POOBLAŠČENA OSEBA ZA
VARSTVO OSEBNIH PODATKOV

USKLADITEV Z GDPR V PRAKSI

Mag. Renata Zatler
Renata.zatler@dataofficer.si

www.dataofficer.si

Kaj se bo zgodilo 25. maja 2018?

- ZVOP-1 preneha veljati
- EU GDPR se prične uporabljati neposredno v vseh državah članicah EU
- ZVOP-2 (le za izvrševanje GDPR) se prične uporabljati

GDPR – koraki do uskladitve

1. **ANALIZA STANJA**
2. SEZNAM UKREPOV
   – uskladitev z GDPR
3. **IZVEDBA**
   UKREPOV – GDPR SKLADNI
4. REVIZIJA (1x letno)

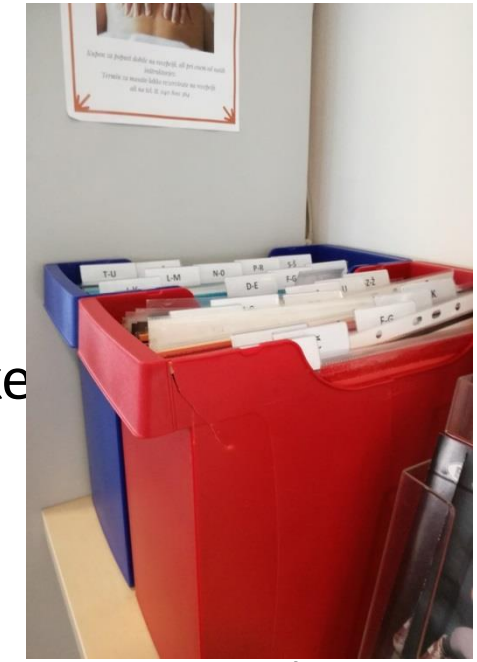
Analiza: Kakšno je naše trenutno stanje skladnosti?

- **Ali smo skladni z ZVOP-1?**

- Kako težek „zalogaj“ nas čaka?
- Stopnja odgovornosti in osveščenosti vodstva in zaposlenih?
- Kaj pogostokrat delamo narobe?
- Kje se osebni podatki nahajajo?
- Pravne podlage, roki hrambe, ukrepi za varstvo?

GDPR – PRILOŽNOST ZA REVIZIJO!?

Analiza: Kje se osebni podatki nahajajo (pravna podlaga, roki hrambe…)?



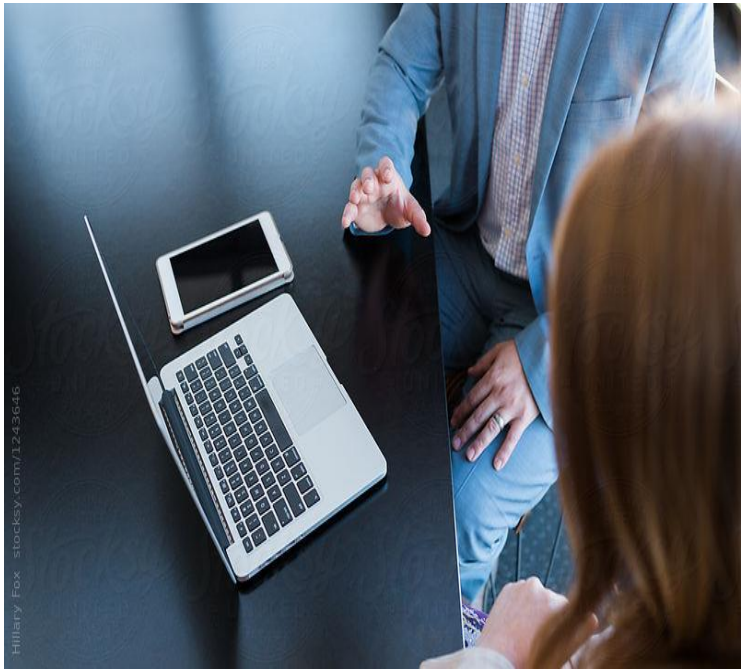
- V različnih evidencah – zbirkah,
- v kadrovskih mapah zaposlenih,
- v računovodskih podatkih…
- v excelovih tabelah, ki vsebujeje različne podatke
- o strankah, kupcih, pacientih, občanih,
- v posnetkih videonadzornega sistema…
- spletnih straneh
- elektronski pošti…
- pri pogodbenih partnerjih („outsorsing“ – IT, videonadzor…)

- Zaposleni,
- Stranke,
- Pacienti,
- Pogodbeni partnerji…

GDPR SE UPORABLJA ZA OBDELAVO VSEH VRST OP (vključno HRM)

Analiza: Ali znamo odgovoriti na vprašanja?

- KAJ? vsebina OP, ki jih obdelujemo.
- KDO? uporabniki OP.
- ZAKAJ Razlog za zbiranje OP.
- KJE? Kje so OP shranjeni.
- KDAJ? Prenehanje uporabe OP.



Analiza: Kako zagotavljamo varstvo OP?

„You're only as secure as your weakest link“

Varen si samo toliko kot je varen najšibkejši člen v verigi.

VARNOST ŠE NE POMENI VARSTVA

Podatki so lahko odlično zaklenjeni, a kaj ko nimamo pravne podlage, da jih sploh smemo imeti ali pa jih uporabljamo za namene, za katere niso bili zbrani. Varstvo podatkov ni samo IT varnost in to ni nekaj, kar uredijo informatiki. Varstvo podatkov je skrb, je proces in ne nekaj, kar narediš in je končano (npr. zgolj sprejem pravilnika). Predvsem človeški faktor je pogosto največje tveganje za zlorabe!.

Vir: Smernice IP

Ali se zavedamo resnične grožnje, ki jih prinaša zloraba osebnih podatkov?

GDPR - ključnih 5 – javni sektor

KAJ MORAMO ZAGOTOVITI?

1. **Zakonitost** in **transparentnost** obdelave – ustrezna pravna podlaga, evidenca obdelave, objava politike varstva OP
2. **Uvedbo ukrepov za ustrezno varstvo OP** - pravnoorganizacijski in tehnični – primerni glede na **stopnjo tveganja** (cilj – skladnost z GDPR – ustrezno varstvo pred kršitvami – „privacy by design and by default“)
3. **Uveljavitev pravic posameznikov** (informiranje, dostop…)
4. **Odziv na kršitve** (evidenca kršitev, poročanje IP…)
5. **DPO** – pooblaščena oseba za varstvo OP

Zakonitost in transparentnost

- **ZAKONITOST OBDELAVE**

USTREZNA PRAVNA PODLAGA ZA **OBDELAVO**

zbiranje, beleženje, urejanje, shranjevanje, priklic, vpogled, …posredovanje…, izbris, uničenje

Evidenca obdelave (katalog)

Zakonitost in transparentnost

ZAKONITOST OBDELAVE *6. člen GDPR*

- ***obdelava je potrebna za izpolnitev zakonske obveznosti upravljavca***
- ***obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu. –***

  *(**zakonska podlaga**! DČ imajo možnost d oločiti podrobneje izvajanje te določbe)**

- *posameznik, na katerega se nanašajo OP, je privolil v obdelavo njegovih OP v enega ali več določenih namenov; ??*

  (Kdaj se lahko uporabi? Javna naloga – obvezno zakon?)

- *obdelava je potrebna za izvajanje pogodbe,*
- *obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo OP*

*Recital 45: **Ta uredba ne zahteva posebnega zakona za vsako posamezno obdelavo**. Zadosten je lahko zakon, ki je podlaga za več dejanj obdelave, ki temeljijo na pravni obveznosti, ki velja za upravljavca, ali za primere, ko je obdelava potrebna za izvajanje naloge v javnem interesu ali izvrševanje javne oblasti.*

ZAKONITOST OBDELAVE 9. člen ZVOP-1

(1) ***Osebni podatki v javnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Z zakonom se lahko določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika.***

(2) **Nosilci javnih pooblastil** lahko obdelujejo osebne podatke tudi na podlagi **osebne privolitve posameznika brez podlage v zakonu, kadar ne gre za izvrševanje njihovih nalog kot nosilcev javnih pooblastil.** Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov, ki nastanejo na podlagi izvrševanja nalog nosilca javnih pooblastil.

(3) Ne glede na prvi odstavek tega člena se lahko **v javnem sektorju obdelujejo osebni podatki posameznikov, ki so z javnim sektorjem sklenili pogodbo** ali pa so na podlagi pobude posameznika z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe.

(4) Ne glede na prvi odstavek tega člena se lahko v javnemu sektorju **izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo**.

Zakonitost in transparentnost

Privolitev v javnem sektorju?

Recital 43:

- ***Za zagotovitev, da je privolitev dana prostovoljno, privolitev ne bi smela biti veljavna pravna podlaga za obdelavo osebnih podatkov v posebnem primeru, ko obstaja očitno neravnotežje med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, zlasti kadar je upravljavec javni organ in je zato malo verjetno, da je bila privolitev dana prostovoljno v vseh okoliščinah te specifične situacije.*** *Za privolitev se domneva, da ni dana prostovoljno, če ne dovoljuje ločene privolitve za različna dejanja obdelave osebnih podatkov, čeprav bi taka ločena privolitev bila v posameznem primeru ustrezna, ali če je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo, čeprav za zadevno izvajanje taka privolitev ne bi bila potrebna.*

Zakonitost in transparentnost

Katalog IP – primeri občin

Pravna podlaga? Rok hrambe?

	PRAVNA PODLAGA	
Evidenca sklenitev zakonskih zvez ter jubilejnih porok	Pooblastilo Upravne enote županu, **privolitev mladoporočencev** in Zakon o zakonski zvezi in družinskih razmerjih	Trajno
Evidenca oddanih pobud preko aplikacije Servis pobude meščanov MOL	**osebna privolitev**	trajno
32. Evidenca uporabe prisilnih sredstev	28.a člen Zakona o občinskem redarstvu (Ur. list RS št. 9/2017)	Podatki v evidenci se hranijo dve leti po datumu uporabe prisilnega sredstva.

14. Evidenca o odločbah o prekrških – Medobčinski inšpektorat	75. člen Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 94/07 – ur. preč. bes.; ZVOP-1), Zakon o prekrških.	Rok hrambe (neobvezno): Ni določen.

Zakonitost in transparentnost

Povejte posameznikom zakaj potrebujete osebne podatke, kaj z njimi počnete, koliko časa jih boste hranili, kakšne so njihove pravice, kako varujete osebne podatke, na koga se lahko obrnejo za informacije in kam se lahko pritožijo (IP).

- Evidenca obdelave (Katalog)
- Objava na spletni strani (politika varstva OP, obvestilo o obdelavi), na oglasni deski občine oziroma v katerikoli drugi obliki informiranja
- Posebna pozornost pri izjavi/privolitvi (način, proces, spletna stran – novosti!…)

Ukrepi za varstvo OP

- *24. člen GDPR – **Odgovornost***

***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.

- *25. člen GDPR – **Vgrajeno in prevzeto varstvo OP***

…izvaja ustrezne tehnične in organizacijske ukrepe, kot je **psevdonimizacija, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, kot je načelo najmanjšega obsega** podatkov, ter v obdelavo vključi potrebne zaščitne ukrepe, da se izpolnijo zahteve te uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki**.**

- *32. člen GDPR – **Varnost obdelave***

… z izvajanjem ustreznih tehničnih in organizacijskih ukrepov **zagotovi ustrezno raven varnosti glede na tveganje…**

- *35. člen GDPR – **Ocena učinka** (veliko tveganje)*

Ukrepi za varstvo OP

POVZETEK

UKREPI: PRIMERNI GLEDE NA STOPNJO TVEGANJA (količina, „občutljivi osebni podatki …)!

- **PRAVNOORGANIZACIJSKI** – imenovanje odgovorne osebe („DPO“), politika varovanja, **notranji akti**, pooblastila in odgovornosti (kdo upravlja bazo, kdo lahko vpogleda ali drugače obdeluje, sistemizacija), ustrezne privolitve posameznikov, pogodbe z zunanjimi izvajalci, **usposabljanja zaposlenih**, evidenca – katalog osebnih podatkov, ustrezne pogodbe (izbira) **podizvajalcev** oz. obdelovalcev – **preverjanje---**
- **TEHNIČNI** – fizično in IT varovanje: zaklepanje prostorov, ustrezno in učinkovito brisanje podatkov, celovito upravljanje informacijskih tehnologij (**informacijska varnost**), pravilno izbrana gesla, aplikativne in infrastrukturne varnostne rešitve, požarni zid, zagotavljanje revizijske sledi, psevdominizacija…

DOKAZLJIVOST!

ODGOVORNA OSEBA PODJETJA JE NADZORNEMU ORGANU SPOSOBNA DOKAZATI, DA JE STORILA VSE KAR JE POTREBNO ZA USTREZNO RAVEN ZAŠČITE VARSTVA OSEBNIH PODATKOV!

„Če pride do kršitve (zlorabe/incidenta) se bo v primeru, da bo kršitelj uspel z dokazili dokazati dolžno skrbnost ravnanja (skladnosti z zakonodajo, praktično izvajanje ukrepov varovanja npr. usposabljanja zaposlenih, preverjanje izvajanja notranjih aktov…), možno izognit sankcijam.

Ukrepi za varstvo OP

GDPR - POGODBENA OBDELAVA

28. člen: Obdelovalec (pogodbeni – *„outsorsing“)* – ***Upravljavec sodeluje le s tistimi, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov (skladno z GDPR).***

Pogodbeni obdelovalec obdeluje OP ***PO DOKUMENTIRANIH NAVODILIH*** *upravljavca.*

Pomembno ***– PISNA POGODBA VSEBUJE obvezne sestavine*** *(3. točka 28. člena GDPR).*

Opomba: OSNUTEK ZVOP-2 določa obveznost DPO tudi za zasebna podjetja, ki obdelujejo podatke na podlagi pogodbe z javnim sektorjem – obdelovalci – (sem spada tudi morebitni videonadzor).

Odzivanje na kršitve varstva OP

DOLOČITE PROCES, ODGOVORNE OSEBE, MOREBITNE POGODBENE (ZUNANJE) PARTNERJE…

- **Obveščanje nadzornega organa** (IP):

  Kdaj? V primeru, **ko so s kršitvijo varstva OP ogrožene pravice in svoboščine posameznikov**. Brez nepotrebnega odlašanja, po možnosti pa **najpozneje v 72 urah** po seznanitvi s kršitvijo. GDPR določa obvezne sestavine obvestila.

- **Obveščanje posameznikov**;

  Kdaj? Ne vedno. Takrat, ko je verjetno, da kršitev varstva OP **povzroči veliko tveganje za pravice in svoboščine posameznikov**!

- **Vodenje evidence; dokumentira se vsaka kršitev varstva OP**, njene učinke, popravne ukrepe (vse kršitve, tudi tiste, ki niso bile sporočene IP).

KLJUČNO VPRAŠANJE: **KAKO HITRO LAHKO UGOTOVIMO KRŠITEV VARSTVA OP?**

„data breach“: *kršitev varnosti, ki vodi do naključnega ali nezakonitega* ***uničenja, izgube, spremembe, nepooblaščene uporabe, razkritju ali dostopu***

Uveljavitev pravic posameznikov

DOLOČITE PROCES ODZIVANJA, ODGOVORNE OSEBE, MOREBITNE POGODBENE (ZUNANJE) PARTNERJE…

- Zagotovite **najvišjo stopnjo informiranja** posameznikov; objavite podatke o DPO, katere podatke obdelujete, politiko varstva OP, kako posamezniki uveljavljajo pravice, kam se lahko pritožijo…

- Zagotovite **pravočasno odzivanje na zahteve posameznikov** v rokih, ki jih določa GDPR

DPO – pooblaščena oseba za varstvo OP

GDPR - Člen 37 – DPO

- **Upravljavec** in **obdelovalec** imenujeta **pooblaščeno osebo za varstvo podatkov** vedno, kadar **obdelavo opravlja javni organ ali telo,** razen sodišč, kadar delujejo kot sodni organ;….
- Kadar je upravljavec ali obdelovalec javni organ ali telo, se lahko za več takšnih organov ali teles ob upoštevanju njihove organizacijske strukture in velikosti imenuje ena sama pooblaščena oseba za varstvo podatkov.
  - ***Pooblaščena oseba za varstvo podatkov (tudi v javnem sektorju) je lahko član osebja upravljavca ali obdelovalca ali pa naloge opravlja na podlagi pogodbe o storitvah.***

OSNUTEK ZVOP – 2 30. do 33. člen – DPO

- **Pooblaščeno osebo morajo imenovati vsi upravljavci ali obdelovalci v javnem sektorju, vključno z obdelovalci v zasebnem sektorju,** ki opravljajo naloge obdelave osebnih podatkov za upravljavce v javnem sektorju;
- **Več upravljavcev v javnem sektorju lahko, upoštevaje njihovo delovno področje, organizacijsko strukturo in velikost, imenuje skupno pooblaščeno osebo**. Pri tem morajo zagotoviti, da je pooblaščena oseba še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana.
- **Za pooblaščeno osebo upravljavca ali obdelovalca v javnem sektorju je lahko imenovan posameznik ali posameznica, ki poleg pogojev iz prejšnjega odstavka (izobrazba, izkušnje s področja …..izpolnjuje še pogoj, da je zaposlen v javnem sektorju, …**

ZAKLJUČEK – pot do uskladitve z GDPR

- Proces:

(1) Analiza stanja / „gap“ analiza (**popis zbirk, procesa/ upravljanje z zbirkami, politika varstva, upravljanja s tveganji – tretje osebe, transparentnost, pravice posameznikov, odziv na incidente – kršitve varstva OP…)**

(2) **Seznam ukrepov** – akcijski načrt za uskladitev z GDPR

(3) **Implementacija ukrepov vključno z usposabljanjem zaposlenih,**

(4) **Preverjanje** (nadzor nad izvajanjem - revizija – izvajanje **nadzornih ukrepov** – najmanj 1 x letno, naloga DPO)

- Dokumenti – varstvo! - prenova aktov, procesov, varnostnih politik…
- Varnost - fizična/IT varnost! - aplikativne in infrastrukturne varnostne rešitve, požarni zid, zagotavljanje revizijske sledi…

Rok: 25. maj 2018 – NE ODLAŠAJTE!

Pomembno: **TREBA BO DAKAZATI (ne samo na papirju), da se VARNOSTNA POLITIKA V PRAKSI DEJANSKO IZVAJA (od „administrativne“ uskladitve z GDPR do dejanske prilagoditve v praksi).**

HVALA ZA POZORNOST

MOREBITNA VPRAŠANJA LAHKO POSREDUJETE NA

Renata.zatler@dataofficer.si

Dataofficer d.o.o., DPO

Pooblaščena oseba za varstvo osebnih podatkov

www.dataofficer.si