Ali veste, kako pripeljati podjetje do GDPR-skladnosti?

Kaj je GDPR?

Uredba GDPR (*angl.: General Data Protection Regulation*), št. 2016/679, sprejeta 27. aprila 2016, je Uredba 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).

Zakaj je treba ščititi osebne podatke?

Razvoj tehnologije in proces digitalizacije sta s seboj prinesla tako lažje in hitrejše zbiranje, obdelovaje in skladiščenje osebnih podatkov kot tudi ogromen porast količine podatkov. Porast in dostopnost podatkov pa sta povzročila tudi pospešen razvoj kriminalitete na tem področju, tako da se v sodobnem času soočamo z incidenti, kot sta recimo kraja identitete ali zloraba osebnih podatkov. Omenjeni primeri so bili vzrok pojava potrebe po zaščiti osebnih podatkov. V ta namen se je z leti sprejemala različna zakonodaja, ki se prilagaja tehnološkim napredkom in tehnikam uporabe. Zadnja na tem področju sprejeta zakonodaja je uredba GDPR, ki naslavlja:

- napredno zaščito osebnih podatkov,
- celovito zaščito osebnih podatkov,
- razumevanje pomembnosti zaščite podatkov,
- zaščito prostega pretoka informacij v Evropski uniji.

Časovnica

27. 4. 2016

Evropski parlament in Svet sprejme Uredbo (EU) 2016/679 Splošna uredba o varstvu podatkov (GDPR).

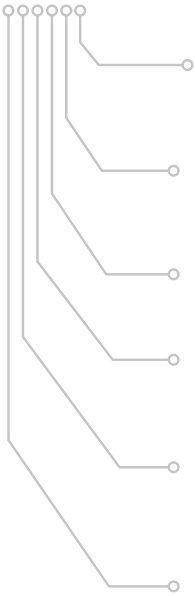
25. 5. 2018

Uredba GDPR stopi v veljavo v vseh članicah EU brez prehodnega obdobja.

od 25. 5. 2018 dalje

Uredba velja v celoti in v nespremenjeni obliki ter zagotavlja enako raven zaščite osebnih podatkov in prostega pretoka informacij na območju celotne EU.

Osnovni principi GDPR:



Obdelava podatkov mora potekati zakonito, urejeno in transparentno.

Zbiranje osebnih podatkov se izvaja le za točno določen in zakonit namen.

Obdelava podatkov mora potekati omejeno, natančno določeno.

Podatki morajo biti točni in osveženi.

Podatki morajo biti v obliki, ki omogoča identifikacijo posameznika le tako dolgo, kot je potrebno za obdelovanje podatkov.

Obdelava podatkov mora potekati v načinu, ki zagotavlja varnost teh podatkov.

Kaj se bo zgodilo v primeru kršitve uredbe?

Če organizacija zazna vdor in/ali krajo osebnih podatkov, mora v roku 72 ur o tem obvezno poročati regulatorju, za Slovenijo je to informacijski pooblaščenec. Če tega ne stori, so organizacija in odgovorne osebe lahko kaznovane s finančnimi kaznimi, ki so določene v uredbi. Zgornja meja kazni sega do 20 milijonov evrov oziroma do 4 % letnega prometa.

Poročilo regulatorju mora vsebovati informacije:

- kakšen je bil vdor v osebne podatke in kako je do njega prišlo;
- kakšne ukrepe je organizacije sprejela, da do vdorov ne bo več prišlo;
- kakšne ukrepe je organizacija sprejela, da omeji posledice vdora.

Glede na GDPR sta lahko odgovorni obe strani, to sta upravljavec in obdelovalec. To je tudi ključna sprememba glede na obstoječo zakonodajo v Republiki Sloveniji.

Ključni pojmi GDPR-uredbe

V uredbi so natančno definirane določene vloge:

»zbirka« pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;

»upravljavec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; ko namene in sredstva obdelave določa pravo Evropske unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Evropske unije ali pravom države članice;

»obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

»uporabnik« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti ne glede na to, ali je tretja oseba ali ne.

Te vloge so pomembe za razjasnitev vloge posameznika in organizacije pri izvajanje uredbe.

Kaj je osebni podatek?

Uredba GDPR ločuje osebne podatke v dve kategoriji. Kot osebni podatek opredeljuje katerokoli informacijo, s katero se lahko neposredno ali posredno identificira posameznika. To velja tudi za informacije, ki so hranjene v digitalni ali fizični obliki. Dodatno GDPR določa še posebno kategorijo – občutljivi osebni podatki, za katere so predvidene strožje zahteve za varovanje.

Osebni podatki po GDPR so:

- ime in priimek,
- naslov,
- elektronska pošta,
- davčna številka,
- št. kreditne kartice,
- podatki o lokaciji,
- IP-naslovi,
- MAC-naslovi,
- piškotki.

Občutljivi osebni podatki po GDPR so:

- zdravstveni podatki,
- religija,
- rasa,
- politična usmeritev.

Pravice posameznikov po GDPR

GDPR določa tudi pravice posameznikov glede zaščite osebnih podatkov:

- **Pravica vedeti**
  Posameznik mora vedeti in razumeti, na kakšen način in zakaj se bodo zbirali in obdelovali njegovi osebni podatki, kdo jih bo obdeloval in koliko časa bodo hranjeni.
- **Pravica do popravka**
  Posameznik ima pravico, da zahteva, da se njegovi osebni podatki popravijo, če ugotovi, da niso točni ali celoviti.
- **Pravica do omejitve obdelave**
  V nekaterih primerih se lahko osebni podatki samo hranijo, ne smejo pa se obdelovati.
- **Pravica do ugovora**
  V času zbiranja osebnih podatkov ima posameznik pravico do ugovora obdelave teh osebnih podatkov. V primeru ugovora mora obdelovalec ali prenehati obdelovati podatke ali dokazati, da ima druge zakonske podlage za nadaljnjo obdelavo teh podatkov.
- **Pravica do dostopa**
  Posameznik ima pravico do dostopa do svojih osebnih podatkov. Posameznik mora vložiti poseben zahtevek, ki se mora obdelati v roku enega meseca.
- **Pravica do izbrisa**
  Posameznik ima pravico zahtevati izbris svojih osebnih podatkov, če osebni podatki niso več potrebni za obdelavo, če je soglasje preklicano, če je posameznik podal ugovor, če so bili podatki nezakonito obdelani ali pa če se morajo osebni podatki izbrisati zaradi drugih zakonskih obveznostih.
- **Pravica do prenosa podatkov**
  Posameznik ima pravico zahtevati kopijo vseh osebnih podatkov, ki jih ima obdelovalec ali upravljavec pri sebi. Kopija mora biti podana v obliki, ki jo uporablja posameznik ali upravljavec – ta oblika se mora določiti pred dostavo kopije.
- **Pravice v odnosu do avtomatske obdelave podatkov - izbira odločitve in profiliranje**
  Če proces obdelave podatkov poteka avtomatsko, mora obdelovalec vanj vključiti postopek, ki omogoča, da lahko posameznik vedno vstopi v ta proces, poda mnenje o njem ali zaprosi za obrazložitev procesa.

Trije koraki do GDPR-skladnosti

1 Zavedanje spremembe

V Sloveniji bo GDPR zamenjal trenutno veljavni zakon o varovanju osebnih podatkov (ZVOP 1). Čeprav bo sprejet zakon ZVOP 2, ta ne bo posegal v samo obliko in vsebino uredbe, ampak bo samo podal izvedbeni okvir in določene dodatne vsebine, ki so že zdaj bile v ZVOP 1.

Za slovenske organizacije je zato najprej ključno zavedanje, da bo GDPR stopil v veljavo s 25. majem 2018 v polni obliki brez prehodnega obdobja in da natančno določa, kakšne so odgovornosti upravljavcev in obdelovalcev osebnih podatkov. Ker večina organizacij v Sloveniji zbira in/ali obdeluje osebne podatke, se bodo morale aktivno lotiti reševanja tematike GDPR s pomočjo različnih formalnopravnih in tehničnih ukrepov. Zavedanje tega pomeni prvi korak k skladnosti poslovanja z GDPR-določili.

2 Prepoznavanje dobre prakse

Organizacije so bile že v preteklosti z različnimi pravnimi regulativami ali z dokazovanji skladnosti na nek način prisiljene ukvarjati se z informacijsko varnostjo. Varovanje osebnih podatkov je del tega, kar pomeni, da organizacije dobre prakse in metodologije že poznajo oziroma jih uporabljajo. Primer dobre prakse je, denimo, implementacija mednarodnega standarda ISO 27001. Kot drugi korak je torej treba izbrati »framework« oziroma proces za doseganje GDPR-skladnosti.

3 Izbira poti za doseganje GDPR-skladnosti

Pot do GDPR-skladnosti je zapletena in mnogim organizacijam predstavlja velik zalogaj. Na tej točki je zato smiseln razmislek, ali bi bilo smiselno na pot do skladnosti stopiti skupaj s partnerjem, ki na podlagi izkušenj in strokovnosti lahko ponudi ustrezne nasvete in rešitve. S&T Slovenija kot eden izmed največjih ponudnikov storitev in rešitev za področje informacijske tehnologije v Sloveniji ponuja celovit pristop, ki povezuje svetovanje in tehnološke rešitve, ki organizacijam omogoča, da lahko postanejo »GDPR Ready« v določenih rokih. Pristop S&T do GDPR-skladnosti si lahko ogledate na naslednji strani.

Celovit pristop S&T h GDPR-skladnosti

svetovanje na formalnopravnem področju

(pravni akti, soglasja, izjave, pogodbe)

svetovanje na tehničnem delu

(izbira metodologije, načini iskanja podatkov, GAP-analiza, varnostni pregledi, varnostne politike, incident response politike)

poslovne rešitve

svetovanje in implementacija na aplikativni ravni
(dodatki ERP-sistemom, data masking, data minimization, data access control)

infrastrukturne rešitve

- **Data discovery** (kje so osebni podatki v strukturirani in nestrukturirani obliki)
- **Data protection** (nadzor dostopov do podatkov, nadzor kanalov prenosa, šifrirni mehanizmi, data masking, data minimization)