

Celje, 22. 5. 2018

Novosti in spremembe Splošne uredbe o varstvu osebnih podatkov

Le še nekaj dni nas loči od neposredne uporabe evropske uredbe o varstvu osebnih podatkov. Da bi lažje razumeli določena stališča, saj se je v zadnjem času v javnosti ustvarilo marsikatero napačno prepričanje glede sprememb in obveznosti, ki jih Uredba prinaša, smo v okviru SPOT svetovanje Savinjska tudi v Žalcu organizirali brezplačno delavnico na to temo. Mag. Rosana Lemut Strle, odvetnica iz Odvetniške družbe Pirc Musar & partnerji o.p., d.o.o., je približno šestdesetim udeležencem (podjetnikom, predstavnikom podjetij in potencialnim podjetnikom) predstavila Splošno uredbo o varstvu osebnih podatkov – GDPR. Za prenos le-te v naš pravni red je pristojno Ministrstvo za pravosodje.

Uredba, katere cilj je omogočiti prebivalcem nadzor nad njihovimi osebnimi podatki in poenotiti ter dvigniti raven varstva osebnih podatkov v EU, bo nadomestila nacionalne zakone o varstvu osebnih podatkov, pri nas Zakon o varstvu osebnih podatkov (ZVOP-1). Že dosedanji zakon je podjetnikom nalagal mnoge obveznosti, GDPR pa nekatere izmed njih le dopolnjuje, predvsem pa prinaša fizičnim osebam več pravic.

Uredba vse subjekte javnega sektorja in številne zasebne poslovne subjekte, katerih temeljne dejavnosti zajemajo dejanja obdelave, ki pomenijo redno in sistematično spremljanje posameznikov (trgovski centri, spletne trgovine, banke, zavarovalnice, kadrovske agencije, agencije za posredovanje študentskega dela, javni prevozniki, komunalna podjetja...) ali pa obsežno obdelavo posebnih vrst podatkov (politične stranke in sindikati, zasebne zdravstvene institucije ter drugi koncesionarji) obvezuje k imenovanju pooblaščenega osebe za varstvo osebnih podatkov – DPO (»Data Protection Officer«). Poslovni subjekti lahko imenujejo zunanjega ali notranjega DPO z ustreznim znanjem s področja varovanja osebnih podatkov, ki pa ne more biti zastopnik podjetja oz. organizacije, zagotoviti pa mu morajo neodvisno delovanje, da bo lahko nemoteno izvajal vse potrebne aktivnosti za doseganje skladnosti poslovanja z novo Uredbo. Vsa druga podjetja (npr. proizvodna podjetja), katerih osnovne storitve niso namenjene posameznikom, ampak drugim podjetjem in ki ne vključujejo obsežne obdelave osebnih podatkov, niso dolžna imenovati DPO. Bodo pa podjetja lahko osebne podatke še naprej zbirala le na podlagi privolitve. Le-ta pa ne bo potrebna, če bo imelo podjetje za zbiranje osebnih podatkov zakonsko podlago, kot na področju delovnih razmerij, kjer Zakon o evidencah na področju dela in socialne varnosti predpisuje zbiranje podatkov o delavcih.

V nadaljevanju so zbrane najpomembnejše novosti za upravljavce in obdelovalce (Vir: Urad informacijskega pooblaščenca):

- Zbiranje osebnih podatkov na podlagi **privolitve – soglasja, ki mora biti jasna in razumljiva izjava, dana z nedvoumnim pritrdilnim dejanjem** in dokazljiva. Posameznik mora torej izrecno podati privolitev v zbiranje in obdelavo svojih osebnih podatkov. Potrebno je natančno **preveriti veljavnost obstoječih privolitev**.
- Postopek 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.
- Upravljavci morajo upoštevati načeli **vgrajenega in privzetega varstva osebnih podatkov**.
- **Pravica do prenosljivosti podatkov** – dolžnost upravljavca, da posamezniku zagotovi osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki.
- Upravljavci morajo posamezniku zagotoviti **pregledne in enostavno dostopne informacije** o obdelavi njegovih podatkov.

- **Obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov** – upravljavec mora o kršitvi brez nepotrebnega odlašanja (najpozneje v 72 urah) obvestiti nadzorni organ. V določenih primerih mora o tem obveščati tudi posameznike.
- **Imenovanje pooblaščenih oseb 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.
- **Evidence obdelav** (namesto dosedanjih katalogov) – upravljavcem ne bo več potrebno prijavljati zbirk osebnih podatkov v centralni register zbirk osebnih podatkov, ostaja pa za določene upravljavce (in po novem v določenem delu tudi za pogodbene obdelovalce) obveznost vodenja katalogu podobne evidence dejavnosti obdelave.
- **Predhodne ocene učinka** v zvezi z varstvom osebnih podatkov – v določenih primerih bodo tovrstne predhodne analize o spoštovanju temeljnih načel varstva osebnih podatkov obvezne za upravljavce.
- **Nadzor vse na enem mestu** - če obdelava osebnih podatkov poteka v več kot eni državi članici, bo načeloma en sam t. i. vodilni nadzorni organ pristojen za spremljanje vseh teh dejavnosti. Pristojni vodilni nadzorni organ bo v teh primerih organ države članice, v kateri je glavna ali edina enota upravljavca ali obdelovalca.
- **Kodeksi ravnanja in potrjevanje** (certifikacija) – večji poudarek kodeksom ravnanja in postopkom potrjevanja kot novim preventivnim mehanizmom za zagotavljanje in izkazovanje ustreznega ravnanja z osebnimi podatki.
- **Sankcije** naj bi bile **učinkovite, sorazmerne in odvračilne**. Upoštevalo se bo veliko meril glede teže kršitve, lahko pa bodo zelo visoke.

Naloga in odgovornost vseh poslovnih subjektov je pravočasna in pravilna ureditev poslovanja v skladu z novo Uredbo o varstvu osebnih podatkov.

Svetovalka SPOT svetovanje Savinjska
Barbara Mesarec Jakopič

Viri:

1. <https://www.dataofficer.si/dpo/>
2. <http://www.svetovanje.si/svetovanje/blogi/kaj-gdpr-prinasa-obrtnikom-in-podjetnikom-5ae18do8bebe227b57608f76>
3. <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/>
4. https://www.iprs.si/fileadmin/user_upload/Pdf/GDPR/Splosna_uredba_o_varstvu_podatkov-letak_maj2017_v2.pdf