

POLITIKA ZA ZAŠTITU OSOBNIH PODATAKA

GRA-PO d.o.o.

(Usvojena na sjednici Uprave dana 15.05.2018.)

I. UVOD

1. Opća uredba o zaštiti podataka

Uredba (EU) 2016/679 (Opća uredba o zaštiti podataka – GDPR) ima izravnu primjenu i podrazumijeva izmjene zakonodavstva država članica u području zaštite osobnih podataka. Njezina je svrha zaštita prava i sloboda fizičkih osoba te osiguravanje da se osobni podaci ne obrađuju bez njihova znanja i, kada je to moguće, da se obrađuju uz njihov pristanak.

2. Područje primjene definirano Općom uredbom o zaštiti podataka

Materijalno područje primjene – GDPR se primjenjuje na obradu osobnih podataka u cijelosti ili djelomično automatiziranim sredstvima, kao i na obradu drugim sredstvima osobnih podataka koji čine dio registra osobnih podataka ili su namijenjeni da budu dio registra osobnih podataka.

Teritorijalno područje primjene – pravila GDPR-a primjenjuju se na sve voditelje obrade osobnih podataka koji imaju sjedište u EU i koji obrađuju osobne podatke fizičkih osoba u kontekstu svoje djelatnosti. Također se primjenjuju i na voditelje obrade izvan EU koji obrađuju osobne podatke u svrhu ponude robe i usluga ili praćenja ponašanja ispitanika koji se nalaze u EU.

3. Pojmovi

„Osobni podaci” – svi podaci koji se odnose na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati („ispitanik”); fizička osoba koja se može identificirati jest osoba koja se može identificirati izravno ili neizravno, osobito pomoću identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili pomoću jednog ili više obilježja specifičnih za fizički, fiziološki, genetski, mentalni, gospodarski, kulturni ili socijalni identitet te fizičke osobe;

„Posebne kategorije osobnih podataka” – osobni podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatima, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije fizičke osobe, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji fizičke osobe.

„Obrada” – svaka radnja ili skup radnji koje se obavljaju na osobnim podacima ili skupovima osobnih podataka, bilo automatiziranim ili neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organiziranje, strukturiranje, pohrana, prilagodba ili izmjena, dohvat, uvid, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

„Voditelj obrade” – svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade određeni pravom EU ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu biti utvrđeni pravom Unije ili pravom države članice;

„Ispitanik” – svaka živa fizička osoba na koju se odnose osobni podaci koje voditelj obrade pohranjuje.

„Privola ispitanika” – svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;

„Dijete” – obrada osobnih podataka djeteta zakonita je samo ako je privolu dao roditelj ili skrbnik. Voditelj obrade ulaže razumne napore kako bi u takvim slučajevima provjerio da je nositelj roditeljske odgovornosti za dijete dao ili ovlastio davanje privole.

„Profiliranje” – svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s fizičkom osobom, a posebno za analizu ili predviđanje aspekata koji se odnose na radni učinak te fizičke osobe, njezino ekonomsko stanje, zdravlje, osobne sklonosti, interese, pouzdanost, ponašanje, lokaciju ili kretanje;

„Povreda osobnih podataka” – povreda sigurnosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

„Glavno mjesto poslovnog nastana” – sjedište voditelja obrade u EU bit će mjesto na kojem se donose glavne odluke o svrsi i sredstvima aktivnosti obrade podataka. U odnosu na izvršitelja obrade, njegovo glavno mjesto poslovnog nastana u EU bit će njegovo administrativno središte.

Ako voditelj obrade ima sjedište izvan EU, mora imenovati svog predstavnika u jurisdikciji u kojoj posluje kako bi djelovao u njegovo ime i surađivao s nadzornim tijelima.

„Primatelj” – fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome radi li se o trećoj strani ili ne. Međutim, tijela javne vlasti koja mogu primati osobne podatke u okviru određene istrage u skladu s pravom Unije ili pravom države članice ne smatraju se „primateljima”; obrada tih podataka od strane navedenih tijela javne vlasti mora biti u skladu s primjenjivim pravilima zaštite podataka prema svrsi obrade;

„Treća strana” – svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade niti osobe koje su pod izravnim nadzorom voditelja obrade ili izvršitelja obrade ovlaštene obrađivati osobne podatke;

II. IZJAVA O POLITICI ZAŠTITE OSOBNIH PODATAKA

1. Uprava društva **GRA-PO d.o.o.** obvezuje se osigurati usklađenost sa zakonodavstvom EU u vezi s obradom osobnih podataka i zaštitom „prava i sloboda” osoba čije osobne podatke društvo **GRA-PO d.o.o.** prikuplja i obrađuje u skladu s GDPR-om.
2. U skladu s GDPR-om, ovom politikom opisani su i usvojeni drugi relevantni dokumenti, kao i povezani procesi i procedure.
3. GDPR i ova politika odnose se na sve funkcije obrade osobnih podataka, uključujući one koje se provode u vezi s osobnim podacima kupaca, zaposlenika, dobavljača i partnera te svih drugih osobnih podataka koje društvo obrađuje iz različitih izvora.
4. Ova politika primjenjuje se na sve zaposlenike društva **GRA-PO d.o.o.**, kao i na vanjske pružatelje usluga. Svako kršenje GDPR-a smatrat će se povredom radne discipline, a u slučaju sumnje na počinjenje kaznenog djela, predmet će u najkraćem mogućem roku biti upućen nadležnim tijelima na razmatranje.
5. Partneri i treće strane koje rade s ili za društvo **GRA-PO d.o.o.**, kao i oni koji imaju ili mogu imati pristup osobnim podacima, dužni su upoznati se s ovom politikom, razumjeti je i postupati u skladu s njom. Nijedna treća strana ne može imati pristup osobnim podacima koje pohranjuje društvo **GRA-PO d.o.o.** bez prethodno sklopljenog sporazuma o povjerljivosti podataka, kojim se trećoj strani nameću obveze koje nisu manje stroge od onih koje je preuzelo društvo **GRA-PO d.o.o.**, te kojim se društvu **GRA-PO d.o.o.** daje pravo provjere poštivanja obveza nametnutih sporazumom.

III. OBVEZE I FUNKCIJE PREMA OPĆOJ UREDBI O ZAŠTITI PODATAKA

1. **GRA-PO d.o.o.** je voditelj obrade i izvršitelj obrade podataka u skladu s GDPR-om.

2. Uprava društva **GRA-PO d.o.o.** odgovorna je za razvoj i promicanje dobre prakse u području obrade informacija unutar društva.
3. Svjesno važnosti ovog pitanja i vođeno namjerom da u najvećoj mogućoj mjeri zaštiti podatke koje obrađuje, društvo **GRA-PO d.o.o.** imenovat će službenika za zaštitu podataka, koji će biti član menadžerskog tima društva i izvještavat će Upravu društva **GRA-PO d.o.o.** o upravljanju osobnim podacima unutar organizacije te o osiguravanju dokazive usklađenosti sa zakonodavstvom o zaštiti podataka i dobrom praksom.
4. Službenik za zaštitu podataka ima posebne odgovornosti u vezi s procedurama te je kontakt osoba za zaposlenike voditelja obrade koji traže pojašnjenja o bilo kojem aspektu poštivanja zaštite podataka.
5. Usklađenost sa zakonodavstvom o zaštiti podataka odgovornost je svih zaposlenika društva **GRA-PO d.o.o.** koji obrađuju osobne podatke.
6. Politika osposobljavanja društva **GRA-PO d.o.o.** određuje posebne zahtjeve za edukaciju i podizanje svijesti povezane s konkretnim ulogama zaposlenika društva **GRA-PO d.o.o.**

IV. NAČELA ZAŠTITE PODATAKA

Sva obrada osobnih podataka mora se provoditi u skladu s načelima zaštite podataka navedenima u članku 5. GDPR-a. Politike i procedure društva **GRA-PO d.o.o.** imaju za cilj osigurati poštivanje tih načela.

1. Osobni podaci moraju se obrađivati zakonito, pošteno i transparentno

Zakonito – prije obrade osobnih podataka potrebno je utvrditi zakonitu osnovu za obradu.

Pošteno – kako bi obrada bila poštena, voditelj obrade mora ispitanicima pružiti određene informacije, u mjeri u kojoj je to praktično moguće. To vrijedi neovisno o tome jesu li osobni podaci prikupljeni izravno od ispitanika ili iz drugih izvora.

Transparentno – obavijesti/izjave o privatnosti moraju biti razumljive i dostupne. Informacije moraju biti priopćene ispitaniku u razumljivom obliku, koristeći jasan i jednostavan jezik.

Pravila za informiranje ispitanika od strane društva **GRA-PO d.o.o.** definirana su u Proceduri transparentnosti pri obradi osobnih podataka.

Specifične informacije koje se moraju pružiti ispitaniku moraju uključivati najmanje:

- podatke koji identificiraju voditelja obrade i kontakt podatke voditelja obrade te, ako postoji, predstavnika voditelja obrade;
- svrhe obrade za koje su osobni podaci namijenjeni, kao i pravnu osnovu obrade;
- razdoblje tijekom kojeg će se osobni podaci pohranjivati;
- postojanje sljedećih prava – pravo zahtijevati pristup podacima, ispravak, brisanje (pravo „na zaborav”), ograničenje obrade, kao i pravo na prigovor u vezi s uvjetima (ili njihovim nepostojanjem) za ostvarivanje tih prava;
- kategorije osobnih podataka;
- primatelje ili kategorije primatelja osobnih podataka, gdje je to primjenjivo;
- gdje je primjenjivo, namjerava li voditelj obrade prenijeti osobne podatke primatelju u trećoj zemlji i razinu zaštite podataka;

- sve dodatne informacije potrebne za osiguravanje poštene obrade.

2. Osobni podaci mogu se prikupljati samo u posebne, izričite i zakonite svrhe

Podaci prikupljeni za određene svrhe ne smiju se koristiti za svrhe koje se razlikuju od onih za koje je dana privola.

Procedura transparentnosti pri obradi osobnih podataka određuje odgovarajuća pravila.

3. Osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno za obradu u skladu s određenom svrhom (načelo smanjenja količine podataka)

GRA-PO d.o.o. ne prikuplja informacije koje nisu strogo potrebne za svrhu za koju su prikupljene.

Svi obrasci za prikupljanje podataka (elektronički ili u papirnatom obliku), uključujući zahtjeve za prikupljanje podataka u novim informacijskim sustavima, moraju sadržavati Izjavu o privatnosti.

Službenik za zaštitu podataka osigurat će da se svi načini prikupljanja podataka periodično pregledavaju od strane interne revizije ili vanjskih stručnjaka kako bi se osiguralo da prikupljeni podaci i dalje ostanu primjereni, relevantni i ne pretjerani.

4. Osobni podaci moraju biti točni i ažurni u svakom trenutku te se moraju poduzeti potrebni naponi kako bi se omogućilo njihovo trenutačno brisanje ili ispravak (u okviru mogućih tehničkih rješenja)

Podaci koje pohranjuje voditelj obrade moraju se pregledavati i ažurirati prema potrebi. Podaci se ne smiju pohranjivati ako postoji vjerojatnost da nisu točni.

Službenik za zaštitu podataka odgovoran je osigurati da je svo osoblje educirano o važnosti prikupljanja točnih podataka i njihova održavanja ažurnima.

Također, ispitanik je odgovoran za točnost i ažurnost podataka koje dostavlja društvu **GRA-PO d.o.o.** na pohranu. Obrasci koje ispitanik ispunjava za voditelja obrade mogu sadržavati izjavu da su podaci navedeni u njima točni na datum podnošenja.

Od zaposlenika, klijenata i drugih osoba mora se zahtijevati da obavijeste društvo **GRA-PO d.o.o.** o svim promjenama okolnosti kako bi se evidencije osobnih podataka mogle ažurirati.

Odgovornost je društva **GRA-PO d.o.o.** osigurati da svaka obavijest o promjeni okolnosti bude evidentirana i da se poduzmu odgovarajuće mjere.

Najmanje jednom godišnje službenik za zaštitu podataka pregledat će rokove pohrane svih osobnih podataka koje obrađuje društvo **GRA-PO d.o.o.**, pozivajući se na evidenciju podataka, te će identificirati sve podatke koji više nisu potrebni u kontekstu registrirane svrhe. Takvi podaci bit će sigurno uništeni u skladu s procedurama i pravilima voditelja obrade.

Službenik za zaštitu podataka odgovoran je za usklađenost sa zahtjevima za ispravak podataka u roku od jednog mjeseca. Taj se rok može produljiti za dodatna dva mjeseca u slučaju složenih zahtjeva. Ako društvo **GRA-PO d.o.o.** odluči ne postupiti prema zahtjevu, službenik za zaštitu podataka mora odgovoriti ispitaniku, objasniti razloge takve odluke te ga informirati o njegovom pravu na podnošenje pritužbe nadzornom tijelu i ostvarivanje pravne zaštite.

Službenik za zaštitu podataka odgovoran je za poduzimanje odgovarajućih mjera u slučajevima kada organizacije trećih strana posjeduju netočne ili zastarjele osobne podatke, uključujući obavješćavanje da su informacije netočne ili zastarjele i da se ne smiju koristiti za donošenje odluka o pojedincima, obavješćavanje relevantnih strana te prosljeđivanje svih ispravaka osobnih podataka trećim stranama kada je to potrebno.

5. Osobni podaci moraju se čuvati u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno za obradu

Kada se osobni podaci zadržavaju nakon završetka obrade, pohranjuju se na odgovarajući način (minimizirani, kriptirani, pseudonimizirani) kako bi se zaštitio identitet ispitanika u slučaju povrede podataka.

Osobni podaci čuvat će se u skladu s Procedurom za pohranu i uništavanje podataka, a nakon isteka roka čuvanja moraju biti sigurno uništeni na način propisan tom procedurom.

Službenik za zaštitu podataka mora posebno odobriti svako zadržavanje podataka koje prelazi rok pohrane definiran Procedurom za pohranu i uništavanje podataka te mora osigurati da je opravdanje jasno definirano i usklađeno sa zahtjevima zakonodavstva o zaštiti podataka. Takvo odobrenje mora biti u pisanom obliku.

6. Osobni podaci moraju se obrađivati na način koji osigurava odgovarajuću sigurnost (čl. 24. i čl. 32. GDPR-a)

Službenik za zaštitu podataka nadzire provođenje procjene učinka (procjene rizika) u skladu s Procedurom procjene učinka na zaštitu podataka, uzimajući u obzir sve okolnosti povezane s operacijama upravljanja ili obrade podataka koje provodi društvo **GRA-PO d.o.o.**

Pri određivanju primjerenosti obrade, službenik za zaštitu podataka mora uzeti u obzir i moguću štetu ili gubitak koji bi mogli biti nanесeni fizičkim osobama (npr. zaposlenicima ili klijentima) u slučaju sigurnosnog incidenta, kao i moguću štetu za ugled voditelja obrade, uključujući eventualni gubitak povjerenja klijenata.

Pri procjeni odgovarajućih tehničkih mjera, službenik za zaštitu podataka razmotrit će sljedeće:

- zaštitu lozinkom;
- automatsko zaključavanje neaktivnih radnih stanica u mreži;
- antivirusni softver i vatrozide;
- prava pristupa privremeno zaposlenog osoblja;
- zaštitu uređaja koji napuštaju prostorije organizacije, kao što su prijenosna računala, pametni telefoni i drugi uređaji;
- sigurnost lokalnih i širokopojsnih mreža;
- tehnologije za poboljšanje privatnosti, kao što su pseudonimizacija i anonimizacija.

Pri procjeni odgovarajućih organizacijskih mjera službenik za zaštitu podataka uzet će u obzir sljedeće:

- razine odgovarajuće edukacije u društvu **GRA-PO d.o.o.**;
- mjere kojima se procjenjuje pouzdanost zaposlenika (npr. evaluacije rada, preporuke i sl.);
- uključivanje zaštite podataka u ugovore o radu;
- utvrđivanje disciplinskih mjera za povrede u vezi s obradom podataka;
- redovitu provjeru usklađenosti zaposlenika s odgovarajućim sigurnosnim standardima;
- kontrolu fizičkog pristupa elektroničkim i papirnatim evidencijama;
- primjenu politike „čistog radnog mjesta”;

- pohranu papirnatih dokumentacije u zaključanim ormarićima;
- ograničavanje uporabe osobnih uređaja zaposlenika na radnom mjestu;
- usvajanje jasnih pravila za izradu i korištenje lozinki;
- nametanje ugovornih obveza poslovnim partnerima da poduzmu odgovarajuće sigurnosne mjere pri prijenosu podataka izvan EU.

Ove kontrole odabrane su na temelju identificiranih rizika za osobne podatke, kao i mogućnosti nastanka štete za osobe čiji se podaci obrađuju.

7. Poštivanje načela odgovornosti

GRA-PO d.o.o. dokazivat će usklađenost s načelima zaštite podataka primjenom politika zaštite podataka, pristupanjem kodeksima ponašanja, uvođenjem odgovarajućih tehničkih i organizacijskih mjera, kao i primjenom načela zaštite podataka u fazi projektiranja i zaštite podataka prema zadanim postavkama, provođenjem procjene učinka na zaštitu osobnih podataka, procedura za obavješćavanje o povredi osobnih podataka i slično.

V. PRAVA ISPITANIKA

1. Ispitanici imaju sljedeća prava u vezi s obradom podataka i podacima koji se o njima pohranjuju:
 - zatražiti potvrdu obrađuju li se osobni podaci koji se odnose na njih te, ako se obrađuju, dobiti pristup tim podacima i informacije o primateljima tih podataka;
 - zatražiti kopiju svojih osobnih podataka od voditelja obrade;
 - zahtijevati od voditelja obrade ispravak osobnih podataka kada su netočni ili više nisu ažurni;
 - zahtijevati od voditelja obrade brisanje osobnih podataka (pravo „na zaborav”);
 - zahtijevati od voditelja obrade ograničenje obrade osobnih podataka, pri čemu će podaci biti samo pohranjeni, ali ne i dalje obrađivani;
 - uložiti prigovor na obradu svojih osobnih podataka;
 - uložiti prigovor na obradu osobnih podataka u svrhu izravnog marketinga;
 - podnijeti pritužbu nadzornom tijelu ako smatra da je prekršena neka od odredbi GDPR-a;
 - zatražiti i primiti osobne podatke u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu;
 - povući svoju privolu za obradu osobnih podataka u bilo kojem trenutku posebnim zahtjevom upućenim voditelju obrade;
 - ne biti predmet automatiziranog donošenja odluka koje ga značajno pogađaju, bez mogućnosti ljudske intervencije;
 - usprotiviti se automatiziranom profiliranju koje se provodi bez njegove privole.
2. **GRA-PO d.o.o.** osigurava uvjete koji jamče ostvarivanje ovih prava ispitanika:
 - ispitanici mogu podnositi zahtjeve za pristup podacima, kako je opisano u Proceduri upravljanja zahtjevima ispitanika; ova procedura također opisuje kako će društvo **GRA-PO d.o.o.** osigurati da odgovor na zahtjev ispitanika bude u skladu sa zahtjevima GDPR-a;

- ispitanici imaju pravo podnositi pritužbe društvu **GRA-PO d.o.o.** u vezi s obradom njihovih osobnih podataka, postupanjem po zahtjevima ispitanika te žalbama ispitanika u vezi s načinom obrade pritužbi, u skladu s Procedurom načina komunikacije kod pritužbi i zahtjeva ispitanika.

VI. PRIVOLA

1. Pod pojmom „privola” društvo **GRA-PO d.o.o.** podrazumijeva svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje ispitanika putem izjave ili jasne potvrdne radnje kojom izražava pristanak na obradu osobnih podataka koji se odnose na njega. Ispitanik može povući svoju privolu u bilo kojem trenutku.
2. Društvo **GRA-PO d.o.o.** smatra „privolom” samo one slučajeve u kojima je ispitanik bio potpuno informiran o planiranoj obradi te dao svoju privolu bez ikakvog pritiska. Privola dobivena pod pritiskom ili na temelju obmanjujućih informacija neće se smatrati valjanom pravnom osnovom za obradu osobnih podataka.
3. Privola se ne može pretpostaviti iz izostanka odgovora na poruku upućenu ispitaniku. Mora postojati aktivna komunikacija između voditelja obrade i ispitanika kako bi se smatralo da je privola dana. Voditelj obrade mora biti u mogućnosti dokazati da je privola za aktivnosti obrade dobivena.
4. Za posebne kategorije podataka mora se pribaviti izričita pisana privola u skladu s Procedurom pribavljanja privole za obradu osobnih podataka ispitanika, osim ako postoji druga zakonita osnova za obradu.
5. U većini slučajeva društvo **GRA-PO d.o.o.** rutinski pribavlja privolu za obradu osobnih podataka i posebnih kategorija podataka korištenjem standardnih dokumenata za privolu (izjava ili izričita klauzula u ugovoru).
6. Kada društvo **GRA-PO d.o.o.** obrađuje osobne podatke djece, mora se pribaviti odobrenje nositelja roditeljske skrbi (roditelja, skrbnika i sl.).

VII. SIGURNOST PODATAKA

1. Svi zaposlenici odgovorni su za osiguravanje sigurnosti podataka za koje su odgovorni i koje društvo **GRA-PO d.o.o.** posjeduje, kao i za to da se podaci pohranjuju na siguran način i ni pod kojim okolnostima ne otkrivaju trećim stranama, osim ako društvo **GRA-PO d.o.o.** nije takvoj trećoj strani dodijelilo odgovarajuća prava putem ugovora/klauzule o povjerljivosti.
2. Svi osobni podaci moraju biti dostupni samo onima kojima su potrebni, a pristup se može odobriti isključivo u skladu s uspostavljenim pravilima kontrole pristupa. Svi osobni podaci moraju se tretirati s najvećom razinom sigurnosti te se moraju pohranjivati:
 - u zasebnoj prostoriji s kontroliranim pristupom ili u zaključanom ormariću odnosno kartoteci; i/ili
 - računalno obrađeni, zaštićeni lozinkom, u skladu s internim zahtjevima navedenima u organizacijskim i tehničkim mjerama za kontrolu pristupa informacijama.
3. Potrebno je uspostaviti organizaciju koja jamči da računalne zaslone i terminale ne mogu pregledavati druge osobe osim ovlaštenih zaposlenika društva **GRA-PO d.o.o.** Svi zaposlenici moraju biti educirani i prihvatiti odgovarajuće ugovorne klauzule/izjavu o poštivanju organizacijskih i tehničkih mjera pristupa, kao i pravila zaključavanja radnih stanica, prije nego što im se omogući pristup informacijama bilo koje vrste.

4. Evidencije u papirnatom obliku ne smiju se ostavljati na mjestima gdje mogu biti dostupne neovlaštenim osobama i ne smiju se iznositi iz određenih uredskih prostora bez izričitog odobrenja. Čim papirnati dokumenti više nisu potrebni za tekući rad na podršci klijentima, moraju biti uništeni u skladu s uspostavljenom procedurom/pravilima i odgovarajućim zapisnikom.
5. Osobni podaci mogu se brisati ili uništavati samo u skladu s Procedurom za pohranu i uništavanje podataka. Evidencije u papirnatom obliku koje su dosegle rok čuvanja moraju se usitniti i uništiti kao „povjerljivi otpad”. Podaci na tvrdim diskovima rashodovanih osobnih računala moraju se izbrisati ili diskovi fizički uništiti, u skladu s uspostavljenim pravilima/procedurama.
6. Obrada osobnih podataka „izvan ureda” predstavlja potencijalno veći rizik od gubitka, krađe ili povrede osobnih podataka. Osoblje mora biti posebno upoznato s pravilima obrade podataka izvan objekata voditelja obrade.

VIII. OTKRIVANJE PODATAKA

1. Društvo **GRA-PO d.o.o.** mora osigurati uvjete u kojima se osobni podaci ne otkrivaju neovlaštenim trećim stranama, uključujući članove obitelji, prijatelje, državna tijela, pa čak i istražna tijela, ako postoji opravdana sumnja da se podaci ne traže na propisan način. Svi zaposlenici moraju biti oprezni kada se od njih traži otkrivanje pohranjenih osobnih podataka o drugoj osobi trećoj strani. Važno je procijeniti je li otkrivanje informacija povezano s potrebama djelatnosti koju organizacija obavlja.

Potrebno je provoditi posebnu edukaciju zaposlenika i periodične upute kako bi se izbjegao rizik od takvih povreda.

2. Svi zahtjevi trećih strana za dostavu podataka moraju biti potkrijepljeni odgovarajućom dokumentacijom, a svako takvo otkrivanje podataka mora posebno odobriti službenik za zaštitu podataka.

IX. POHRANA I UNIŠTAVANJE PODATAKA

1. Društvo **GRA-PO d.o.o.** ne pohranjuje osobne podatke u obliku koji omogućuje identifikaciju ispitanika dulje nego što je potrebno za svrhe za koje su podaci prikupljeni.
2. Društvo **GRA-PO d.o.o.** može pohranjivati podatke tijekom duljeg razdoblja samo ako će se osobni podaci obrađivati u svrhe arhiviranja, u javnom interesu, za znanstvena ili povijesna istraživanja ili za statističke svrhe, i to samo uz primjenu odgovarajućih tehničkih i organizacijskih mjera za zaštitu prava i sloboda ispitanika.
3. Razdoblje pohrane za svaku kategoriju osobnih podataka bit će određeno u Proceduri za pohranu i uništavanje podataka, kao i kriteriji koji se koriste za određivanje tog razdoblja, uključujući sve zakonske obveze društva **GRA-PO d.o.o.** vezane uz čuvanje podataka.
4. Procedura za pohranu i uništavanje podataka primjenjivat će se u svim slučajevima.
5. Osobni podaci moraju se sigurno uništavati, u skladu s načelom osiguravanja odgovarajuće razine sigurnosti (čl. 5. st. 1. t. e GDPR-a) – uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja, primjenom odgovarajućih tehničkih i organizacijskih mjera („cjelovitost i povjerljivost“).

X. PRIJENOS PODATAKA

1. Svaki prijenos podataka izvan EU u zemlje izvan EU (u GDPR-u označene kao „treće zemlje”) nezakonit je osim ako ne postoji odgovarajuća „razina zaštite temeljnih prava ispitanika”.

Prijenos osobnih podataka izvan EU zabranjen je osim ako se primjenjuje jedna ili više navedenih zaštitnih mjera ili iznimaka: zemlje članice Europskog gospodarskog prostora ili zemlje koje primjenjuju GDPR.

2. Odluka o primjerenosti

Europska komisija može procijeniti treće zemlje, teritorije i/ili određene sektore u trećim zemljama kako bi utvrdila postoji li odgovarajuća razina zaštite prava i sloboda fizičkih osoba. U takvim slučajevima nije potrebno posebno odobrenje.

Države članice Europskog gospodarskog prostora (EGP), iako nisu članice EU, smatraju se zemljama koje ispunjavaju uvjete za odluku o primjerenosti.

3. EU-U.S. Privacy Shield

Ako organizacija želi prenijeti osobne podatke iz EU u treću zemlju u SAD-u, mora provjeriti je li organizacija pristupila okviru „Privacy Shield” pri Ministarstvu trgovine SAD-a.

4. Obvezujuća korporativna pravila

GRA-PO d.o.o. može usvojiti odobrena obvezujuća korporativna pravila za prijenos podataka izvan EU. To zahtijeva njihovo podnošenje nadležnom nadzornom tijelu na odobrenje.

5. Standardne ugovorne klauzule

GRA-PO d.o.o. može usvojiti standardne ugovorne klauzule za zaštitu podataka pri prijenosu podataka izvan Europskog gospodarskog prostora.

Ako društvo **GRA-PO d.o.o.** prihvati standardne ugovorne klauzule odobrene od strane nadležnog nadzornog tijela, primjerenost zaštite automatski se priznaje.

6. Iznimke

U nedostatku odluke o primjerenosti, članstva u sustavu US Privacy Shield, obvezujućih korporativnih pravila i/ili ugovornih klauzula, prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju dopušten je samo pod jednim od sljedećih uvjeta:

- ispitanik je dao izričitu privolu za predloženi prijenos nakon što je informiran o mogućim rizicima takvog prijenosa;
- prijenos je nužan za izvršenje ugovora između ispitanika i voditelja obrade ili za provedbu predugovornih mjera poduzetih na zahtjev ispitanika;
- prijenos je nužan za sklapanje ili izvršenje ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe;
- prijenos je nužan zbog važnih razloga javnog interesa;
- prijenos je nužan za uspostavljanje, ostvarivanje ili obranu pravnih zahtjeva;
- prijenos je nužan radi zaštite životno važnih interesa ispitanika ili drugih osoba kada ispitanik fizički ili pravno nije sposoban dati svoju privolu;
- prijenos se obavlja iz registra koji je prema pravu EU ili pravu države članice namijenjen pružanju informacija javnosti i dostupan je javnosti na uvid ili bilo kojoj osobi koja može

dokazati legitiman interes, ali samo u mjeri u kojoj su u konkretnom slučaju ispunjeni uvjeti za uvid utvrđeni pravom Unije ili pravom države članice.

XI. PROCJENA RIZIKA PRI OBRADI PODATAKA

1. Društvo **GRA-PO d.o.o.** uspostavilo je procedure u vezi s aktivnostima obrade i pohrane podataka.
2. Društvo **GRA-PO d.o.o.** svjesno je rizika povezanih s obradom određenih vrsta osobnih podataka.
3. Društvo **GRA-PO d.o.o.** procjenjuje razinu rizika za osobe povezane s obradom njihovih osobnih podataka. Procjene učinka na zaštitu podataka provode se u vezi s obradom osobnih podataka koju provodi društvo **GRA-PO d.o.o.**, kao i u vezi s obradom koju u ime društva **GRA-PO d.o.o.** provode druge organizacije.
4. Društvo **GRA-PO d.o.o.** upravlja svim rizicima identificiranim procjenom učinka kako bi smanjilo vjerojatnost neusklađenosti s ovim pravilima.

Kada određena vrsta obrade može dovesti do visokog rizika za prava i slobode fizičkih osoba, osobito pri uporabi novih tehnologija te uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, društvo **GRA-PO d.o.o.** prije početka obrade mora provesti procjenu učinka planiranih postupaka obrade na zaštitu osobnih podataka. Jedna opća procjena učinka može obuhvatiti skup sličnih postupaka obrade koji predstavljaju slične visoke rizike.

5. Kada je iz procjene učinka jasno da će društvo **GRA-PO d.o.o.** započeti obradu osobnih podataka koji bi zbog visokog rizika mogli prouzročiti štetu ispitanicima, odluka o tome hoće li se obrada nastaviti mora biti dostavljena službeniku za zaštitu podataka na pregled.
6. Ako službenik za zaštitu podataka ima ozbiljne zabrinutosti u vezi s mogućom štetom ili opasnošću, odnosno količinom predmetnih podataka, dužan je eskalirati pitanje nadzornom tijelu.