Erih Skočir, IIBA Slovenija

Kako poslovna analitična znanja pomagajo pri implementaciji uredbe **GDPR** in delu **DPO?**

Povzetek:

Kot že veste, se zadnjih nekaj mesecev največ govori o **GDPR** (**General Data Protection Regulation)** – Splošni uredba EU o varovanju podatkov. Ta bo pretresla EU podjetja in organizacije. Prinaša največje spremembe v zadnjih dvajsetih letih. Cilj uredbe je omogočiti prebivalcem EU nadzor nad njihovimi osebnimi podatki, ter hkrati omogočiti uporabo osebnih podatkov zasebnim družbam in javnim organom z zagotavljanjem najvišjih standardov varnosti. Uredba od vseh subjektov javnega sektorja in tudi večjega števila zasebnih poslovnih subjektov zahteva imenovanje **pooblaščene osebe za varstvo podatkov – DPO** (»Data Protection Officer«). Glede na dejstvo, da več kot 80% podjetij nima urejenih podatkov po novi uredbi, dejstvu, da so predvidene visoke kazni ob neizpolnjevanju zahtev iz uredbe, ter datumu, ki se hitro bliža (datum, ko nastopi veljavnost uredbe je 25.5.2018), je jasno, da je sedaj skrajnji čas za realizacijo tega projekta.

Ključne besede: GDPR, DPO, varovanje osebnih podatkov, BACC model

Vloga: DPO, CEO, CIO, PM, BI

Kaj nam prinaša uredba?

Splošna uredba o varovanju podatkov **GDPR** (**General Data Protection Regulation),** je začela veljati 24. 5. 2016, uporabljati pa se začne neposredno in hkrati v vseh državah članicah EU 25.5.2018.

Za začetek poglejmo, kakšne **pravice posameznikom** prinaša nova uredba:

- pravica biti informiran, kako se osebni podatki obdelujejo;
- pravica dostopa do podatkov o njem;
- pravica do popravka in pozabe;
- pravica do omejitve obdelave;
- pravica prenosljivosti;
- pravica do ugovora;
- pravica glede sprejemanja posameznih avtomatiziranih odločitev in profiliranja;
- pravica do odškodnine, če ste jo utrpeli.

Obveznosti upravljavca podatkov (ki je subjekt zasebnega ali javnega sektorja, odgovoren za obdelavo osebnih podatkov, na primer zdravnik, podjetje, športni klub, javna uprava itd.) so naslednje:

- zagotoviti, da se **vaše pravice spoštujejo** (npr. mora vas obveščati, vam omogočiti dostop do vaših podatkov),
- da se podatki zbirajo samo za **določene, posebne in zakonite namene,**
- da so **točni in posodabljani** ter da se ne hranijo dlje, kot je potrebno,
- zagotoviti, da so izpolnjena merila za **zakonito obdelavo podatkov**, na primer, da daste soglasje, podpišete pogodbo ali ste pravno zavezani itn.,
- **zaupnost obdelave**, varnost obdelave,
- v nekaterih primerih **obveščanje organa za varstvo podatkov**, zagotoviti, da v primeru prenosa podatkov v države zunaj EU te države jamčijo ustrezno raven varstva.

Novost je tudi ta, da je treba **Pooblaščeno osebo za varstvo osebnih podatkov** (interni »informacijski pooblaščenec«; **DPO** → Data Protection Officer) imenovati v naslednjih primerih:

- v primeru javnega sektorja,
- če je potrebno zaradi narave, obsega in/ali namenov zbiranja osebnih podatkov posameznike, na katere se nanašajo ti podatki, redno in sistematično obsežno spremljati in/ali
- če gre za obsežno obdelavo občutljivih osebnih podatkov.

Dobra novica je ta, da je Interni pooblaščenec lahko tudi **zunanji pogodbeni sodelavec (podjetje)**.

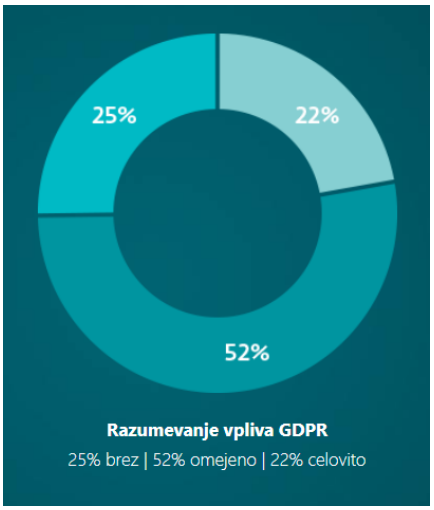
Ena od »manjših podrobnosti« iz GDPR je tudi ta, da so za neizpolnjevanje zahtev iz uredbe zagrožene zelo visoke kazni, v najslabšem primeru tudi **20.000.000 €** ali **4% letnega prometa** (odvisno od tega kateri znesek je večji) – in to na Komisiji mislijo resno!

Vse to so novosti iz uredbe GDPR, ki zahtevajo in bodo zahtevale, veliko dela in sprememb v vsaki organizaciji, tako veliki, kot majhni.

DEJSTVO – Kje smo!

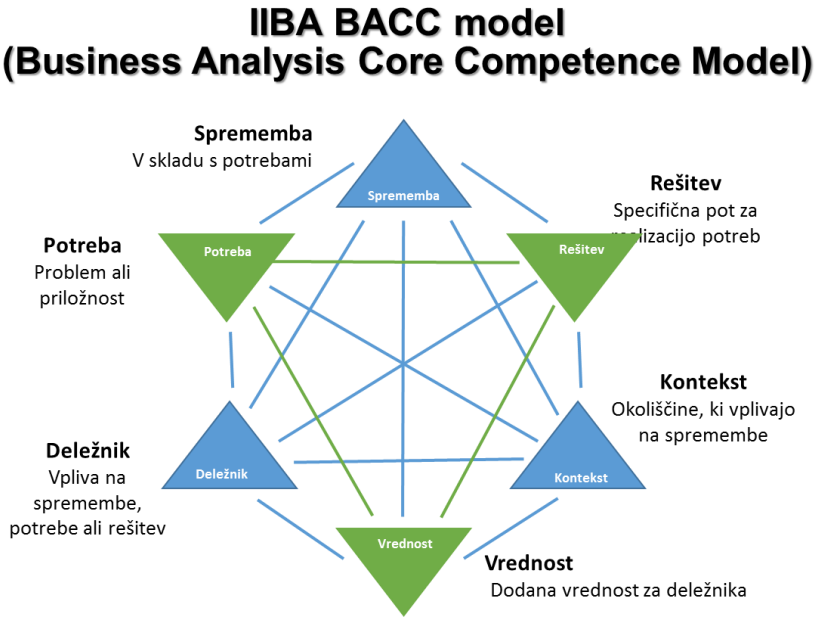
IDC je v analizi, v katero je vključil IT strokovnjake iz več kot 700 podjetij ugotovil, da okoli **80% podjetij še ni pripravljeno** na GDPR.

Večina podjetij nima evidenc, kje in kako se obdelujejo podatki v podjetju, kdo je za njih zadolžen, kako se upravlja z grožnjami in incidenti, nihče se ne vpraša ali res potrebujemo vse zbrane podatke itd.



Kje je tukaj poslovni analitik in kako poslovno analitična znanja lahko pomagajo?

Poslovni analitiki delamo po BACC modelu, zato bom v nadaljevanju naštel aktivnosti (vprašanja), ki bodo omogočale lažjo realizacijo projekta GDPR in olajšali delo DPO po tem modelu.



Deležniki

- Kateri deležniki zbirajo osebne podatke?
- Kako poiščemo prave deležnike?
- Katere tehnike uporabiti pri iskanju deležnikov?
- Ali smo katerega deležnika pozabili?
- Kateri deležniki imajo največji vpliv na obdelavo osebnih podatkov?

Potreba

- Ali imamo podporo vodstva?

- Katere potrebe imajo posamezni deležniki v zvezi z obdelavo osebnih podatkov?
- Ali smo izdelali analizo vrzeli?
- Ali potrebujemo vse zbrane podatke pri delu z našimi strankami?
- Ali lahko zagotovimo zahteve iz uredbe o pozabi podatkov?
- Ali lahko enostavno naredimo spremembe obstoječih osebnih podatkov?
- Ali znamo posamezniku odgovoriti, katere podatke o njem zbiramo in zakaj?
- Kje vse so zbrani osebni podatki, ki jih potrebujemo za poslovanje in v kakšnih datotekah/ bazah?
- Ali smo zagotovili preglednost in skladnost podatkov z GDPR?
- Ali znamo spremljati in obvladovati grožnje v zvezi z obdelavo osebnih podatkov?
- Ali vemo kako bomo spremljali spremembe na varnostnih in arhivskih kopijah?
- Kako bomo šifrirali in anonimizirali podatke?

Vrednost

- Kako bomo vrednotili uvedbo zahtev iz GDPR?
- Kaj bodo od podpore GDPR imele naše stranke (v krajšem in daljšem obdobju)?

Sprememba

- Ali potrebujemo DPO in kako bodo definirane njegove naloge?
- Ali vemo kaj moramo vse spremeniti, da smo skladni z GDPR?
- Ali vemo za katero dokumentacijo mora skrbeti DPO?

Rešitev

- Kdo bo izdelal nove spletne rešitve?
- Kako bomo obladovali osebne podatke, ki se trenutno vodijo ročno?
- Kako bomo olajšali delo marketingu in drugim oddelkom, ki komunicirajo z našimi strankami?
- Kdo bo poročal o incidentih »Informacijskem pooblaščencu« (v 72 urah)?

Kontekst

- Ali vemo katera zakonodaja podpira naše obdelave podatkov na poslovnem področju v zvezi z uredbo GDPR
- Ali vemo kako se zagotavlja konsistentnost z že delujočimi standardi npr. ISO 27k?

Če bomo delali po poslovno analitičnem modelu (BACC), in si odgovorili na večino zgoraj zastavljenih vprašanj, bo projekt implementacije uredbe GDPR in delo DPO izveden hitreje, kvalitetneje in predvsem pravočasno.

Ali nam pri uvajanju GDPR lahko pomaga standard ISO 27k?

Če že imamo vpeljan standard ISO 27001, smo že naredili velik korak k uspešni uvedbi zahtev GDPR. Po nekaterih ocenah je cca 70% zahtev realizirano če uporabljamo standard o varovanju informacijskih sistemov, vendar bodite pozorni, še vedno je ena tretjina odprtih nalog. Tako velik procent realiziran zahtev je, ker so osnovna načela GDPR in standarda ISO27k enaka. Ta načela so **celovitost, razpoložljivost in zaupnost** podatkov, kot je prikazano na sliki:

Kakšna znanja in kompetence mora imeti DPO?

GDPR zahteva tudi imenovanje pooblaščene osebe za varstvo podatkov **DPO** - »Data Protection Officer«. Pooblaščena oseba za varstvo podatkov se imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov (37. člen uredbe). Glede na naloge DPO (39. člen uredbe) in odprtih vprašanj iz BACC modela je jasno, da potrebuje tudi **znanja s področja strateške analize, načrtovanja in spremljanja izvedbe poslovne analize, izvabljanja in sodelovanja, analize zahtev, upravljanja življenjskega cikla zahtev ter tudi ocene rešitve**. Vsa ta področja znanj, ki bi jih moral poznati DPO so tudi področja znanj poslovnega analitika in objavljena v **BABOK v3** (Business Analysis Body of Knowledge® - BABOK Guide®).

Poleg tega bi PDO moral imeti (ali bi moral pridobiti) naslednje **veščine**:

- analitično razmišljanje in reševanje problemov,
- ustrezne vedenjske lastnosti,
- obvladovati poslovna znanja,
- obvladovati veščine komuniciranja,
- poznati veščine medsebojnega sodelovanja,
- obvladovati orodja in tehnologije poslovne analitike.

Vse te veščine so tudi navedene v BABOK v3.

Zato ne razmišljajte, ampak si **pridobite poslovno analitična znanja**, ki vam ne bodo pomagala samo na področju uvajanja GDPR, ampak na vseh področjih, od dela na projektih, optimizaciji poslovnih procesov, delu z velikimi količinami podatkov, pri agilnih metodah dela itd.