonodaja.



Resnost tveganj in načelo točnosti

Poleg višin potencialnih kazni upoštevati še naslednje elemente:

- **možnost diskriminatornih posledic za posameznike** na podlagi rasnega ali etničnega porekla, političnega mnjenja, vere ali prepričanja, članstva v sindikatu, genetskega ali zdravstvenega stanja, spolne usmerjenosti ali učinki, ki privedejo do ukrepov, ki imajo takšne posledice (uvodna določba št. 71);
- ocena, ali gre za takšno tveganje za pravice in svoboščine posameznika, ki bi lahko povzročilo **fizično, premoženjsko in ali nepremoženjsko škodo**, zlasti:
 - kadar obdelava lahko privede do **diskriminacije, kraje ali zlorabe identitete, finančne izgube, okrnitve ugleda, izgube zaupnosti osebnih podatkov, zaščitnih s poklicno molčečnostjo, neodobrene reverzije psevdonimizacije** ali katere koli druge **znatne gospodarske ali socialne škode**;
 - kadar bi bile posameznikom **lahko odvzete pravice in svoboščine** ali bi jim bilo **preprečeno izvajanje nadzora** nad njihovimi osebnimi podatki;



Resnost tveganj in načelo točnosti

- kadar se obdelujejo posebne vrste osebnih podatkov,
- kadar se **vrednotijo osebni vidiki**, zlasti **analiziranje** ali predvidevanje vidikov, ki zadevajo **uspešnost pri delu, ekonomski položaj, zdravje, osebni okus ali interese, zanesljivost ali vedenje, lokacijo ali gibanje**, da bi se ustvarili ali uporabljali osebni profili,
- kadar se obdelujejo **osebni podatki ranljivih posameznikov, zlasti otrok**;
- ali kadar obdelava vključuje veliko število osebnih podatkov in zadeva veliko število posameznikov (uvodna določba št. 75).



Resnost tveganj in načelo točnosti

- Glede na uvodno določbo št. 76 bi bilo **tako verjetnost kot resnost tveganja** za pravice in svoboščine posameznika treba **ugotavljati glede na vrsto, obseg, okoliščine in namene obdelave**.
- Tveganje bi bilo treba oceniti na podlagi **objektivne ocene**, s katero se določi, ali dejanja obdelave podatkov pomenijo tveganje ali veliko tveganje.

Kot dodatne **možne elemente ocene resnosti** predlagamo tudi naslednje:

- ali bi uresničitev tveganja za posameznika (in/ali za organizacijo) pomenila **trajne/nepopravljive posledice**;
- ali bi uresničitev tveganja imela **resne posledice ne samo za posameznika temveč za druge, z njim povezane posameznike** (npr. sorodnike, partnerje, ostale udeležene v določeni socialno ekonomski skupini ali združenju ipd.);
- z vidika organizacije: ali bi uresničitev tveganja imela **visoke posledice z vidika potrebnih popravljalnih ukrepov ter finančnih in nefinančnih posledic za organizacijo** (npr. izguba ugleda, zaupanja) ter **trajnost** takšnih posledic.



Nekaj primerov za razmislek

Kakšna je resnost uresničitve naslednjih tveganj oz. groženj?

- Hekerski vdor v centralizirano zbirko podatkov o pacientih
- Nepooblaščen dostop in objava videoposnetka z vhoda v kliniko za prekinitev nosečnosti
- Pošiljanje novičnika ministrstva na napačen e-naslov
- Vdor v informacijski sistem, kjer se izdelujejo potne listine
- Pomota v EMŠO mladoletnika, ki ga išče policija zaradi storitve kaznivega dejanja
- Pridobitev lokacije telefona napačne osebe (ki ni pogrešana)
- Nerazpoložljivost informacijskega sistema za izdajo zdravil na recept
- Napačna identifikacija stranke pri prodaji parcele
- Pridobivanje prometnih komunikacijskih podatkov brez sodne odredbe
- Nenamenska uporaba podatkov sicer pooblaščene osebe za dostop do podatkov v sistemu eSociala



Hvala za
pozornost!