





GDPR ZA MIKRO, MALE I SREDNJE PODUZETNIKE

✓ ZAKONITOST OBRADE

Osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani te se mogu prikupljati u svrhu s kojom su ispitanici upoznati, koja je izričita, posebna i zakonita te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. U ulozi voditelja obrade odgovorni ste za zakonitu obradu tih osobnih podataka (nužno je postojanje valjanog pravnog temelja/pravne osnove za obradu osobnih podataka).

✓ OGRANIČENJE POHRANE

Osobne podatke potrebno je pohranjivati što je kraće moguće (samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju ili prema pravnim obvezama odnosnim na čuvanje/pohranu). Pri određivanju razdoblja pohrane potrebno je uzeti u obzir svrhu u koju ste kao voditelj obrade prikupili i obrađivali osobne podatke kao i sve pravne obveze čuvanja tih podataka (primjenjive na konkretnu obradu osobnih podataka). **Iznimno!!!** Osobni podaci mogu se čuvati duže vrijeme u svrhe arhiviranja u javnom interesu ili u svrhe znanstvenog ili povijesnog istraživanja, pod uvjetom da su uspostavljene odgovarajuće tehničke i organizacijske mjere.

✓ TEHNIČKA I INTEGRIRANA ZAŠTITA PODATAKA

U ulozi voditelja obrade dužni ste provoditi odgovarajuće tehničke i organizacijske mjere zaštite kojima će se osigurati da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca. Pod tehničkim mjerama zaštite uputno bi bilo za svakog individualnog korisnika korištenje korisničkih imena i generiranih lozinki za pristup računalima, postavljanje adekvatnih programa na računala koji sprječavaju neovlaštene pristupe, moguće i pseudonimizacije dok bi se papirnata dokumentacija trebala nalaziti u ormarićima, sefovima ili sobama pod ključem ili protuprovalnim sustavom. Također uputno je nabavljati i koristiti provjerene/certificirane uređaje i programe te ostalu tehničku opremu koja se koristi za obradu osobnih podataka (kako bi se pouzdano znalo sve njihove funkcionalnosti i performanse). Organizacijske mjere zaštite odnose se na dokumentirano uređenje unutar društva/organizacije/obrta na način da se internim aktima uredi područje zaštite osobnih podataka koje obrađujete, odnosno da se, primjerice, odredi kojim podacima zaposlenici imaju pristup prilikom obavljanja svojih poslova te da vodite svaku evidenciju pristupa osobnim podacima koje prikupljate.

✓ PRAVA ISPITANIKA

Osim temelnjog prava da upoznate ispitanike u koju svrhu (i na kojem pravnom temelju/osnovi) se prikupljaju njihovi osobni podaci istima morate omogućiti: pristup osobnim podacima, ispravak njihovih osobnih podataka, dopunu, pravo na brisanje/zaborav, pravo na ograničenje obrade, pravo na prenosivost osobnih podataka, pravo na podnošenje prigovora. Sve navedene informacije kao voditelj obrade trebate dostaviti (omogućiti tj. učiniti dostupnim) ispitaniku u pisanim oblicima ili drugim sredstvima, te ako je prikladno, elektroničkim putem.

✓ SLUŽBENIK ZA ZAŠTITU PODATAKA

Službenik za zaštitu podataka mora dobro razumjeti postupke koji se provode, informacijske odnosno informatičke sustave voditelja obrade te njegove potrebe u pogledu sigurnosti podataka i zaštite podataka. Službenik za zaštitu podataka trebao bi se prvenstveno brinuti za sukladnost poslovanja sa Općom uredbom o zaštiti podataka. Službenik za zaštitu podataka ima ključnu ulogu u njegovanju kulture zaštite podataka unutar organizacije i pomaže u provedbi bitnih elemenata Opće uredbe o zaštiti podataka kao što su načela obrade podataka, prava ispitanika, tehnička i integrirana zaštita podataka, evidencija aktivnosti obrade, sigurnost obrade te izvješćivanje i obavješćivanje o povredama podataka.