Varstvo osebnih podatkov po GDPR in ZVOP-2

mag. Andrej Tomšič

Uvodna pojasnila

- Seminar je namenjen predstavitvi **ključnih določb GDPR in ZVOP-2**.
- **GDPR** se uporablja od **25.5.2018.**
- **ZVOP-2** se uporablja od **26.1.2023**.
- V praksi: potrebno poznavanje in spoštovanje **tako GDPR kot ZVOP-2 (skupaj)**
  - Samo ZVOP-2 ne bo dovolj!
- **Kompleksna naloga**
  - **GDPR: 99 členov, 173 uvodnih določb**
  - **ZVOP-2: 127 členov**

- **Zakon o varstvu osebnih podatkov (Ur.l. RS št. 163/22; ZVOP-2):**

https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187

Zakaj ZVOP-2?

- Splošna uredba o varstvu podatkov (GDPR) je v uporabi že od **25.5.2018!**
- GDPR prepušča urejanje določenih področij državam članicam
  - Biometrija, genski podatki, zdravstvo, postopkovni vidiki, relacije do drugih področij…
- ZVOP-1 je prenašal direktivo iz leta 1995
- **Brez ZVOP-2 ni bilo možno izrekanje sankcij po GDPR – upravne globe**
  - DPO, evidence dejavnosti, pravne podlage, informiranja posameznikov, pogodbena obdelava, ocena učinka, varnost…
- Zadnja država, ki še ni „pospremila“ GDPR v celoti v uporabo - pritiski Evropske komisije

Ključni pojmi in definicije

določa jih Splošna uredba (4. člen)

1. **OSEBNI PODATEK** pomeni katero koli informacijo v zvezi z **določenim** ali **določljivim posameznikom**;

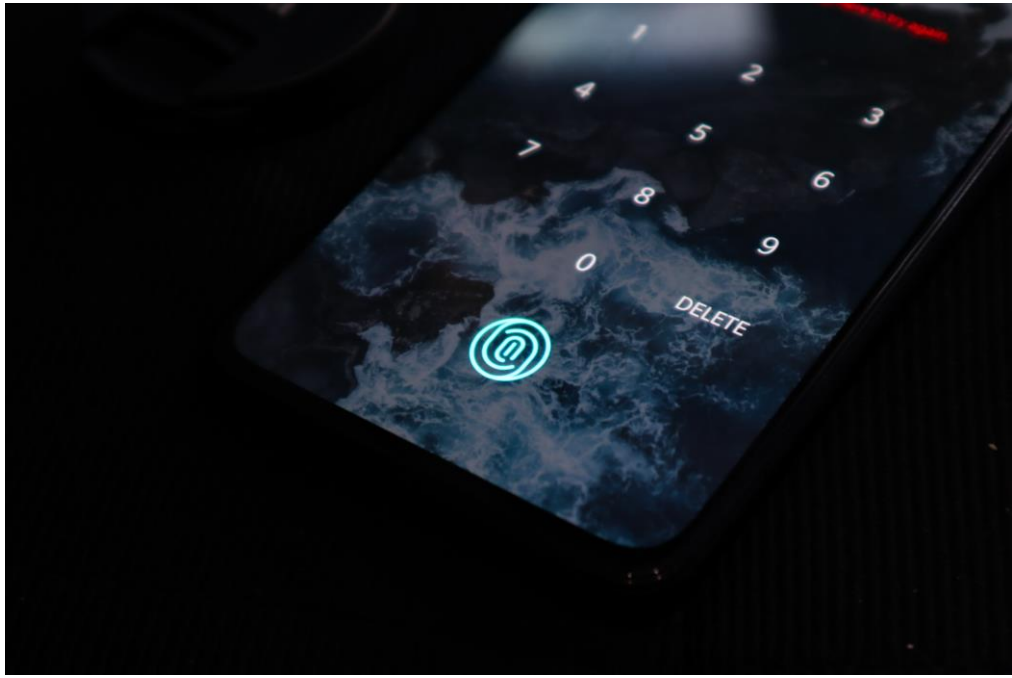
določljiv posameznik je tisti, ki ga je mogoče **neposredno** ali **posredno** določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno,gospodarsko, kulturno ali družbeno identiteto tega posameznika.

2. <u>ZBIRKA OSEBNIH PODATKOV</u> - elektronsko ali na papirju vodene zbirke podatkov o fizičnih osebah (tabele, aplikacije, razvidi, šifranti, baze, personalne mape….)

- **kadrovske evidence** (evidence o stroških dela, izrabi delovnega časa itd.);
- **druge zbirke o zaposlenih** (npr. evidence dodeljene opreme, podatki u uporabi interneta, službenih vozil…);
- **podatki o strankah** (**starši/otroci/učitelji**, **udeleženci**, komitenti, zavarovanci, člani klubov zvestobe, člani društva, …);
- **zbirke podatkov o tretjih osebah**, npr. druge zbirke, ki nastajajo v določenem okolju, npr. posnetki videonadzora, seznam prijavljenih na____, zbirka sodelujočih v nagradni igri, seznam naročnikov na e-novice…

- **Zakonodaja o varstvu OP se nanaša na zbirke, ki jih vodijo podjetja/inštitucije oz. na procese obdelav OP**
    - med cca 5 in 50 zbirk, odvisno od sektorja, velikosti…
- **In na avtomatizirano obdelavo OP**

3. <u>OBDELAVA OSEBNIH PODATKOV</u> je **kakršnokoli delovanje ali niz delovanj**, ki se izvaja z OP, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje**, priklicanje, vpogled**, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje, obdelava pa je lahko ročna ali avtomatizirana.



- **torej: kakršno koli ravnanje z osebnimi podatki!**
- **izjema domače rabe**

4. <u>UPRAVLJAVEC</u> - fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi **določa namene in sredstva obdelave OP** oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

5. <u>OBDELOVALEC</u> - najet s strani upravljavca na podlagi **pisne pogodbe/dogovora**, da **v imenu in za račun upravljavca** obdeluje OP: (*„pogodbena obdelava osebnih podatkov“*)

- vzdrževalec spletne strani
- izvajalec videonadzora
- računovodski servis

- Osebnih podatkov **ne sme uporabljati za svoje namene**.
- **Upoštevati zahteve 28. člena Splošne uredbe – pogodba!** (vzorec na www.ip-rs.si)
  - ZVOP-2 pogodbene obdelave ne ureja/spreminja!

Definicije iz ZVOP-2

- »**javni sektor**« so državni organi, samoupravne lokalne skupnosti, nosilci javnih pooblastil v delu, kjer izvršujejo javna pooblastila, **javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi, zasebni vrtci in zasebne osnovne ter srednje šole, ki izvajajo javno veljavne vzgojno-izobraževalne programe**, samoupravne narodne skupnosti, Svet romske skupnosti Republike Slovenije in druge osebe javnega prava, ustanovljene z zakonom;

- »**zasebni sektor**« so pravne in fizične osebe, ki opravljajo dejavnost v skladu z zakonom, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in druge osebe zasebnega prava; **zasebni sektor so tudi javni gospodarski zavodi, javna podjetja in gospodarske družbe in izvajalci gospodarskih javnih služb**, ne glede na delež oziroma vpliv države ali samoupravne lokalne skupnosti ali samoupravne narodne skupnosti ali dejstvo, da so nosilci javnega pooblastila;

- »**zakon**« je ta zakon, drugi zakoni, obvezujoče mednarodne pogodbe, ki zavezujejo Republiko Slovenijo, ter pravni akti ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite;

Temeljna načela v zvezi z obdelavo OP (5. člen Splošne uredbe)

- **zakonitost, poštenost 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 – **Proaktivnost! Dolžnost upravljavca!**

Zakonitost obdelave po GDPR in ZVOP-2

Pravne podlage (6. člen ZVOP-2) – veljajo podlage iz 6. in 9. člena GDPR

a) **Privolitev (točka (1)a)) 6. člena GDPR**
b) **Pogodba (točka (1(b))**
c) **Zakon (točka (1(c))**
d) **Reševanje posameznika (točka (1(d))**
e) **Javni interes, izvajanje javne oblasti (točka 1(e))**
f) **Zakoniti interesi (točka (1(f))**

- **c) in e) 6(1) GDPR mora določati zakon**
- **vsebine zakona**: obdelava OP, vrste OP, ki naj se obdelujejo, kategorije posameznikov, namen obdelave in rok hrambe OP ali rok za redni pregled potrebe po hrambi …

Pogoji za veljavno privolitev

- **DOKAZLJIVA**: upravljavec zmožen dokazati, da je posameznik privolil v obdelavo svojih OP.
- LOČENA **OD DRUGIH ZADEV, V RAZUMLJIVI IN LAHKO DOSTOPNI OBLIKI TER V JASNEM IN PREPROSTEM JEZIKU**.
- Posameznik ima pravico, da svojo **PRIVOLITEV KADAR KOLI PREKLIČE**. Preklic privolitve **ne vpliva na zakonitost obdelave** na podlagi privolitve pred njenim preklicem. Privolitev je **enako enostavno preklicati** kot dati.
- **PROSTOVOLJNA**: Pri ugotavljanju, ali je bila privolitev dana **prostovoljno**, se med drugim zlasti upošteva, **ali je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo v obdelavo OP, ki ni potrebna za izvedbo zadevne pogodbe. Ne, da nima možnosti dejanske ali prostovoljne izbire** ali privolitve **ne more zavrniti ali preklicati brez škode**
- **AKTIVNO PODANA** - dana z **jasnim pritrdilnim dejanjem**, ki pomeni, da je posameznik, **prostovoljno, konkretno, ozaveščeno in nedvoumno izrazil** soglasje k obdelavi OP.
  - To lahko vključuje **označitev okenca** ob obisku spletne strani, **izbiro tehničnih nastavitev** za storitve informacijske družbe ali katero koli **drugo izjavo** ali **ravnanje**, ki v tem okviru **jasno kaže** na to, da posameznik sprejema predlagano obdelavo svojih OP. **Molk, vnaprej označena okenca ali nedejavnost ne pomenijo privolitve.**
- **INFORMIRANA (glej 13. člen Splošne uredbe):** komu, kaj, zakaj, kakšne pravice ima…

- **Ločiti morate med obdelavo zaradi pogodbe od obdelave na podlagi privolitve!**
- Podrobno si poglejte uvodne določbe 32, 42, 43 in 171, ter člene 7, 8 in 9 in ocenite, ali vaše privolitve ustrezajo zahtevam teh določbe. **Neveljavne privolitve lahko namreč pomenijo nezakonito obdelavo osebnih podatkov.**
- Privolitev mora biti - z drugimi besedami - **aktivno podana, nedvoumna, prostovoljna, dokazljiva ni INFORMIRANA** Kaj to pomeni v preprostem jeziku? Posameznik mora vedeti, komu daje podatke, katere podatke, za katere namene. Nameni morajo biti dovolj jasno opredeljeni. Posameznik ne bi smel biti prisiljen v podajo podatkov, ki niso potrebni za konkretno storitev – razmislite, kateri osebni podatki so v posameznem primeru **nujni za konkretno pogodbo oz. storitev**, kateri pa so **lahko prostovoljni** (in slednjih ne označujte kot obvezne).
- **Ne zahtevajte podatkov na zalogo**, **če ne veste, da (ali zakaj) jih boste rabili** in ne zahtevajte podatkov od vseh vnaprej, če jih boste rabili samo od določenih, ko nastopijo določene okoliščine.
- Razmislite, kako boste dokazovali podajo privolitve, če je podana po elektronski poti ali po telefonu, vendar ne pretiravajte z nesorazmernimi ukrepi, kot je npr. kopiranje osebnih izkaznic, snemanje vseh pogovorov ipd.

Člen 30 GDPR- Evidenca dejavnosti obdelave

1. Vsak **upravljavec in predstavnik upravljavca**, kadar ta obstaja, vodi **evidenco dejavnosti obdelave OP**. Ta evidenca vsebuje:

a) **naziv ali ime in kontaktne podatke upravljavca** in, kadar obstajajo, **skupnega upravljavca**, **predstavnika upravljavca** in **pooblaščene osebe za varstvo** podatkov;
b) **namene** obdelave;
c) **opis kategorij** posameznikov, na katere se nanašajo OP, in **vrst** OP;
d) **kategorije prejemnikov**, ki so jim bili ali jim bodo razkriti OP, vključno s prejemniki v tretjih državah ali mednarodnih organizacijah;
e) kadar je ustrezno, **informacije o prenosih OP v tretjo državo ali mednarodno organizacijo**, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov iz drugega pododstavka člena 49(1) pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
f) kadar je mogoče, **predvidene roke za izbris** različnih vrst podatkov;
g) kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov** iz člena 32(1).

Informacije, ki se zagotovijo, kadar se OP pridobijo od posameznika (člen 13 GDPR)

Posameznike je treba informirati o obdelavi osebnih podatkov – načelo preglednosti.
V praksi zelo slabo spoštovano – kršitve in možne kazni!!!
Ne glede na vrsto pravne podlage!

Na ustrezen način, npr.:

- ustrezno **izpolnjen obrazec/e-pošta/navadna pošta z informacijami**,
- **kot letak z informacijami,**
- **sestavni del pogodbe** oziroma splošnih pogojev ali na drug ustrezen način

- **Pri zbiranju OP prek spletnih strani** lahko te informacije podate **na spletni strani ob poljih, v katere vnesejo svoje podatke** ali z **enostavno dostopno povezavo** na takšno besedilo („Politika zasebnosti“ ali „Informacije o obdelavi osebnih podatkov…..).

Katere informacije jim je treba dati?

Informacije, ki se zagotovijo, kadar se OP pridobijo od posameznika (člen 13.**1** GDPR)

a) identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja - (**KDO STE**);
b) kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja – (**ČE IMATE IMENOVANO POOBLAŠČENO OSEBO, KDO TO JE**);
c) namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo - (**ZAKAJ VSE UPORABLJATE NJEGOVE PODATKE**);
d) kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba - (**OBRAZLOŽITEV PODLAGE PREVLADUJOČIH INTERESOV; ČE JE TO PODLAGA);**
e) uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo – (**KATERIM TRETJIM PRAVNIM OSEBAM POSREDUJETE NJEGOVE PODATKE**);
f) kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo - (**ALI PRENAŠATE PODATKE V T.I. TRETJE DRŽAVE**).

LAHKO UPORABITE VZOREC NA SPLETNI STRANI IP:
Vzorec obvestila posameznikom glede obdelave osebnih podatkov (člen 13 Splošne uredbe)

Informacije, ki se zagotovijo, kadar se OP pridobijo od posameznika (člen 13.2 GDPR)

a) **obdobje hrambe OP** ali, ko to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
b) **obstoj pravice**, da se od upravljavca zahtevajo **dostop do OP** in **popravek ali izbris OP ali omejitev** obdelave, obstoj pravice do **ugovora** obdelavi in pravice do **prenosljivosti** podatkov;
c) kadar obdelava temelji na privolitvi, **obstoj pravice**, da se lahko **privolitev kadar koli prekliče**, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica;
d) pravico do **vložitve pritožbe pri nadzornem organu**;
e) ali je **zagotovitev OP statutarna ali pogodbena obveznost ali pa obveznost**, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik zagotoviti OP ter kakšne so morebitne **posledice, če se taki podatki ne zagotovijo**, in
f) **obstoj avtomatiziranega sprejemanja odločitev**, vključno z oblikovanjem profilov: **razlogi, pomen in predvidene posledice**.

Posebne določbe ZVOP-2

Rok hrambe osebnih podatkov, določitev roka in vezanost na rok (43. člen ZVOP-2)

- rok hrambe podatkov – minimizacija glede na namen obdelave, razen če drug zakon za posamezne obdelave določa rok hrambe
  - Kdo določa rok hrambe in kakšni so?
- **redno dokumentirano preverjanje**
  - Določitev rokov hrambe – 2. odst. 13. člena GDPR
  - Redno?
  - Dokumentirano?
  - DPO?

- če drug zakon ne določa drugače: **izbris, uničenje ali anonimizacija po preteku rokov**, oziroma se izvede drug postopek, ki onemogoča identifikacijo posameznika, na katerega se nanašajo osebni podatki , zlasti omejevanje dostopa do njih, njihovo blokiranje ali arhiviranje.

Obdelava kontaktnih podatkov in osebnih dokumentov

92. člen ZVOP-2 (javni kontaktni podatki)

- Osebe javnega ali zasebnega sektorja lahko javnosti posredujejo in javno objavijo:
  - **osebno ime, naziv ali funkcijo, službeno telefonsko številko in naslov službene elektronske pošte**
  - **vodilnih oseb in tistih zaposlenih, katerih delo je potrebno zaradi poslovanja s strankami.**

93. člen ZVOP-2 (obdelava OP za izvajanje določenih dejavnosti osebe javnega ali zasebnega sektorja)

Za namene **organiziranja uradnih srečanj, izobraževanj, ipd.,** dajanja **izjav za javnost**, **razen izvajanja neposrednega trženja dovoljena uporaba kontaktnih podatkov** posameznikov iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog, če

- so ji jih posamezniki prostovoljno razkrili,
- ali dali privolitev,

- Te zbirke morajo biti **ločene od drugih zbirk OP** (oblastnega delovanja).
- **Le naslednje OP:** osebno ime, telefonsko številko, naslov elektronske pošte ali drugo komunikacijsko številko/oznako, podatke o delodajalcu/ organizaciji ter podatke o področju dela, položaju, funkciji, članstvu v klubu ali hobiju posameznika.
- Na podlagi **privolitve posameznika** lahko oseba javnega sektorja za iste namene obdeluje **tudi naslov stalnega ali začasnega prebivališča in druge OP**, **posebne vrste OP pa le izjemoma in če ima za to izrecno privolitev posameznika**.

Za **namene obveščanja javnosti** sme oseba javnega ali zasebnega sektorja obdelovati, vključno z objavo:

osebna imena, nazive, **fotografije in videoposnetke posameznikov, pridobljene na dogodkih**, ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba, **če posameznik te obdelave ni prepovedal.**

Obdelava kontaktnih podatkov in osebnih dokumentov

94. člen ZVOP-2 (obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta)

- Upravljavec, obdelovalec ali uporabnik smejo **za namen identifikacije posameznika**, ali **za namen zagotavljanja točnosti in posodobljenosti OP, vpogledati** v njegove uradne identifikacijske dokumente.

- Upravljavec, **ki izvaja z zakonom predpisano nalogo***, sme za namen identifikacije posameznika ali za namen zagotavljanja točnosti in posodobljenosti OP **tudi prepisati, kopirati ali drugače obdelati podatke iz njegovih uradnih identifikacijskih dokumentov** (po tem členu):
  - osebna izkaznica,
  - potni list,
  - obmejna prepustnica,
  - vozniško dovoljenje,
  - orožni list in
  - uradni identifikacijski dokumenti drugih držav ali mednarodnih organizacij.

- * Ni isto kot „vse, kar piše/je podlaga v zakonu“
- Druge pravne podlage? Za upravljavce, ki **ne** izvajajo z zakonom predpisanih nalog?

Hvala za pozornost!