Novosti na področju varstva osebnih podatkov Splošna uredba EU o varstvu osebnih podatkov (GDPR)

mag. Andrej Tomšič

namestnik informacijske pooblaščenke

7. konferenca komunalnega gospodarstva

Rimske toplice, 21. In 22. september 2017

UREDBA (EU) 2016/679 - Splošna uredba o varstvu podatkov
(General Data Protection Regulation – GDPR)

- **Zakaj?**
  - evropski sistem varstva osebnih podatkov (OP) temelji na direktivi iz leta 1995 (95/46)
  - posodobitev ob tehnološkem razvoju in globalizaciji podatkovnih tokov
    - Google, Facebook, cloud computing, internet stvari…
  - potreba po večji harmonizaciji
    - tolmačenj, pooblastil, sankcij (npr. Španija, VB)
    - primer Google Street View
  - pritiski multinacionalk
    - lažji pretok podatkov
    - različna pravila v EU državah (številna odstopanja nacionalnih zakonodaj)
    - manj administrativnih bremen (npr. prijava zbirk v 28 nacionalnih registrov)
  - več pravic za posameznike

Reforma

Prvi predlog Evropske komisije 2012

- splošna uredba za vse sektorje
- direktiva za policijski sektor/pregon KD
- uredba ima neposredno veljavo v državah članicah
- ogromno lobiranja, različna stališča EK, EP in Sveta

Sprejem v EP 14.4.2016

- Uredba začela veljati 20 dni po objavi v Uradnem listu EU – **25.5.2016**
- Razveljavlja Direktivo 95/46
- Njene določbe se bodo morale neposredno uporabljati v vseh državah članicah **v dveh letih** – **25.5.2018**.
- Rok za prenos določb direktive v nacionalno zakonodajo je prav tako **dve leti**.
  - sprejem izvedbenih aktov, nova izvedbena uredba v SI, morebitne spremembe ZVOP-1 –> **ZVOP-2?**
- Veljavno(!) besedilo uredbe:
  - http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016R0679&from=SL
  - na prosojnicah so povzetki

POGLAVJE II - 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 z temeljnimi načeli in je to skladnost tudi zmožen dokazati -> več poudarka **preventnim/proaktivnim** ukrepom

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 24 - Odgovornost upravljavca

Ob upoštevanju **narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj** za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec izvede ustrezne **tehnične in organizacijske ukrepe**, da **zagotovi** in je **zmožen dokazati, da obdelava poteka v skladu s to uredbo**. Ti ukrepi se **pregledajo in dopolnijo**, kjer je to potrebno.

Kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi vključujejo **izvajanje ustreznih politik** za varstvo podatkov s strani upravljavca.

Spoštovanje odobrenih **kodeksov ravnanja** ali izvajanje **odobrenega mehanizma potrjevanja** se lahko uporabi za **dokazovanje izpolnjevanja obveznosti upravljavca**.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

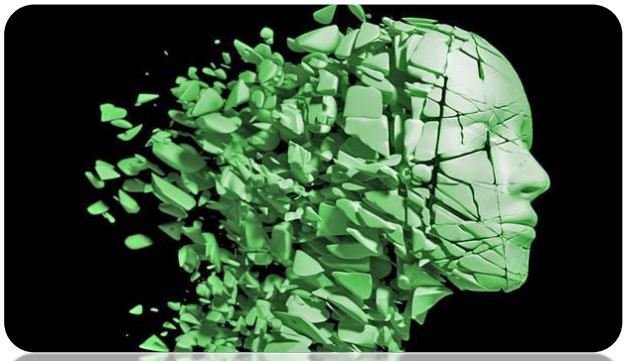
Člen 25 - Vgrajeno in privzeto varstvo podatkov

1. 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**.

2. **Privzeto** se obdelajo **samo OP, ki so potrebni za vsak poseben namen obdelave:**

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



3. Pridobljeni certifikat izkazuje skladnost.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 28 – Obdelovalec

- Najame se lahko le obdelovalce, ki **zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov za varnost OP**.
- **Obdelovalec ne zaposli drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca**.
  - **Ponudniki gostovanja, oblačnih in drugih IT storitev, računovodskio servisi, klicni centri…**
- 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 z zunanjimi izvajalci**:
  - **obveznosti obdelovalca** do upravljavca,
  - **vsebina in trajanje obdelave**,
  - **narava** in **namen** obdelave,
  - **vrsta OP**,
  - **kategorije posameznikov** ter
  - **obveznosti in pravice upravljavca**.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 30 - Evidenca dejavnosti obdelave („katalogi“)

Upravljavci, **obdelovalci in njihov predstavniki**, kadar obstajajo, vodijo evidenco vseh vrst dejavnosti obdelave.

Evidenca predstavlja **opis zbirk**, ki jih vodijo (vsebino zbirk, namene, pravne podlage, varnostne postopke…).

Register zbirk (prijava zbirk) osebnih podatkov pri nadzornih organih **se ukinja, katalogi pa ostajajo!**

- 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, posebne vrste podatkov.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 32 - Varnost obdelave

1. 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.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 32 - Varnost obdelave

2. Pri določanju ustrezne ravni varnosti se upoštevajo zlasti **tveganja**, ki jih pomeni obdelava, zlasti zaradi **nenamernega** ali **nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja** ali **dostopa** do OP, ki so poslani, shranjeni ali kako drugače **obdelani**.

3. Spoštovanje odobrenega **kodeksa ravnanja** ali izvajanje **odobrenega mehanizma potrjevanja** se lahko uporabi za **dokazovanje izpolnjevanja** zahtev glede varnosti.

4. Upravljavec in obdelovalec zagotovita, da **katera koli fizična oseba**, ki ukrepa pod vodstvom upravljavca ali obdelovalca, ki ima dostop do **OP**, slednjih **ne sme obdelati brez navodil upravljavca**, razen če to od nje zahteva pravo Unije ali pravo države članice.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 33 - Uradno obvestilo nadzornemu organu o kršitvi varstva OP

1. V primeru kršitve varstva OP upravljavec brez nepotrebnega odlašanja, po možnosti pa **najpozneje v 72 urah** po seznanitvi s kršitvijo, **o njej uradno obvesti pristojni nadzorni organ**, razen če ni verjetno, da bi bile s kršitvijo varstva OP ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo **ni podano v 72 urah, se mu priloži navedbo razlogov** za zamudo.
2. **Obdelovalec** po seznanitvi s kršitvijo varstva OP **brez nepotrebnega odlašanja uradno obvesti upravljavca**.
3. Uradno obvestilo vsebuje vsaj:

a) **opis vrste kršitve** varstva OP, po možnosti tudi **kategorije** in **približnoštevilo 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 varstva OP;

d) **opis ukrepov**, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva OP, pa tudi ukrepov **za ublažitev morebitnih škodljivih učinkov** kršitve, če je to ustrezno.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 33 - Uradno obvestilo nadzornemu organu o kršitvi varstva OP

4. **Kadar** in kolikor informacij **ni mogoče zagotoviti istočasno**, se informacije lahko zagotovijo **postopoma brez nepotrebnega dodatnega odlašanja**.

5. Upravljavec **dokumentira vsako kršitev varstva OP**, vključno z **dejstvi** v zvezi s kršitvijo varstva OP, njene **učinke** in **sprejete popravne ukrepe**. Ta dokumentacija **nadzornemu organu omogoči, da preveri skladnost s tem členom.**

V določenih, huduh primerh potrebno obvestizti tudi posameznike (člen 34).

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 34 - Sporočilo **posamezniku** o kršitvi varstva OP

1. Kadar je verjetno, da kršitev varstva OP povzroči **veliko tveganje za pravice in svoboščine posameznikov**, upravljavec brez nepotrebnega odlašanja **sporoči posamezniku, da je prišlo do kršitve varstva OP.**
2. V sporočilo posamezniku je v **jasnem** in **preprostem jeziku** opisana **vrsta kršitve** varstva OP ter so vsebovane vsaj **informacije in priporočila** (po 33(3) (b), (c) in (d).

3. Sporočilo posamezniku **ni potrebno, če** je izpolnjen kateri koli izmed naslednjih pogojev:

a) upravljavec je izvedel **ustrezne tehnične in organizacijske zaščitne ukrepe** in so bili ti ukrepi uporabljeni za OP, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo OP **nerazumljivi vsem**, ki niso pooblaščeni za dostop do njih, **kot je šifriranje**;
b) upravljavec je sprejel **naknadne ukrepe** za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, **verjetno ne bo več udejanjilo**;
c) to **bi zahtevalo nesorazmeren napor**. V takšnem primeru se namesto tega objavi **javno sporočilo** ali izvede **podoben ukrep**, s katerim so posamezniki **enako učinkovito obveščeni**.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 37 - Imenovanje pooblaščene osebe za varstvo podatkov *(DPO)*

Upravljavec in **obdelovalec** imenujeta **DPO** vedno, kadar:

a) **javni organ ali telo, razen sodišč**, kadar delujejo kot sodni organ;
b) temeljne dejavnosti zajemajo dejanja **obdelave**, pri katerih je treba **zaradi njihove narave, obsega in/ali namenov posameznike redno in sistematično obsežno spremljati**, ali
c) temeljne dejavnosti upravljavca ali obdelovalca zajemajo **obsežno obdelavo *posebnih* vrst podatkov** in OP v zvezi s KDin prekrški.

DPO:

- se imenuje na podlagi **poklicnih odlik** in zlasti **strokovnega znanja** o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog.
- je **lahko član osebja** upravljavca ali obdelovalca ali pa naloge opravlja **na podlagi pogodbe o storitvah**.
- upravljavec ali obdelovalec **objavi kontaktne podatke DPO** in jih sporoči nadzornemu organu.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 38/39 - Položaj in naloge pooblaščene osebe za varstvo podatkov

Položaj:

- **ustrezno in pravočasno vključen** v vse zadeve v zvezi z varstvom OP**,**
- **ima sredstva, dostop do OP in dejanj obdelave, ter ohranjanje znanja,**
- pri opravljanju teh nalog **ne prejema nobenih navodil**,
- **ne sme biti razrešena** ali **kaznovana** zaradi opravljanja svojih nalog,
- **poroča neposredno najvišji upravni ravni** upravljavca ali obdelovalca,
- pri opravljanju svojih nalog **zavezana varovati skrivnost ali zaupnost,**
- **lahko opravlja druge naloge in dolžnosti** (če ni **nasprotja interesov).**

Naloge DPO :

- **obveščanje** upravljavca in zaposlenih ter **svetovanje** o njihovih obveznostih po uredbi in predpisih o VOP;
- **spremljanje skladnosti** z uredbo, drugimi predpisi VOP, politikami upravljavca ali obdelovalca,
- **svetovanje** glede ocene učinka v zvezi z varstvom OP in spremljanje izvajanja;
- **sodelovanje** z nadzornim organom.

POGLAVJE IV - UPRAVLJAVEC IN OBDELOVALEC

Člen 42 – Potrjevanje (*certification*)

- **Uredba spodbuja vzpostavitev mehanizmov potrjevanja** ter **pečatov** in **označb za varstvo podatkov** za dokazovanje skladnosti z uredbo.

- Potrjevanje je **prostovoljno** in po preglednem **postopku.**

- **Potrdilo:**
  - **ne zmanjšuje odgovornosti upravljavca** ali **obdelovalca**.
  - **Izdajo organi za potrjevanje** iz člena **43 ali pristojni nadzorni organ**, in sicer **na podlagi meril**, ki jih odobri ta pristojni **nadzorni organ** ali **odbor**.
  - se izda za največ **tri leta** in
  - se pod enakimi pogoji lahko podaljša/prekliče..

- Poleg nadzornega organa lahko potrdilo **izda in podaljša strokoven in neodvisen organ za potrjevanje (pooblastilo/akreditacija s strani IP in/ali Slovenske akreditacije, pet let).**

POGLAVJE VIII - PRAVNA SREDSTVA, ODGOVORNOST IN KAZNI

Člen 83 - Splošni pogoji za naložitev upravnih glob

Upravne globe so **učinkovite, sorazmerne in odvračilne**.

Upošteva se:

a) **narava, teža in trajanje kršitve**, **število posameznikov**, **raven škode**, ki so jo utrpeli;
b) ali je kršitev **namerna** ali posledica **malomarnosti**;
c) vsi **ukrepi, ki jih je sprejel upravljavec ali obdelovalec**, da bi ublažil škodo,
d) **stopnja odgovornosti upravljavca ali obdelovalca**, pri čemer se upoštevajo tehnični in organizacijski ukrepi, ki jih je sprejel v skladu s členoma 25 in 32;
e) vse zadevne **predhodne kršitve** upravljavca ali obdelovalca;
f) **stopnja sodelovanja z nadzornim organom** pri odpravljanju kršitve in blažitvi morebitnih škodljivih učinkov kršitve;
g) **vrste osebnih podatkov**, ki jih zadeva kršitev,
h) **kako je nadzorni organ izvedel za kršitev**,;
i) če so bili **ukrepi že prej odrejeni** zoper zadevnega upravljavca ali obdelovalca v zvezi z enako vsebino, skladnost s temi ukrepi;
j) **upoštevanje odobrenih kodeksov ravnanja** ali **odobrenih mehanizmov potrjevanja**, in
k) morebitni **drugi oteževalni ali olajševalni dejavniki** npr. pridobljene finančne koristi.

POGLAVJE VIII - PRAVNA SREDSTVA, ODGOVORNOST IN KAZNI

Člen 83 - Splošni pogoji za naložitev upravnih glob

Upravne globe v znesku **do 10 000 000 EUR** ali v primeru družbe v znesku do **2% skupnega svetovnega letnega prometa** v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji:

a) obveznosti upravljavca in obdelovalca v skladu s členi 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 in 43;
b) obveznosti organa za potrjevanje v skladu s členoma 42 in 43;
c) obveznosti organa za spremljanje v skladu s členom 41(4).

Upravne globe v znesku **do 20 000 000 EUR** ali v primeru družbe v znesku do **4% skupnega svetovnega letnega prometa** v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji:

a) osnovna načela obdelave, vključno s pogoji za privolitev, v skladu s členi 5, 6, 7 in 9;
b) pravice posameznika, na katerega se nanašajo podatki, v skladu s členi 12 do 22;
c) prenosi osebnih podatkov prejemniku v tretji državi ali mednarodni organizaciji, v skladu s členi 44 do 49;

KLJUČNE TOČKE GDPR PRIPRAVLJENOSTI

1. PREVERITE **VELJAVNOST OBSTOJEČIH PRIVOLITEV**
2. PREVERITE **NAČIN PRIDOBIVANJA PRIVOLITVE V BODOČE**
3. PRILAGODITE **POGODBE** S POGODBENIMI OBDELOVALCI
4. PREVERITE IN PRILAGODITE KATALOGE – **EVIDENCE DEJAVNOSTI OBDELAVE** (OBDELOVALCI!)
5. PREGLEJTE POSTOPKE ZA ZAGOTAVLJANJE **PRAVIC POSAMEZNIKA** (SEZNANITEV, UGOVOR, OMEJITEV, IZBRIS, PRENOSLJIVOST)
6. PRIPRAVITE SE NA **IZVAJANJE NAČELA ODGOVORNOSTI**
   a) PREVERITE, ALI BOSTE MORALI IZVAJATI **OCENE UČINKA**
   b) PREVERITE, ALI BOSTE MORALI IMENOVATI **DPO**
   c) RAZMISILTE, KAKO BOSTE UPOŠTEVALI **NAČELO VGRAJENEGA IN PRIVZETEGA VARSTVA PODATKOV**
7. PREGLEJTE IN PRILAGODITE **VARNOSTNE POLITIKE IN NJIHOVO IZVAJANJE**
8. PRIPRAVITE **POSTOPEK POROČANJA IN UPRAVLJANJA KRŠITEV VARNOSTI**
9. **DOLOČITE, KDO BO POROČAL V PRIMERU VARNOSTNEGA INCIDENTA**
10. OCENITE INTERES GLEDE **CERTIFICIRANJA**

Hvala za pozornost!

Spremljate GDPR novosti na:

https://www.ip-rs.si/
(mnenja, letaki, smernice…)