Usmeritve pri revidiranju varovanja osebnih podatkov pri proračunskem uporabniku

mag. Andrej Tomšič

namestnik informacijske pooblaščenke

KONFERENCA IZVAJALCEV NOTRANJEGA REVIDIRANJA PRORAČUNSKIH UPORABNIKOV

15. oktober 2019, Ljubljana

Reforma zakonodajnega okvira v EU

UREDBA (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)

(General Data Protection Regulation – GDPR)

Ključni elementi pri revidiranju varovanja osebnih podatkov pri proračunskem uporabniku

- Podrobno poznavanje določb zakonodaje, smernic, mnenj in nadzorne **prakse IP**: https://www.ip-rs.si/varstvo-osebnih-podatkov/praksa-ip/

- Sodelovanje in sinergije s pooblaščenimi osebami za varstvo osebnih podatkov (DPO)

- **Ključna področja nadzora:**
  - Zakonitost obdelave (vključno s področnimi ureditvami)
  - Informacijska varnost
  - Ureditev pogodbene obdelave
  - Informiranje posameznika
  - Dolžnosti glede ocen učinka, pooblaščenih oseb
  - Prenos podatkov v tretje države in medn. organizacije

POMEMBNE DEFINICIJE

- (5)„**psevdonimizacija**“ - **obdelava OP** na tak način, da OP brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo OP, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se OP ne pripišejo določenemu ali določljivemu posamezniku;
- (6) „**zbirka**“ pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
- (8) „**obdelovalec**“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- (11) „**privolitev posameznika, na katerega se nanašajo OP**“ pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo OP, s katero z **izjavo** ali **jasnim pritrdilnim dejanjem** izrazi soglasje z obdelavo OP, ki se nanašajo nanj;
- (12)„**kršitev varnosti OP**“ pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do OP, ki so poslani, shranjeni ali kako drugače obdelani;

TEMELJNA NAČELA

Člen 5 - Načela v zvezi z obdelavo OP

- zakonitost, pravičnost in preglednost (*lawfulness, fairness and transparency*)
- omejitev namena (*purpose limitation*)
- najmanjši obseg podatkov (*data minimisation*)
- točnost (*accuracy*)
- omejitev shranjevanja (*storage limitation*)
- celovitost in zaupnost (*integrity and confidentiality*),
  - razpoložljivost?
- **odgovornost (*accountability*)**
  - **odgovoren za skladnost s temeljnimi načeli in je to skladnost tudi zmožen dokazati**

ČLEN 25 - VGRAJENO IN PRIVZETO VARSTVO PODATKOV

Ob upoštevanju **tehnološkega razvoja**, **stroškov** izvajanja ter **narave, obsega, okoliščin in namenov obdelave ter tveganj** upravljavec **v času določanja sredstev obdelave** kot tudi **v času same obdelave** izvaja ustrezne tehnične in organizacijske ukrepe, **kot je psevdonimizacija** in **načelo najmanjšega obsega podatkov**, ter v obdelavo vključi primerne **varovalke**.

ANONIMNI PODATKI >>>>>> **PSEVDONIMNI (OSEBNI) PODATKI** >>>>> **SUROVI OSEBNI PODATKI**

Privzeto se obdelajo **<u>samo OP, ki so potrebni za vsak poseben namen obdelave</u>:**

- **količina** zbranih OP,
- **obseg** obdelave,
- **obdobje hrambe,**
- **dostopnost podatkov**.

Primeri: nova zbirka osebnih podatkov, aplikacija, storitev, zamenjava informacijskega sistema ali velikega pogodbenega izvajalca…

ČLEN 28 – UREDITEV POGODBENE OBDELAVE

- Najame se lahko le obdelovalce, ki **zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov** na tak način, da obdelava izpolnjuje zahteve iz uredbe in zagotavlja varstvo pravic posameznika.

- **Obdelovalec ne zaposli drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca**.
- V primeru splošnega pisnega dovoljenja **obdelovalec upravljavca obvesti** o vseh nameravanih spremembah **glede zaposlitve dodatnih obdelovalcev** ali njihove zamenjave, s čimer se **upravljavcu omogoči, da nasprotuje tem spremembam**.
- Več zahtev za pogodbe:
  - **obveznosti obdelovalca** do upravljavca,
  - **vsebina in trajanje obdelave**,
  - **narava** in **namen** obdelave,
  - **vrsta OP**,
  - **kategorije posameznikov** ter
  - **obveznosti in pravice upravljavca**.

Pogodba ali drug pravni akt zlasti **določa, da <u>obdelovalec</u>**:

a) OP obdeluje **samo po dokumentiranih navodilih upravljavca**, vključno glede prenosov OP v tretjo državo ali mednarodno organizacijo,
b) zagotovi, da so **osebe, ki so pooblaščene za obdelavo OP, zavezane k zaupnosti** ali jih k zaupnosti zavezuje ustrezen zakon;
c) sprejme vse **ukrepe**, potrebne v skladu s členom 32 (inf. varnost);
d) spoštuje pogoje za **zaposlitev drugega obdelovalca**;
e) pomaga **upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi** pri uresničevanju pravic posameznika,
f) **upravljavcu pomaga pri izpolnjevanju obveznosti** iz členov 32 do 36;
g) **v skladu z odločitvijo upravljavca izbriše ali vrne vse OP upravljavcu** po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, (razen izjem).
h) **omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje**.
- obdelovalec nemudoma obvesti upravljavca, če po njegovem mnenju navodilo krši to uredbo ali druge predpise.

ČLEN 30 - EVIDENCA DEJAVNOSTI OBDELAVE („KATALOGI“)

U<u>pravljavec in njegovi predstavniki (</u>kadar obstajajo), vodijo **evidenco dejavnosti obdelave OP**, ki vsebuje:

- **naziv ali ime in kontaktne podatke upravljavca** in, kadar obstajajo, **skupnega upravljavca**, **predstavnika upravljavca** in **pooblaščene osebe za varstvo** podatkov;
- **namene** obdelave;
- **opis kategorij** posameznikov in **vrst** OP;
- **kategorije prejemnikov**, ki so jim bili ali jim bodo razkriti OP, vključno s prejemniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, **informacije o prenosih OP v tretjo državo ali mednarodno organizacijo**;
- kadar je mogoče, **predvidene roke za izbris** različnih vrst podatkov;
- kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov**.

Vsak **obdelovalec in predstavnik obdelovalca**, kadar ta obstaja, vodita evidenco vseh vrst dejavnosti obdelave, ki jih izvajata v imenu upravljavca, ki vsebuje:

a) **naziv ali ime in kontaktne podatke obdelovalca** ali obdelovalcev in vsakega **upravljavca**, v imenu katerega deluje obdelovalec, ter, kadar obstajajo, **predstavnika** upravljavca ali obdelovalca, in **pooblaščene osebe za varstvo OP**;

b) **vrste obdelave**, ki se izvaja v imenu posameznega upravljavca;

c) Informacije o **prenosih OP v tretjo državo ali mednarodno organizacijo**, kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov.**

- Evidence so v **pisni**, **vključno v elektronski obliki**.
- **Nadzorni organ ima na zahtevo dostop do evidenc**.
- Izjema: zaposluje **manj kot 250 oseb**, razen če visoka tveganja, ne gre za občasno obdelavo ali posebne vrste poDatkov.

ČLEN 32 - VARNOST OBDELAVE

Ob **upoštevanju najnovejšega tehnološkega razvoja** in **stroškov** izvajanja ter **narave, obsega, okoliščin in namenov obdelave**, pa tudi **tveganj** za pravice in svoboščine posameznikov, ki se razlikujejo po **verjetnosti** in **resnosti**, **upravljavec** in **obdelovalec** z izvajanjem **ustreznih tehničnih** in **organizacijskih** ukrepov zagotovita **ustrezno raven varnosti glede na tveganje**, vključno med drugim z naslednjimi ukrepi, kot je ustrezno:

(a) **psevdonimizacijo** in **šifriranjem** OP;

(b) zmožnostjo zagotoviti stalno **zaupnost, celovitost, dostopnost** in **odpornost** *(*resilience)* sistemov in storitev za obdelavo;

(c) zmožnostjo pravočasno **povrniti razpoložljivost** in dostop do OP v primeru fizičnega ali tehničnega incidenta;

(d) postopkom **rednega testiranja**, **ocenjevanja** in **vrednotenja učinkovitosti** tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

- **Smernice o zavarovanju osebnih podatkov**

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf

- **Vprašalnik o informacijski varnosti – za večje upravljavce**

https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/

Najpogostejše kršitve:

- Poudarek na tehničnih ukrepih, premalo pozornosti organizacijskim ukrepom
- Interni akti, ki ne ustrezajo dejanskemu stanju
- Odsotnost rednega izobraževanja
- Neurejene dostopne pravice
- Ni sledljivosti obdelave OP
- Pomanjkljiv nadzor nad priviligiranimi uporabniki
- Neupoštevanje politike čiste mize in čistega zaslona
- Pomanjkljiv nadzor in nejasne pogodbene zahteve pri pogodbeni obdelavi osebnih podatkov
- Premalo pozornosti informacijski varnosti pri razvoju novih rešitev

ČLEN 33 - URADNO OBVESTILO NADZORNEMU ORGANU O KRŠITVI VARNOSTI OP

- V primeru kršitve varnosti OP upravljavec brez nepotrebnega odlašanja oz. **najpozneje v 72 urah** po seznanitvi s kršitvijo, **o njej uradno obvesti pristojni nadzorni organ**, razen če ni verjetno, da bi bile s kršitvijo varnosti OP ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo **ni podano v 72 urah, se mu priloži navedbo razlogov** za zamudo.
- **Obdelovalec** po seznanitvi s kršitvijo varstva OP **brez nepotrebnega odlašanja uradno obvesti upravljavca**.
- Uradno obvestilo vsebuje vsaj:
  - **a)** **opis vrste kršitve** varnosti OP, po možnosti tudi **kategorije** in **približno število zadevnih posameznikov**, ter **vrste** in približno **število zadevnih evidenc** OP;
  - b) sporočilo o **imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov** ali druge točke, pri kateri je mogoče pridobiti več informacij;
  - **c)** **opis verjetnih posledic** kršitve varnosti OP;
  - **d)** **opis ukrepov**, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varnosti OP, pa tudi ukrepov **za ublažitev morebitnih škodljivih učinkov** kršitve, če je to ustrezno.

ČLEN 35 - OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV (Data Protection Impact Assesment)

Ocena zajema vsaj:

a) **sistematičen opis predvidenih dejanj** obdelave in **namenov** obdelave, kadar je ustrezno pa tudi **zakonitih interesov**, za katere si prizadeva upravljavec;

b) oceno **potrebnosti** in **sorazmernosti** dejanj obdelave glede na njihov namen;

c) **oceno tveganj** za pravice in svoboščine posameznikov ter

d) **ukrepe za obravnavanje tveganj**, vključno z zaščitnimi ukrepi, **varnostne ukrepe** ter mehanizme za zagotavljanje varstva OP in za **dokazovanje skladnosti** s to uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo OP, ter drugih oseb, ki jih to zadeva.

Ocena se revidira, ko se spremenijo ključne okoliščine.

Smernice IP: Smernice o ocenah učinkov na varstvo podatkov

Seznam dejanj obdelave, ki terjajo izvedbo ocene učinka:

1. OBSEŽNO VREDNOTENJE IN PROFILIRANJE POSAMEZNIKOV
2. AVTOMATIZIRANO ODLOČANJE S PRAVNIM ALI PODOBNIM UČINKOM
3. SISTEMATIČEN NADZOR NAD POSAMEZNIKOM BREZ NJEGOVEGA ZAVEDANJA
4. OBDELAVA POSEBNIH VRST OSEBNIH PODATKOV
5. MNOŽIČNOST OBDELAVE OSEBNIH PODATKOV
6. PRIMERJANJE IN KOMBINIRANJE RAZLIČNIH ZBIRK PODATKOV (NPR. PRIDOBLJENIH SKOZI RAZLIČNE AKTIVNOSTI UPRAVLJAVCA) IN ANALITIKA NA OSNOVI MASOVNIH PODATKOV
7. NESORAZMERJE MOČI
8. INOVATIVNA UPORABA OBSTOJEČIH IN NOVIH TEHNOLOGIJ
9. OMEJITEV DOSTOPA DO STORITVE/POGODBE
10. NEPOSREDNO TVEGANJE ZA ZDRAVJE IN VARNOST POSAMEZNIKOV

ČLEN 39 - NALOGE POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV

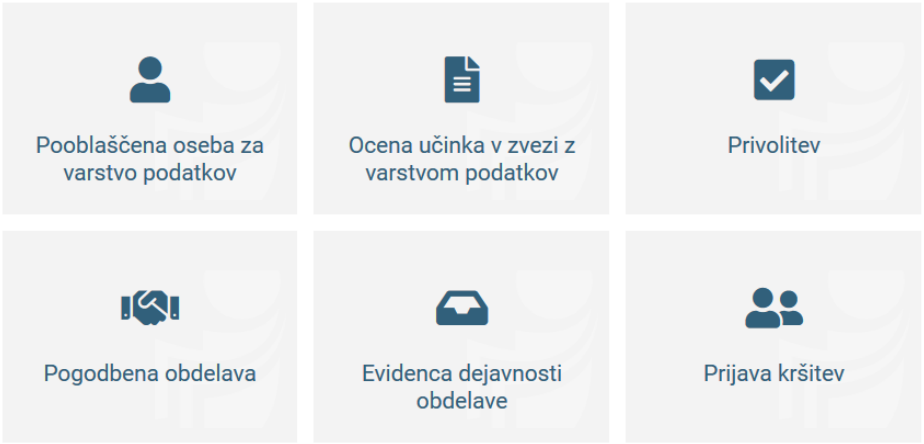
Naloge DPO :

a) **obveščanje upravljavca** ali **obdelovalca** in **zaposlenih** ter **svetovanje** navedenim o njihovih **obveznostih** po uredbi in predpisih o VOP;
b) **spremljanje skladnosti** z uredbo, drugimi predpisi VOP, **politikami upravljavca** ali obdelovalca, vključno z **dodeljevanjem nalog**, **ozaveščanjem** in **usposabljanjem** osebja, vključenega v dejanja obdelave, ter s tem povezanimi **revizijami**;
c) **svetovanje** glede **ocene učinka** v zvezi z varstvom OP in spremljanje njenega izvajanja;
d) **sodelovanje z nadzornim organom**;
e) delovanje kot **kontaktna točka za nadzorni organ** pri vprašanjih v zvezi z obdelavo, vključno s **predhodnim posvetovanjem**.

DPO pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave.

NOVA GRADIVA IP

Ključna področja



Obrazci

- Informacije za posameznike (13.čl.)
- Evidentiranje dejavnosti (30. čl.)
- Prijava kršitev varnosti (33. čl.)
- Imenovanje DPO (37. čl.)

Infografike

- Pravne podlage za javni sektor - PDF | PNG
- Pravne podlage za zasebni sektor - PDF | PNG
- Neposredno trženje - PDF | PNG
- Prenos v tretje države - PDF | PNG

Prenova smernic

- Pogodbena obdelava, informirani potrošnik, prenos v tretje države, šolstvo….

Projekt RAPID.SI ----------> **projekt iDECIDE**

(mala podjetja in posamezniki) **(javna uprava in posamezniki)**

- upravljavec.si
- tiodlocas.si
- 080 2900

POMEMBNE SMERNICE

Ocene učinkov

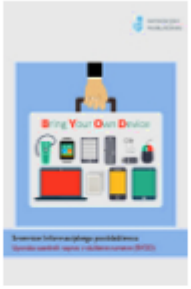
Smernice o varstvu osebnih podatkov pri uporabi GPS naprav

Smernice o zavarovanju osebnih podatkov

Smernice za razvoj informacijskih rešitev

Smernice o pogodbeni obdelavi

Smernice za varstvo osebnih podatkov v delovnih razmerjih



Smernice o uporabi zasebnih naprav v službene namene (BYOD)

Socialni inženiring in kako se pred njim ubraniti

Smernice za varstvo osebnih podatkov in računalništvo v oblaku

Hvala za pozornost!

www.ip-rs.si

www.upravljavec.si

www.tiodlocas.si