ŠTO SVE TREBATE NAPRAVITI KAKO BI SE USKLADILI S UREDBOM O ZAŠTITI OSOBNIH PODATAKA

Što trebate napraviti?	Primjer, savjet, opis	Tko Vam može pomoći?
PREDRADNJE		
Koje osobne podatke imate?	ime i prezime, e-mail adrese, brojevi telefona, OIB, kućne adrese	analizu podataka jedino možete napraviti Vi ili netko od Vaših zaposlenika koji je dobro upoznat s cijelim poslovanjem
Gdje držite osobne podatke?	u e-mail pretincu, u mobitelu, u tablicama na računalu, na papirima, u nekoj poslovnoj aplikaciji (računalnom programu)	
Tko ima pristup podacima?	Samo Vi ili i Vaši zaposlenici? Prosljeđujete li nekom podatke ako morate zbog zakonskih obveza (npr. prijava gosta) ili imate neku web aplikaciju (npr. fiskalna blagajna u cloudu/oblaku)	
U koje svrhe prikupljate podatke?	Pri zapošljavanju radnika, za izdavanje računa, za slanje e-mail obavijesti, za poslovnu komunikaciju s klijentima	
Čuvate li podatke i kako dugo? Koji je razlog čuvanja podataka? Možete li neke podatke obrisati ako Vam više nisu potrebni?	Svakako nemojte čuvati podatke „tek tako“, da ih imate. Za sve osobne podatke koje imate, morate imati razlog zašto ih čuvate.	
Kako ste osigurali da netko neovlašteno ne pristupi podacima?	lozinke na računalu i mobitelu, izjave o povjerljivosti zaposlenika, alarmni sustavi u prostorijama	
IZRADA DOKUMENTACIJE		
Napisati interni pravilnik	Odredite i napišite procedure i pravila kojih ćete se pridržavati u vezi sa zaštitom pojedinaca u pogledu obrade osobnih podataka. Dokument mora biti napisan uključujući elektronički format.	Aplikacija eGDPR U aplikaciji se izrađuje unaprijed napisani pravilnik u kojem su propisane sve potrebne mjere kojih se morate pridržavati, a odnose se i na voditelje i na izvršitelje obrade.
Napisati proceduru u slučaju povrede podataka	Procedura koju prema čl. 33. Uredbe propisujete za slučaj da se podaci npr. otkriju neovlaštenoj osobi, da izgubite podatke (npr. gubitak mobitela ili krađa laptopa), da se slučajno unište (npr. poplava, kvar računala).	Aplikacija eGDPR Izrađuje se dokument u kojem je opisana obvezna procedura i procedura za najčešće slučajeve povrede podataka.

Popisati tehničke i organizacijske sigurnosne mjere koje primjenjujete	Potrebno je opisati i propisati sve sigurnosne mjere koje poduzimate ili ćete poduzimati kako ne bi došlo do povrede podataka.	Aplikacija eGDPR Izrađuje se dokument u kojem je opisana praksa koju trebate provoditi barem kako biste zaštitili podatke na najosnovniji način.
Potpisati s radnicima i svima koji imaju pristup podacima Ugovor o povjerljivosti	Kao primjenu organizacijskih sigurnosnih mjera svakako je dobro potpisati Ugovore o povjerljivosti sa zaposlenicima kako biste ih osvijestili da je kršenje Internog pravilnika ozbiljno kršenje radnih obveza.	Aplikacija eGDPR Izrađuje se Ugovor o povjerljivosti za svakog zaposlenika.
Propisati proceduru procjene učinka poduzetih mjera	Nije obavezno u svim situacijama, ali svakako je dobro procijeniti učinak mjera koje ste početno postavili. U dokumentu je opisana procedura procjene.	Aplikacija eGDPR Izrađuje se dokument s točnim uputama kako provesti procjenu učinka i kako će se i u kojoj mjeri procjena u budućnosti izrađivati.
Imenovati službenika za zaštitu podataka (nije obvezno za sve)	Ako ste prema članku 37. Uredbe obvezni imati službenika za zaštitu podataka.	Aplikacija eGDPR Kroz aplikaciju se upisuje službenik i izrađuje se odluka.
Voditi evidenciju aktivnosti obrade	Popisati sve obrade podataka koje radite kao voditelj (npr. osobni podaci vaših zaposlenika) ili izvršitelj, napisati svrhe, zakonske osnove, kategorije podataka, rokove čuvanja podataka, sigurnosne mjere...	Aplikacija eGDPR U aplikaciju upisujete sve zakonski propisane podatke o svakoj obradi i na temelju upisanog se automatski izrađuju evidencije.
Izraditi Izjavu o privatnosti za svaku obradu kojom ćete upoznati ispitanika sa svrhom obrade, prosljeđivanjem podataka, njegovim pravima	Kod prikupljanja podataka, a najkasnije pri prvom kontaktu, sve ispitanike (pojedince na koga se osobni podaci odnose) morate upoznati s obradom podataka (što prikupljate, zašto, koliko dugo, kako se može uložiti zahtjev za ispunjavanje prava).	Aplikacija eGDPR Za svaku kategoriju obrade koju ste odredili kao voditelj obrade se automatski izrađuje dokument Izjave o privatnosti sa svim zakonski propisanim elementima.
Provjeriti lokaciju izvršitelja, sigurnosne mjere koje izvršitelj primjenjuje i s kime dalje dijeli podatke	Ako nekome na bilo koji način prosljeđujete podatke (npr. web poslovna aplikacija) ili netko vanjski ima pristup podacima (npr. serviser računala ili netko tko se spaja na Vaše računalo), to znači da imate izvršitelja i da morate provjeriti njegovu pouzdanost kako biste nastavili suradnju.	Aplikacija eGDPR Izrađuje se upitnik koji sadrži sva relevantna pitanja i koji šaljete svojim izvršiteljima kako biste se uvjerili da su pouzdani i da s njima možete nastaviti suradnju.
Potpisati ugovor s izvršiteljima obrade podataka	Sa svim izvršiteljima morate potpisati ugovor u kojem	Aplikacija eGDPR

	definirate o kakvoj se obradi radi, koje su obveze izvršitelja, koje su mu sigurnosne mjere...	Kroz aplikaciju se automatski izrađuje ugovor između Vas i Vašeg izvršitelja.
Dati pisani nalog izvršitelju koje podatke obrađuje i na koji način	Ako imate nekoga tko ima pristup Vašim podacima, morate mu pisanim nalogom dati uputu o obradi podataka i jedino po toj uputi izvršitelj smije djelovati.	Aplikacija eGDPR Kroz aplikaciju se automatski kao dodataka ugovoru izrađuje lista svih kategorija obrade u kojima sudjeluje izvršitelj.
Provjeriti pouzdanost podizvršitelja ako ste Vi izvršitelj (Vi u nečije ime obrađujete podatke)	Ako kao izvršitelj koristite nečije tuđe usluge za obradu podataka koje Vam je proslijedio voditelj morate provjeriti pouzdanost i lokaciju tih podizvršitelja. Vi ste odgovorni za svoje podizvršitelje.	Aplikacija eGDPR Kroz aplikaciju se automatski izrađuje upitnik za podizvršitelje koji se kao pdf forma za ispunjavanje šalje podizvršiteljima.
Voditi evidenciju povreda osobnih podataka	Popisati sve povrede podataka koje su se dogodile u poslovanju bez obzira koliko ozbiljne bile i jeste li ih sve prijavili AZOP-u.	Aplikacija eGDPR - u pripremi U evidenciju će se upisivati povrede i bit će špranca prema kojoj ste donesli odluku o neprijavljivanju povrede i špranca prijave AZOP-u.
AKTIVNO PROVOĐENJE MJERA UREDBE I MJERA PROPISANIH VAŠIH PRAVILNIKOM		
Pridržavati se svih propisanih organizacijskih i sigurnosnih mjera	Osvijestite u Vašem poslovnom okruženju da je bitno da se ne dogode propusti u zaštiti osobnih podataka. Mjere nije dovoljno propisati.	Vi i Vaš kolektiv se aktivno morate pridržavati mjera i sprječavati kako Vam se zbog nekog malog propusta ne bi dogodila velika šteta.
Pridržavati se procedura i pravila propisanih Vašim internim pravilnikom	Osvijestite u Vašem poslovnom okruženju koji je ispravan način prikupljanja i obrade podataka.	
Privole	Ako Vam se obrada temelji na privolama, morate ih na ispravan način prikupiti i na zahtjev ispitanika povući. To se odnosi i na postojeće podatke ako su prikupljeni na temelju starih, ali neodgovarajućih privola.	Aplikacija GDPR HQ U aplikaciji se automatski izrađuju privole za svakog ispitanika, prikuplja se datum i vrijeme dobivanja privole, na zahtjev se ukidaju privole.
Legitimni interes	Ako Vam se obrada temelji na legitimnom interesu (npr. direktni marketing), za svakog ispitanika morate znati je li uložio prigovor.	Aplikacija GDPR HQ Aplikacija se preko API-ja povezuje s Vašim vanjskim poslovnim sustavima i na jednom mjestu prati sve aktivnosti koje se događaju u svim Vašim aplikacijama.
Izjave o kolačićima i vezane privole	Ako imate web stranicu i kolačiće (cookies) koji su uglavnom sastavni dio svake	Vaš web dizajner treba implementirati privolu za kolačiće, a kroz API ih može

	web stranice, potrebno je pratiti privole koje Vam je posjetitelj dao.	povezati s aplikacijom GDPR HQ
Upoznavanje ispitanika sa svrhom obrade, proslijeđivanjem podataka, njegovim pravima	Kod prikupljanja podataka, a najkasnije pri prvom kontaktu, sve ispitanike (pojedince na koga se osobni podaci odnose) morate upoznati s obradom podataka (što prikupljate, zašto, koliko dugo, kako se može uložiti zahtjev za ispunjavanje prava).	Ako imate npr. na web stranici neku formu za upis podataka, Vaš web dizajner bi za svaku obradu trebao staviti link na Izjavu o privatnosti (koju možete izraditi preko aplikacije eGDPR). To se odnosi i na čitavi web stranicu (obično se nalazi u podnožju svake stranice).
Djelovanje po zahtjevu ispitanika i upravljanje zahtjevima	Ispitanici (pojedinci čiji se podaci obrađuju) imaju prema novoj Uredbi čitav niz svojih prava (npr. pravo na brisanje, ispravak, ograničenje obrade, pristup). Zakonski morate odgovoriti na svaki zahtjev ispitanika bez nepotrebnog odlaganja, a najviše unutar 30 dana.	Aplikacija GDPR HQ Unutar aplikacije se nalazi forma i unaprijed definiran gumb koji možete staviti na svoju stranicu. Preko gumba se daje zahtjev, a unutar aplikacije se nalaze predefinirani e-mailovi kojima obavještavate ispitanika kad zaprimite zahtjev i kad postupite po zahtjevu. Upravljanje zahtjevima je moguće i bez gumba za predaju zahtjeva.
Obavještavanje AZOP-a i ispitanika o povredi podataka	Ako Vam se dogodi neovlašteni pristup, slučajno brisanje ili gubitak osobnih podataka, o tome ste u slučaju velikog rizika za prava ispitanika obvezni obavijestiti AZOP i u nekim slučajevima samog ispitanika.	Kroz aplikaciju eGDPR će uskoro biti moguće popuniti prijavu AZOP-u (kad AZOP deinira formu i postupak) i upisati povredu u evidenciju.
Konstantna edukacija i preispitivanje poduzetih mjera	Upoznajte cijeli svoj tim s mjerama koje moraju poduzimati, pratite provođenje tih mjera, educirajte se dalje, provjeravajte jesu li svi zaposlenici dobro shvatili mjere (zaštita osobnih podataka je odgovornost tvrtke i krivnja/kazna se svaljuje na tvrtku i direktora)	Educirajte se na internetu ili sudjelovanjem na seminarima, ako imate visokorizične obrade uzimte savjetnika (Raverus), kroz eGDPR provjeravajte dio o edukaciji, pitajte AZOP ili pouzdanog odvjetnika za tumačenja i savjete...

Ova lista ne pokriva sve situacije Vašeg poslovnog okruženja, već su nabrojane najčešće minimalne mjere koje morate poduzeti. Ako se bavite direktnim marketingom, dijelite podatke s trećim zemljama, obrađujete podatke posebnih kategorija i slične posebne situacije, predlažemo da se posavjetujete s AZOP-om ili nekim stručnjakom.