Usklađivanje s EU GDPR Uredbom

Značaj

Zaštita privatnosti kroz tretman osobnih podataka danas je jedno od temeljnih ljudskih prava. Do sada se ovo pitanje uređivalo nacionalnom regulativom, tako da su se pristupi u pojedinim zemljama EU-a jako razlikovali. Zbog toga je Europska zajednica donijela Uredbu 2016/679 pod nazivom GDPR – *General Data Protection Regulation* i njene odredbe su iznad nacionalnog zakonodavstva. GDPR područje zaštite osobnih podataka uređuje cjelovito i transparentno, ali poslodavcima donosi mnoge nove obveze. Jedna od novosti su i drastične kazne za prekršitelje njenih zahtjeva. Obveza ove Uredbe na snazi je od 25. svibnja 2018.g.

GDPR dužne su primjenjivati sve pravne osobe koje prikupljaju i obrađuju osobne podatke – tijela državne uprave (ministarstva, središnji državni uredi, agencije, regionalna i lokalna samouprava (gradovi, županije), gospodarske tvrtke, ustanove koje je osnovala RH ili regionalna samouprava, političke stranke, udruge, sindikati itd.

Prvi „val“ obveza primjene ove Uredbe je za sada prošao, no u praksi rješenja su najčešće necjelovita i relevantna istraživanja pokazuju da su im obveznici pristupili vrlo površno. Zbog toga su potrebni daljnji napori u primjeni GDPR-a, jer to i nije jednokratni projekt, već kontinuirani poduhvat. Nadzor primjene ove Uredbe provodi Agencija za zaštitu osobnih podataka RH.

Usluge ZIH-a

Konzultantske usluge

- Snimka trenutačnog stanja zaštite osobnih podataka
  Snimka postojećih obrada osobnih podataka i njihovih zaštita, identifikacija novih zahtjeva iz okruženja, definiranje što sve predstavlja osobne podatke prema Uredbi, gdje se sve oni nalaze, koja su im sredstva pohrane, tko su im vlasnici itd.
- Kreiranje registra obrada osobnih podataka / kataloga podataka i dokumenata koji sadrže osobne podatke
- GAP analiza u odnosu na GDPR
  Njen cilj je odrediti razinu (ne)sukladnosti / odstupanja od zahtjeva Uredbe te načiniti prijedloge potrebnih organizacijskih, procesnih, pravnih i tehničko-tehnoloških usklađivanja.
- DPIA (Data Protection Impact Assessment)
  Njen cilj je u svim obradama osobnih podataka, identificirati aktivnosti takvih obrada, procijeniti rizike, odrediti metrike za njihovo usklađivanje itd.
- Izrada preporuka za poboljšanja / usklađivanja
  Na osnovi DPIA rezultata definiraju se konkretne aktivnosti i njihovi prioriteti

- Integracija GDPR rješenja u druge sustave upravljanja (ISO 9001 upravljanje kvalitetom, ISO 27001 upravljanje informacijskom sigurnošću, ISO 22301 upravljanje kontinuitetom rada itd.)
- Stručni nadzor provedbe Programa usklađivanja
  Cilj je nadzirati ostvarenje potrebnih prilagodbi i po potrebi inicirati korektivne radnje

Seminari

- Prezentacija poslovodstvu o zahtjevima GDPR Uredbe i načinima njihovog zadovoljenja
- Edukacije tima za realizaciju GDPR projekta, ključnih dionika unutar tvrtke i djelatnika koji dolaze u dodir s osobnim podacima u dnevno-operativnom poslovanju
- Edukacija DPO-a (Data Protection Officer-a / Službenika za zaštitu osobnih podataka), uključivo njegovo certificiranje (Certified DPO) po međunarodnoj akreditaciji za GDPR

Način rada

ZIH putem svojih eksperata za primjenu GDPR Uredbe, u uskoj suradnji s korisnicima, može razviti, sudjelovati u implementaciji njenih zahtjeva te u njegovom unapređenju. Na početku ovog poduhvata predlaže se održati prezentaciju poslovodstvu *Zahtjevi GDPR-a i načini njihovog zadovoljenja.* Nakon toga radi se plan projekta te provodi njegova realizacija. Tijekom ovog postupka uputno je da odgovorna osoba korisnika završi i edukaciju za DPO.