

VARSTVO OSEBNIH PODATKOV

Dr. Bojan Himmelreich,
arhivski svetnik

Zgodovinski arhiv Celje, 24. 4. 2019

GDPR je kratica za **General Data Protection Regulation** oziroma za Splošno uredbo EU o varstvu podatkov, ki določa nova pravila glede varstva osebnih podatkov

Besedilo je dostopno na:

http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SLV&toc=OJ:L:2016:119:FULL

Novosti po GDPR

- Posameznikom – več pravic**
- Upravljalcem – več dolžnosti**

- Poleg pojma **upravljalec OP** se pojavlja tudi pojem **obdelovalec OP**. Obdelovalec je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljalca:
- najem storitev podjetja, ki bo za nas izvajalo videonadzor vhoda v poslovne prostore,
- najem storitev klicnega centra,
- najem računovodskih storitev, npr. obračun plač
- najem storitev arhiviranja in hrambe osebnih podatkov
- zunanje vzdrževanje spletnih strani,
- prevoz osebnih podatkov na uničenje in samo uničenje itd.

Več o tem glejte v:

- Smernice Informacijskega pooblaščenca o (pogodbeni) obdelavi osebnih podatkov

(https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_pogodbeni_obdelavi_web.pdf)

Pravice posameznika

Zbiranje osebnih podatkov na podlagi privolitve – privolitev mora biti podana z jasnim pritrdilnim dejanjem, ki pomeni, da je posameznik prostovoljno, specifično, ozaveščeno in nedvoumno izrazil soglasje k obdelavi osebnih podatkov. Posameznik mora torej izrecno podati privolitev v zbiranje in obdelavo svojih osebnih podatkov. **Treba je podrobno preveriti veljavnost obstoječih privolitev.**

Način za preklic privolitve mora biti enako enostaven kot podaja privolitve. Posameznik ima **pravico do umika soglasja** za nadaljnjo obdelavo osebnih podatkov, posebej v primeru neposrednega trženja.

Posameznik, na katerega se nanašajo osebni podatki:

- ima pravico do obveščенosti o obdelavi njegovih osebnih podatkov
- ima pravico do popravka osebnih podatkov v zvezi z njim in do popravka („pravica do pozabe“)
- se njegovi osebni podatki izbrišejo in se ne obdelujejo več
- je dal svojo privolitev kot otrok in se ni v celoti zavedal tveganj, želi pozneje take osebne podatke odstraniti

- pravica do prenosljivosti pomeni pravico, da posameznik prejme osebne podatke v zvezi z njim, in te podatke posreduje drugemu upravljavcu,
- pravica do ugovora pomeni, da posameznik lahko proti nekaterim vrstam obdelav njegovih osebnih podatkov kadarkoli ugovarja in mora upravljalec dokazati legitimne interese za obdelavo oziroma prenehati z obdelavo (vedno v primeru trženja),
- pravica glede samodejne obdelave in profiliranja pomeni, da za posameznika ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov

Obveznosti za upravljalce in obdelovalce podatkov

Imenovanje pooblaščene osebe za varstvo podatkov – javni sektor ter podjetja, katerih temeljne dejavnosti zajemajo dejanja obdelave, ki pomenijo redno in sistematično obsežno spremljanje posameznikov, ali pa obsežno obdelavo posebnih vrst podatkov, bodo morali imenovati odgovorno osebo za varstvo osebnih podatkov.

Obveznost imenovanja pooblaščenih oseb ni vezana na število zaposlenih v podjetju, temveč GDPR določa **kriterije, po katerih morate sami oceniti**, ali ste takšno podjetje ali institucija, ki mora imeti pooblaščenca oseba. Imenovati jih bodo morali:

Javni sektor so državni organi, organi samoupravnih lokalnih skupnosti, nosilci javnih pooblastil, javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi in samoupravne narodne skupnosti.

Podjetja, katerih temeljne dejavnosti zajemajo dejanja obdelave, pri katerih je treba zaradi njihove narave, obsega in/ali namenov posameznike redno in sistematično obsežno spremljati (banke, zavarovalnice, operaterji elektronskih komunikacij, trgovci s klubi zvestobe). Prav tako kadrovske agencije, številne spletne trgovine in IT podjetja, ki vzdržujejo rešitve za obdelavo osebnih podatkov posameznikov. **Proizvodna podjetja in druga podjetja**, katerih temeljne storitve niso namenjene posameznikom, temveč drugim podjetjem in ki ne vključujejo obsežne obdelave osebnih podatkov, ne bodo dolžna imenovati pooblašcene osebe.

Podjetja in institucije, ki izvajajo obsežno obdelavo zdravstvenih in drugih občutljivih podatkov, ki sodijo med t.i. **posebne vrste podatkov** – klinični centri, bolnišnice in klinike, zdravstveni in socialno-varstveni zavodi, ponudniki zdravstvenih informacijskih sistemov in storitev, zapor in prevzgojni zavodi. Posamezen zasebni zdravnik, zobozdravnik ali odvetnik ne bo dolžan imenovati pooblaščene osebe.

Posebne vrste osebnih podatkov (po ZVOP-1 občutljivi osebni podatki) naslednje: osebni podatki o rasnem ali etničnem poreklu, političnem mnenju, verskem ali filozofskem prepričanju ali članstvu v sindikatu, genski podatki, biometrijskih podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

Upravljaljenci ne bodo več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema katalogov.

Večji poudarek daje uredba tudi (predhodnim) izvedbam analiz učinkov na varstvo osebnih podatkov, v primeru varnostnih incidentov, kot je npr. izguba osebnih podatkov, pa se uvaja obveznost poročanja nadzornemu organu in v določenih primerih tudi obveščanja vseh prizadetih posameznikov.

Nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo OP izvaja **Informacijski pooblaščenec**:

- dostop do informacij javnega značaja
- inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo OP oziroma iznos OP iz RS,
- odločanje o pritožbi posameznika, kadar upravljavec OP ne ugotovi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki

Predlagane aktivnosti upravljalcev

- Preveriti obstoječe privolitve

Obdelava je zakonita le in kolikor je izpolnjen vsaj ena od naslednjih šestih možnih pravnih podlag (privolitev, sklepanje ali izvajanje pogodbe, zakonske obveznosti, zaščita življenjskih interesov posameznika, naloge v javnem interesu, zakoniti interesi upravljavca ali tretjih oseb) ter točno določen čas, ko je to potrebno.

- Preverite načine pridobivanja privolitev v bodoče

- **Prilagodite pogodbe s pogodbenimi obdelovalci**
- **Preverite in prilagodite popis zbirk osebnih podatkov (katalog zbirke osebnih podatkov!)**
- **Preglejte postopke za zagotavljanje pravic posameznika**

- **Preglejte in prilagodite vaše varnostne politike in njihovo izvajanje**

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

- **Določite, kdo bo poročal v primeru varnostnega incidenta**

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti pristojni nadzorni organ.

- **Pripravite se na izvajanje načela odgovornosti**
- Če so osebni podatki temelj vašega delovanja, ukrepajte pred obiskom inšpekcije in sami preverite, ali boste morali
- izvajati oceno učinka
- imenovati odgovorno osebo za varstvo osebnih podatkov (»DPO«)
- preverite vaše postopke za minimizacijo. minimizirate lahko količino zbranih podatkov, obseg njihove obdelave, obdobje njihove hrambe in število oseb, ki jih obdelujejo.

Primeri iz prakse:

- če ste z nekom v stiku preko e-pošte, ali jo lahko hranite in kontaktirate z njim kasneje?
- zbiranje podatkov za ureditev kakšne usluge udeležencu dogodka (rezervacija hotela, najem avtomobila itd); smemo hraniti podatke, pridobljene za te namene?
- ali lahko delodajalec zahteva telefonske številke zaposlenih?
- kopiranje osebnih dokumentov za kadrovske evidence?

Še zadnji novici:

Še zadnji novici:

- Informacijski pooblaščenec bo vse do septembra 2020 izvajal evropski projekt RApiD.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), ki je namenjen izobraževanju manjših in srednje velikih podjetij ter posameznikov o reformi zakonodaje s področja varstva osebnih podatkov.

Še zadnji novici:

- Informacijski pooblaščenec bo vse do septembra 2020 izvajal evropski projekt RApiD.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), ki je namenjen izobraževanju manjših in srednje velikih podjetij ter posameznikov o reformi zakonodaje s področja varstva osebnih podatkov.
- Priporočila Informacijskega pooblaščenca glede delovanja pooblaščenca osebe za varstvo osebnih podatkov

Hvala za pozornost

Novosti v ZVOP-2

Na novo so razdelane definicije in obdelave v zvezi s **posebnimi vrstami osebnih podatkov** (dosedaj: občutljivi osebni podatki), vključno s pravnimi podlagami za obdelavo. Od posebnih vrst osebnih podatkov so sedaj ločene pravne podlage glede obdelave osebnih podatkov o kazenskih obsodbah ter o kaznovanjih za prekrške, vendar se pravila zavarovanja osebnih podatkov s področja posebnih vrst osebnih podatkov uporabljajo tudi za njih.

Določena je ureditev za osebe, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov, namreč **pooblašcene osebe za varstvo osebnih podatkov**. Ne uvaja se reguliran poklic, ampak neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj preprečijo tveganja ali kršitve varstva osebnih podatkov

Nadzorni organ za varstvo osebnih podatkov Republike Slovenije po določbah ZVOP-2 ostaja Informacijski pooblaščenec (IP), kot je bil do sedaj po določbah ZVOP-1 in po Zakonu o IP. Ostaja pristojen za inšpekcijski nadzor glede varstva osebnih podatkov glede vseh obdelav osebnih podatkov v Republiki Sloveniji, razen izjem: npr. ustavne določbe; za področje (kriminalistične) policije; obveščevalno-varnostne dejavnosti – ni možno izvajati inšpekcijskih nadzorov s strani IP, če bi se lahko razkrile identitete tajnih delavcev in tajnih sodelavcev, podobno tudi glede zaščitnih prič po Zakonu o zaščiti prič.

Hvala za pozornost