

Uskladite se s GDPR-om,  
čak i ako ste tek sada počeli razmišljati o tome



Vaši prvi koraci su  
kvalitetna edukacija i  
pouzdana partneri.  
Nastavite čitati i riješite  
prve korake.

Zadnjih par mjeseci u zraku se osjećala panika i brzopletost te još uvijek kruže dezinformacije o samim načelima GDPR uredbe, a pogotovo o potrebnim alatima i implementacijskim praksama. GDPR Uredba niti je počela niti završila 25.5.2018. Radi se o kontinuiranom procesu interne organizacije koji štiti korisnike a samoj tvrtki daje dodatnu vrijednost.

Svi govore o zaštiti osobnih podataka i GDPR-u.  
Okrenimo priču malo i sagledajmo za početak GDPR-ove osobne podatke.

## GDPR uredba - osobna iskaznica

Ime i prezime:	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)
Nadimak:	GDPR uredba
Datum rođenja:	27.04.2016.
Datum punoljetnosti:	25.05.2018. (rok za prilagodbu)
Državljanstvo:	obvezujuća regulativa za sve zemlje EU, odnosi se na sve tvrtke
Cilj:	regulirati obradu osobnih podataka
Mjere:	ograničavanje svrhe, smanjenje količine podataka, točnost, ograničenje pohrane, cjelovitost, povjerljivost, pouzdanost, zakonitost obrade
Zadatak:	za UPRAVU TVRTKE - bez jasnog interesa Uprave nije moguće provesti potrebne promjene - Uprava mora razumjeti važnost Uredbe i njene posljedice na poslovanje - Uprava je odgovorna za razvoj poslovne strategije koja podržava GDPR
Odgovornost:	svih u tvrtki koji dolaze u kontakt s osobnim podacima
Posebna odgovornost:	službenik za zaštitu osobnih podataka
Voditelj obrade:	fizička ili pravna osoba koje određuje svrhe i sredstva obrade osobnih podataka (eng. controller) - sama TVRTKA
Izvršitelj obrade:	fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade (eng. processor) - primjer: tiskara u koju se šalju računi na tisak i distribuciju
Priroda projekta:	organizacijska, pravna i tehnološka
Edukacija:	ključan čimbenik u usklađivanju s GDPR-om i daljem provođenju politika
IT vještine:	IT ne daje rješenje samo po sebi - presudno je postavljanje procesa i procjena rizika, a potom pomoću tehnologije (IT) implementirati definirane procese
Kazne za kršenje:	20 milijuna eura ili 4% ukupnog godišnjeg prihoda (što je veće)
Rok za prijavu kršenja:	72 sata

Ponekad je prava umjetnost postaviti prava pitanja. Stoga, prije nego vam netko ponudi gomilu nestručnih savjeta, naoružajte se pravim pitanjima, jer ovakve kazne su preozbiljne da bi se olako shvatile.

## Pitanja za moju tvrtku

1. Osobni podaci: Kojim osobnim podacima raspoložemo? Kako smo ih prikupili? S kim dijelimo te podatke?
2. Svijest zaposlenih: Koliko su zaposlenici tvrtke upoznati s povjerljivošću i ključnim zahtjevima regulative?
3. Terminologija: Znam li što znači ispitanik, posebne kategorije osobnih podataka, izrada profila, sustav pohrane?
4. Zakonska osnova: Znam li za koje podatke imam uporište u zakonu pa ih smijem obrađivati bez privole?
5. Privole: Znam li dovoljno o transparentnosti, povlačenju privola, obradi u skladu s privolama, evidencijama, vremenskim rokovima?
6. Rizici: Jesam li razvio/la plan analize rizika te upravljanja rizicima informacijske sigurnosti?
7. Incidenti: Što učiniti u slučaju incidenta? Koje su procedure? Koji su načini izvještavanja? Koga sve treba izvijestiti?
8. Prava ispitanika: Jesam li razvio/la plan implementacije prava na pristup, prava na zaborav, prava na ispravak, prava na ograničenje obrade, prava na prenosivost podataka, prava na prigovor?

Tek sad kad smo se bolje upoznali s Uredbom, možemo početi razvijati akcijski plan.

## Usklađivanje s GDPR uredbom

Problematika je složena i zahtijeva multidisciplinarni pristup. Članovi tima moraju biti eksperti za pravne aspekte, procese unutar organizacije i za IT tehnologiju. U slučaju angažiranja vanjske

konzultantske kuće treba imati na umu da je vanjskim savjetnicima nužan iskreni angažman djelatnika tvrtke koji poznaju problematiku (pravne akte, procese, IT infrastrukturu).

Usklađivanje s GDPR uredbom se sastoji iz tri koraka:

### 1. Priprema za usklađivanja s GDPR uredbom

Sve započinje procjenom sadašnjeg stanja temeljem čega se detektiraju postojeće nesukladnosti i definiraju mjere za otklanjanje istih. Rezultat procesa je Plan aktivnosti koji sadrži sva potencijalna rješenja (organizacijska, pravna i tehnološka) kojima se otklanjaju pronađene nesukladnosti (GAP-ovi). Pri procjeni rješenja evaluiraju se potrebni ljudski, financijski i vremenski resursi na strani tvrtke potrebni za implementaciju pojedinog rješenja.

### 2. Primjena mjera i usklađivanje s GDPR uredbom

Sukladno Planu aktivnosti primjenjuju se definirane mjere za usklađivanje s Uredbom: izmjene i donošenje novih pravnih akata, promjene postojećih i uvođenje novih procedura, izmjene poslovnih procesa, tehnološke mjere (usklađivanje IT sustava i upravljanja IT sustavima)

### 3. Praćenje usklađenosti i provođenje poboljšanja

Nakon što se tvrtka u potpunosti uskladila s Uredbom, posao nije gotov. Tvrtka je živi organizam, procesi se mijenjaju, usluge i proizvodi se mijenjaju, mijenja se i regulativa. Stoga je potrebno provoditi interne audite i audite treće strane (vanjskih tvrtki) na kojima se provjerava usklađenost s Uredbom i otkrivaju novonastale nesukladnosti. Izlazni rezultati takvih provjera su mjere (pravne, procesne, tehnološke) za usklađivanje koje je potrebno provesti u definiranom vremenskom roku.

# Kako vam Megatrend poslovna rješenja mogu pomoći?

Zbog kompleksnosti problematike smatramo da najefikasniji način usklađivanja s GDPR uredbom za većinu tvrtki predstavlja dodjela internih resursa uz korištenje vanjskih kompetencija specijalizirane tvrtke kao što je Megatrend poslovna rješenja.

Megatrend poslovna rješenja nudi usluge poslovnog savjetovanja pri izradi snimke stanja i preporuka za usklađivanje s Uredbom (pravne, procesne i IT aspekte), pomažemo u provođenju usklađivanja kao i u kasnijem praćenju usklađenosti.

## Što možete očekivati u Megatrendovom procesu usklađivanja s GDPR-om?

U discovery fazi potrebno je nedvosmisleno (i neporecivo) pronaći gdje se sve privatni podaci nalaze, bez obzira radilo se o strukturiranim (baze podataka) ili nestrukturiranim (mail, dokumenti, prezentacije itd.) podacima. Vrlo često korisnici nisu svjesni gdje im se podaci sve nalaze i tko sve može i na koji način pristupiti tim podacima.

Nakon otkrivanja vrste i svih lokacija podataka koji u sebi nose privatne podatke potrebno je razraditi cijeli niz procedura i procesa upravljanja tim podacima. Ispravno odabrani i implementirani IT alati će u svakom slučaju omogućiti kvalitetno upravljanje privatnim podacima.

Alati za nadzor nestrukturiranih podataka prvenstveno moraju omogućiti praćenje i kontrolu lokacije podataka te kontrolu pristupa. Alati za nadzor strukturiranih podataka imaju nešto opsežniju primjenu jer osim kontrole i zapisa pristupa moraju omogućiti i maskiranje privatnih podataka.

## Zašto odabrati Megatrend poslovna rješenja?

Tvrtka Megatrend poslovna rješenja već više od četrnaest godina radi na projektima koji rješavaju poslovne probleme korištenjem tehnologije. Kroz te projekte stečena su iskustva u brojnim industrijama i tvrtkama različitih veličina i složenosti. Projekte izvodimo u roku i budžetu u potpunoj suradnji s korisnikom, a educiranje korisnika dio je svakog našeg projekta. Stoga se tehnološki segment provedbe GDPR projekata nalazi u sferi naše dugogodišnje ekspertize.

U sagledavanju i unapređenju procesa i procedura unutar tvrtke Megatrend koristi znanja svojih zaposlenika koji su auditori za ISO norme koje obrađuju: sustave upravljanja kvalitetom (ISO 9001), sustave upravljanja informacijskom sigurnošću (ISO 27001) i sustave upravljanja uslugama u informacijskim tehnologijama (ISO 20000). Pravne aspekte rješavamo u suradnji s renomiranim odvjetničkim društvom koje pokriva cijeli teritorij Hrvatske i iskusno je u području GDPR-a.

Osigurajte da podaci vaše organizacije umjesto obveze postanu vrijednost.

Kontaktirajte nas za procjenu stanja vaše tvrtke ili ako imate dodatna pitanja vezana za GDPR Uredbu.

**megatrend**  
poslovna rješenja



Pošaljite upit na e-mail  
[poslovna.rjesenja@megatrend.com](mailto:poslovna.rjesenja@megatrend.com)