**PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA**

**(„Pravilnik“)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naslov** | Pravilnik o zaštiti osobnih podataka | | |
| **Datum** | ${pzop\_01\_a} | **Verzija** | 1.0 |

**Voditelj obrade:** ${pzop\_01\_b}

**Ime i prezime osobe ovlaštene za zastupanje:** ${pzop\_01\_c}

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Potpis ovlaštene osobe za zastupanje**

U skladu s regulatornim zahtjevima Uredbe 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom o osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (u nastavku: **Uredba**) i Zakona o provedbi Opće uredbe o zaštiti podataka (u nastavku: **Zakon**), voditelj obrade ${pzop\_01\_d} (u nastavku: **Voditelj obrade**) donosi sljedeću Pravilnik o zaštiti osobnih podataka (u daljnjem tekstu: **Pravilnik**).

1. Opseg i cilj

Donošenjem ovog Pravilnika Voditelj obrade ima za cilj uspostavljanje sustava zaštite podataka sukladno Uredbi. Pravilnikom se uspostavljaju odgovarajuće organizacijske mjere zaštite osobnih podataka ispitanika, odnosno klijenata, zaposlenika i poslovnih partnera te drugih fizičkih osoba čiji se podaci obrađuju od strane Voditelja obrade.

1. Primjena

Pravilnik se primjenjuje na sve poslovne procese koji na bilo koji način uključuju obradu osobnih podataka koja se obavlja automatizirano te neautomatiziranu obradu osobnih podataka koja čini dio sustava pohrane, te obvezuje Voditelja obrade, sve zaposlenike, kao i fizičke i pravne osobe koje rade za i u ime Voditelja obrade.

1. Pojmovi

Pojmovi korišteni u ovom Pravilniku imaju jednako značenje kao i pojmovi korišteni u Uredbi i Zakonu te ih nije potrebno sve navoditi, a kao temeljni pojmovi ovog Pravilnika izdvajaju se:

**Osobni podatak** - znači svaki podatak koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi (“ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

**Obrada** - znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

**Voditelj obrade** - znači 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 utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice.

**Izvršitelj obrade** - znači svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

**Povreda osobnih podataka** - znači 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.

1. Načela obrade podataka

Pravilnik se temelji na sljedećim načelima, u skladu s čl. 5. Uredbe:

1. Načelo zakonitosti, poštenosti i transparentnosti - obrada osobnih podataka se mora temeljiti na jednog od pravnih osnova (privola, pravna obveza, legitimni interes, ugovor, javni interes, životno važni interesi ispitanika), a informacije koje se pružaju ispitaniku moraju biti sažete, transparente, razumljive i lako dostupne.
2. Načelo ograničavanje svrhe - osobni podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama.
3. Načelo smanjenja količine podataka - osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.
4. Načelo točnosti - osobni podaci moraju biti točni, potpuni, prema potrebi ažurirani te pravovremeno ispravljeni u slučaju promjena podataka. Mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave.
5. Načelo ograničenja pohrane - osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci koriste.
6. Načelo cjelovitosti i povjerljivosti - obrada podataka na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja kroz redovno testiranje i primjenu odgovarajućih tehničkih ili organizacijskih mjera.
7. Načelo pouzdanosti - Voditelj obrade je odgovoran za usklađenost Uredbom te je mora biti u mogućnosti dokazati.
8. Obrada osobnih podataka

Voditelj obrade obrađuje osobne podatke samo i u onoj mjeri ako je ispunjen jedan od sljedećih uvjeta:

1. ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
2. obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
3. obrada je nužna radi poštovanja pravnih obveza voditelja obrade
4. obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe
5. obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade
6. 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, osobito ako je ispitanik dijete
7. Svrha i opseg obrade osobnih podataka

${pzop\_02}

${pzop\_02\_item}

${/pzop\_02}

1. Pravni temelj za obradu osobnih podataka

${pzop\_03}

${pzop\_03\_item}

${/pzop\_03}

1. Razdoblje čuvanja osobnih podataka

Voditelj obrade osigurava da se podaci ispitanika čuvaju samo onoliko koliko je to nužno radi ispunjenja svrhe za koju su prikupljeni. Podaci za koje ne postoji pravni temelj za daljnju obradu i pohranu moraju se bez odgađanja obrisati.

${pzop\_04}

${pzop\_04\_item}

${/pzop\_04}

${pzop\_05}

1. Evidencija aktivnosti obrade

Voditelj obrade vodi Evidenciju aktivnosti obrade za osobne podatke ispitanika koje redovito obrađuje u okviru poslovnih aktivnosti. Evidencija se vodi u pisanom obliku, uključujući i elektronički oblik.

Evidencija sadržava sljedeće podatke:

* ime i kontakt podatke Voditelja obrade i službenika za zaštitu podataka
* pravne temelje
* svrhu obrade
* opis kategorije ispitanika i kategoriju osobnih podataka
* kategoriju primatelja
* ako je primjenjivo, prijenos osobnih podataka ispitanika u treće zemlje i mjere zaštite
* rokove za brisanje kategorije podataka
* opis tehničkih i organizacijskih mjera zaštite

${/pzop\_05}

1. Primatelji osobnih podataka

Voditelj obrade otkriva osobne podatke ispitanika ako to nalaže svrha obrade ili postoji pravna obveza, u kojem slučaju se osobni podaci otkrivaju drugim fizičkim ili pravnim osobama, tijelima javne vlasti, agencijama ili drugim tijelima.

${pzop\_06}

1. Osobe ovlaštene za obradu osobnih podataka

Osobe ovlaštene za obradu osobnih podataka određuje odgovorna osoba unutar Voditelja obrade, a određuju se s obzirom na radno mjesto i sukladno poslovnim procesima koje obavljaju.

${pzop\_07}

1. Tehničke i organizacijske mjere

Voditelj obrade poštuje privatnost i štiti osobne podatke svojih zaposlenika, poslovnih partnera, klijenata, a čije osobne podatke obrađuje u svom svakodnevnom poslovanju, u skladu s odredbama mjerodavnog prava.

Voditelj obrade će osigurati da se podaci ispitanika čuvaju samo onoliko dugo koliko je to nužno za ispunjenje svrhe za koju su prikupljeni.

Voditelj obrade provodi odgovarajuće tehničke i sigurnosne mjere zaštite koje za cilj imaju osigurati sigurnost i povjerljivost obrade osobnih podataka, odnosno sprečavanja neovlaštenog pristupa ili neovlaštenog raspolaganja osobnim podacima kao i tehničkoj opremi kojom se koristi Voditelj obrade.

Pohrana podataka se vrši pomoću mapa u informacijskom sustavu Voditelja obrade te se zaposlenicima dodjeljuje pristup ovisno o radnom mjestu.

Tehničke mjere koje primjenjuje Voditelj obrade:

${pzop\_08\_a}

* ${pzop\_08\_a\_item}

${/pzop\_08\_a}

Organizacijske mjere koje primjenjuje Voditelj obrade:

${pzop\_08\_b}

* ${pzop\_08\_b\_item}

${/pzop\_08\_b}

1. Procjena učinka na zaštitu podataka

Ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, Voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka.

Pri provođenju procjene učinka na zaštitu podataka Voditelj obrade traži savjet od službenika za zaštitu podataka.

Procjena učinka na zaštitu podataka obvezna je osobito u slučaju:

1. 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 koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca
2. opsežne obrade posebnih kategorija osobnih podataka iz članka 9. stavka 1. Uredbe ili podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10. Uredbe, ili
3. sustavnog praćenja javno dostupnog područja u velikoj mjeri.

${pzop\_9}

1. Obavijest o povredi osobnih podataka

U slučaju sigurnosnog incidenta, koji je u skladu s Uredbom povreda osobnih podataka, Voditelj obrade će provesti procjenu rizika bez nepotrebnog odgađanja te u skladu s procjenom poduzeti potrebne radnje i obavijestiti nadzorno tijelo i ispitanike.

U slučaju povrede osobnih podataka Voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo (Agenciju za zaštitu osobnih podataka), 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.

U slučaju izvješćivanja o povredama osobnih podataka, Voditelj obrade će koristiti obrazac Agencije za zaštitu osobnih podataka dostupan na: <https://azop.hr/izvjescivanje-o-povredi-osobnih-podataka/>.

Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti naprijed navedene informacije, informacije je moguće pružati bez nepotrebnog odgađanja.

Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući i činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete.

${pzop\_10}

1. Izvršitelji obrade

Osobne podatke Voditelj obrade prosljeđuje svojim izvršiteljima obrade kada je to nužno radi eksternalizacije određenog poslovnog procesa. Zaposlenici Voditelja obrade provode ispitivanje prilikom postupka odabira izvršitelja obrade i provjere imaju li izvršitelji obrade adekvatne kontrole za zaštitu podataka, uključujući odgovarajuće tehničke i organizacijske mjere za zaštitu podataka.

Voditelj obrade sa izvršiteljima obrade sklapa ugovor o obradi podataka kojim od njih traži pridržavanje primjenjivih politika Voditelja obrade, Zakona i Uredbe. Svaki ugovor o obradi podataka mora sadržavati obvezne podatke iz čl. 28. Uredbe. Voditelj obrade će prijenos osobnih podataka izvršiteljima obrade dopustiti samo ako se provedu odgovarajući postupci za osiguranje potrebne razine zaštite podataka.

${pzop\_11}

1. Prijenos osobnih podataka u treće zemlje

${pzop\_12\_a}

${pzop\_12\_b}

${pzop\_12\_c}

Na naše prijenose se primjenjuje:

${pzop\_12\_d}

* ${pzop\_12\_d\_item}

${/pzop\_12\_d}

1. Prava ispitanika

Voditelj obrade obrađuje osobne podatke ispitanika, uz poštovanje njihovih prava propisanih Uredbom.

Prava ispitanika su sljedeća:

1. **Pravo na brisanje („pravo na zaborav“)** - ispitanik ima pravo od Voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose, a Voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

* osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni,
* ispitanik povuče privolu na kojoj se obrada temelji, a ne postoji druga pravna osnova za obradu,
* ispitanik uloži prigovor na obradu, a legitimni razlozi za realizaciju prava na brisanje imaju veću težinu od legitimnog interesa Voditelja obrade za obradu i/ili čuvanje osobnih podataka,
* osobni podaci nezakonito su obrađeni,
* osobni podaci moraju se brisati radi poštovanja pravne obveze,
* osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva iz članka 8. stavka 1. Uredbe.

1. **Pravo na pristup podacima** - ispitanik ima pravo dobiti od Voditelja obrade potvrdu obrađuju li se njegovi osobni podaci te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i svrsi obrade, kategorijama podataka, potencijalnim primateljima kojima će osobni podaci biti otkriveni, u skladu s odredbama mjerodavnog prava.
2. **Pravo na ispravak** - ispitanik ima pravo ishoditi od Voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.
3. **Pravo na prigovor** - ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega.
4. **Pravo na ograničenje obrade** – ispitanik ima pravo od Voditelja obrade tražiti ograničenje obrade u slučaju da:
   * ispitanik osporava točnost osobnih podataka, na razdoblje kojim se voditelju obrade omogućuje provjera točnosti osobnih podataka,
   * je obrada nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe,
   * ako Voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva, ili
   * ako je ispitanik uložio prigovor na obradu očekujući potvrdu nadilaze li legitimni razlozi Voditelja obrade razloge ispitanika.
     1. **Pravo na prenosivost podataka** - ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada temelji na privoli, ili na ugovoru ili se provodi automatiziranim putem.

${pzop\_13}

* + 1. **Pravo na prigovor i automatizirano pojedinačno donošenje odluka** - ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega,, uključujući izradu profila koja se temelji na tim odredbama. Voditelj obrade više ne smije obrađivati osobne podatke osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva. Ako se osobni podaci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se odnose na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom. Ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati u takve svrhe. Najkasnije u trenutku prve komunikacije s ispitanikom, ispitaniku se izričito mora skrenuti pozornost na navedena prava te se to mora učiniti na jasan način i odvojeno od bilo koje druge informacije.
    2. **Ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila**, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu. Navedeno se ne primjenjuje ako je odluka:

|  |  |
| --- | --- |
|  | * potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka; |

|  |  |
| --- | --- |
|  | * dopuštena pravom Unije ili pravom države članice kojem podliježe voditelj obrade te koje također propisuje odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika; ili |

|  |  |
| --- | --- |
|  | * temeljena na izričitoj privoli ispitanika. |

${/pzop\_13}

* + 1. Uz navedeno, ispitanik ima **pravo podnijeti pritužbu nadležnom nadzornom tijelu** (u Republici Hrvatskoj - Agenciji za zaštitu osobnih podataka) te biti obavješten o primateljima ili kategorijama primatelja kojima su podaci bili ili će u budućnosti biti otkriveni, a posebno primateljima u trećim zemljama.

1. Ostvarivanje prava ispitanika

${pzop\_14\_a}

Voditelj obrade ispitaniku na zahtjev za ostvarenje prava iz toč. 13. pruža informacije bez nepotrebnog odgađanja i u svakom slučaju u roku od mjesec dana od dana zaprimanja zahtjeva.

${pzop\_14\_b}

Ako Voditelj obrade ne postupi po zahtjevu ispitanika, Voditelj obrade (zaposlenik zadužen za postupanje po zahtjevima ispitanika) bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvješćuje ispitanika o razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu (Agenciji za zaštitu osobnih podataka).

${pzop\_15\_a}

1. Službenik za zaštitu podataka

Radi usklađivanja i nadzora poslovanja Voditelja obrade u skladu s odredbama Uredbe, Voditelj obrade je imenovao službenika za zaštitu podataka ${pzop\_15\_b}. Podaci o službeniku za zaštitu podataka se prijavljuju Agenciji za zaštitu osobnih podataka putem online obrasca: <https://azop.hr/obrazac-za-imenovanje-sluzbenika-za-zastitu-podataka/> te službenik za zaštitu podataka komunicira s Agencijom u slučaju pitanja ili nadzora.

Službenik služi kao kontaktna točka za sve ispitanike te odgovara na zahtjeve ispitanika u skladu s Uredbom i procedurama Voditelja obrade.

Svi zaposlenici su dužni obavijestiti službenika za zaštitu podataka o bilo kakvoj povredi osobnih podataka te će službenik sudjelovati u procjeni rizika povrede te dati svoje mišljenje o riziku i mjerama.

Zaposlenici se obraćaju službeniku za zaštitu podataka u slučaju novih poslovnih suradnji, dvojbi oko obrade osobnih podataka pri čemu službenik provodi odgovarajuće analize legitimnog interesa i procjene učinka na zaštitu podataka, u skladu s odlukom Agencije za zaštitu osobnih podataka i Uredbom te provjeru tehničkih i organizacijskih mjera izvršitelja obrade, nadzor izvršitelja obrade te savjetovanje prilikom sastava ugovora o poslovnoj suradnji i ugovora o obradi podataka.

Službenik za zaštitu podataka također provjerava prijenose osobnih podataka u treće zemlje te predlaže odgovarajuće zaštitne mjere za prijenos podataka (npr. standardne ugovorne klauzule).

Službenik za zaštitu podataka dužan je svake godine napraviti plan edukacije zaposlenika Voditelja obrade te provesti ili dogovoriti redovnu edukaciju relevantnih zaposlenika barem jedan put godišnje na aktualnu temu iz zaštite podataka.

Voditelj obrade je dužan osigurati adekvatne resurse i edukaciju službeniku za zaštitu podataka radi obavljanja svojih zadaća u skladu s Uredbom.

Službenik za zaštitu podataka je dužan nadzirati usklađenost poslovanja Voditelja obrade s ovim Pravilnikom te barem jednom godišnje podnijeti upravi Voditelja obrade izvješće o statusu usklađenosti Voditelja obrade s Uredbom i poduzetim mjerama.

${/pzop\_15\_a}

1. Završne odredbe

Pravilnik stupa na snagu osam dana od dana potpisa te se objavljuje na oglasnoj ploči/internoj mreži Voditelja obrade.