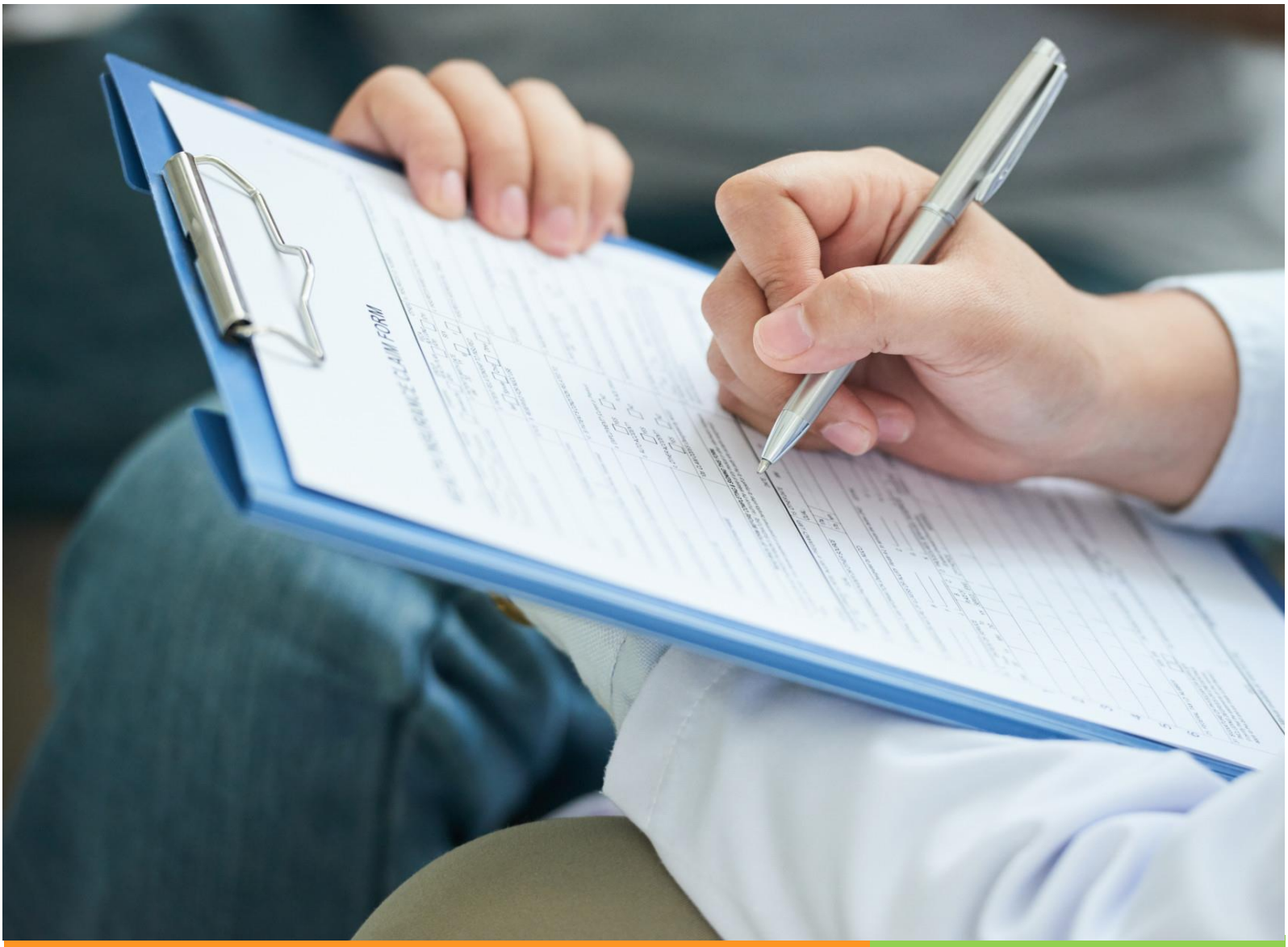
Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)



UPUTE ZA VOĐENJE EVIDENCIJE AKTIVNOSTI OBRADE

Awareness raising campaign for SMEs

UVOD

U nekim slučajevima poduzeće kao voditelj obrade mora voditi evidenciju o svojim aktivnostima obrade koja, između ostalog, uključuje podatke o svrsi obrade, kategorijama ispitanika/osobnih podataka, kategorijama primatelja podataka, prijenos osobnih podataka u treće zemlje, vremenska razdoblja za brisanje podataka te koliko je moguće opis tehničkih i organizacijskih mjera zaštite.

PREPORUKA PODUZETNICIMA! Preporučamo da vodite evidenciju aktivnosti obrade čak i ako po Općoj uredbi o zaštiti podataka niste u obvezi istu voditi jer je evidencija aktivnosti obrade jedan od dokumenta kojim možete dokazati usklađenost s Općom uredbom o zaštiti podataka!

VAŽNO! Voditelji obrade prema Općoj uredbi o zaštiti podataka nemaju obvezu dostave navedenih evidencija obrade osobnih podataka Agenciji za zaštitu osobnih podataka, već evidencije aktivnosti obrade vode i čuvaju kod sebe u pisanom obliku, uključujući elektronički oblik te su istu dužni dati na uvid na zahtjev nadzornog tijela (Agenciji za zaštitu osobnih podataka).

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 (**primjerice: 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 (**primjerice: obrada osobnih podataka zaposlenika u svrhu isplate plaća od strane poslodavca**),
- ako obrada uključuje posebne kategorije podataka (**primjerice: zdravstveni podaci, biometrijski podaci, genetski podaci)**,
- ako obrada uključuje **osobne podatke u vezi s kaznenim osudama i kažnjivim djelima**

Ako imate manje od 250 zaposlenika i ne ispunjavate gore navedene uvjete NISTE U OBVEZI voditi evidenciju aktivnosti obrade. Svakako vam preporučamo da ipak vodite evidenciju aktivnosti obrada jer je evidencija jedan od alata za dokazivanje usklađenosti s Općom uredbom o zaštiti podataka.

NAPOMENA: Što znači povremena obrada? Veliki broj obrada je stalan, kao što je obrada osobnih podataka zaposlenika u svrhu isplata plaća, obrada osobnih podataka putem kolačića, obrada osobnih podataka putem videonadzora, obrada osobnih podataka u CRM sustavima (softver za upravljanje odnosima s kupcima), obrada osobnih podataka u svrhu prodaje putem internetske trgovine, aktivnosti direktnog marketinga itd. U svim tim slučajevima, voditelj obrade je dužan voditi evidenciju aktivnosti obrade.

Primjer 1:

Kako bi što uspješnije plasirao svoje proizvode na tržištu i povećao prodaju, voditelj obrade, mali proizvođač prirodne kozmetike s 20 zaposlenika, angažira marketinšku agenciju koja izrađuje profile korisnika društvenih mreža i koristi njihove osobne podatke za ciljano oglašavanje. Iako poduzeće ima manje od 250 zaposlenika, obrada koju je povjerila izvršitelju obrade (marketinškoj agenciji) može dovesti do rizika za prava i slobode ispitanika (inovativna tehnologija, profiliranje), te je dužno voditi evidenciju o aktivnostima obrade. Isto tako i izvršitelj obrade je u ovom slučaju dužan voditi evidenciju aktivnosti obrade.

Primjer 2: Staračkidom zapošljava samo 5 zaposlenika, ali obrađuje zdravstvene podatke svojih korisnika. Budući da podaci koje obrađuje o svojim korisnicima uključuju i posebne kategorije osobnih podataka, dužan je voditi evidenciju aktivnosti obrade.

VAŽNO JE IMATI NA UMU!

Vođenje evidencije aktivnosti obrade izvrstan je način za postizanje kontrole nad obradama osobnih podataka u poduzeću, a posjedovanje ovih informacija na jednom mjestu (u fizičkom i elektroničkom obliku) olakšava poštivanje Opće uredbe o zaštiti podataka.

Osim veće usklađenosti, kvalitetna evidencija aktivnosti obrade pokazuje da je poduzeće promišljalo o vlastitim obradama osobnih podataka, napravilo svojevrsnu reviziju nad obradama koje provodi te uspostavilo kontrolu nad svim procesima koji se tiču osobnih podataka, a čime se dakako smanjuje i rizik od povreda osobnih podataka.

Evidencija aktivnosti obrade mora sadržavati sve sljedeće informacije (čl. 30 GDPR-a):

1. **ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;**

2. **svrhe obrade;**

3. **opis kategorija ispitanika i kategorija osobnih podataka;**

4. **kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;**

5. **ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. drugog podstavka, dokumentaciju o odgovarajućim zaštitnim mjerama;**

6. **ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;**

7. **ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.**

Na poveznici https://arc-rec-project.eu/wp-content/uploads/2022/09/ARC-obrazac-Evidencija-aktivnosti-obrade.xlsx možete pronaći obrazac evidencije aktivnosti obrade s nekoliko primjera koji vam mogu poslužiti boljem razumijevanju načina na koji se evidencija aktivnosti obrade vodi. Ovaj obrazac mogu koristiti svi voditelji obrade, ali obrazac pritom moraju prilagoditi svojim specifičnim obradama i poslovnim procesima.

Rubrike u obrascu označene **tamnozelenom bojom** niste u obavezi popunjavati (iako preporučamo), a **bijelo-sive rubrike** ste dužni ispuniti. Iako nije propisano čl. 30 GDPR-a, svakako preporučamo navesti **pravni temelj za obradu osobnih podataka**. U nastavku slijede upute koje vam mogu pomoći prilikom vođenja evidencije aktivnosti obrade.

1. IME I KONTAKTNI PODACI VODITELJA OBRADE I, AKO JE PRIMJENJIVO, ZAJEDNIČKOG VODITELJA OBRADE, PREDSTAVNIKA VODITELJA OBRADE I SLUŽBENIKA ZA ZAŠTITU PODATAKA

U prvom dijelu evidencije aktivnosti obrade potrebno je navesti ime/naziv i kontakt podatke:

- voditelja obrade;
- ako je primjenjivo, zajedničkog voditelja obrade;
- predstavnika voditelja obrade i
- službenika za zaštitu podataka

a. voditelj obrade

Voditeljem obrade Opća uredba o zaštiti podataka naziva sve one koji obrađuju osobne podatke.

To mogu biti fizičke ili pravne osobe, mikro, mala i srednje velika poduzeća, tijela javne vlasti, trgovačka društva, organizacije.

Primjeri voditelja obrade: putnička agencija, frizerski salon, cvjećarnica, proizvođač kozmetike, trgovina, starački dom, marketinška agencija, iznajmljivač apartmana koji je fizička osoba itd.

b. zajednički voditelj obrade

Da bi se dva ili više poduzeća mogla okarakterizirati kao zajednički voditelji obrade potrebno je zajedničko sudjelovanje u određivanju svrha i sredstava obrade.

Zajedničko sudjelovanje u određivanju svrha i sredstva obrade može se očitovati u smislu:

- donošenja zajedničkih odluka u vezi obrade osobnih podataka ili
- međusobno nadopunjavanje odluka gdje je takvo nadopunjavanje potrebno da bi se obrada odvijala na takav način da zajedničko donošenje odluka ima opipljiv utjecaj na određivanje svrha i sredstava obrade.

Važan kriterij je da obrada ne bi bila moguća bez sudjelovanja obiju strana u smislu da je obrada svakog poduzeća neodvojiva, tj. neraskidivo povezana.

Primjer 3: Putnička agencija šalje osobne podatke svojih klijenata aviokompaniji i hotelskom lancu u svrhu rezervacije karata i smještaja. Aviokompanija i hotelski lanac izvršavaju rezervacije, a putnička agencija izdaje vouchere. Svaka strana radi svoje aktivnosti i obrade i svaka je samostalni voditelj obrade. No, ako se sve tri strane dogovore da će zajedno uspostaviti web stranicu za prodaju paket aranžmana, a pritom svi zajedno određuju koji osobni podaci se obrađuju, kako će se vršiti rezervacije, tko će ih moći vidjeti te međusobno dijele osobne podatke za zajedničke marketinške aktivnosti. U ovom slučaju putnička agencija, hotel i aviokompanija su zajednički voditelji obrade.

Primjer 4:
Konzultantsko poduzeće angažira agenciju za zaopošljavanje u svrhu pronalaska odgovarajućih zaposlenika. Konzultantsko poduzeće dostavlja agenciji za zapošljavanje životopise kandidata koje već posjeduje, a agencija traži odgovarajuće kandidate i među životopisima koje je koje ima u svojoj bazi podataka. Agencija za zapošljavanje takvu bazu podataka kreira i njome samostalno upravlja. Dakle, ne radi se o poduzećima koja su formalno zajedno donijela odluku o obradama osobnih podataka, ali oba poduzeća zajedno sudjeluju u obradi osobnih podataka u svrhu pronalaska odgovarajućih kandidata.

Takve obrade osobnih podataka nadopunjuju se, neodvojive su i potrebne za pronalazak prikladnih kandidata.

c. predstavnik voditelja obrade

Opća uredba o zaštiti podataka primjenjuje se na obradu osobnih podataka ispitanika u EU koju obavlja poduzeće bez poslovnog nastana u EU, ako su:

- aktivnosti obrade povezane s nuđenjem robe ili usluga takvim ispitanicima u EU ili
- ako su aktivnosti obrade povezane s praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar EU

U tom slučaju poduzeće bez poslovnog nastana u EU mora imenovati svog predstavnika, odnosno fizičku ili pravnu osobu s poslovnim nastanom u EU pisanim putem, a koja bi predstavljala poduzeće u pogledu njegovih obveza temeljem Opće uredbe o zaštiti podataka.

Funkcija predstavnika može se ostvariti na temelju ugovora o pružanju usluga istog, sklopljenog s pojedincem ili određenim društvom te ju sukladno tome može preuzeti veliki broj subjekata, kao što su primjerice odvjetnička društva, konzultantska društva itd. pod uvjetom da su takvi subjekti osnovani u EU, a jedan predstavnik može djelovati u ime nekoliko poduzeća koji nemaju sjedište u EU.

Izvršitelj obrade i službenik za zaštitu podataka ne bi mogli biti imenovani kao predstavnici poduzeća.

Predstavnik poduzeća smatra se polazišnom točkom za obradu osobnih podataka poduzeća bez poslovnog nastana u EU.

Imajući u obzir navedeno, predstavnik mora biti u stanju učinkovito komunicirati s ispitanicima o obradi osobnih podataka i surađivati s relevantnim nadzornim tijelima za zaštitu osobnih podataka.

2. SVRHA OBRADE OSOBNIH PODATAKA

Prije početka obrade osobnih podataka, poduzeće je dužno identificirati svrhu obrade osobnih podataka i to u trenutku prikupljanja podataka.

Svrha obrade osobnih podataka prvenstveno znači da je poduzeće upoznato s razlozima potrebe za obradom određenih osobnih podataka.

Dakle, poduzeće je dužno preispitati zašto mu određeni podaci uopće trebaju za postizanje svrhe u koju se isti obrađuju. Svrha dakako mora biti zakonita.

U mnogim slučajevima je **svrha obrade osobnih podataka zakonska obveza.**

Primjer 5:
Poduzeće je dužno voditi evidenciju o radnicima. Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c). U ovom slučaju voditelj obrade osobne podatke obrađuje sukladno Zakonu o radu (NN 93/2014, 127/2017, 98/2019) i Pravilniku o sadržaju i načinu vođenja evidencije o radnicima (NN 32/15, 97/15).

Ponekad je riječ o **ispunjenju ugovorne obveze poduzeća**.

Primjer 6: Poduzeće prodaje svoje proizvode putem webshopa. U svrhu sklapanja kupoprodajnog ugovora putem webshopa poduzeću su nužni podaci o imenu/prezimenu i adresi kupca.

U određenim slučajevima postoje određeni **legitimni interesi** poduzeća za obradom određenih osobnih podataka.

Primjer 7: Trgovina mještovitom robom imala je nekoliko provala u godinu dana, a tijekom posljednje provale ozlijeđena je zaposlenica trgovine. Trgovina je nakon toga instalirala vidoenadzorni sustav u svrhu zaštite imovine i života i tjelesnog integriteta pojedinaca. Prethodno je proveden i dokumentiran test legitimnog interesa te je na vidljivo mjesto postavljena obavijest o videonazdoru koja sadrži sve elemente sukladno GDPR-u i Zakonu o provedbi Opće uredbe o zaštiti podataka.

Osobne podatke potrebno je obrađivati u točno određenu svrhu i za takvu obradu mora postojati zakonita pravna osnova.

3. KATEGORIJA ISPITANIKA I KATEGORIJE OSOBNIH PODATAKA

Ispitanici su pojedinci čije osobne podatke poduzeće obrađuje.

Ako se poduzeće bavi organizacijom događaja i prodajom ulaznica za događaje, ispitanici poduzeća su **kupci** koji su kupnju obavili u poslovnici, **posjetitelji web stranice** ako su ulaznice kupili putem webshopa, **posjetitelji društvenih mreža**-sudionici nagradne igre, ako je na istoj organizirana nagradna igra. Ako isto poduzeće ima program vjernosti kojim skupljajući bodove ostvaruje određene pogodnosti, ispitanici su **članovi programa vjernosti**. Osobama kojima poduzeće šalje newsletter također se smatraju ispitanicima.

Također, za pretpostaviti je da poduzeće ima svoje **zaposlenike** temeljem ugovora o radu, koji su također ispitanici poduzeća, a recimo da poduzeće ima svoje sjedište u zgradi koja je ujedno i kulturno dobro te radi zaštite tog dobra ima instaliran videonadzorni sustav na ulazu u zgradu, sve **osobe koje bi bile zabilježene videosnimkom** također bi se smatrale ispitanicima poduzeća.

Opća uredba o zaštiti podataka definira pojam „**osobni podatak**“ široko, stoga su osobni podaci sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

Stoga i različite informacije koje same po sebi ne identificiraju pojedinca ako su prikupljene zajedno s drugima te mogu rezultirati utvrđivanjem identiteta određene osobe, također se smatraju osobnim podatkom.

Neki od primjera osobnih podataka su:

- Ime i prezime,
- Poštanska adresa, adresa e-pošte, telefonski broj
- Datum rođenja, dob pojedinca
- OIB, broj osobne iskaznice
- Podatak o sindikalnom članstvu
- IP adresa

- Podatak o lokaciji
- Broj kreditne/debitne kartice
- Podaci o zdravlju
- Biometrijski podaci (primjerice otisak prsta)
- Prikaz pojedinca na videonadzornoj snimci ili fotografiji, audio zapis
- Registarska oznaka vozila
- I mnogi drugi

Osobnim podacima smatraju se i **pseudonimizirani podaci**. Pseudonimizacija je proces obrade osobnih podataka na način da se oni više ne mogu pripisati konkretnom pojedincu bez upotrebe dodatnih podataka. Ti dodatni podaci mogu se smatrati nekom vrstom ključa, bez kojeg se pseudonimizirani podaci ne mogu koristiti u izvornom obliku. Osobni podaci koji otkrivaju podatke o rasnom ili etničkom podrijetlu, političkim mišljenjima, vjerskim ili filozofskim uvjerenjima ili članstvu u sindikatu, kao i genetski podaci, biometrijski podaci, podaci o zdravlju ili podaci o spolnom životu ili seksualnoj orijentaciji fizičke osobe **posebna su kategorija podataka** za koju postoji načelna zabrana obrade sukladno članku 9. stavku 1. Opće uredbe o zaštiti podataka. Kada je riječ o navedenim posebnim kategorijama podataka, posve je jasan razlog načelne zabrane od obrade osobnih podataka. Naime, svaki od tih vrsta podataka predstavlja svojevrstan rizik za pojedinca ako bi takav podatak bio nezakonito obrađen.

Nadalje, kada je riječ o povećanom riziku, isti postoji i u slučaju obrade osobnih podataka određenih kategorija ispitanika. Primjerice, podaci o djeci, starijim osobama, tražiteljima azila i svim drugim skupinama koje su na određeni način ranjive zaslužuju posebnu zaštitu u pogledu svojih osobnih podataka budući da ranjive kategorije ispitanika mogu biti manje svjesne rizika, posljedica i predmetnih zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka. Takvi podaci smataju se **osjetljivim podacima**.

Na kraju, potrebno je spomenuti koji podaci ne spadaju pod režim Opće uredbe o zaštiti podataka, a to su **podaci preminulih osoba** te **anonimizirani podaci** kojima identifikacija pojedinca više nije moguća.

4. KATEGORIJE PRIMATELJA OSOBNIH PODATAKA

Informacije o primateljima/kategorijama primatelja podataka poduzeće će uvrstiti u evidenciju aktivnosti obrade ako je to primjenjivo.

Primatelj može biti drugo poduzeće, tijelo javne vlasti, organizacija, osoba izvan poduzeća ili zaposlenik/ustrojstvena jedinica unutar organizacijskog ustroja poduzeća koji obrađuje osobne podatke u okviru svojih radnih zadaća, a podatke obrađuje u ime i prema uputama poduzeća kao voditelja obrade.

Primjer 8: Poduzeće obrađuje osobne podatke zaposlenika u svrhu vođenja evidencije o radnicima i obračun plaće. Zakonska obveza poduzeća je osobne podatke proslijediti Hrvatskom zavodu za mirovinsko osiguranje, Hrvatskom zavodu za zdravstveno osiguranje i Poreznoj upravi. U ovom slučaju primatelji osobnih podataka su HZMO, HZZO i Porezna uprava.

5. PRIJENOSI OSOBNIH PODATAKA U TREĆE ZEMLJE (ZEMLJA IZVAN EU/EGP)

U današnje digitalno doba nije rijetkost da osobni podaci cirkuliraju izvan granica EU, međutim u tom slučaju poduzeća moraju voditi računa da se osigura zadovoljavajuća razina zaštite pojedinca čiji se osobni podaci prenose.

Primjer 9: Poduzeće koje se bavi proizvodnjom i prodajom kožne galanterije angažira poduzeće iz Bosne i Hercegovine da šalje kupcima newslettere te analizira njihovu marketinšku učinkovitost.

Prijenosom podataka o mail adresama na koje treba slati newsletter poduzeće vrši transfer u treću zemlju te mora voditi računa o zakonitosti takvih prijenosa, a kako bi se osigurala zakonitost takvih prijenosa, poduzeće mora voditi računa o pravilima iz poglavlja V. Opće uredbe o zaštiti podataka.

Prijenos osobnih podataka trećim zemljama bit će u skladu s pravilima poglavlja V. Opće uredbe o zaštiti podataka ako između ostalog:

- **postoji odluka o primjerenosti**

Odluku donosi EK koja je odlučila da treća zemlja osigurava odgovarajuću razinu zaštite podataka, što znači da u pogledu prijenosa nema rizika za pojedinca i njegovo pravo na zaštitu osobnih podataka.
Dakle, odluka EK ima učinak da osobni podaci mogu slobodno cirkulirati u treću zemlju za koju je odluka donesena jednako kao da je prijenos izvršen unutar EU/EGP, a popis zemalja za koje je donesena odluka možete pronaći putem poveznice: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_hr

- **ako prijenosi podliježu odgovarajućim zaštitnim mjerama**

Primjerice, prijenos se vrši, između ostalog, temeljem standardnih ugovornih klauzula o zaštiti podataka.

Standardne ugovorne klauzule sadrže ugovorne obveze poduzeća koji prenosi podatke te društva koji prima osobne podatke pojedinca te njihova međusobna prava i obveze.

Standardne ugovorne klauzule možete pronaći na poveznici: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en

Napominjemo kako je prilikom upotrebe standardnih ugovornih klauzula u odnosu na prijenose osobnih podataka u Sjedinjene Američke Države, zbog postojanja određenih bojazni na primjerenu razinu zaštite osobnih podataka, potrebno da poduzeće koje prenosi osobne podatke u SAD, uz standardne ugovorne klauzule poduzme dodatne zaštitne mjere koje se mogu primijeniti zajedno sa standarnim ugovornim klauzulama u svrhu održavanja odgovarajuće razine zaštite.

Napominjemo kako postoje i drugi mehanizmi prijenosa osobnih podataka u treće zemlje, međutim gore navedeni mehanizmi su najrelevantniji za mikro, male, srednje poduzetnike i obrtnike.

6. POHRANA OSOBNIH PODATAKA

U vezi s pitanjem pohrane osobnih podataka, kao i za pitanje pravne osnove za obradu istih, važno je poznavati strukovne zakone koji uređuju djelatnost kojom se poduzeće bavi.

Naime, čuvanje i zadržavanje osobnih podataka često je propisano zakonima i podzakonskim aktima.

Ako predmetno nije određeno, poduzeće se treba voditi načelom **„ograničenja razdoblja pohrane“** koji određuju da se osobni podaci čuvaju onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju, a pohraniti se mogu na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

S tim u vezi, poduzeće samostalno mora znati koliko dugo su mu određeni osobni podaci nužni za svrhe u koje se obrađuju, a predmetno je potrebno potkrijepiti i urediti internim pravilima.

Svakako, ako je moguće poduzeće bi trebalo navesti i kriterije pomoću kojih je odredilo rok pohrane.

7. TEHNIČKE I ORGANIZACIJSKE MJERE ZAŠTITE

Poduzeće je dužno provesti prikladne tehničke i organizacijske mjere zaštite kako bi se osigurala odgovarajuća razina sigurnosti koja je proporcionalna riziku obrade osobnih podataka, a sve u svrhu sprečavanja potencijalne povrede osobnih podataka.

Naime, povreda osobnih podataka uključuje svako kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Povredu osobnih podataka poduzeće treba prevenirati implementiranjem pravilnih i pravodobnih organizacijskih i tehničkih mjera zaštite u svoje poslovanje.

Organizacijske mjere zaštite odnose se na dokumentirano uređenje te organizacijsku kulturu poslovne prakse na način da se internim aktima, ugovornim klauzulama te podizanjem razine svijesti aktivno radi na usklađenosti sa zahtjevima iz Opće uredbe o zaštiti podataka.

Primjerice, određena pitanja unutar poduzeća potrebno je regulirati **internim pravilima (pravilnici o zaštiti osobnih podataka i informacijskoj sigurnosti, ovlaštenja za obradu osobnih podataka, izjave o povjerljivosti, pristup određenim podacima, rokovi pohrane, postupanje sa zahtjevima prava ispitanika, ugovori s izvršiteljima obrade, sigurno korištenje interneta i službene opreme poduzeća itd.).** Od iznimne je važnosti podizanje razine svijesti u cijelom poduzeću, posebice kad uzmemo u obzir da se većina povreda podataka događa zbog pogrešaka uzrokovanih ljudskim faktorom.

Tehničke mjere zaštite odnose se na zaštitne mjere koje se postavljaju na fizička mjesta, IT sustave/uređaje koji se koriste unutar poduzeća ili u sklopu krajnjih proizvoda koji se koriste, a vezano uz obradu osobnih podataka. Također, poduzeće tehničke mjere ugovorno regulira s trećim stranama koje imaju uvid u osobne podatke ili s kojima sudjeluje u obradi podataka.

Neke od tehničkih mjera su: korištenje snažnih lozinki na računalima, izrada sigurnosnih kopija podataka, pseudonimizacija ili šifriranje osobnih podataka - posebice za posebne kategorije podataka, korištenje antivirusnih programa i dr.

DODATNO:

PRAVNE OSNOVE ZA OBRADU OSOBNIH PODATAKA

Pitanje zakonitosti obrade osobnih podataka od ključne je važnosti za usklađivanje s Općom uredbom o zaštiti podataka, a regulirano je člankom 6. Opće uredbe o zaštiti podataka.

Svatko tko obrađuje osobne podatke **mora osigurati postojanje jedne od šest pravnih osnova za obradu** propisanih gore navedenim člankom, kao i, ako poduzeće obrađuje posebne kategorije podataka, mora osigurati jednu od iznimaka propisanih člankom 9. stavkom 2. Opće uredbe o zaštiti podataka.

U suštini, svaki put kada poduzeće postavlja pitanje smije li se obraditi osobne podatke, primjerice čuvati, obrisati ih ili možda dostaviti podatke trećoj strani, odgovor se nalazi u postojanju pravne osnove za obradu osobnih podataka. Na taj način poduzeće brine i da poštuje jedno od najvažnijih načela Opće uredbe o zaštiti podataka– **načelo zakonitosti**.

a. Privola

Početno treba naglasiti da privola nema prvenstvo u odnosu na druge pravne osnove već se radi o jednakovrijednoj pravnoj osnovi za obradu osobnih podataka.

Među voditeljima obrade koji pripadaju skupini mikro, malih i srednjih poduzetnika često se pogrešno misli da je za svaku obradu osobnih podataka (bez obzira primjerice na pravni propis, ugovor ili legitiman interes) potrebna određena suglasnost pojedinca.

Štoviše, poduzeće kao voditelj obrade treba najprije provjeriti ima li drugu pravnu osnovu za obradu podataka, primjerice u obliku pravnih zahtjeva iz zakona ili ugovora, a tek u nedostatku druge osnove osloniti se na privolu upravo iz razloga što je potrebno ispitanicima omogućiti da privolu u svakom trenutku mogu valjano i jednostavno povući, stoga ona predstavlja za poduzetnikove nužne obrade određeni rizik.

Kao što je već rečeno, potrebno je osigurati da ispitanik može povući privolu u bilo kojem trenutku, a da to ne utječe na zakonitost obrade prije povlačenja.

Iz gore navedenih razloga, **preporučujemo da poduzeća pažljivo razmotre je li privola najprikladniji pravni temelj za obradu i ako jest, ispunjava li privola sve uvjete propisane Općom uredbom o zaštiti podataka.**

Opća uredba o zaštiti podataka postavlja visoke standarde za valjanu privolu.

Naime, privola mora biti dana jasnom potvrdnom radnjom, mora biti dobrovoljna, posebna i nedvosmislena, utemeljena na informacijama koje pojedincima omogućuju određenu kontrolu nad vlastitim osobnim podacima.

Privola mora biti slobodan izbor, a pitanje slobodnog izbora ne smije ovisiti o postojanju nekih negativnih posljedica za pojedinca u slučaju da ne pristane na obradu.

Primjer: Poliklinika dentalne medicine traži privolu pacijenta za obradu njegovih osobnih podataka u svrhu liječenja zuba. Ako ispitanik ne da privolu, ne može dobiti uslugu liječenja. Ovakva privola nije u skladu s GDPR-om jer je uvjetovana pružanjem usluge. U ovom slučaju privola nije valjani pravni temelj za obradu osobnih podataka, već je pravni temelj zakonska obveza prema kojoj je liječnik dužan obrađivati osobne podatke pacijenta u svrhu liječenja.

Primjer: Poduzeće za trgovanje nekretninama sklapa s kupcem kupoprodajni ugovor. U tom ugovoru od pojedinca se traže određeni osobni podaci koji nisu nužni za sklapanje ugovora. Ugovor nije odgovarajući pravni temelj za obradu osobnih podataka koji nisu nužni za izvršenje ugovora i ispitaniku ne smije biti uvjetovano davanje tih osobnih podataka u svrhu sklapanja ugovora. Za obradu osobnih podataka koji nisu nužni za sklapanje ugovora, pravni temelj može biti privola.

S druge strane, dobrovoljni pristanak može biti doveden u pitanje ako postoji značajna nejednakost između poduzeća i pojedinca. Primjerice, obrada osobnih podataka u kontekstu radnog odnosa gdje se smatra da se radnik u odnosu na poslodavca smatra „slabijom stranom“ jer je u određenom zavisnom, nepovlaštenom položaju.

Zbog toga se u većini slučajeva ne preporučuje zasnivati obradu podataka zaposlenika na privoli, jer nije rijetkost da radnik pristaje na određenu obradu osobnih podataka samo zato što se boji nekih negativnih posljedica, primjerice, strah od otkaza ako ne pristane na određenu obradu podataka ili bojazan od lošeg postupanja poslodavca u slučaju nepristanka.

Privola mora biti posebna, što znači da obrada i svrha u koju se daje moraju biti dovoljno specificirane kako bi se pojedincima omogućila veća kontrola nad vlastitim osobnim podacima. Poduzeće mora voditi računa o granularnosti u dobivanju privole te jasno odvajati informacije koje se odnose na dobivanje privole od bilo koje druge važne informacije.

Razdvajanje svrha obrade može se postići ostavljanjem praznog okvira ispred svake svrhe obrade tako da pojedinac može označiti okvir ako želi. Poveznica na obrazac privole: https://arc-rec-project.eu/wp-content/uploads/2022/01/Obrazac-privole.docx.

Naposljetku, potrebno je voditi računa o tome da poduzeće mora informirati pojedince o obradi, kako bi osigurali valjanu individualnu odluku o njihovom izboru da daju privolu za obradu ili ne.

Neke od informacija koje treba pružiti su tko je voditelj obrade, svrhe obrade, informacije o vrsti podataka, informacije o pravu na povlačenje privole, informacije o korištenju podataka za automatizirano donošenje odluka, informacije o mogućim rizicima prijenosa podataka, odgovarajuće zaštitne mjere i dr.

Važna je i kvaliteta pruženih informacija, što znači da se jezik i rječnik moraju prilagoditi skupini od koje poduzeće traži privolu. S tim u vezi, informacije moraju biti pružene jasnim i jednostavnim jezikom koji svaki prosječan pojedinac može razumjeti te moraju biti lako dostupne. Informacije će ispitaniku najčešće biti pružene putem dokumenta politika privatnosti. Poveznica na obrazac politike privatnosti: https://arc-rec-project.eu/wp-content/uploads/2022/01/politika-privatnosti_obrazac.docx.

Što se tiče privole djeteta, ističemo kako je u Republici Hrvatskoj propisano da samo poslovno sposobna osoba može vlastitim očitovanjima volje stvarati pravne učinke te da poslovnu sposobnost fizička osoba stječe punoljetnošću. Umjesto osobe koja nema poslovnu sposobnost očitovat će svoju volju njezin zakonski zastupnik ili skrbnik.

Obiteljskim zakonom propisano je da u sadržaj roditeljske skrbi ulazi pravo i dužnost zastupanja djetetovih osobnih i imovinskih prava i interesa.

Dakle, u slučaju da se radi o privoli maloljetnog djeteta, privolu za obradu njegovih osobnih podataka daje njegov roditelj odnosno zakonski zastupnik, osim ako je riječ o pružanju usluga informacijskog društva direktno djetetu. **Tada dijete samo daje privolu ako ima više od 16 godina, a dužnost poduzeća je da dobnu granicu djeteta razumnim mjerama provjeri.**

b. Ugovor

Ako postoji ugovorni odnos između pojedinca i poduzeća ili postoje radnje koje prethode sklapanju ugovora (primjerice predugovor, obvezujuća ponuda) a obrada osobnih podataka je nužna za izvršenje ugovora pravna osnova za takvu obradu je ugovor.

Važno je naglasiti da poduzeća moraju osigurati nužnost i proporcionalnost izvršenja ugovora. U pravilu, to znači da obrada podataka mora biti neophodna, stoga, ako poduzeće može razumno obraditi manje podataka ili koristiti podatke na manje nametljiv način neće se smatrati da se radi o osobnim podacima koji su nužni za sklapanje/izvršenje ugovora, a samim time za obradu takvih osobnih podataka poduzeće neće imati uporište u ugovoru kao pravnoj osnovi za obradu podataka.

Primjerice, podaci koji su potrebni za online kupnju su ime, prezime i adresa. Ako potrošača poduzeće traži podatak o broju djece, bračnom statusu i sl. kako bi mu moglo ponuditi personalizirane proizvode putem newslettera, ti podaci ne bi bili nužni za predmet ugovora, a pravni temelj za takvu obradu ne bi mogao biti ugovor.

c. Pravna obveza poduzeća

Ovdje je potrebno naglasiti kako poduzeće prvenstveno ima dužnost poznavati strukovne zakone i podzakonske propise koji uređuju djelatnost kojom se poduzeće bavi.

Naime, zakonima i podzakonskim propisima često su određene obrade osobnih podataka, a sadržaj tih obrada je u biti pravna obveza poduzeća, a samim time takva je obrada zakonita jer postoji adekvatna pravna osnova.

Primjer: Hotel (poduzeće koji se bavi turističkom djelatnošću) dužno je poznavati Zakon o turističkoj pristojbi te Pravilnik o sustavu eVisitor i znati da primjerice, obrada osobnih podataka gostiju putem sustava e-Visitor ima svoje utemeljenje u navedenim propisima te se samim time smatra zakonitom s aspekta zaštite osobnih podataka.

Također važna je informacija da ako se osobni podaci obrađuju temeljem zakonske obveze, pojedinac nema pravo na brisanje, pravo na prenosivost podataka ili pravo na prigovor.

d. Legitiman interes

Iako postoji raznolik spektar legitimnih interesa poduzeća radi kojih je potrebna određena obrada osobnih podataka **(primjerice, legitiman interes može uključivati komercijalne interese, sigurnosne interese, individualne interese ili čak šire društvene koristi**), važno je napomenuti da isti uvijek neće biti zakonit.

Ne postoji iscrpan popis legitimnih interesa za koje je potrebno obrađivati osobne podatke, ali neki od potencijalnih zakonitih legitimnih interesa bili bi primjerice, **marketing, sprječavanje prijevara, razmjena informacija unutar poduzeća, IT sigurnost, zaštita imovina i pojedinaca** i dr.

Legitiman interes poduzeća ili treće strane pravna je osnova za obradu osobnih podataka koja se može primijeniti ako ne prevladavaju interesi ili temeljna prava i slobode pojedinaca.

Za korištenje legitimnog interesa kao pravne osnove za obradu osobnih podataka, **obrada mora biti nužna u smislu proporcionalnosti u postizanju ciljeva poduzeća**, što znači da treba imati na umu da, ako postoji alternativna opcija koja manje utječe na prava i slobode, obrada radi ostvarenja legitimnog interesa vjerojatno nije nužna, a samim time ni zakonita.

Nadalje, postojanje legitimnog interesa zahtijeva pažljivu procjenu, mogu li pojedinci razumno očekivati određenu obradu u određenu svrhu, s tim da očekivanja pojedinaca moraju biti razumna.

Primjerice, ako je u poduzeću instaliran videonadzorni sustav radi postizanja cilja zaštite imovine ili posjeda nije razumno očekivati instalaciju istog u kabini za presvlačenje ili sanitarnim prostorijama, dok je razumno očekivati isti na hodniku ili u prostoriji gdje se čuvaju za poduzeće vrijedni dokumenti ili stvari.

Stoga, ako interesi i temeljna prava pojedinaca nadmašuju interese voditelja obrade, legitimni interes kao pravni temelj ne bi se trebao primjenjivati, a isto se može procijeniti u nekoliko koraka prije početka obrade **provedbom testa legitimnog interesa kojeg možete pronaći na web stranici Agencije za zaštitu osobnih podataka** https://azop.hr/obrasci-predlosci/ **i web stranici ARC projekta** https://arc-rec-project.eu/wp-content/uploads/2022/01/primjer-Test-razmjernosti-.docx**.**

Spomenuti test legitimnog interesa ključna je komponenta za oslanjanje na legitiman interes kao pravu osnovu za obradu osobnih podataka jer njime poduzeće uspostavlja konačnu ravnotežu poduzimanjem dodatnih mjera zaštite, utvrđuje postoji li mogućnost dokazivanja usklađenosti, osigurava transparentnost i razmatra kako nastaviti s ostvarivanjem prava pojedinaca, posebice prava na prigovor kojeg je najkasnije do trenutka prve komunikacije s pojedincem potrebno uputiti pojedincu, prezentirano jasno i odvojeno od svih drugih informacija.

Napominjemo kako postoje i druge pravne osnove za obradu osobnih podataka, međutim gore navedene pravne osnove su najrelevantnije za mikro, male, srednje poduzetnike i obrtnike.

ULOGA SLUŽBENIKA ZA ZAŠTITU PODATAKA

Imenovanje službenika za zaštitu osobnih podataka u određenim slučajevima je obvezno. Više informacija o imenovanju službenica za zaštitu podataka možete pronaći na poveznici: https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/.

Primjerice, kada se osnovna djelatnost sastoji od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri ili se osnovna djelatnost sastoji od opsežne obrade posebnih kategorija osobnih podataka odnosno podataka u vezi s kaznenim osudama i kažnjivim djelima.

Dakle, obveza ne ovisi o veličini organizacije, stoga za pitanje obveznog imenovanja nije relevantno pripada li voditelj obrade kategoriji mikro/malog ili srednjeg poduzetnika.

Agencija za zaštitu osobnih podataka napominje da je moguće imenovati službenika za zaštitu podataka čak i kada to nije obvezno, ali u tom slučaju važno je napomenuti da ako poduzeće dobrovoljno imenuje službenika za zaštitu podataka, na njegovo se imenovanje, položaj i zadaće primjenjuju svi zahtjevi iz Opće uredbe o zaštiti podataka kao da je imenovanje bilo obvezno.

U slučaju imenovanja (obveznog ili neobveznog), poduzeće objavljuje kontaktne podatke službenika za zaštitu podataka i priopćuje ih Agenciji za zaštitu osobnih podataka. Obrazac izvješća o imenovanju službenika za zaštitu podataka može se pronaći na poveznici: https://azop.hr/wp-content/uploads/2020/12/izvjesce_o_imenovanju_sluzbenika_za_zastitu_podataka-selska.pdf.

Dakle, nije dovoljno u pojedinačnom ugovoru o radu navesti da će određena osoba obavljati zadaće službenika za zaštitu osobnih podataka, potrebno je tu osobu imenovati zasebnom odlukom te istu dostaviti Agenciji za zaštitu osobnih podataka.

Službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti, ali poduzeće mora osigurati da takve zadaće i dužnosti ne dovedu do sukoba interesa.

Što se tiče pojma „sukoba interesa“, nepisano je pravilo da radna mjesta koja mogu biti u sukobu interesa u okviru poduzeća su uglavnom položaji u višem rukovodstvu, ali i niže uloge u hijerarhijskoj strukturi organizacije ako takvi položaji ili uloge podrazumijevaju utvrđivanje svrhe i načina obrade osobnih podataka.

Službenik za zaštitu podataka može biti zaposlenik poduzeća ili vanjski suradnik temeljem ugovora o djelu sklopljenog s pojedincem ili organizacijom izvan organizacije poduzeća.

U svakom slučaju radi kvalitetnog obavljanja svojih zadaća službeniku je potrebno osigurati sve potrebne resurse za obavljanje poslova (financijska potpora, vrijeme, ljudski resursi, profesionalni razvoj i sl.).

Službenik za zaštitu podataka mora biti neovisan te u tom smislu ne smije dobivati upute za izvršavanje svojih zadataka, ne smije biti razriješen svoje dužnosti ili kažnjen zbog istih, a službenik podnosi izvještaje najvišoj razini upravljanja.

Službenik za zaštitu podataka ne mora biti određene struke (primjerice pravne ili tehničke), ali mora poznavati propise u vezi zaštite osobnih podataka te procese obrade osobnih podataka u poduzeću. Njegova stručnost mora biti proporcionalna osjetljivosti, složenosti i količini podataka koje organizacija obrađuje.

Dakle, tamo gdje je aktivnost obrade podataka posebno složena ili kada je uključena velika količina osjetljivih podataka, službenik za zaštitu podataka trebat će višu razinu stručnosti i podrške.

VAŽNA NAPOMENA!

Svaki izvršitelj obrade i predstavnik izvršitelja obrade, ako je primjenjivo, vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju za voditelja obrade, koja sadržava:

1) ime i kontaktne podatke jednog ili više izvršitelja obrade i svakog voditelja obrade u čije ime izvršitelj obrade djeluje te, ako je primjenjivo, predstavnika voditelja obrade ili izvršitelja obrade te službenika za zaštitu podataka;

2) kategorije obrade koje se obavljaju u ime svakog voditelja obrade;

3) ako je primjenjivo, prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. točke (h), dokumentaciju o odgovarajućim zaštitnim mjerama;

4) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.

UGOVOR IZMEĐU VODITELJA I IZVRŠITELJA OBRADE

Primjer: Trgovina odjećom (voditelj obrade) ima veći broj zaposlenika te je odlučila potpisati ugovor s knjigovodstvenim servisom (izvršiteljem obrade) koji će obračunavati plaće zaposlenicima. Trgovina odjećom određuje kad plaće trebaju biti isplaćene, obavještava knjigovodstveni servis o tome kad zaposlenik sklapa ugovor o radu ili isti prekida, kad zaposlenik dobiva povišicu ili stimulaciju, te pruža knjigovodstvenom servisu sve nužne osobne podatke zaposlenika vezane za platni izvod i isplatu plaća.

Knjigovodstveni servis pohranjuje podatke zaposlenika (samo one koje su potrebne u svrhu izvršenja ugovorne obveze) u svojim bazama podataka. Za pohranu osobnih podataka koristi IT sustav pohrane te je poduzelo sve odgovarajuće tehničke i organizacijske mjere za zaštitu osobnih podataka. Izvršitelj obrade voditelju obrade mora jamčiti zaštitu i povjerljivost obrade osobnih podataka.

VAŽNO! Svaka obrada osobnih podataka koju provodi izvršitelj obrade u ime voditelja obrade mora biti uređena ugovorom ili drugim pravnim aktom u pisanom obliku i mora biti obvezujuća. U Općoj uredbi o zaštiti podataka navode se elementi koji moraju biti određeni u ugovoru o obradi (**članak 28. Opće uredbe o zaštiti podataka**). U okviru projekta ARC izradili smo obrazac Ugovora o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3. Opće uredbe o zaštiti podataka https://arc-rec-project.eu/wp-content/uploads/2022/01/Ugovor-o-obradi-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-prema-clanku-28-OUZP-template-ARC.docx kojeg možete prilagoditi svojim poslovnim procesima i obradama osobnih podataka koje povjeravate izvršitelju obrade.