KRATKI VODIČ

10 ključnih koraka za usklađivanje s GDPR-om

Sufinancirano kroz Program o pravima, jednakosti i građanstvu Europske unije

Kampanja podizanja svijesti o zaštiti osobnih podataka


GDPR

OPĆI POJMOVI

VODITELJ OBRADE

Poslovni subjekt koji određuje svrhe i sredstva obrade osobnih podataka

(primjer 1: marketinška agencija, a ne odjel marketinške agencije koji planira obrađivati podatke u svrhe istraživanja tržišta, primjer 2: IT poduzeće, a ne knjigovotkinja ili administrativna tajnica, primjer 3: voditelj obrade može biti i fizička osoba npr. iznajmljivač apartmana)

IZVRŠITELJ OBRADE

Poslovni subjekt koji obrađuje osobne podatke u ime voditelja obrade i prema njegovim uputama te određuje sredstva obrade

(npr. društvo XY specijalizirano za pohranu podataka u oblaku koje upravlja podacima o kupcima voditelja obrade, zaštitarska tvrtka koja održava sustav videonadzora za druge tvrtke, knjigovodstveni servis kad pruža svoje usluge drugim tvrtkama itd.)

ISPITANIK

Pojedinac čiji se identitet može utvrditi izravno ili neizravno

(npr. kupac, klijent, pretplatnik na newsletter, posjetitelj web stranice, zaposlenik)

OSOBNI PODATAK

Svaki podatak koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi, a pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno

(npr. ime/prezime, spol, podaci o zdravlju, vjerskom uvjerenju, OIB, adresa, otisak prsta, podatak o lokaciji, fotografija, registarska oznaka automobila i mnogi drugi)

OBRADA

Svaki postupak koji se obavlja na osobnim podacima

(npr. prikupljanje, bilježenje, pohrana, izmjena, obavljanje uvida, uporaba, otkrivanje prijenosom, brisanje ...)

ŠTO JE OPĆA UREDBA O ZAŠTITI PODATAKA I ZAŠTO JE VAŽNA?

OPĆA UREDBA O ZAŠTITI PODATAKA (poznatija kao **GDPR**- General Data Protection Regulation) je obvezujući zakonodavni akt koji se izravno i u cijelosti primjenjuje u Republici Hrvatskoj i u ostalim državama članicama Europske unije, odnosno Europskog gospodarskog prostora od 25. svibnja 2018. godine. Područje zaštite osobnih podataka u Republici Hrvatskoj dodatno je regulirano i Zakonom o provedbi Opće uredbe o zaštiti podataka kojim se osigurava provedba GDPR-a.

CILJ: zaštititi osobne podatke fizičkih osoba, pružiti kontrolu građanima nad njihovim osobnim podacima te stvoriti visoku i ujednačenu razinu zaštite osobnih podataka u Europskoj uniji.
Uz navedeno, cilj je i olakšati poduzećima poslovanje na jedinstvenom digitalnom tržištu te olakšati prekogranični protok osobnih podataka i korištenje usluga informacijskog društva.

Usklađivanje s GDPR-om nije još jedno administrativno opterećenje i nepotreban trošak koji će samo otežati vaše poslovanje. Naprotiv, GDPR je prilika da bolje iskoristite osobne podatke koje posjedujete, povećate operativnu učinkovitost i steknete prednost pred konkurencijom na tržištu koja ne posvećuje potrebnu pažnju zaštiti osobnih podataka.
U današnje digitalno doba pojedincima je sve važnije da su podaci koje povjeravaju različitim društvima adekvatno zaštićeni te će biti skloniji koristiti proizvode/usluge onih organizacija koje vode odgovarajuću brigu o njihovim osobnim podacima i privatnosti.

Sve organizacije u Republici Hrvatskoj (mikro, mala, srednja, velika poduzeća, obrti, društva, tvrtke, tijela javne vlasti, državna tijela, udruge, nevladine organizacije itd.) koje obrađuju osobne podatke građana dužne su poštovati odredbe GDPR-a i Zakona o provedbi Opće uredbe o zaštiti podataka.

GDPR se primjenjuje na sve poslovne subjekte (odnosno voditelje i izvršitelje obrade) koji obrađuju osobne podatke građana Europske unije, neovisno o tome obavlja li se obrada u EU ili ne. Također, GDPR se primjenjuje na obradu osobnih podataka u Europskoj uniji koju obavlja voditelj ili izvršitelj obrade bez poslovnog nastana u EU, ako su te aktivnosti obrade povezane s nuđenjem roba ili usluga pojedinicima u EU ili praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar EU.

Možda smatrate da ne obrađujete osobne podatke, ali već se i sama pohrana osobnih podataka zaposlenika/klijenata/korisnika u datoteku na računalu ili u papirnatom obliku smatra obradom osobnih podataka.

Opća uredba o zaštiti podataka ne propisuje obvezne obrasce, interne politike i procedure potrebne za usklađivanje te se proces usklađivanja razlikuje od poduzeća do poduzeća, organizacije do organizacije, ovisno o poslovnim procesima i postupcima obrade koje organizacija provodi na osobnim podacima. Ipak, postoje ključni koraci koje su dužni poduzeti SVI voditelji obrade na svom putu prema usklađivanju s GDPR-om:

10 KLJUČNIH KORAKA ZA USKLAĐIVANJE S GDPR-OM

1 NAPRAVITI ANALIZU OSOBNIH PODATAKA KOJE OBRAĐUJETE

Prvi korak koji biste trebali učiniti je utvrditi čije osobne podatke obrađujete (npr. zaposlenika, klijenata, korisnika usluga), zatim koje osobne podatke prikupljate (npr. ime i prezime, OIB, broj osobne iskaznice, adresa, e-mail, fotografija, videosnimke, IP adresa, podaci o lokaciji, podaci o plaći itd.) i gdje se ti osobni podaci nalaze (u papirnatom i digitalnom obliku). Osobit oprez potreban je ako obrađujete posebne kategorije osobnih podataka (npr. osobni podaci koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, zdravlje ili spolni život). Takvi podaci mogu se obrađivati isključivo ako postoji pravni temelj za obradu iz članka 6. GDPR-a i jedna od taksativno navedenih iznimaka iz članka 9. stavka 2. GDPR-a.

OSNOVNA PITANJA NA KOJA BISTE TREBALI ODGOVORITI SU:

1) U koju svrhu prikupljate osobne podatke?
2) Jesu li vam ti podaci neophodni za poslovanje?
3) Koji je pravni temelj za obradu osobnih podataka?
4) Gdje se osobni podaci nalaze?
5) Tko ima pristup osobnim podacima?
6) Koliko se dugo osobni podaci čuvaju?
7) Prosljeđujete li osobne podatke trećim stranama?
8) Koji je izvor osobnih podataka (npr. pojedinac, treće strane, javno dostupni izvori)?
9) Jesu li podaci adekvatno zaštićeni?
10) Što se događa s osobnim podacima nakon isteka svrhe za koju su prikupljeni?

Primjer:

Frizerski salon pruža frizerske usluge i prodaje frizerske proizvode putem online trgovine. Prilikom naručivanja za frizerske usluge, djelatnik frizerskog salona prikuplja ime, prezime i broj telefona klijenta te zapisuje navedene podatke u knjigu narudžbi. Isto tako, naručivanje za frizerske usluge moguće je i putem online obrasca dostupnog na društvenim mrežama i web stranici salona, a pritom se prikupljaju i e-mail adrese klijenata. Frizerski salon nudi klijentima i mogućnost učlanjenja u program vjernosti. U tom slučaju, uz sve prethodno navedene osobne podatke, frizerski salon prikuplja i adresu i datum i godinu rođenja klijenta, bilježi svaki dolazak klijenta u salon, proizvode i usluge koje klijent koristi.

Frizerski salon zapošljava 25 radnika, prikuplja i obrađuje njihove osobne podatke sukladno zakonskim propisima. Frizerski salon koristi usluge vanjskog knjigovodstvenog servisa koji obračunava plaće zaposlenika i obavlja druge računovodstvene poslove. Također, frizerski salon koristi usluge IT tvrtke za održavanje i hosting internetske stranice te za održavanje online trgovine. Frizerski salon je ugovorio uslugu instalacije i održavanja videonadzornog sustava u svrhu zaštite ljudi i imovine. Frizerski salon u svom poslovanju koristi društvene mreže te na njima organizira nagradne igre, objavljuje osobne podatke dobitnika i objavljuje fotografije svojih klijenata.

2 PRONAĆI ODGOVARAJUĆU PRAVNU OSNOVU ZA OBRADU OSOBNIH PODATAKA

Jedno od prvih pitanja na koje bi trebale odgovoriti sve organizacije koje obrađuju osobne podatke (voditelji obrade) prije početka obrade je: "Koji je moj razlog ili opravdanje za obradu osobnih podataka?". To je od ključne važnosti jer obrada može biti zakonita samo ako ste prethodno utvrdili razlog/opravdanje za obradu osobnih podataka te identificirali i dokumentirali pravni temelj.

PREMA ČLANKU 6. GDPR-a OBRADA JE ZAKONITA SAMO AKO I U ONOJ MJERI U KOJOJ JE ISPUNJENO NAJMANJE JEDNO OD SLJEDEĆEGA (pravne osnove za obradu osobnih podataka):

ispitanik je dao **privolu** za obradu svojih osobnih podataka
(npr. privola za obradu osobnih podataka putem kolačića, privola za objavu fotografije na web stranici poduzeća ili društvenim mrežama)

obrada je **nužna za izvršavanje ugovora** u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora (npr. kupoprodaja putem webshop-a, obrada podataka osiguranika radi izvršenja ugovora o osiguranju)

obrada je **nužna radi poštovanja pravnih obveza** voditelja obrade
(npr. slanje podataka o radnicima HZZO-u ili HZMO-u, pohrana osobnih podataka umirovljenih radnika, upis gostiju u sustav E-visitor)

obrada je nužna kako bi se **zaštitili životno važni interesi ispitanika ili druge fizičke osobe** (npr. davanje osobnih podataka unesrećene osobe Hrvatskoj gorskoj službi spašavanja)

obrada je **nužna za potrebe legitimnih interesa voditelja obrade ili treće strane**, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka (npr. slanje promidžbene e-pošte prijašnjim kupcima)

obrada je nužna za izvršavanje **zadaće od javnog interesa ili pri izvršavanju službene ovlasti** voditelja obrade

PRIVOLA

Važno je naglasiti da je **privola jedna od 6 mogućih pravnih osnova za obradu osobnih podataka** i ako postoji neka druga pravna osnova na koju se oslanjate, nije potrebno tražiti privolu (npr. kad prijavljujete novog zaposlenika na Hrvatski zavod za mirovinsko osiguranje, pravna osnova za obradu osobnih podataka zaposlenika je zakonska obveza i nije potrebna privola zaposlenika; kad prijavljujete gosta u sustav E-visitor, to je zakonska obveza pružatelja usluge smještaja i nije potrebna privola gosta; kad obrađujete osobne podatke putem videonadzornog sustava i takvu obradu temeljite na legitimnom interesu, nije potrebna privola posjetitelja/klijenata/zaposlenika itd.)

Ne postoji hijerarhija ili preferirana opcija unutar ovog popisa, odnosno svaka obrada osobnih podataka treba se temeljiti na pravnoj osnovi koja je najprikladnija u određenim okolnostima. Važno je upamtiti da osim što nije jedina pravna osnova, **privola vrlo često nije niti odgovarajuća pravna osnova za obradu osobnih podataka**. Prema GDPR-u, da bi bila valjana, privola mora biti dana jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak pojedinca na obradu njegovih/njezinih osobnih podataka, a osoba uvijek mora imati mogućnost povući privolu.

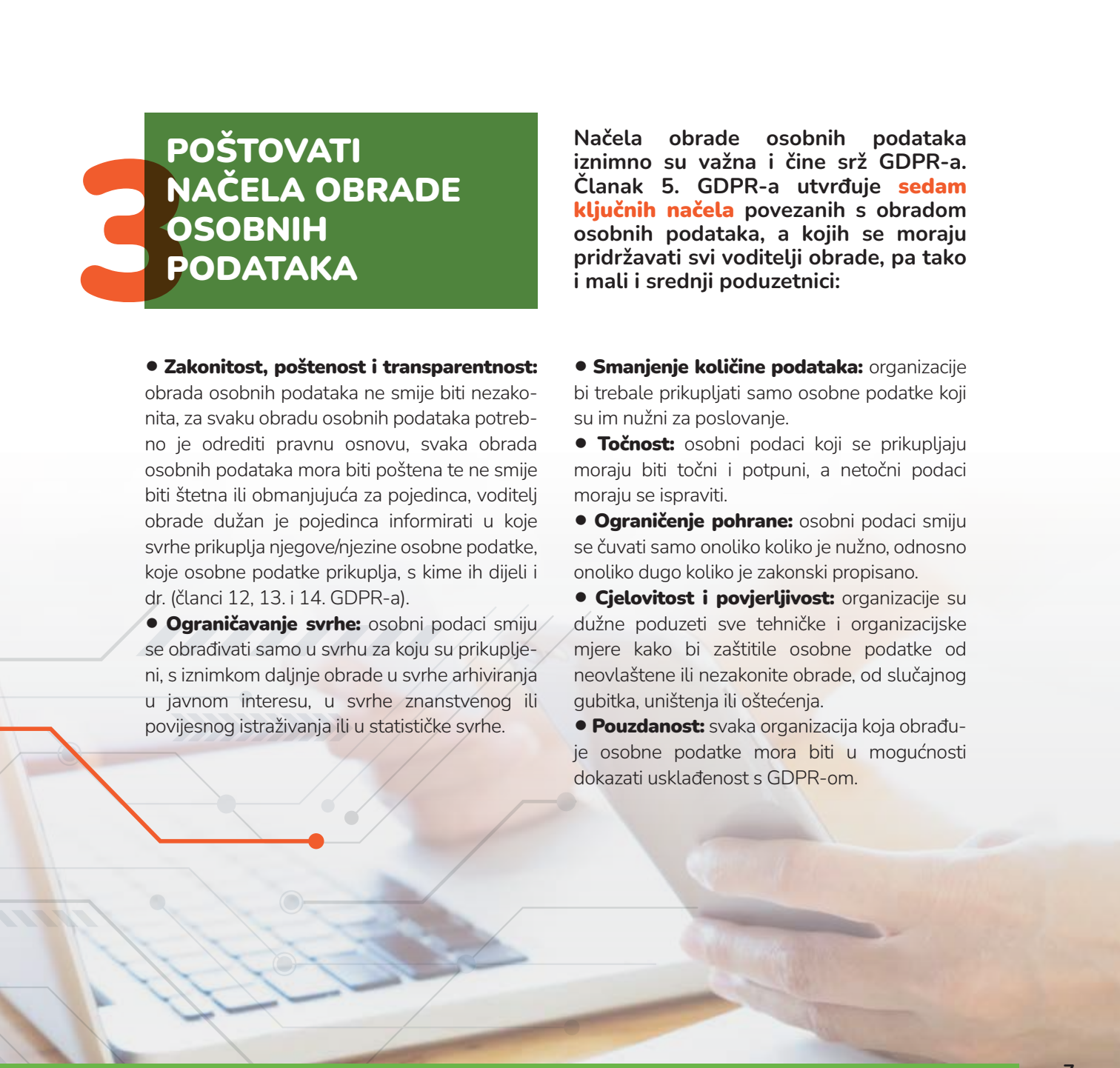
Nakon što je osoba povukla privolu, organizacija mora prestati obrađivati njegove/njezine osobne podatke. U tom smislu privola nije odgovarajuća pravna osnova npr. za obradu osobnih podataka zaposlenika u svrhu prijave na Hrvatski zavod za mirovinsko osiguranje, obrade osobnih podataka kandidata koji su se prijavili na natječaj za posao, prijavljivanje gosta hotela u sustav E-visitor, obradu osobnih podataka pacijenata u svrhu pružanja zdravstvenih usluga, obrade osobnih podataka koji su nužni za izvršenje ugovora itd.

VAŽNO! **Ključno je da ste dobro upoznati s tzv. strukovnim propisima koji uređuju djelatnost kojom se bavite u kojima se vrlo često nalaze odredbe koje reguliraju obradu osobnih podataka.** Primjerice, ako se bavite zaštitarskom djelatnošću svakako morate biti dobro upoznati s Zakonom o privatnoj zaštiti, Zakonom o zaštiti novčarskih institucija i Zakonom o zaštiti na radu. Ukoliko se bavite marketinškom djelatnošću vrlo je važno da ste upoznati s Zakonom o elektroničkim komunikacijama, Zakonom o elektroničkoj trgovini, Zakonom o obveznim odnosima, Zakonom o zaštiti potrošača i Zakonom o nedopuštenom oglašavanju.

3 POŠTOVATI NAČELA OBRADE OSOBNIH PODATAKA

Načela obrade osobnih podataka iznimno su važna i čine srž GDPR-a. Članak 5. GDPR-a utvrđuje sedam ključnih načela povezanih s obradom osobnih podataka, a kojih se moraju pridržavati svi voditelji obrade, pa tako i mali i srednji poduzetnici:

- **Zakonitost, poštenost i transparentnost:** obrada osobnih podataka ne smije biti nezakonita, za svaku obradu osobnih podataka potrebno je odrediti pravnu osnovu, svaka obrada osobnih podataka mora biti poštena te ne smije biti štetna ili obmanjujuća za pojedinca, voditelj obrade dužan je pojedinca informirati u koje svrhe prikuplja njegove/njezine osobne podatke, koje osobne podatke prikuplja, s kime ih dijeli i dr. (članci 12, 13. i 14. GDPR-a).
- **Ograničavanje svrhe:** osobni podaci smiju se obrađivati samo u svrhu za koju su prikupljeni, s iznimkom daljnje obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.
- **Smanjenje količine podataka:** organizacije bi trebale prikupljati samo osobne podatke koji su im nužni za poslovanje.
- **Točnost:** osobni podaci koji se prikupljaju moraju biti točni i potpuni, a netočni podaci moraju se ispraviti.
- **Ograničenje pohrane:** osobni podaci smiju se čuvati samo onoliko koliko je nužno, odnosno onoliko dugo koliko je zakonski propisano.
- **Cjelovitost i povjerljivost:** organizacije su dužne poduzeti sve tehničke i organizacijske mjere kako bi zaštitile osobne podatke od neovlaštene ili nezakonite obrade, od slučajnog gubitka, uništenja ili oštećenja.
- **Pouzdanost:** svaka organizacija koja obrađuje osobne podatke mora biti u mogućnosti dokazati usklađenost s GDPR-om.



4 PODUZETI ODGOVARAJUĆE TEHNIČKE I ORGANIZACIJSKE MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Jedna od glavnih obveza prema GDPR-u je osigurati odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštenih ili nezakonitih obrada (uključujući krađu, uništavanje, oštećenje i otkrivanje) osobnih podataka. Kako biste zaštitili osobe podatke svojih klijenata/korisnika usluga/zaposlenika (ukratko pojedinaca čijim osobnim podacima raspolažete), **dužni ste provoditi odgovarajuće tehničke i organizacijske mjere.** Na ovaj način svest ćete mogućnost nezakonite obrade osobnih podataka i povreda osobnih podataka na minimum.

Sve organizacije (mikro, mala, srednja, velika poduzeća, tijela javne vlasti i svi ostali voditelji i izvršitelji obrade) trebaju biti svjesne važnosti ove obveze, a posebice organizacije koje prikupljaju i pohranjuju posebne kategorije osobnih podataka. Jedno od prvih pitanja koje će postaviti nadzorno tijelo za zaštitu podataka (Agencija za zaštitu osobnih podataka – AZOP) u slučaju povrede osobnih podataka i prilikom nadzornih postupanja, upravo je **koje su mjere poduzete kako bi se osigurala sigurnost osobnih podataka.**

GDPR ne definira koje konkretno tehničke i organizacijske mjere je potrebno poduzeti, a iste ovise o poslovnim procesima, postupcima obrade koje organizacija provodi, kategoriji osobnih podataka koje prikuplja i rizičnosti obrade. Što su osobni podaci osjetljiviji, to im treba osigurati veću razinu zaštite. **Primjerice, laboratorij koji obrađuje posebno osjetljive medicinske podatke implementirat će strože mjere koje će osigurati veću razinu zaštite osobnih podataka od frizerskog salona koji obrađuje osobne podatke zaposlenika i prikuplja imena, prezimena, broj telefona i e-mail adrese klijenata.**

Neke od **tehničkih mjera** za zaštitu osobnih podataka su pseudonimizacija, enkripcija, korištenje korisničkih imena i snažnih lozinki za pristup računalima i računalnoj opremi, postavljanje adekvatnih programa na računala koji sprječavaju neovlaštene pristupe, redovito izrađivanje sigurnosnih kopija podataka itd. Papirnata dokumentacija koja sadrži osobne podatke trebala bi se nalaziti u zaključanim ormarićima i prostorijama, sefovima ili bi trebala biti zaštićena protuprovalnim sustavom. Također, trebali biste koristiti provjerene/certificirane uređaje, programe i tehničku opremu te redovito nadograđivati operativni sustav računala, mobilnih uređaja i računalnih programa.

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, vodi evidencija pristupa osobnim podacima (tzv. logovi) i odredi kojim osobnim podacima zaposlenici imaju pristup prilikom obavljanja svojih poslova.

Neki od takvih internih akata su:

- **Pravilnik o informacijskoj sigurnosti** kojim se, između ostalog, propisuju tehničke mjere zaštite koje se primjenjuju za zaštitu podataka od neovlaštenog pristupa u poslovnom subjektu.

- **Pravilnici kojima se uređuje obrada osobnih podataka:** propisuju tko obrađuje osobne podatke, u koju svrhu, koji je pravni temelj obrade, koji je opseg osobnih podataka u obradi, tko ima pravo pristupa i obrade osobnih podataka, koliko dugo se podaci čuvaju, koje su tehničke mjere zaštite provedene za taj sustav pohrane (bazu podataka) itd.

- **U ugovornim klauzulama unutar ugovora o radu** mogu biti definirani sustavi pohrane koje će zaposlenik obrađivati i koja ovlaštenja će imati za obradu tih sustava pohrane (baza podataka).

- **Izjavom o povjerljivosti** zaposlenik poslovnog subjekta ili vanjski suradnik daje pisanu izjavu da će osobne podatke obrađivati u skladu sa zakonskim odredbama o zaštiti osobnih podataka kao i da će nad istima provoditi odgovarajuće mjere zaštite te da ih neće zlorabiti i davati neovlaštenim trećim stranama.

- **Ugovor o obradi osobnih podataka između voditelja i izvršitelja obrade**

** obrasce i vodiče za usklađivanje s GDPR-om možete pronaći na web stranici projekta ARC i AZOP-a*

VAŽNO:

Ljudski faktor je najbitniji u postupku **provođenja informacijske sigurnosti i zaštite podataka**. Ako svi zaposlenici nemaju razvijenu svijest o važnosti informacijske sigurnosti i o zaštiti podataka, poduzete tehničke i organizacijske mjere neće biti od prevelike koristi. Naime, do najvećeg broja povreda osobnih podataka dolazi iz ljudske nepažnje, nemara ili neznanja.

Upravo iz tog razloga važno je sve zaposlenike educirati o računalnim virusima i prijevarama (ransomware, phishing, socijalni inženjering itd.), potencijalnim rizicima od krađe, zlouporabe i gubitka osobnih podataka, zatim pomoću kojih zaštitnih mjera se osobni podaci mogu zaštititi, kao i o posljedicama krađe, zlouporabe i gubitka osobnih podataka.

** više o informacijskog sigurnosti i tehničkim i organizacijskim mjerama možete pronaći u vodičima na web stranici projekta ARC: https://arc-rec-project.eu/vodici/*

5 POŠTOVATI PRAVA ISPITANIKA (OSOBA ČIJE OSOBNE PODATKE OBRAĐUJETE) I OMOGUĆITI IM DA OSTVARE SVOJA PRAVA

Svaka organizacija koja obrađuje osobne podatke pojedinaca, dužna je poštovati njihova prava zagarantirana GDPR-om i Zakonom o provedbi Opće uredbe o zaštiti podataka, informirati pojedince o njihovim pravima (npr. putem politike privatnosti) te im omogućiti da ostvaruju svoja prava.

Ukoliko u svom poslovanju koristite web stranicu, preporuka Agencije je da na web stranici objavite obrazac zahtjeva putem kojeg ispitanik može ostvariti svoja prava.

Na zahtjeve pojedinaca za ostvarivanje njihovih prava iz GDPR-a dužni ste odgovoriti bez nepotrebnog odgađanja, a najkasnije u roku od mjesec dana od primitka zahtjeva. Rok za odgovor je moguće produžiti za još dva mjeseca ako je zahtjev složen, no u tom slučaju morate obavijestiti pojedinca u roku od mjesec dana o razlozima zbog kojeg i koliko će taj rok biti produžen.

** obrazac namijenjen pojedincima u svrhu ostvarivanja njihovih prava vezano za zaštitu osobnih podataka možete pronaći na web stranici projekta ARC: https://arc-rec-project.eu/obrasci/*

6 OSIGURATI MINIMUM DOKUMENTACIJE POTREBNE ZA DOKAZIVANJE USKLAĐENOSTI S GDPR-om

Dokumentacija koju će ovlašteni službenici Agencije zatražiti prilikom provedbe nadzornih aktivnosti:

- Dokument iz kojeg je vidljivo da je fizička osoba ovlaštena od strane društva za komunikaciju s nadzornim tijelom (npr. punomoć za zastupanje ili punomoć odvjetnika, Odluka o imenovanju službenika za zaštitu podataka)
- Interne akte kojima je regulirana zaštita osobnih podataka (npr. Pravilnik o zaštiti osobnih podataka, Politika privatnosti, Obavijest/informacije koje se pružaju ispitanicima o njihovim pravima)
- Akte iz kojih su vidljive ovlasti zaposlenika ili vanjskih suradnika (primjerice: Ugovor u radu ili drugi akt koji propisuje razine ovlasti kao npr. Pravilnik o ovlaštenjima)
- Izjave o povjerljivosti
- Evidencije aktivnosti obrade
- Ugovor o obradi osobni podataka između voditelja i izvršitelja obrade
- Dokumentaciju odnosnu na mjere zaštite (organizacijske i tehničke)
- Dokumentaciju odnosnu na određeni slučaj i pojedince, na koji način su prikupljeni određeni osobni podaci, temeljem koje pravne osnove i u koju točno svrhu (npr. obrazac privole ako se obrada temelji na privoli, test legitimnog interesa ako se obrada temelji na legitimnom interesu, dokumentiranu procjenu učinka na zaštitu osobnih podataka ako je provedena procjena učinka, dokument iz kojeg je vidljiva zakonitost obrade između dvije ili više strana, dokumentacija odnosna na videonadzorni sustav te uvid u videozapise, logove, baze podataka i dr.)

** obrasce i vodiče za usklađivanje s GDPR-om možete pronaći na web stranici projekta ARC i AZOP-a*

7 INFORMIRATI POJEDINCE O OBRADI NJIHOVIH OSOBNIH PODATAKA

Svaka organizacija koja obrađuje osobne podatke dužna je pojedince informirati o vrstama osobnih podataka koje prikuplja i njihovim pravima iz GDPR-a, u koju svrhu i po kojoj pravnoj osnovi obrađuje osobne podatke, na koji način i tko koristi osobne podatke te koje mjere zaštite osobnih podataka provodi i dr. (članci 12., 13. i 14. GDPR-a).

Svaki voditelj obrade je pritom dužan koristiti jednostavan i lako razumljiv jezik te pružiti osobama navedene informacije u sažetom obliku.

** obrazac politike privatnosti možete pronaći na web stranici projekta ARC: https://arc-rec-project.eu/obrasci/*

U tu svrhu preporučamo da izradite politiku privatnosti i objavite je na službenoj web stranici svoje organizacije. U slučaju da u svom poslovanju ne koristite web stranicu, politiku privatnosti dužni ste učiniti javno dostupnom na drugi način, npr. na vidljivom mjestu u svojim poslovnim prostorijama.

Primjer: Hostel u svom poslovanju ne koristi web stranicu. Politika privatnosti gostima je jasno vidljiva na recepciji te recepcionar na istu gostima dodatno ukazuje, a primjerci politike privatnosti nalaze se i u sobama hostela.

8 VODITI EVIDENCIJE AKTIVNOSTI OBRADE (AKO JE PRIMJENJIVO)

Evidencija aktivnosti obrade je obrazac koji može služiti kao dokaz da je obrada osobnih podataka zakonita. Ista mora sadržavati informacije **iz članka 30. GDPR-a**, a podaci sadržani u evidenciji obrade moraju biti na odgovarajući način zaštićeni.

Neovisno o broju zaposlenika, bilo da ste voditelj obrade ili izvršitelj obrade, DUŽNI ste voditi evidenciju obrade ukoliko je ispunjen jedan od sljedećih uvjeta:

- ako će obrada vjerojatno prouzročiti visoki rizik za prava i slobode ispitanika (npr. uvođenje novih tehnologija kao što su biometrijski čitači, prepoznavanje lica, IT servisa koji obrađuju osobne podatke),
- ako obrada nije povremena, odnosno ako je obrada stalna (npr. obrada osobnih podataka zaposlenika u svrhu isplate plaća),
- ako obrada uključuje posebne kategorije podataka (npr. zdravstveni podaci, biometrijski podaci, genetski podaci),
- ako obrada uključuje osobne podatke u vezi s kaznenim osudama i kažnjivim djelima

Evidenciju **NISTE DUŽNI** voditi ako zapošljavate manje od 250 zaposlenika i ako nije ispunjen niti jedan od prethodno navedenih uvjeta.

** obrasce za vođenje evidencije aktivnosti obrade namijenjene voditeljima i izvršiteljima obrade možete pronaći na https://arc-rec-project.eu/obrasci/*

PREPORUKA AGENCIJE!

Preporučamo da vodite evidenciju aktivnosti obrade čak i ako istu niste obvezni voditi jer je evidencija aktivnosti obrade jedan od dokumenta kojim možete dokazati usklađenost s GDPR-om.

NAPOMENA!

Evidencije aktivnosti obrade **NE dostavljate Agenciji za zaštitu osobnih podataka**, već ih vodite i čuvate u pisanom obliku u poslovnom prostoru, a dajete ih na uvid ako vas AZOP to zatraži.

9 IMENOVATI SLUŽBENIKA ZA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)

Osnovna uloga službenika za zaštitu osobnih podataka:

- brine o tome da su poslovni procesi organizacije usklađeni s GDPR-om
- brine o svim pitanjima koja se odnose na zaštitu osobnih podataka u organizaciji

Imenovanje službenika za zaštitu podataka (čl. 37 GDPR-a) obvezno je:

a) Ako obradu provodi tijelo javne vlasti ili javno tijelo (bez obzira na to koji se podaci obrađuju);

b) Ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri (npr. osiguravajuće društvo koje izrađuje profile u svrhe određivanja premije osiguranja, marketinška agencija koja se bavi bihevioralnim oglašavanjem, veliki trgovački lanac koji kupcima nudi program vjernosti, zaštitarsko poduzeće (izvršitelj obrade) koje nadzire više privatnih trgovačkih centara i javnih prostora);

c) Ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka ili osobnih podataka koji se odnose na kaznene osude i kažnjiva djela (npr. poduzeće koje se bavi pružanjem usluga ugovornog obavljanja poslova zaštite na radu).

Primjer: Frizerski salon koji zapošljava 25 djelatnika i obrađuje osobne podatke zaposlenika te prikuplja osobne podatke klijenata kao što su ime, prezime, adresa, datum rođenja nije u obvezi imenovati službenika za zaštitu podataka.
Privatna poliklinika koja zapošljava 10 djelatnika i obrađuje, između ostalog, i osobne podatke o zdravlju te genetske podatke, podatke osjetljivih skupina pojedinaca (primjerice djece, starijih osoba), prenosi osobne podatke u treće zemlje, te u svom poslovanju koristi tehnologije koje mogu predstavljati veći rizik za pojedince trebala bi imenovati službenika za zaštitu podataka.

Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja njegovih zadaća (članci 37, 38 i 39 GDPR-a).

Imenovanje službenika mora biti u pisanom obliku i dostavljeno u izvorniku s potpisom i pečatom odgovorne osobe na sjedište Agencije za zaštitu osobnih podataka: Selska cesta 136, 10 000 Zagreb.

* *obrazac za imenovanje službenika za zaštitu podataka možete pronaći na web stranici AZOP-a: https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/*

10 PROVESTI PROCJENU UČINKA NA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)

Najbolji način za provjeru je li vaše poslovanje usklađeno s Općom uredbom o zaštiti podataka je provođenje procjene učinka na zaštitu podataka. U slučaju da je za neku vrstu obrade vjerojatno da će prouzročiti visok rizik za prava i slobode pojedinaca, provođenje procjene učinka je **NUŽNO.**

Procjena učinka na zaštitu podataka obvezna je u slučaju:

a) sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila i na temelju koje se donose odluke koje proizvode pravne učinke za pojedinca;
b) opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima ili
c) sustavnog praćenja javno dostupnog područja u velikoj mjeri.

Procjena učinka za zaštitu podataka je postupak osmišljen za:

1. opisivanje obrade - procjenu njezine nužnosti i proporcionalnosti

2. upravljanje rizicima za prava i slobode pojedinaca koji nastaju obradom osobnih podataka što uključuje procjenu rizika i određivanjem mjera za njihovo ublažavanje.

Prilikom procjene koji će postupci prouzročiti vjerojatno visok rizik za prava pojedinaca, potrebno je uzeti u obzir devet kriterija koji su detaljno opisani u Vodiču za provedbu procjene učinka na zaštitu podataka, dostupnom na web stranici projekta ARC: **https://arc-rec-project.eu/vodici/**

Popis vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka možete pronaći na web stranici AZOP-a:
https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/

Napominjemo kako ovaj popis nije konačan te je potrebno uzeti u obzir ispunjava li obrada dva ili više prethodno spomenutih kriterija i je li vjerojatno da će ista prouzročiti visok rizik za prava pojedinaca.

DODATAK!

VAŽNO JE ZNATI!

1. Svaka obrada osobnih podataka koju provodi izvršitelj obrade u ime voditelja obrade mora biti uređena ugovorom ili drugim pravnim aktom u pisanom obliku. U Općoj uredbi o zaštiti podataka navode se **elementi koji moraju biti određeni u ugovoru o obradi osobnih podataka između voditelja i izvršitelja obrade** (čl. 28 GDPR-a).

Primjer: trgovina mješovite robe želi instalirati videonadzorni sustav u svrhu zaštite ljudi i imovine. Poslove instalacije i održavanje videonadzornog sustava u trgovini povjerava zaštitarskoj tvrtki. Voditelj obrade je trgovina koja mora sklopiti ugovor o obradi osobnih podataka sa zaštitarskom tvrtkom kao izvršiteljem obrade.

** predložak ugovora o obradi osobnih podataka između voditelja i izvršitelja obrade dostupan je na web stranici projekta ARC: https://arc-rec-project.eu/obrasci/ te isti možete prilagoditi svojim poslovnim procesima i obradama osobnih podataka koje povjeravate izvršitelju obrade*

2. Obrada osobnih podataka putem **videonadzora dodatno je uređena Zakonom o provedbi Opće uredbe, a može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine**, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem videonadzora.

Sustav videonadzora mora biti zaštićen od pristupa neovlaštenih osoba, a odgovorne osobe koje imaju pravo pristupa osobnim podacima ne smiju koristiti snimke suprotno svrsi u koju je postavljen videonadzor.

Ukoliko planirate ili već imate postavljen **videonadzor** u vašem poslovnom prostoru, dužni ste označiti da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod videonadzorom, **a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja te sadržavati jednostavnu i razumljivu sliku uz tekst kojim se osobama pružaju najmanje sljedeće informacije:**

- da je prostor pod videonadzorom
- podatke o voditelju obrade (poduzeću/društvu/obrtu/organizaciji/tijelu javne vlasti, državnom tijelu): naziv, adresa i kontakt podaci voditelja obrade
- svrhu obrade
- pravnu osnovu
- prava ispitanika
- poveznicu na politiku privatnosti/drugi odgovarajući dokument ili informaciju o tome gdje je takav dokument ispitaniku dostupan (npr. u poslovnici)

** predložak obavijesti o videonadzoru možete pronaći na stranici projekta ARC: https://arc-rec-project.eu/obrasci/*

** detaljne informacije o obradi osobnih podatka putem videonadzora možete pronaći na: https://arc-rec-project.eu/vodici/*

Naziv voditelja obrade (poduzeća/organizacije/poslovnog subjekta/fizičke osobe): *upisati naziv*

Adresa voditelja obrade: *upisati adresu*

Kontakt podaci voditelja obrade: *upisati e-mail adresu* poduzeća/organizacije/poslovnog subjekta, broj telefona

Svrha obrade: zaštita ljudi i imovine

Pravna osnova: legitimni interes

Prava ispitanika (fizičkih osoba koje su snimljene videonadzornim kamerama): pravo na pristup svojim osobnim podacima, pravo na njihovo brisanje, pravo na ograničenje njihove obrade, te pravo na ulaganje prigovora na njihovu obradu

Cjelovite informacije o obradi Vaših osobnih podataka možete pronaći u *Politici privatnosti na poveznici.../prostorijama voditelja obrade.*

PROSTOR JE POD VIDEONADZOROM

3. Ukoliko u vašem poslovanju koristite web stranicu i **obrađujete osobne podatke putem kolačića**, dužni ste o tome obavijestiti posjetitelje svoje web stranice putem jasno vidljive obavijesti (skočnog prozora/bannera) te na web stranici uz politiku privatnosti ili u okviru iste morate imati objavljenu i obavijest o kolačićima.

Informacije o kolačićima ispitaniku možete pružiti unutar politike privatnosti u zasebnom poglavlju na pregledan i jasno razumljiv način ili u zasebnom dokumentu. U svakom slučaju, oba dokumenta moraju biti jasno vidljiva i najčešće se nalaze u podnožju web stranice.

Obavijest o kolačićima treba sadržavati sve informacije o tome što su kolačići, vrsti kolačića koji se na web stranici koriste i njihovoj funkciji. **Korisnik treba imati mogućnost na jednako jednostavan način odbiti i prihvatiti kolačiće.**

"Prozorčić" (banner) koji se korisniku pojavi u pregledniku kad posjeti stranicu i ima unaprijed označenu opciju "prihvaćam kolačiće" ili čak ima samo opciju "prihvaćam kolačiće" bez opcije "ne prihvaćam" kolačiće nije u skladu s GDPR-om.

Bitno za napomenuti je da navedene informacije trebaju opisivati stvarno stanje na vašoj web stranici, tj. stvarne vrste i kategorije kolačića koji se na istoj koriste, odnosno koji se osobni podaci doista prikupljaju pomoću tih kolačića, koja je njihova stvarna svrha i rokovi pohrane te prenose li se podaci u treće zemlje ili međunarodne organizacije. Vrlo često su takve informacije preuzete s neke druge web stranice samo kako bi se zadovoljila forma te ne odgovaraju stvarnom stanju stvari.

** detaljne informacije o obradi osobnih podatka putem kolačića možete pronaći na web stranici projekta ARC: https://arc-rec-project.eu/vodici/*

4. U slučaju **povrede osobnih podataka, dužni ste obavijestiti Agenciju za zaštitu osobnih podataka bez odgađanja**, ako je moguće, najkasnije 72 sata nakon saznanja o toj povredi, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

5. Ako provodite aktivnosti direktnog marketinga u svrhu promocije i prodaje svojih roba i usluga, imajte na umu da za takvu obradu morate imati pravni temelj (legitimni interes ili privola).

** detaljne informacije o izvješćivanju o povredi osobnih podataka i obrazac izvješća možete na web stranici projekta ARC: https://arc-rec-project.eu/vodici/*

6. Sankcije za prekršitelje Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka

Prema odredbama Opće uredbe o zaštiti podataka **svaka povreda će se sankcionirati upravnim novčanim kaznama koje će se izricati uz ili umjesto drugih sankcija poput upozorenja, opomena, zabrana, ograničenja, itd. Iznimno, ako je riječ o manjoj povredi fizičke osobe i ako bi upravna novčana kazna bila nerazmjerna, ista se neće izricati nego će se izreći opomena.**

Postoje dva seta kršenja; za neka kršenja (obveze voditelja i izvršitelja obrade te certifikacijskog tijela i tijela za praćenje kodeksa ponašanja) propisana je maksimalna kazna u iznosu od **10 milijuna eura ili 2% godišnjeg prometa na svjetskoj razini, a za druga kršenja (načela obrade, prava ispitanika, prijenosi u treće države, obveze u skladu s nacionalnim pravom, nepoštovanja naredbe ili pravo pristupa nadzornog tijela) propisana je maksimalna kazna do 20 milijuna eura ili 4% godišnjeg prometa na svjetskoj razini, ovisno o tomu što je veće.**

Sukladno članku 51. Zakona o provedbi Opće uredbe o zaštiti podataka, upravnom novčanom kaznom u iznosu do 50.000,00 kuna kaznit će se:

- voditelj obrade i izvršitelj obrade koji ne označe objekt, prostorije, dijelove prostorije te vanjsku površinu objekta na način propisan člankom 27. ovoga Zakona

- voditelj obrade i izvršitelj obrade koji ne uspostave automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora, sukladno članku 28. stavku 4. ovoga Zakona

- osobe iz članka 28. stavka 1. ovoga Zakona koje snimke iz sustava videonadzora koriste suprotno članku 28. stavku 2. ovoga Zakona.

O AGENCIJI ZA ZAŠTITU OSOBNIH PODATAKA

Agencija za zaštitu osobnih podataka je samostalno i neovisno državno tijelo koje nadzire provedbu Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. 04. 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka (Opće uredbe o zaštiti podataka) i obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, br. 42/18) kojim se osigurava provedba Opće uredbe o zaštiti podataka. Sukladno članku 58. Opće uredbe o zaštiti podataka **Agencija ima istražne, korektivne i savjetodavne ovlasti.**

Agencija za zaštitu osobnih podataka kontinuirano ulaže napore da zaštita osobnih podataka, kao jedno od temeljnih ljudskih prava, postane opće prihvaćeno načelo rada svih koji prikupljaju, obrađuju i prenose osobne podatke.

Agencija provodi niz aktivnosti s ciljem podizanja svijesti o važnosti zaštite osobnih podataka, sa snažnim naglaskom na prevenciju jer vrlo često do kršenja GDPR-a i Zakona o provedbi Opće uredbe o zaštiti podataka dolazi zbog neznanja i neinformiranosti voditelja i izvršitelja obrade.

O PROJEKTU

AWARENESS RAISING CAMPAING FOR SMEs (ARC) - Kampanja podizanja razine svijesti o zaštiti podataka za male i srednje poduzetnike

PROJEKT SUFINANCIRAN IZ PROGRAMA EUROPSKE UNIJE „PRAVA, JEDNAKOST I GRAĐANSTVO 2014-2019“, REC-RDAT-TRAI-AG-2019
TRAJANJE PROJEKTA: od ožujka 2020. do rujna 2022.
KOORDINATOR PROJEKTA: AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA
PARTNERI: DATA PROTECTION COMMISSION IRELAND, VRIJE UNIVERSITY BRUXELLES

Opća uredba o zaštiti podataka ključan je dio dosljednog i moderniziranog zakonodavstva EU-a o zaštiti podataka koji se primjenjuje u Europskoj uniji od 25. svibnja 2018. godine. Zaštiti podataka pristupa se ozbiljnije nego ikad prije, a što ima dalekosežan učinak na različite dionike i sektore.
Niz dionika ukupnog koncepta zaštite osobnih podataka, s posebnim naglaskom na male i srednje poduzetnike, smatra da nisu dobro informirani o zahtjevima koje pred njih stavlja Opća uredba i da nadzorna tijela za zaštitu podataka ne pružaju dovoljno potpore prilikom usklađivanja s novim propisima o zaštiti podataka.

Vrlo često mali i srednji poduzetnici nemaju dovoljno financijskih i ljudskih resursa potrebnih za razumijevanje i implementaciju GDPR-a te se i dalje suočavaju s brojnim nedoumicama prilikom usklađivanja. U svrhu pružanja što bolje podrške malim i srednjim poduzetnicima, Europska komisija osigurava bespovratna sredstva tijelima za zaštitu podataka za provedbu projektnih aktivnosti koje imaju za cilj podizanje razine svijesti I znanja o zaštiti osobnih podataka s naglaskom na mikro, male i srednje poduzetnike.

CILJ PROJEKTA:

ARC je transnacionalni projekt koji ima za cilj pružiti podršku mikro, malim i srednjim poduzetnicima prilikom usklađivanja s Općom uredbom kroz provedbu različitih projektnih aktivnosti kao što su održavanje savjetodavnih aktivnosti i izradu edukativnih materijala prilagođenih njihovim specifičnim potrebama.

KLJUČNE AKTIVNOSTI:

- provođenje ankete među mikro, malim i srednjim poduzetnicima u svrhu identificiranja i analize njihovih potreba te sukladno tome izrada edukativnih modula i promotivnih materijala
- organizacija edukacija i radionica u Hrvatskoj i Irskoj s ciljem pružanja podrške poduzetnicima u usklađivanju s zakonodavnim okvirom za zaštitu osobnih podataka
- izrada vodiča i smjernica za usklađivanje s Općom uredbom o zaštiti podataka
- organizacija dvije međunarodne konferencije s ciljem širenja znanja o Općoj uredbi i prezentiranja rezultata projekta cjelokupnoj javnosti
- digitalna medijska kampanja
- izrada animiranog promotivnog spota
- izrada web stranice s interaktivnim materijalima i alatima za pomoć prilikom usklađivanja s GDPR-om

REZULTATI:

- povećano poznavanje i razumijevanje GDPR-a kod mikro, malih i srednjih poduzetnika
- jačanje sposobnosti rješavanja izazova primjene GDPR-a u nacionalnom kontekstu
- podizanje razine svijesti o zaštiti osobnih podataka kod cjelokupne javnosti
- podizanje svijesti i razumijevanja uloge, nadležnosti i glavnih odgovornosti tijela za zaštitu osobnih podataka
- jačanje prekogranične suradnje, razmjena znanja i iskustva s transnacionalnim partnerima

Sufinancirano kroz Program o pravima, jednakosti i građanstvu Europske unije

Kampanja podizanja svijesti o zaštiti osobnih podataka

OVAJ PROJEKT JE SUFINANCIRAN IZ PROGRAMA EUROPSKE UNIJE "PRAVA, JEDNAKOST I GRAĐANSTVO", UGOVOR O DODJELI BESPOVRATNIH SREDSTAVA № 874524.

GDPR JE DOŠAO S NAMJEROM DA OSTANE!

Saznajte više na
www.azop.hr i https://arc-rec-project.eu/arc/