SPLOŠNA UREDBA O VARSTVU PODATKOV – GDPR
MITI IN RESNICE

mag. Andrej Tomšič
namestnik informacijske pooblaščenke

Konferenca Mreža znanja

22. november 2017

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)

Podatki so (RES)nova nafta

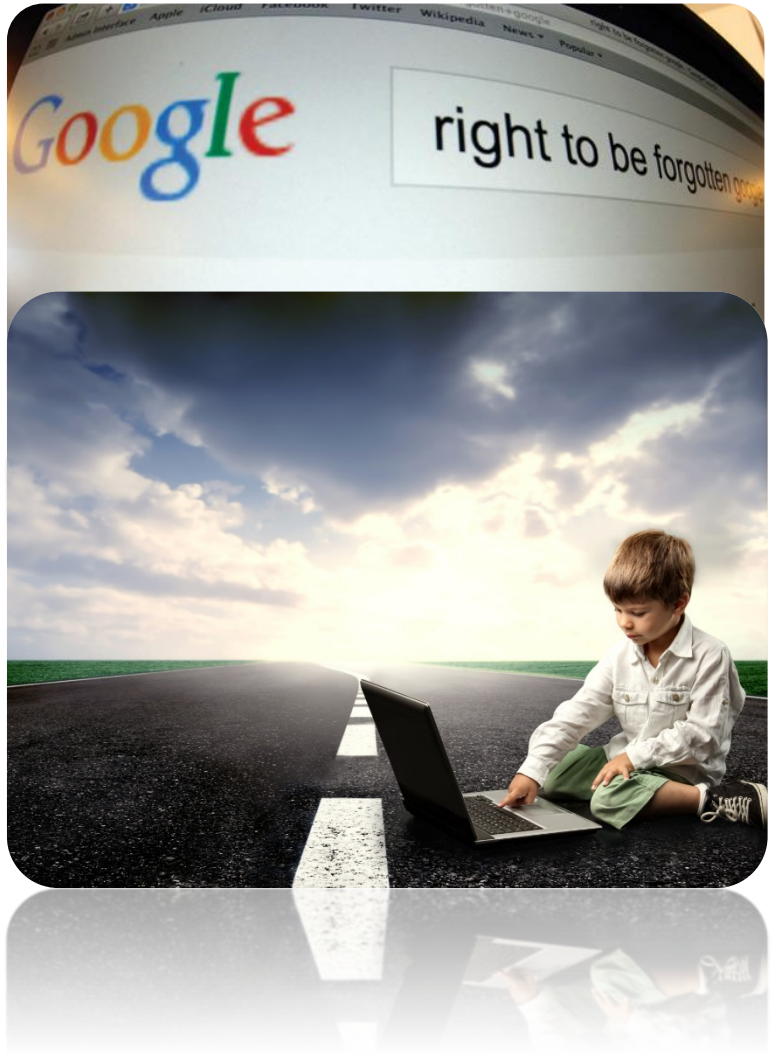
“NA ZAHTEVO POSAMEZNIKA BOMO SEDAJ MORALI IZBRISATI VSE NJEGOVE PODATKE“

Člen 17

- **Ni** pravica do izbrisa zgodovine, pravica do cenzure!
- **Umik podatkov oz. povezav do nepotrebnih, zastarelih, izrazito škodljivih podatkov o posamezniku**
  - npr. nepremišljene izjave/objave v mladosti
  - primer pianista in lastnika avtokampa

- **Tehtanje pravic**!
- **Druge pravne podlage!**

- **Številne izjeme**: svoboda izražanja in obveščanja, pravna obveznost, javni interes, arhiviranje v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene…



„POSAMEZNIK BO LAHKO DOBIL ELEKTRONSKO VERZIJO SVOJIH PODATKOV”

Člen 20

Posameznik ima pravico, da prejme OP v zvezi z njim, ki jih je posedoval upravljavcu, **v strukturirani, splošno uporabljani in strojno berljivi obliki**, in **pravico, da te podatke posreduje drugemu upravljavcu**, ne da bi ga upravljavec pri tem oviral, **kadar**:

a) obdelava temelji na privolitvi (ali pogodbi),
b) se obdelava izvaja z avtomatiziranimi sredstvi.

- Posameznik ima **pravico, da se OP neposredno prenesejo od enega upravljavca k drugemu, *kadar je to tehnično izvedljivo*.**
- Uresničevanje pravice ne posega v pravico do pozabe – dobiš **kopijo podatkov** in ne v **pravice drugih (npr. intelektulano lastnino).**
- Ta pravica se **ne uporablja za obdelavo, potrebno za opravljanje naloge, ki se izvaja v javnem interesu** ali pri izvajanju javne oblasti, dodeljene upravljavcu.

Bomo tako (počasi) spoznali pravo vrednost naših osebnih podatkov?

„PROFILIRANJE NE BO DOVOLJENO“

Člen 22

Posameznik ima pravico, da zanj ne velja **odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov**, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva.


"On the Internet, nobody knows you're a dog."

Avtomatizirano odločanje in profiliranje **dopustno**, če je odločitev:

a) **nujna za sklenitev ali izvajanje pogodbe** med posameznikom in upravljavcem;
b) **dovoljena v pravu Unije ali pravu države članice**, ki velja za upravljavca in določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, ali
c) **utemeljena z izrecno privolitvijo posameznika**.

Pravica do :

- **osebnega posredovanja** (**human intervention*) **upravljavca**,
- do **izražanja lastnega stališča in**
- **izpodbijanja odločitve**.

Avtomatizirane odločitve ne temeljijo na *posebnih vrstah OP* (možne izjeme).

„VSI BOMO MORALI IMETI POOBLAŠČENO OSEBO (DPO)“

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

a) **javni organ ali telo, razen sodišč**, kadar delujejo kot sodni organ; ***ZVOP-2***

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 KD in prekrški.

DPO:

- se imenuje na podlagi **poklicnih odlik** in zlasti **strokovnega znanja** o zakonodaji in praksi na področju VOP ter zmožnosti za izpolnjevanje nalog.
- je **lahko član osebja** ali pa naloge opravlja **na podlagi pogodbe o storitvah**
- upravljavec ali obdelovalec **objavi kontaktne podatke DPO** in jih sporoči nadzornemu organu
  → **Smernice Article 29 Working Party**
- **Nevarnosti**:
  - DPO ni odgovoren za skladnost, odgovoren je upravljavec/obdelovalec!
  - DPO ne sme postati edini, ki kaj ve/mora vedeti o varstvu OP!
  - DPO ne bi smeli biti „lastniki procesov“, ki odločajo o namenih in sredstvih obdelave.

POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV (DPO) (ČLENI 37-39)

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.

„ZA KRŠITVE BOMO DOBILI 20 000 000 EUR KAZNI“

Sankcije bodo **učinkovite**, **sorazmerne** in **odvračilne**.

Upravne globe v znesku **do 10 000 000 EUR** ali v primeru družbe v znesku do **2 % skupnega svetovnega letnega prometa oz. do 20 000 000 EUR** ali v primeru družbe v znesku do **4% skupnega svetovnega letnega prometa** odvisno od tega, kateri znesek je višji.

Upoštevalo se bo 11 kriterijev:

a) **narava, teža in trajanje kršitve**, pri čemer se upoštevajo narava, obseg ali namen zadevne obdelave ter **število posameznikov**, na katere se nanašajo osebni podatki in ki jih je kršitev prizadela, in **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, ki so jo utrpeli posamezniki;
d) **stopnja odgovornosti upravljavca ali obdelovalca**, pri čemer se upoštevajo tehnični in organizacijski ukrepi;
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**, zlasti če in v kakšnem obsegu ga je upravljavec ali obdelovalec uradno obvestil o kršitvi;
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** v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve.

IN ŠE…

„KUPITE NAŠO GDPR ŠKATLO IN REŠITE VSE TEŽAVE„

„VSI BOMO MORALI DOBITI NOVE PRIVOLITVE“

„GDPR POMENI KONEC (SVETA) ZA <*vstavi*>“

…

Kaj moramo glede GDPR in ZVOP-2 storiti in kdaj?

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**

Vzemite zadevo resno, a ne nasedajte zastraševanju z 20-milijonskimi kaznimi!

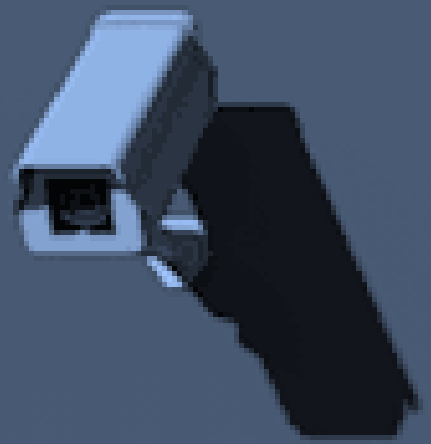
Spremljajte novosti na https://www.ip-rs.si/

- **Smernice na EU ravni**
  - DPO, ocene učinkov, profiliranje, prenosljivost…

Letaki

- **Pogosta vprašanja in odgovori**
  - Katere so glavne novosti, kaj pomenijo za nas kot podjetje ali ustanovo?
  - Ali po GDPR ostajajo izjeme, ki jih je ZVOP-1 predvideval za podjetja z manj kot 50 zaposlenimi?
  - Ali moramo ponovno dobiti privolitev naših strank?
  - Ali moramo imenovati pooblaščeno osebo za varstvo osebnih podatkov (DPO)?
  - …

Priporočam
http://www.socialcooling.com/



Hvala za pozornost!

andrej.tomsic@ip-rs.si

Vir: https://ru.pinterest.com/pin/558868634988583261/