Hrvatska revizorska komora

GDPR – Opća uredba o zaštiti osobnih podataka

STRUČNO SAVJETOVANJE OVLAŠTENIH REVIZORA I RAČUNOVOĐA

27. - 28. studeni, 2017

Prof. dr. sc. Mario Spremić

Ekonomski fakultet Zagreb

Sadržaj

- Uvod
- Važni pojmovi za razumijevanje GDPR-a
- Pravila GDPR-a
- Prava ispitanika i zaštita
- Kako se uskladiti?
- Studija slučaja provedbe GDPR

GDPR - General Data Protection Regulation

- Novi pravni okvir zaštite osobnih podataka na razini EU – Opća uredba o zaštititi osobnih podataka
- Odobrena od strane Europskog parlamenta 14.4.2016
- Zamjenjuje Direktivu o zaštiti osobnih podataka 95/46/EC iz 1995. godine
- Direktno se primjenjuje u državama članicama bez potrebe za implementacijom u nacionalno zakonodavstvo
- AZOP-a bit će ovlaštena za primjenu Uredbe i osiguranje sukladnosti s njenim odredbama
- Stupa na snagu 25.05.2018.

http://www.privacy-regulation.eu/hr/index.htm

4.5.2016. HR Službeni list Europske unije L 119/1

I.

(Zakonodavni akti)

UREDBE

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA

od 27. travnja 2016.

o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 16.,

GDPR osnovne informacije

- Ciljevi:
  - usklađivanje zakona o zaštiti podataka u cijeloj EU,
  - zaštita i osnaživanje osobnih podataka svih građana EU,
  - promjena načina pristupa zaštiti podataka u organizacijama
- Kazne - novčane kazne u iznosu do **€20 milijuna ili 4% ukupnog godišnjeg prometa** (što je veće)
- Obveznici – svi poslovni subjekti koji barataju s podacima korisnika koji žive na području EU, neovisno o lokaciji tvrtke
- Osobni podatak po GDPR-u – ime, prezime, oib/jmbg, IP adresa, gps lokacija, RFID tag, web cookies, MAC adrese, IMEI brojevi, itd.

25.05.2018

- Želite vidjeti kako kartičarska kuća koristi vaše podatke o kupnji?
- Želite saznati tko točno u MUP-u pristupa podacima o vašoj registraciji automobila, boravištu i podacima s osobne iskaznice?
- Želite da od banke dobijete popis svih osoba koje su unatrag mjesec dana pristupale vašim financijskim podacima?
- Želite zatražiti osobne podatke koje o vama prikuplja bilo koja mobilna aplikacija poput vaših GPS lokacija i IMEI broja?
- Moći ćete zatražiti i informaciju o tome koje podatke o vama prikuplja svaka web stranica koja vas je zatražila da prihvatite njen cookie

Osobni podatak i ostali važni pojmovi

- **Osobni podatak** više nije samo ime, prezime i oib/jmbg, nego i IP adresa, GPS lokacija, RFID tag, web cookies, MAC adrese, IMEI brojevi itd.
- **Obrada osobnih podataka** je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne
- **Zbirka osobnih podataka** je svaki strukturirani skup osobnih podataka koji je dostupan prema posebnim kriterijima
- **Voditelj zbirke osobnih podataka** je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka
- **Primatelj** je fizička ili pravna osoba, državno ili drugo tijelo kojem se osobni podaci otkrivaju, neovisno o tome je li on ujedno i treća strana ili nije

Pravila GDPR-a – prava korisnika

- Pravo na pristup
  - Korisnik ima pravo dobiti od voditelja obrade podataka potvrdu obrađuju li se njegovi osobni podaci, zašto se obrađuju i koliko dugo
- Pravo na ispravljanje pogrešaka
- Pravo na zaborav (brisanje podataka)
  - Korisnik ima pravo od voditelja obrade ishoditi brisanje prikupljenih osobnih podataka koje se na njega odnose
- Izvješćivanje o povredi osobnih podataka
  - U slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi izvješćuje nadzorno tijelo i ispitanika

Pravila GDPR-a – prava korisnika

- „Jasan i pozitivan pristanak" na obradu osobnih podataka od strane ispitane osobe
- Pravo da se ograniči upotreba podataka (neželjeno oglašavanje)
- Pravo na prenosivost podataka
  - Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega te ima pravo prenijeti te podatke drugom voditelju obrade
- Pravila o privatnosti moraju biti objašnjena jasnim i razumljivim jezikom

Prava ispitanika i zaštita

Voditelj zbirke osobnih podataka dužan je

1. dostaviti potvrdu o tome da li se osobni podaci koji se odnose na njega obrađuju ili ne
2. dati obavijest u razumljivom obliku o podacima koji se odnose na njega
3. omogućiti uvid u evidenciju zbirke osobnih podataka te uvid u osobne podatke sadržane u zbirci osobnih podataka
4. dostaviti izvatke, potvrde ili ispise osobnih podataka sadržanih u zbirci osobnih podataka koji se na njega odnose
5. dostaviti ispis podataka o tome tko je i za koje svrhe i po kojem pravnom temelju dobio na korištenje osobne podatke koji se odnose na njega

Što treba učiniti da se uskladimo s GDPR?

- Postati svjestan problema - napraviti inicijalnu procjenu rizika (revizija upravljanja podacima), odrediti područja u kojima očekujemo probleme
- Postati odgovoran ('*accountable*') – popisati sve osobne podatke koje pohranjujemo i s kojima baratamo. Zašto ih pohranjujemo? Trebamo li ih? Gdje pohranjujemo podatke? Baratamo li njima na siguran način? Gdje se nalaze osobni podaci i u kojem su formatu (nestrukturirani formati, tablice, ppt, dopisi, web stranica …)
- Kako stvaramo korisničke podatke i zašto? Izvori podataka (pronaći rizične izvore podataka)
- Procedure pristupa/baratanja podacima
- Provjeriti procedure dodjele ovlasti rada s podacima (pristup podacima, brisanje i prijenos podataka)

Implementacija GDPR-a

- Informirati zaposlenike i korisnike o procedurama koje se odnose na privatnost podataka
- Napraviti plan zaštite podataka (oblikovanje kontrola u radu s podacima, osobito kontrola koje su sukladne GDPR-u)
- Izvještavanje o povredama i problemima u baratanju s podacima (data breach)
- Provjeriti procedure sigurnosne pohrane i povrata podataka (neovisno o tome kakva je IT infrastruktura, gdje su podaci pohranjeni, itd)

Agencija za zaštitu osobnih podataka

- AZOP će biti ovlaštena za primjenu Uredbe i osiguranje sukladnosti s njenim odredbama u RH
  - nadzire provođenje zaštite osobnih podataka,
  - ukazuje na uočene zloupotrebe prikupljanja osobnih podataka,
  - sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka,
  - rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom,
  - vodi središnji registar.
- Voditelji zbirki podataka bit će dužni unutar 72 sata AZOP-u prijaviti neovlašteni pristup podacima

Kazne u primjeni GDPR-a

- Upozorenje u pisanom obliku u slučaju prve pogreške i bez namjernog nepoštivanja Uredbe
- Ravnatelj agencije, zamjenik ravnatelja, zaposlenici stručne službe te voditelji zbirki odgovaraju kaznama od 20.000 do 40.000 kn
- Kompanije ovisno o veličini i vrsti pogreške mogu biti kažnjene s 4% ukupnog godišnjeg prometa ili 20 milijuna eura
- Visina ovih novčanih kazni praktički osigurava da će privatnost podataka biti tema o kojoj će se razgovarati na razini upravnog odbora

Tko treba biti uključen u GDPR projekt?

Otvoriti 'GDPR projekt'

Uključiti stručnjake iz različitih područja:

- pravni stručnjaci,
- stručnjaci u području informacijske sigurnosti,
- administratori i analitičari podataka,
- arhitekti poslovnih procesa,
- tehnološki stručnjaci,
- voditelj projekta

Nužna potpuna predanost i potpora Uprave!

Zaključak

- GDPR stupa na snagu 25.05.2018 i donosi velike promjene u upravljanju podacima
- Potrebno je pregledati organizacijske i tehnološke procedure upravljanja podacima i provjeriti usklađenost s GDPR
- Potrebno je napraviti procjenu rizika (GDPR pozicioniranje)
- Potrebno je odrediti što točno treba napraviti da bi bili usklađeni
- Potrebno je uskladiti organizacijsku strukturu (DPO)
- Potrebno je pregledati i uskladiti procedure (odrediti uloge i odgovornosti, oblikovati nove politike i procedure i provesti tehnološke kontrole)

Hvala na pozornosti

Prof.dr.sc. Mario Spremić
Sveučilište u Zagrebu, Ekonomski fakultet
Trg J.F.Kennedya 6, 10000 Zagreb

e-mail: mspremic@efzg.hr
web: http://www.efzg.hr/mspremic
linkedin: https://hr.linkedin.com/pub/mario-spremic/15/149/a90