Dom za odrasle osobe Jalžabet
Kolodvorska 1
42203 Jalžabet
OIB: 40551161324
Tel: 042 215 670
domjalzabet@gmail.com

GDPR-PRAVILNIK

Pravilnik o zaštiti osobnih podataka

Verzija 1.0

	Ime i prezime, funkcija	**Datum donošenja:**	**Potpis:**
Izradio:	mr. sc. Anica Ister Težak, dipl. Inf. Službenik za zaštitu podataka (DPO)	25.5.2018.	
Odobrio:	Silvija Šincek Humek, ravnateljica	25.5.2018.	

SADRŽAJ

1. UVOD

1.1. Područje primjene

Ovim Pravilnikom definiraju se pravila za zaštitu osobnih podataka koja se primjenjuju u svim obradama osobnih podataka koje provodi DOM ZA ODRASLE OSOBE JALŽABET, Kolodvorska 1, 42203 Jalžabet, OIB: 40551161324 (u daljnjem tekstu: Voditelj obrade).

1.2. Pojmovi i definicije

Opća uredba o zaštiti podataka (GDPR)

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

Zakon o provedbi Opće uredbe o zaštiti podataka

Zakon o provedbi Opće uredbe o zaštiti podataka (805) NN 42/2018 od 27. travnja 2018. godine.

Osobni podaci

svi podaci koji se odnose 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

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

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

fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;

Primatelj

fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke

u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;

Treća strana

fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;

Privola ispitanika

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

Povreda osobnih podataka

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;

Posebne kategorije podataka

Posebne kategorije osobnih podataka su:

- rasno ili etničko podrijetlo;
- politička mišljenja;
- vjerska ili filozofska uvjerenja;
- članstvo u sindikatu;
- genetski ili biometrijski podaci u svrhu identifikacije pojedinca;
- podaci o zdravlju, spolnom životu ili seksualnoj orijentaciji pojedinca.

Obrada takvih podataka je dozvoljena isključivo ako je ispitanik dao izričitu privolu ili ako je obrada nužna zbog zaštita interesa ispitanika ili zbog javnog interesa.

Nadzorno tijelo

Nadzorno tijelo u smislu odredbe članka 51. Opće uredbe o zaštiti podataka je Agencija za zaštitu osobnih podataka (AZOP).

1.3. Referentni dokumenti

- Opća uredba o zaštiti podataka (GDPR) UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. godine
- Zakon o provedbi Opće uredbe o zaštiti podataka (805) NN 42/2018 od 27. travnja 2018. godine
- Opća politika zaštite osobnih podataka
- Evidencija aktivnosti obrada osobnih podataka
- Procedura za obradu zahtjeva u vezi osobnih podataka
- Procedura za postupanje u slučaju povrede osobnih podataka
- Procedura za provedbu redovite provjere usklađenosti
- Izjava o povjerljivosti i postupanju u slučaju povrede osobnih podataka

- Odluka o imenovanju osoba odgovornih za obradu osobnih podataka

2. PRAVILA

2.1. Opća pravila

Voditelj obrade se pridržava općih pravila vezano uz zaštitu osobnih podataka koja su definirana Općom uredbom o zaštiti podataka i Zakonom o provedbi Opće uredbe o zaštiti podataka. Voditelj obrade je donio Opću politike zaštite osobnih podataka koja je javno objavljena.

Za uspostavu sustava u kojem će postupanje s osobnim podacima biti zakonito i sigurno, provedeno je slijedeće:

- izrađena je potrebna dokumentacija sustava zaštite podataka,
- analizirani su rizici i poduzete potrebne mjere zaštite,
- definirani su načini postupanja u radu s osobnim podacima,
- poduzete su odgovarajuće organizacijske i tehničke mjere zaštite osobnih podataka,
- donesena je odluka o imenovanju osoba odgovornih za obradu osobnih podataka,
- imenovan je službenika za zaštitu podataka,
- obavljena je edukacija zaposlenika.

2.2. Načela obrade osobnih podataka

Osobni podaci obrađuju se isključivo u skladu s Općom uredbom o zaštiti podataka. Prema tome, osobni podaci moraju biti (Članak 5. Uredbe):

(a) zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika („zakonitost, poštenosti transparentnost”);
(b) prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 89. stavkom 1. ne smatra se neusklađenom s prvotnim svrhama („ograničavanje svrhe”);
(c) primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka”);
(d) točni i prema potrebi ažurni; 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 („točnost”);
(e) čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti 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 u skladu s člankom 89. stavkom 1., što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih ovom Uredbom radi zaštite prava i sloboda ispitanika („ograničenje pohrane”);
(f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („cjelovitost i povjerljivost”);

2.3. Zakonitost obrade

Posebnu pažnju potrebno je posvetiti zakonitosti obrade. Obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega (Članak 6. Uredbe):

(a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
(b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
(c) obrada je nužna radi poštovanja pravnih obveza Voditelja obrade;
(d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
(e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti Voditelja obrade;
(f) 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.

Voditelj obrade će za obradu osobnih podataka tražiti privolu ispitanika samo u onim slučajevima kada ne postoji neka druga osnova za zakonitost obrade podataka. Ispitanik ima pravo u svakom trenutku povući privolu.

2.4. Prava ispitanika

Voditelj obrade u svom redovnom poslovanju omogućava Ispitanicima ostvarenje svih njihovih prava vezanih uz obradu osobnih podataka. Osim toga, Ispitanik može podnijeti zahtjev za ostvarivanje prava Voditelju obrade ili ga dostaviti na e-mail adresu Službenika za zaštitu podatka info@expera.hr.

Prava ispitanika obuhvaćaju:

Pravo na pristup - Ispitanik ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega, te mu se mora omogućiti pristup njegovim osobnim podacima.

Pravo na ispravak - Ispitanik ima pravo bez nepotrebnog odgađanja 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.

Pravo na brisanje („pravo na zaborav“) - Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose, te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja, osim ako postoji opravdani razlog (npr. pravna obveza voditelja obrade)

Pravo na ograničenje obrade - Ispitanik ima pravo od voditelja obrade ishoditi ograničenje obrade ako su ispunjeni uvjeti iz Članka 18. Uredbe.

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.

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, u skladu s člankom 6. stavkom 1. točkom (e) ili (f), uključujući izradu profila koja se temelji na tim odredbama (vidi Zakonitost obrade).

Automatizirano pojedinačno donošenje odluka, uključujući izradu profila - 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.

3. POSTUPANJE

3.1. Evidencija aktivnosti obrada

Prilikom usklađivanja sustava s Uredbom uspostavljena je Evidencija aktivnost obrada osobnih podataka. Ta evidencija sadrži slijedeće informacije:

- podaci o Voditelju/izvršitelju obrade i službeniku za zaštitu podataka,
- odgovorna osoba Voditelja obrade,
- svrha obrade,
- opis kategorija ispitanika i kategorija osobnih podataka,
- kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni,
- ako je moguće, predviđene rokove za brisanje različitih kategorija podataka,
- ako je moguće, opis tehničkih i organizacijskih sigurnosnih mjera.

U slučaju da se pojavi potreba i pojavi neka nova aktivnost obrade osobnih podataka, potrebno je prije pokretanja procesa obrade samu obradu evidentirati i napraviti sve potrebne mjere da bi postupanje s osobnim podacima bilo zakonito i sigurno.

Uspostavljen sustav potrebno je održavati pa su predviđene redovite provjere usklađenosti.

3.2. Evidencija privola

Za obrade podataka za koje ne postoje osnove za obradu iz stavaka (b), (c), (d), (e) i (f) iz točke 2.3. Pravilnika, Voditelj obrade će prikupljati privole ispitanika i postupati s njima u skladu s Općom uredbom o zaštiti podataka.

3.3. Upravljanje zahtjevima ispitanika

Svaki ispitanik može zatražiti i ostvariti svoja prava kod Voditelja obrade, a postupanje sa zahtjevima ispitanika opisano je u Proceduri za obradu zahtjeva vezanih za osobne podatke. Svi zahtjevi evidentiraju se u Evidenciji zahtjeva u vezi osobnih podataka.

3.4. Upravljanje povredama/incidentima u vezi osobnih podataka

Cilj svih poduzetih mjera vezanih uz zakonitost i sigurnost obrade osobnih podataka je izbjegavanje povreda/incidenata. U slučaju da se takav neželjeni događaj ipak dogodi, postupanje u slučaju povrede/incidenta u vezi osobnih podataka opisano je u Proceduri za postupanje u slučaju povrede osobnih podataka. Sve eventualne povrede evidentiraju se u Evidenciji povreda osobnih podataka, te se prema potrebi izvješćuju ispitanici i/ili nadzorno tijelo.

Izvješćivanje nadzornog tijela

> 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 nadležno u skladu s člankom 55. o povredi 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.

Izvješćivanje Ispitanika

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, Voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka. Obavješćivanje ispitanika nije obvezno ako je Voditelj obrade poduzeo mjere kojima se osigurava da nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika.

3.5. Provođenje kontrole i nadzora u procesima obrade osobnih podataka

Sva postupanja vezana uz obradu osobnih podataka moraju biti u skladu s propisanim pravilima i procedurama. U slučaju promjena u organizaciji ili zakonskoj regulativi, sustav je potrebno odmah uskladiti s novonastalim promjenama. Da bi se osiguralo trajna usklađenost sustava, propisane su redovite provjere usklađenosti koje se provode u skladu s Procedurom za provedbu redovite provjere usklađenosti.

3.6. Organizacijske i tehničke mjere zaštite osobnih podataka

Da bi se izbjegao neovlašteni pristup osobnim podacima, podaci u pisanom obliku čuvaju se u registratorima, u zaključanim ormarima, u prostorijama koje se zaključavaju i kojima imaju pristup samo ovlaštene osobe.

Pristup osobnim podacima koji su pohranjeni u elektroničkom obliku dozvoljen je samo ovlaštenim osobama uz korištenje korisničkog imena i lozinke. Redovito, najmanje jednom tjedno, izrađuje se zaštitna kopija podataka koja se sigurno pohranjuje na drugoj lokaciji. Voditelj obrade obvezuje se imenovati osobu zaduženu za izradu zaštite podataka.

Na serveru i svim računalima instaliran je antivirusni program koji se redovito obnavlja. Svi radnici koji u radu koriste računala upoznati su sa osnovama sigurnog rada na računalima, obvezom da se ne otvaraju e-mail poruke nepoznatih pošiljatelja i sumnjivog sadržaja, i obvezom da se koristi samo licencirani softver koji odobri nadležna osoba Voditelja obrade.

3.7. Kontrola nadzornog tijela

U slučaju kontrole od strane nadzornog tijela (AZOP – Agencija za zaštitu osobnih podataka) daju im se na uvid sve tražene informacije vezane uz postupanje u vezi s Općom uredbom o zaštiti podataka. Službenik za zaštitu podataka ima obvezu suradnje s nadzornim tijelom i radi na rješavanju svih eventualnih problema.

4. DUŽNOSTI I ODGOVORNOSTI

4.1. Voditelj obrade

Voditelj obrade dužan je poduzimati tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka koje su potrebne da bi se osobni podaci zaštitili od slučajnog gubitka ili uništenja, kao i od neovlaštenog pristupa, nedopuštene promjene, nedopuštenog objavljivanja i svake drugo zloupotrebe, te utvrditi obvezu osoba koje provode obradu osobnih podataka, na čuvanje tajnosti podataka odnosno potpisivanje Izjave o povjerljivosti.

Voditelj obrade obvezuje se, vezano uz obradu osobnih podataka, koristiti usluge provjerenih dobavljača koji su se također obvezali na poduzimanje adekvatnih mjera zaštite osobnih podataka, uključujući i potpisivanje izjave o povjerljivosti za zaposlenike dobavljača koji na bilo koji način obrađuju ili mogu pristupiti podacima Voditelja obrade.

Voditelj obrade će:

- pružiti aktivnu potporu visokog rukovodstva službeniku za zaštitu podataka;
- omogućiti službeniku za zaštitu podataka nužan pristup ostalim službama, kao što su ljudski resursi, pravna služba, informacijske tehnologije, sigurnost, itd., kako bi službenik za zaštitu podataka od tih službi dobio neophodnu potporu, doprinos i informacije;
- informirati službenika za zaštitu podataka o svim promjenama u organizaciji koje bi mogle imati utjecaj na zaštitu osobnih podataka.

Voditelj obrade donosi Odluku o imenovanju osoba zaduženih za obradu i zaštitu svih osobnih podataka koji se obrađuju i postupanje vezano uz ostvarivanje prava ispitanika iz točki 3.1., 3.2. i 3.3. ovog Pravilnika.

4.2. Izvršitelj obrade

Obrade osobnih podataka koje provodi Izvršitelj obrade uređuju se ugovorom između Voditelja obrade i Izvršitelja obrade. U ugovoru su definirane obrade koje provodi Izvršitelj obrade, svrha obrade i trajanje obrade, te obveze i prava Izvršitelja obrade i Voditelja obrade.

Izvršitelj obrade u ugovoru jamči provedbu odgovarajućih tehničkih i organizacijskih mjera zaštite podataka.

4.3. Službenik za zaštitu osobnih podataka

Službenik za zaštitu podataka obavlja slijedeće zadaće:

- usklađivanje dokumentacije vezane uz Uredbu s novonastalim promjenama u organizaciji ili zakonskoj regulativi;
- informiranje i savjetovanje Voditelja/izvršitelja obrade o njihovoj obvezi vezano uz Uredbu;
- nadziranje da postupanje sa osobnim podacima bude u skladu s Uredbom;
- dizanje razine svijesti i podučavanje o značaju zaštite osobnih podataka;
- pružanje savjeta vezano uz procjenu rizika na zaštitu osobnih podataka;
- po potrebi suradnja sa nadzornim tijelom za zaštitu osobnih podataka (AZOP).

Službenik za zaštitu podataka dužan je čuvati povjerljivost svih informacija koje sazna u obavljanju svoje dužnosti. Kontakt podaci službenika za zaštitu podataka objavljeni su na web stranici Voditelja obrade.

4.4. Ostali zaposlenici

Svi zaposlenici Voditelja obrade dužni su u svom djelokrugu rada i odgovornosti postupati u skladu s ovim Pravilnikom i potpisanoj Izjavi o povjerljivosti i postupanju u slučaju povrede osobnih podataka.

Svaku novost ili promjenu u načinu postupanja s osobnim podacima, dužni su odmah po saznanju prijaviti nadređenoj osobi i/ili službeniku za zaštitu podataka. Nije dozvoljeno uvoditi bilo kakvu novu obradu osobnih podataka bez da se ta obrada prethodno evidentira u Evidenciju aktivnosti obrada osobnih podataka, te poduzmu sve predviđene sigurnosne mjere za tu obradu.

5. ZAVRŠNE ODREDBE

Ovaj Pravilnik stupa na snagu danom donošenja i bit će objavljen na oglasnoj ploči Voditelja obrade.

6. POVIJEST VERZIJA

POVIJEST VERZIJA				
Verzija	Datum donošenja	Izradio	Odobrio	Opis
1.0	25.5.2018.	Anica Ister Težak		Početna verzija izrađena prilikom usklađivanja s Uredbom.