

Uredba GDPR – Nova pravila o varstvu osebnih podatkov v EU

Vpliv na delo revizorjev

Dr. Urška Kežmah, odvetnica



Uredba (EU) 2016/679 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)

**Začetek uporabe 25.5.2018
(neposredna uporaba v DČ)**

Katera pravila pri obdelavi OP torej moramo upoštevati?

- **Splošna uredba**
- **ZVOP-1**
- **Področna zakonodaja**



Obdelava OP je v celoti ali delno avtomatizirana oz. gre za zbirko OP. Uredba se ne uporablja za obdelavo OP:

1. Če gre za dejavnosti zunaj področja uporabe prava EU (nacionalna varnost)
2. Ko DČ izvajajo skupno zunanjo in varnostno politiko
3. Če jih obdeluje fizična oseba za popolnoma osebno/domačo uporabo
4. Organi za preprečevanje/pregon/preiskovanje/odkrivanje KD ali izvrševanje kazenskih sankcij, grožnje javni varnosti
5. Sodišča, ko gre za sojenje

Kaj je OP po uredbi?



- **katera koli informacija v zvezi z določenim ali določljivim posameznikom na katerega se nanašajo osebni podatki;**
- **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;**
- **OP so spletni identifikatorji, ID piškotov, IP naslovi**

Posebne vrste osebnih podatkov (9. člen):

- **osebni podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo**

Kakšno vlogo ima revizor?



**Uredba posebej določa obveznosti
upravljavca in obdelovalca OP!**

Upravljavci:

Fizične ali pravne osebe, javni organi, agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave

(t. j. tisti, ki zbira, shranjuje in uporablja osebne podatke)

Obdelovalci:

Fizične ali pravne osebe, javni organi, agencije ali drugo telo, ki obdeluje osebne podatke za druga podjetja

Kako razmejiti vloge?



Obdelovalec je tisti, ki obdelavo OP izvršuje:

- **izključno v imenu in za račun upravljavca osebnih podatkov,**
- **bo pri tem črpal podlago za obdelavo osebnih podatkov iz upravičenj upravljavca ter**
- **bo v zvezi s samimi dejanji obdelave vezan na navodila upravljavca.**



Revizijska družba je upravljavec OP kadar nastopa kot pooblaščen revizor.

Pri opravljanju drugih storitev pa je lahko RD tudi pogodbeni obdelovalec (npr. izvajanje notranje revizije).

Preizkušeni revizor je pogodbeni obdelovalec (npr. revizor informacijskih sistemov, ...).



6. člen GDPR določa šest različnih zakonitih podlag za obdelavo osebnih podatkov

Glede na namen obdelave mora upravljavec še PRED začetkom obdelave določiti katero podlago bo uporabljal

V splošnem obdelava podatkov za določen namen NE MORE temeljiti na več zakonskih podlagah



Zakonite podlage NI MOGOČE zamenjati med obdelavo osebnih podatkov!

- **Upravljalavec ne more preklapljati/izbirati med zakonitimi podlagami**

To ne preprečuje, da bi lahko iste podatke obdelovali na podlagi več zakonskih podlag

- **Kadar podatke obdelujemo za več različnih namenov in imamo za vsak namen drugo zakonito podlago**

- **Zagotavljanje ustrezne zakonite podlage za obdelavo OP je obveznost upravljavca (to ni dolžnost pogodbenega obdelovalca)**
- **Ko je revizija predpisana v zakonu je zakonita podlaga po točki c 1. odst. 6. čl. GDPR**
- **„obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca“**



Ko RD OP obdeluje kot pogodbeni obdelovalec je ustreznost zakonite podlage odgovornost upravljavca – naročnika.

Priporočilo naročnikom:

Točka f 1. odst. 6. čl. GDPR:

„obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba“

Tudi obdelava osebnih podatkov, nujno potrebna za preprečevanje zlorab, pomeni zakoniti interes zadevnega upravljavca podatkov. (47. odst. preambule)

Ukrepi in obveznosti revizorjev in revizijskih družb po GDPR

- 1. Prilagoditev pogodb z obdelovalci**
- 2. Vzpostavitev evidence dejavnosti obdelav**
- 3. Vzpostavitev postopkov za varovanje pravic posameznika**
- 4. Obvestilo nadzornemu organu v primeru kršitev**
- 5. Ocena učinka v zvezi z varstvom osebnih podatkov**
- 6. Imenovanje pooblaščenice osebe za varstvo osebnih podatkov (?)**

Kakšne so obveznosti za revizorja oz. RD?



Če je upravljavec:

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 z uredbo.

Vgrajeno in privzeto varstvo OP

Upravljavalec mora izvesti ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave.

Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost.



Če je obdelovalec:

Osnova za obdelavo osebnih podatkov med naročnikom in izvajalcem storitev je pogodba

- **Upravljavec določi naloge obdelovalca**
 - **Dokumentirano v pogodbi**
 - Katere podatke obdeluje, roki hrambe!
 - Kako jih obdeluje
- **Obdelovalec mora zagotoviti tehnične in organizacijske ukrepe za zaščito podatkov**
 - **Podrobno dokumentirano v pogodbi**



V pogodbah je treba urediti zlasti:

- naravo in namen obdelave,**
- vsebino in trajanje obdelave,**
- vrste osebnih podatkov,**
- kategorije posameznikov, na katere se nanašajo osebni podatki,**
- obveznosti in pravice pogodbenih strank (upravljavca in obdelovalca),**



Podrobne določbe:

- **Da obdeluje podatke samo po navodilih upravljavca**
- **Zagotovi, da so osebe, pooblaščne za obdelavo, zavezane k zaupnosti,**
- **Sprejme vse ukrepe iz 32. člena GDPR**
- **Dogovor glede „pod-obdelovalcev“**
- **Dogovor glede nalog pri pomoči upravljavcu za uresničevanje pravic posameznika**



Podrobne določbe:

- **Naloge in pomoč upravljavcu pri izpolnjevanju obveznosti po 32. do 36. členu GDPR (varnost obdelave, obveščanje o kršitvah, ocena učinka, posvetovanja z IP-RS)**
- **Dogovor glede izvajanja revizij/pregledov (glede ukrepov za varno obdelavo OP)**

Ni obvezna za organizacije, ki zaposlujejo manj kot 250 oseb.

Kljub temu obvezno, če

- **je verjetno, da obdelava predstavlja tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in ni občasna**
- **Obdelava vključuje posebne vrste podatkov (zdravje, sindikat!)**

Vzpostavitev postopkov za varovanje pravic posameznika

Upravljavlec mora sprejeti ustrezne ukrepe, s katerimi zagotovi posamezniku, na katerega se nanašajo osebni podatki, vse informacije iz členov 13 in 14 Splošne uredbe ter sporočila iz členov 15 do 22 in 34 Splošne uredbe, povezana z obdelavo, v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku.

Katere pravice imajo posamezniki po GDPR?



- **Pravica do informiranosti (13. in 14. člen GDPR)**
- **Pravica do dostopa (15. člen GDPR)**
- **Pravica do popravka (16. člen GDPR)**
- **Pravica do izbrisa (17. člen GDPR)**
- **Pravica do omejitve uporabe (18. člen GDPR)**
- **Pravica do prenosljivosti podatkov (20. člen GDPR)**
- **Pravica do ugovora (21. člen GDPR)**
- **Pravica do pritožbe nadzornemu organu (77. člen GDPR)**

Obvestilo nadzornemu organu v primeru kršitev (33. člen)

V primeru kršitve varnosti osebnih podatkov mora upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej obvestiti pristojni nadzorni organ v skladu s členom 55 (IP RS), razen če ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov.

Kadar obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedba razlogov za zamudo.



Tudi obdelovalec mora po seznaitvi s kršitvijo varnosti osebnih podatkov brez nepotrebnega odlašanja uradno obvestiti upravljavca.

Upravljavec je dolžan dokumentirati vsako kršitev varnosti osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varnosti osebnih podatkov, njene učinke in sprejete popravne ukrepe.



Upravljavci IN obdelovalci naj bi vnaprej načrtovali in vzpostavili

- **Procese za zaznavanje in omejevanje incidentov**
- **Oceno tveganja za posameznike**
- **Postopek ugotavljanja ali je treba obvestiti nadzorni organ**
- **Postopek ugotavljanja ali je treba obvestiti posameznike**



GDPR določa:

- **Kdaj in koga je treba obvestiti v primeru incidenta**
- **Katere informacije je treba posredovati v obvestilu**
- **Informacije je mogoče posredovati v več fazah (postopno)**
- **Upravljalci se morajo nemudoma odzvati na incident**



Ocena učinka v zvezi z varstvom podatkov je postopek, katerega namen je opisati obdelavo, oceniti njeno potrebnost in sorazmernost ter obvladati tveganja za pravice in svoboščine posameznikov, ki izhajajo iz obdelave osebnih podatkov

Namen

- **Sistematično izpolnjevanje zahtev GDPR**
- **Dokazovanje, da so bili sprejeti ustrezni ukrepi zagotovitev skladnosti**



Je postopek za vzpostavitev in dokazovanje skladnosti

Ni vedno obvezen. Zahteva se, kadar:

„je možno, da bi (obdelava lahko) povzročila veliko tveganje za pravice in svoboščine posameznikov“

Imenovanje pooblaščene osebe za VOP = DPO

Upravljavec/obdelovalec morata imenovati DPO, če:

- **obdelavo izvaja javni organ (tudi javna telesa: npr. agencije, ...) – ne glede na vrste podatkov, ki se obdelujejo,**
- **je obdelava OP njuna temeljna dejavnost, kjer je zaradi narave obsega ali namenov obdelave treba posameznike redno in sistematično spremljati (npr. direktni marketing, segmentiranje, analitika...)**
- **njune temeljne dejavnosti zajemajo obsežno obdelavo posebnih vrst OP (t. i. občutljivi osebni podatki) in OP v zvezi s KE/PE.**



Imenovanje DPO torej odvisno od števila in obsega osebnih podatkov ter posameznikov, ki jih obdeluje

- **Število osebnih podatkov v smislu števila podatkov o ENEM posamezniku**
- **Obsega v smislu številčnosti vrst osebnih podatkov, ki jih obdeluje**
- **Števila posameznikov na katere se osebni podatki nanašajo**

Kaj so temeljne dejavnosti?

- temeljne dejavnosti upravljavca se nanašajo na *„njegove osnovne dejavnosti in ne na obdelavo osebnih podatkov kot postranske dejavnosti“*.
- Za „temeljne dejavnosti“ se lahko štejejo ključne dejavnosti, ki so potrebne za doseganje ciljev upravljavca ali obdelovalca.

Kaj pomeni obsežna obdelava OP?

- **uredba ne opredeljuje, kaj pomeni obsežna obdelava**
- **Določitev „*velikega obsega*“ je prepuščena praksi**

Člen 37 se v zvezi z imenovanjem DPO uporablja tako za upravljavce kot obdelovalce.

DPO mora glede na to, kdo izpolnjuje merila za obvezno imenovanje, v nekaterih primerih imenovati le upravljavca oziroma obdelovalca, v drugih primerih pa tako upravljavca kot njegov obdelovalec (ki morata nato medsebojno sodelovati).



Pooblaščenca oseba za varstvo podatkov, ki jo imenuje obdelovalec, nadzoruje tudi dejavnosti, ki jih izvaja organizacija obdelovalca, ko opravlja vlogo upravljavca podatkov zase (npr. človeški viri, informacijska tehnologija, logistika).



- **Za povezane osebe: pogoj - ta oseba je „dostopna iz vsake enote“.**
- **Za več javnih organov ali teles ob upoštevanju njihove organizacijske strukture in velikosti se lahko imenuje ena sama pooblaščenca oseba za varstvo podatkov.**

Kdo je DPO?



**Ustrezno strokovno znanje in poklicne
odlike ter zmožnost za izpolnjevanje nalog.**



**Upravljavec kontaktne podatke DPO objavi
in sporoči IP.**

**Pooblaščen oseba za varstvo podatkov je
pri opravljanju svojih nalog zavezana
varovati skrivnost ali zaupnost v skladu s
pravom Unije ali pravom države članice
(člen 38(5)).**

Naloge DPO (39. člen)



Obvešča upravljavca + svetuje o VOP in zahtevah GDPR

Spremlja skladnost obdelave OP po GDPR in drugih predpisih

Izvaja izobraževanja za zaposlene in sodeluje pri revizijah

Kontaktna točka glede obdelave OP



DPO zlasti:

- **zbira informacije za opredelitev dejavnosti obdelave,**
- **analizira in preverja skladnost dejavnosti obdelave ter**
- **obvešča upravljavca ali obdelovalca, mu svetuje in zanj izdaja priporočila.**

Sodelovanje z nadzornim organom (IPRS)

DPO deluje kot kontaktna točka, da bi nadzornemu organu olajšala dostop do dokumentov in informacij za izvajanje nalog iz člena 57 ter za izvajanje njegovih preiskovalnih in popravljalnih pooblastil ter pooblastil v zvezi z dovoljenji in svetovalnih pristojnosti iz člena 58.

Obveznost varovanja skrivnosti/zaupnosti DPO ne prepoveduje, da stopi v stik z nadzornim organom in ga zaprosi za mnenje.

Nasprotje interesov

DPO v organizaciji ne sme zavzemati položaja, v okviru katerega lahko določi namene in sredstva obdelave osebnih podatkov.

Zaradi posebne organizacijske strukture vsake organizacije je treba to obravnavati za vsak primer posebej.

Nasprotje interesov lahko npr. nastopi, če je zunanja pooblaščenca oseba za varstvo podatkov zaprošena, da upravljavca ali obdelovalca v zadevah, povezanih z varstvom podatkov, zastopa pred sodišči.



Glede prenosa osebnih podatkov v tretje države ali mednarodne organizacije je treba ločiti med:

- prenosi na podlagi sklepa o ustreznosti,
- prenosi za katere se uporabljajo ustrezni zaščitni ukrepi (46. člen)
- ter odstopanje v posebnih primerih (49. člen).

Vsak posameznik, ki je utrpel premoženjsko ali nepremoženjsko škodo kot posledico kršitve Splošne uredbe, ima pravico, da od upravljavca ali obdelovalca dobi odškodnino za nastalo škodo.

Za ugotavljanje odškodninske odgovornosti veljajo splošna pravila OZ.



Hvala za pozornost.

?

urska@kezmah.si