KPMG

# Zaštita podataka o ličnosti

## GDPR i povezani zakoni

Zaštita podataka i privatnost postali su imperativ u današnjem digitalnom svetu. Klijenti i regulatori sve više zahtevaju adekvatnu zaštitu podataka o ličnosti.

**Da li ste spremni ?**

IT Advisory and Legal services
KPMG d.o.o. Beograd

# Nova regulativa i izazovi na tržištu

Generalna regulativa o zaštiti podataka (EU General Data Protection Regulation - GDPR) je formalno usvojena u aprilu 2016. od strane Evropskog parlamenta. Za razliku od direktiva, nije potrebno da vlade zemalja usvajaju lokalne regulative, tako da **GDPR formalno stupa na snagu u maju 2018. godine i od tada organizacije moraju biti usklađene.**


## Nove tehnologije i uticaj na poslovanje

Razvoj novih tehnologija (Big Data, mobilne aplikacije, društvene mreže, aplikacije za profilisanje potrošača, itd.) utiče na privatnost podataka i direktno **raste i broj skandala** koji su povezani sa privatnošću.

Ukoliko lični podaci nisu adekvatno zaštićeni, **organizacije rizikuju da izgube poverenje svojih klijenata i zaposlenih.**

Organizacije će morati da procene da li su postojeće organizacione, procesne, administrativne i tehničke mere zaštite dovoljne u pogledu svrhe i obima obrade podataka, količine prikupljenih podataka, perioda čuvanja, kao i njihove dostupnosti.

## Zašto je ova regulativa važna za Vas?

**GDPR definiše pravila koja se odnose na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti kao i pravila koja se odnose na slobodno kretanje podataka.**

Ova regulativa je najveća i najdalekosežnija promena u regulaciji privatnosti i zaštite podataka u istoriji.

GDPR zahteva od organizacije da implementira adekvatne i prilagođene okvire kontrola podataka i upravljanja rizikom. **Puko ažuriranje dokumenata neće biti dovoljno.** Potrebno je implementirati proces zaštite podataka i povezane kontrole, jer se zahteva upravljanje implementacijom i održavanjem koje se može kasnije pratiti i proveriti.

## Kako GDRP ima uticaj na srpske organizacije, iako Srbija nije članica EU?

Regulativa se neće primenjivati samo za kompanije sa sedištem u EU (ili njihovim filijalama u EU), već i za one čije je sedište izvan EU, a koje nude robu ili usluge unutar EU.

**Velike kazne**

Mogu iznositi do **20 miliona evra ili 4% globalnog godišnjeg prometa**, zavisno od toga koji iznos je veći.

**Nove funkcije**

Ukoliko su predmet posebne kategorije ličnih podataka ili masovni podaci, treba imenovati **Rukovodioca za zaštitu podataka.**

**Registar**

Organizacije će morati da vode **inventar o ličnim informacijama.**

**Izveštavanje o curenju podataka**

Potrebno prijaviti nadležnim organima **u roku od 72h** (a potencijalno i korisnicima). Incidente je potrebno logovati.

**Bezbednost**

Jasni zahtevi oko monitoringa, logovanja, enkripcije i anonimizacije.

**Procene uticaja i analize**

Treba sprovoditi procene uticaja na privatnost podataka (DPIA). Ako rezultat pokazuje visok rizik, nadzorni organ treba da bude konsultovan.

**Prava korisnika**

Prava su proširena i obuhvataju **mogućnost prenosa podataka i pravo na brisanje.**

**Osetljivi podaci o ličnosti**

Pored ranije obuhvaćenih, sada se proširuju i na **biometrijske i genetske podatke.**

**Pristanak korisnika**

Treba da se dobije **na nedvosmislen način**, putem izjave ili jasne potvrde (unapred obeležena polja su neprihvatljiva).

**Servisne organizacije**

Mere moraju biti primenjene i od organizacija koje kontrolišu i od onih koje ih obrađuju. Potrebno je postojanje jasnih sporazuma.

KPMG

# Kada i kako reagovati ?

- Da li ste upoznati sa svim propisima o privatnosti i zaštiti podataka kojih se Vaša organizacija mora pridržavati?
- Da li relevantni akteri u Vašoj organizaciji znaju koje (lične) informacije Vaša organizacija obrađuje, gde se sve nalaze, u kojim oblicima i ko upravlja njima?
- Da li Vaša organizacija ima adekvatne kontrole kojima obezbeđuje sigurne tokove podataka u skladu sa GDPR?
- Da li obradu i čuvanje poverljivih podataka korisnika *„autsorsujete“*, držite u *cloud-u*, delite sa drugim kompanijama ili planirate ove aktivnosti?
- Da li Vaša organizacija poseduje adekvatne tehničke i organizacione mere kako bi se nadzirala obrada podataka i sprečilo njihovo curenje?
- Da li ste spremni za korišćenje novih tehnologija na način usklađen sa zahtevima privatnosti?

### Povezani zakoni u Srbiji

- U Srbiji postoji važeći **Zakon o zaštiti podataka** o ličnosti koji nije usklađen sa novom EU regulativom i ima posebne odredbe sa kojima je takođe potrebno ostati usklađen.
- Sa druge strane, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je započeo javnu raspravu o novom modelu Zakona o zaštiti podataka, ali još uvek ne postoje jasni datumi i koraci usvajanja.
- U toku 2016. godine usvojen je **Zakon o informacionoj bezbednosti** kojim se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica kao i nadležni organi. Zakon je u direktnoj vezi sa ISO/IEC 27000 porodicom standarda.

Ukoliko niste sigurni za odgovor na bilo koje od gore navedenih pitanja, **možete nas kontaktirati**. Predstojeće izmene u regulativi o zaštiti podataka zahtevaće značajne organizacione, procesne, tehnološke i administrativne promene.

**Treba delovati odmah!**

# Kako Vam mi možemo pomoći

KPMG koristi **okvir za upravljanje zaštitom podataka** koji se proširuje na 4 glavne faze i grupe aktivnosti (I) **procena**, (II) **dizajn**, (III) **implementacija** i (IV) **praćenje**.

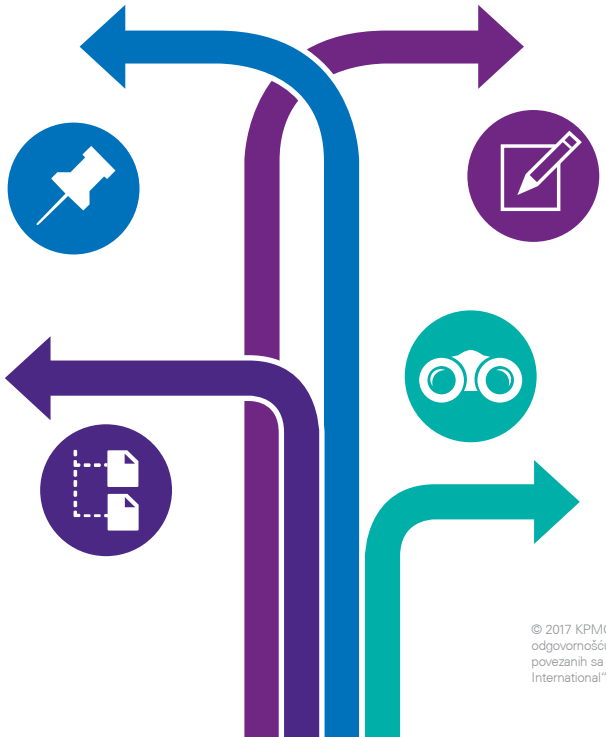
Za utvrđivanje kako GDPR utiče na Vašu organizaciju, prvi korak je **procena trenutne usklađenosti** i spremnosti za zaštitu podataka (sa tehničke i pravne strane). Dodatno vrši se i **mapiranje sa zahtevima regulative u Srbiji** i posebno davanje pažnje na suprotstavljene zahteve različitih zakona.

### Implementacija

Pomoć u implementaciji procesa, politika i kontrola kako bi smanjili rizike koje se odnose na privatnost i poverljivost

### Procena

Nezavisna procena trenutnog stanja i gepova koji postoje u odnosu na nove regulatorne zahteve uz davanje preporuka za usklađivanje



### Dizajn

Zajednički rad sa Vama na pripremi programa za privatnost radi usklađivanja sa zahtevima regulative u Srbiji i EU a u skladu sa strategijom organizacije.

### Praćenje

Tehnička i pravna podrška u održavanju kontrolnog okruženja za očuvanje privatnosti i poverljivosti podataka

# Ko smo mi

KPMG je globalna mreža profesionalnih firmi koje pružaju usluge **revizije**, **poreskog**, **finansijskog**, **pravnog** i **IT savetovanja**.

KPMG d.o.o. Beograd je izgradio jaku nacionalnu praksu koja se zasniva na kombinaciji lokalnog i međunarodnog znanja i iskustva zaposlenih. Srpska kancelarija poseduje značajno iskustvo u pružanju punog obima usluga poslovnog savetovanja domaćim privrednim društvima, vladinim organizacijama, stranim investitorima, bankama i finansijskim institucijama, agencijama za finansiranje i drugim firmama koje posluju u Srbiji.

Multidisciplinarni tim sastavljen od visoko kvalifikovanih stručnjaka poseduje sve potrebne veštine, znanja i iskustvo da vam pruži podršku prilikom rešavanja najizazovnijih problema. Naši stručnjaci pokrivaju sve aspekte iz oblasti privatnosti, uključujući, pravna pitanja, upravljačke kontrole i tehnologiju.

Članovi našeg tima su stručnjaci sa značajnim iskustvom, međunarodnim sertifikatima i položenim ispitima u Srbiji:

- **CISA** - Sertifikovani revizori informacionih sistema
- **ITIL v3** foundation
- **ISO/IEC 27001:2013 ISMS Lead Auditor**
- **Sertifikovani interni revizori**
- **Advokati**

Prisutni u **152** zemlje

**189.000** zaposlenih širom sveta

**46** zaposlenih sa međunarodnim sertifikatima u Srbiji: **CISA**, **ITIL**, **ISO27001**, **ACCA**, **ICAEW**, **ICAO**, **CFAI**, **CIA**

U Beogradu od **1996.** godine

**290** zaposlenih u Srbiji i Crnoj Gori

# Kontaktirajte nas:


**KPMG d.o.o. Beograd**
Kraljice Natalije 11
11000 Belgrade, Serbia

**T:** +381 11 20 50 500
**F:** +381 11 20 50 550
**E:** itadvisory@kpmg.rs
**www.kpmg.com/rs**

**Dušan Tomić**
Partner, Head of Financial Institutions & Services
**T:** +381 11 20 50 521
**M:** +381 60 20 55 521
**E:** dtomic@kpmg.com

**Nebojša Janković, CISA, ITILF, ISO27001 LA**
Manager, IT Advisory
**T:** +381 11 20 50 603
**M:** +381 60 20 55 603
**E:** njankovic@kpmg.com

**Marija Milojević**
Senior Manager, Tax & Legal
**T:** +381 11 20 50 526
**M:** +381 60 20 55 526
**E:** mmilojevic@kpmg.com


KPMG

stručnjaci pomažu klijentima da usklade bezbednosne, IT pravne i poslovne funkcije kako bi zajedno doprineli strateškim ciljevima poslovanja