

**PRAVNE PREPORUKE ZA
UGOVORE KOJI SE POTPISUJU S
IZVRŠITELJIMA OBRADE**

Zagreb, ožujak 2018.

SADRŽAJ

UVOD.....	3
SADRŽAJ UGOVORA O OBRADI PODATAKA.....	4
ODREDBA OPĆE UREDBE O ZAŠTITI PODATAKA.....	5
UGOVOR O ZAŠTITI PODATAKA.....	7
PRIJEDLOG DODATKA ZA ZAŠTITU OSOBNIH PODATAKA	8
ZAKLJUČAK.....	13
Dodatak 1 – Odredbe Opće uredbe o zaštiti podataka Europske unije	14
A. Definicije.....	14
B. Uloge i opseg	14
C. Relevantne obveze koje proizlaze iz GDPR-a: članci 28, 32 i 33.....	14
Dodatak 2 – Dodatne Odredbe GDPR-a - PODIZVOĐAČI	16
A. Podizvođači.....	16
B. Pomoć voditelju obrade za odgovore na zahtjeve ispitanika.....	16
C. Obrada osobnih podataka	17
D. Sigurnost.....	17
E. Povreda Osobnih podataka	17
F. Evidencija aktivnosti obrade	17
G. Izmjene, dopune i trajanje.....	17

UVOD

Stupanjem na snagu Uredbe (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 (Opća uredba o zaštiti podataka) – (u daljnjem tekstu: GDPR), potrebno je uskladiti i poslovanje tvrtke te između svega ostalog uskladiti i postojeće ugovore kako bi bili sukladni GDPR-u.

Obveza voditelja obrade je da radi samo s izvršiteljima obrade koji osiguravaju dovoljne garancije vezane uz zaštitu osobnih podataka.

Prema GDPR-u, voditelj obrade može raditi samo s izvršiteljima obrade koji pružaju "dovoljno jamstva za provođenje odgovarajućih tehničkih i organizacijskih mjera na takav način da će obrada ispuniti zahtjeve GDPR-a i osigurati zaštitu prava nositelja podataka. " Preambula propisuje da se jamstva koja se pružaju odnose na stručno znanje, pouzdanost i resurse.

Ova je obveza vrlo striktna i zahtijeva od voditelja obrade detaljnu procjenu sposobnosti svakog izvršitelja obrade, uključujući njegovu financijsku stabilnost. Isto tako, obveza je voditelja obrade da sklopi ugovor o obradi podataka.

Voditelji obrade dužni su sklopiti pisani ugovor ili drugi obvezujući pravni akt prema zakonu EU ili država članica, sa svakim izvršiteljem obrade.

SADRŽAJ UGOVORA O OBRADI PODATAKA

Ugovor ili drugi pravni akt mora sadržavati predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka koji se obrađuju, kategorije nositelja podataka te obveze i prava voditelja obrade.

Konkretno, mora se propisati da će izvršitelj obrade:

- obrađivati osobne podatke samo uz dokumentirane upute voditelja obrade, uključujući prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama, osim ako zakonom EU ili države članice na koju izvršitelj obrade podliježe drugačije ne određuje;
- osigurati da se osobe ovlaštene za obradu osobnih podataka obvezuju ugovorom o čuvanju tajnosti;
- poduzeti sve odgovarajuće tehničke i organizacijske mjere;
- dobiti pismenu suglasnost voditelja obrade za uključivanje podizvršitelja;
- ugovorom obvezati podizvršitelje da se osigurava zaštita podataka;
- uzimajući u obzir prirodu obrade, pomagati voditelju obrade poduzimajući odgovarajuće tehničke i organizacijske mjere kako bi što više osiguralo ispunjavanje obveza voditelja obrade da odgovori na zahtjeve ispitanika koji ostvaruju svoja prava;
- pomažu voditelju obrade u osiguravanju poštivanja svoje sigurnosti i određenih drugih obveza, uzimajući u obzir prirodu obrade i informacije dostupne izvršitelju obrade;
- po izboru voditelja obrade, brisanje ili vraćanje svih osobnih podataka voditelju po završetku usluga obrade i vraćanje postojećih kopija podataka, osim ako zakonodavstvo EU ili RH ne zahtijeva pohranu osobnih podataka;
- staviti na raspolaganje voditelju sve informacije potrebne za dokazivanje sukladnosti sa svojim obvezama i omogućiti i surađivati u cijelosti s revizijama koje provodi voditelj obrade ili druga osoba koju je za to ovlastio voditelj obrade.

Ugovor o obradi podataka može se temeljiti na standardnim ugovornim odredbama koje je odredila Europska komisija ili nacionalna nadzorna tijela. Iz navedenog mora biti jasno da su obvezne odredbe koje treba uključiti u sporazum o obradi podataka brojnije i značajnije u okviru GDPR-a nego prema Direktivi 95/46 / EZ. Razlog tome je da je voditelj obrade u

konačnici odgovoran ne samo za osobne podatke koji se obrađuju, već i za strane koji obrađuju podatke u njegovo ime.

Slijedom navedenog potrebno je izmijeniti postojeće ugovore o obradi podataka ili zaključiti nove, odnosno izraditi dodatak ugovorima o obradi podataka, postavljajući minimalne sigurnosne zahtjeve.

Ovo nije samo zbog popisa minimalnih sadržaja ugovora o obradi podataka koji je izričito predviđen člankom 28. Uredbe, već i zbog toga što GDPR daje niz obveza prema izvršiteljima obrade koji moraju biti adekvatno regulirani u ugovoru o obradi podataka.

Temeljem navedenog potrebno je:

- prilagoditi ugovor o obradi podataka sukladno poslovanju izvršitelja obrade;
- osigurati popis za provjeru kako bi se ocijenila razina usklađenosti dobavljača s Uredbom, uključujući primjerenost tehničkih zahtjeva za ispunjavanje standarda koje propisuje Uredba;
- propisati postupak za prijavu povreda osobnih podataka na obrascima kako bi se osiguralo da se informacije pravovremeno šalju nadzornom tijelu te se na taj način minimalizirali negativni učinci povreda osobnih podataka.

Preporuka je da se postojeći ugovori aneksiraju odredbama vezanim uz zaštitu osobnih podataka ili da se potpiše Dodatak za zaštitu osobnih podataka koji se odnosi na članak 28. GDPR-a čiji prijedlog je sastavni dio ovih preporuka.

ODREDBA OPĆE UREDBE O ZAŠTITI PODATAKA

Članak 28.

Izvršitelj obrade

1. Ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika.

2. Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade. U slučaju općeg pisanog odobrenja, izvršitelj obrade obavješćuje voditelja obrade o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom drugih izvršitelja obrade kako bi time voditelju obrade omogućio da uloži prigovor na takve izmjene.

3. *Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. Tim se ugovorom ili drugim pravnim aktom osobito određuje da izvršitelj obrade:*

- (a) obrađuje osobne podatke samo prema zabilježenim uputama voditelja obrade, među ostalim s obzirom na prijenose osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, osim ako to nalaže pravo Unije ili pravo države članice kojem podliježe izvršitelj obrade; u tom slučaju izvršitelj obrade izvješćuje voditelja obrade o tom pravnom zahtjevu prije obrade, osim ako se tim pravom zabranjuje takvo izvješćivanje zbog važnih razloga od javnog interesa;*
- (b) osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim obvezama o povjerljivosti;*
- (c) poduzima sve potrebne mjere u skladu s člankom 32.;*
- (d) poštuje uvjete iz stavaka 2. i 4. za angažiranje drugog izvršitelja obrade;*
- (e) uzimajući u obzir prirodu obrade, pomaže voditelju obrade putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika koja su utvrđena u poglavlju III.;*
- (f) pomaže voditelju obrade u osiguravanju usklađenosti s obvezama u skladu s člancima od 32. do 36., uzimajući u obzir prirodu obrade i informacije koje su dostupne izvršitelju obrade;*
- (g) po izboru voditelja, briše ili vraća voditelju obrade sve osobne podatke nakon dovršetka pružanja usluga vezanih za obradu te briše postojeće kopije osim ako sukladno pravu Unije ili pravu države članice postoji obveza pohrane osobnih podataka;*
- (h) voditelju obrade stavlja na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obveza utvrđenih u ovom članku i koje omogućuju revizije, uključujući inspekcije, koje provodi voditelj obrade ili drugi revizor kojeg je ovlastio voditelj obrade, te im doprinose.*

U pogledu točke (h) prvog podstavka, izvršitelj obrade odmah obavješćuje voditelja obrade ako prema njegovu mišljenju određena uputa krši ovu Uredbu ili druge odredbe Unije ili države članice o zaštiti podataka.

4. *Ako izvršitelj obrade angažira drugog izvršitelja obrade za provođenje posebnih aktivnosti obrade u ime voditelja obrade, iste obveze za zaštitu podataka kao one koje su navedene u ugovoru ili drugom pravnom aktu između voditelja obrade i izvršitelja obrade iz stavka 3. nameću se tom drugom izvršitelju obrade ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, a osobito obveza davanja dostatnih jamstava za provedbu odgovarajućih tehničkih i organizacijskih mjera na način da se obradom udovoljava zahtjevima iz ove Uredbe. Ako taj drugi izvršitelj obrade ne ispunjava obveze zaštite podataka, početni izvršitelj obrade ostaje u cijelosti odgovoran voditelju obrade za izvršavanje obveza tog drugog izvršitelja obrade.*

5. *Poštovanje od strane izvršitelja obrade odobrenih kodeksa ponašanja iz članka 40. ili odobrenog mehanizma certificiranja iz članka 42. može se koristiti kao element za dokazivanje pružanja dovoljnih jamstava iz stavaka 1. i 4. ovog članka.*

6. *Ne dovodeći u pitanje pojedinačni ugovor između voditelja obrade i izvršitelja obrade, ugovor ili drugi pravni akt iz stavaka 3. i 4. ovog članka može se temeljiti, u cijelosti ili*

djelomično, na standardnim ugovornim klauzulama iz stavaka 7. i 8. ovog članka, među ostalim klauzulama koje su dio certifikata dodijeljenog voditelju obrade ili izvršitelju obrade u skladu s člancima 42. i 43.

7. Komisija može utvrditi standardne ugovorne klauzule za pitanja iz stavka 3. i 4. ovog članka, a u skladu s postupkom ispitivanja iz članka 93. stavka 2.

8. Nadzorno tijelo može donijeti standardne ugovorne klauzule za pitanja iz stavka 3. i 4. ovog članka, a u skladu s mehanizmom za usklađivanje iz članka 63.

9. Ugovor ili drugi pravni akt iz stavaka 3. i 4. mora biti upisanom obliku, uključujući elektronički oblik.

10. Ne dovodeći u pitanje članke 82., 83. i 84., ako izvršitelj obrade krši ovu Uredbu utvrđivanjem svrhe i načine obrade podataka, izvršitelj obrade smatra se voditeljem obrade u pogledu te obrade.

UGOVOR O ZAŠTITI PODATAKA

Ako izvršitelj obrade obavlja obradu u ime voditelja obrade, treba postojati ugovor u pisanom obliku između dviju stranaka koji uključuje, najmanje, dvije sljedeće odredbe:

- Izvršitelj obrade mora postupati samo prema uputama voditelja obrade.
- Izvršitelj obrade mora koristiti odgovarajuće tehničke i organizacijske mjere za sprječavanje neovlaštene ili nezakonite obrade podataka, te slučajnog gubitka ili oštećenja podataka

Treba postojati pisani ugovor kad izvršitelj obrade obrađuje osobne podatke u ime voditelja obrade, ali klauzulu koja se odnosi na zaštitu podataka može (ako se tvrtke samo žele pridržavati apsolutnog minimalnog zakonskog zahtjeva) biti vrlo kratka i jednostavna.

Standardni ugovor trebao bi sadržavati sljedeće odredbe:

- Sažetak sadržaja podataka
- Duljinu vremena trajanja obrade
- Prirodu i svrhu obrade
- Vrstu osobnih podataka koji će se obrađivati
- Kategorije Ispitanika čiji će se osobni podaci obrađivati
- Izjava o pravima i obvezama voditelja obrade
- Izvršitelj obrade mora djelovati samo prema dokumentiranim uputama voditelja obrade
- Svi zaposlenici izvršitelja obrade koji pristupaju podacima moraju biti podložni odgovarajućim obvezama povjerljivosti
- Izvršitelj obrade će udovoljiti zahtjevima u GDPR u pogledu sigurnosnih mjera i enkripcije

- Izvršitelj obrade mora pomagati voditelju obrade u rješavanju zahtjeva ispitanika koji se odnose na povrede osobnih podataka i provođenjem procjene utjecaja
- Izvršitelj obrade mora izbrisati ili vratiti (po izboru voditelja obrade) sve osobne podatke na kraju ugovora ili kada prestane potreba za obradom
- Izvršitelj obrade mora pružiti sve podatke koje traži voditelj obrade kako bi se dokazala sukladnost s GDPR i dopustiti voditelju obrade da provede reviziju i provjerava sukladnost izvršitelja obrade
- Izvršitelj obrade ne smije prenijeti proces obrade podizvođaču bez pisane suglasnosti voditelja obrade (a zatim samo na temelju pisanog ugovora koji sadrži slične pojmove na gore navedenom popisu)

Osim navedenog, voditelju obrade dopušteno je samo sklapanje ugovora s izvršiteljima obrade koji osiguravaju dovoljna jamstva za provođenje odgovarajućih tehničkih i organizacijskih mjera kako bi se ispunili zahtjevi GDPR-a i zaštitila prava nositelja podataka.

PRIJEDLOG DODATKA ZA ZAŠTITU OSOBNIH PODATAKA

PRIJEDLOG DODATKA ZA ZAŠTITU OSOBNIH PODATAKAK KOJI SE ODNOSI NA ČLANAK 28. GDPR-a (UVJETI IZVRŠITELJA OBRADE) I UGRADIVANJE STANDARDNIH UGOVORNIH KLAUZULA

Nova Uredba EU-a o zaštiti podataka 2016/679 između ostalog nameće stroge zahtjeve za imenovanje izvršitelja obrade od strane voditelja obrade, uključujući propisivanje različitih pitanja koja moraju biti određena ugovorom ili drugim pravnim aktom (članak 28.).

Ovaj predložak ugovora je prijedlog usklađivanja.

VAŽNA NAPOMENA: Ovaj predložak i komentar koji se nalazi u njemu su prijedlozi elemenata ugovora te se mogu usklađivati s obzirom na okolnosti svakog pojedinog ugovornog odnosa. GDPR je složeno zakonodavstvo koje je otvoreno za dodatna tumačenja. Trenutno postoje vrlo ograničene smjernice i komentari članka 28. GDPR-a. Preporuča se da tvrtka traži pravni savjet vezano za ponovno sklapanje ugovora s izvršiteljima obrade / voditeljima obrade.

Ovaj Dodatak za zaštitu podataka ("Dodatak") čini dio _____ ("Glavni ugovor") između: (i) _____ ("Naručitelja"), i (_____ ("Ponuditelja")

Pojmovi korišteni u ovoj Dodatku imaju značenja navedena u ovom Dodatku. Pojmovi s velikim slovom koji nisu drugačije definirani ovdje imaju značenje koje im se daje u glavnom ugovoru i značenje koje im daje GDPR. Osim dolje izmijenjenih i dodanih odredbi, uvjeti

Glavnog ugovora ostat će i dalje na snazi.

Uzimajući u obzir uzajamne obveze navedene u ovom Ugovoru, stranke su suglasne da će se dodatni uvjeti i odredbe dodati kao Dodatak glavnom ugovoru.

1. Definicije

1.1 U ovom Dodatku, sljedeći pojmovi imaju značenja navedena u nastavku, a identični izrazi će se tumačiti u skladu s tim:

1.1.1 "Primjenjivi zakoni" su: (a) zakoni Europske unije ili RH u odnosu na bilo koje osobne podatke Naručitelja za koje podliježe zakonima o zaštiti podataka

1.1.2. "Osobni podaci tvrtke" su svi osobni podaci obrađivani s ugovorenim izvršiteljem obrade u vezi s glavnim ugovorom;

1.1.3 "Ugovoreni izvršitelj obrade" znači ponuditelj ili podizvođač;

1.1.4. "Zakoni o zaštiti podataka" označavaju zakone o zaštiti podataka Europske unije i, u mjeri u kojoj su primjenjivi, zakon o zaštiti podataka RH, uključujući i GDPR i propise koji primjenjuju ili dopunjuju GDPR ;

1.1.5 "GDPR" označava Uredbu EU za zaštitu podataka od 2016/679;

1.1.6 "Usluge" podrazumijevaju usluge i druge aktivnosti koje će ponuditelj dostaviti ili ih provoditi u skladu s Glavnim ugovorom;

1.1.7 "Podizvršitelj" označava svaku osobu koje imenuje Ponuditelj ili bilo koji dobavljač u procesu obrade osobnih podataka Naručitelja u vezi s glavnim ugovorom.

2. Obrada osobnih podataka

2.1 Ponuditelj i svaki podizvršitelj ponuditelja dužni su:

2.1.1 pridržavati se svih važećih propisa o zaštiti podataka u obradi osobnih podataka Naručitelja; i

2.1.2 ne obrađivati osobne podatke osim onih definiranih u dokumentiranim uputama Naručitelja

2.2 U Prilogu 1. ovog Dodatka navode se određene informacije o obrađivanju osobnih podataka u skladu s člankom 28. stavkom 3. GDPR-a (i eventualno jednakim zahtjevima drugih zakona o zaštiti podataka). Naručitelj može razumno izmijeniti Dodatak 1 pisanom obavijesti Ponuditelju kada je to opravdano neophodno za ispunjavanje ugovornih obveza.

3. Ponuditelj

Ponuditelj će poduzeti sve razumne korake kako bi osigurao pouzdanost bilo kojeg zaposlenika, ili bilo kojeg Ugovorenog podizvršitelja koji može imati pristup osobnim podacima tvrtke, osiguravajući u svakom slučaju da je pristup strogo ograničen na one pojedince koji trebaju pristupiti relevantnim osobnim podacima Naručitelja, koji su neophodni za potrebe Glavnog sporazuma.

4. Sigurnost

4.1 Uzimajući u obzir stanje tehnike, troškove provedbe, prirodu, opseg, kontekst i svrhe obrade, kao i rizik od vjerojatnosti i ozbiljnosti za povredu prava i slobode fizičkih osoba, Ponuditelj i svaki podizvođač u vezi s osobnim podacima Naručitelja treba poduzeti odgovarajuće tehničke i organizacijske mjere kako bi se osigurala razina sigurnosti koja odgovara tom riziku, uključujući, prema potrebi, mjere iz članka 32. stavka 1. GDPR-a.

4.2 Pri procjeni odgovarajuće razine sigurnosti, dobavljač i svaki dobavljač partnera moraju posebno uzeti u obzir rizike koje predstavlja obrada.

5. Podizvršitelj

5.1 Naručitelj ovlašćuje Ponuditelja da imenuje Podizvršitelja u skladu s ovim Dodatkom ugovora i u skladu s Glavnim ugovorom.

5.2 Ponuditelj može nastaviti koristiti one podizvršitelje koji su već angažirani s njihove strane.

5.3. Ponuditelj je dužan Naručitelja prethodno pismeno obavijestiti o imenovanju bilo kojeg novog podizvršitelja, uključujući i sve pojedinosti obrade koje će poduzeti Podizvršitelj.

6. Prava ispitanika

6.1 Uzimajući u obzir prirodu obrade, Naručitelj i svaki podizvršitelj pomažu u provođenju odgovarajućih tehničkih i organizacijskih mjera, u mjeri u kojoj je to moguće, za ispunjavanje obveza nad zaštitom osobnih podataka.

6.2 Ponuditelj je dužan odmah obavijestiti Naručitelja ako bilo koji ugovoreni izvršitelj obrade primi zahtjev od ispitanika u skladu sa Zakonom o zaštiti podataka u odnosu na osobne podatke Naručitelja.

7. Povreda osobnih podataka

Ponuditelj će bez odgode obavijestiti Naručitelja o povredi osobnih podataka koja utječe na osobne podatke Naručitelja, pružajući Naručitelju dovoljno informacija kako bi se mogle ispuniti sve obveze obavješćivanja o povredi osobnih podataka.

8. Procjena utjecaja na zaštitu podataka i prethodna konzultacija

Naručitelj treba pružiti pomoć ponuditelju vezano uz procjene utjecaja na zaštitu podataka, te prethodne konzultacije s nadzornim tijelima ili drugim nadležnim tijelima za zaštitu podataka, koje Naručitelj smatra potrebnim prema članku 35. ili 36. GDPR-a ili ekvivalentne odredbe bilo kojeg drugog Zakona o zaštiti podataka, u svakom slučaju isključivo u vezi s obradom osobnih podataka Naručitelja.

9. Brisanje ili vraćanje osobnih podataka tvrtke

9.1 U skladu s odjeljcima 9.2 i 9.3, Ponuditelj će odmah i u svakom slučaju u roku od [] datuma prestanka ugovora koje uključuju obradu osobnih podataka Naručitelja ("datum prestanka"), brisati i osigurati brisanje svih kopija tih osobnih podataka Naručitelja.

9.2 Naručitelj može, u skladu s odredbama odjeljka 9.3., pismeno obavijestiti Naručitelja o datumu prestanka i zahtijevati od Ponuditelja da:

- (a) vrati potpunu kopiju svih osobnih podataka Naručitelja; i
- (b) brisati i osigurati brisanje svih ostalih kopija osobnih podataka tvrtke koje je obrađivao bilo koji ugovoreni izvršitelj obrade.

9.3 Svaki Ugovoreni Izvršitelj obrade može zadržati osobne podatke Naručitelja u onoj mjeri koja je propisana primjenjivim zakonima, i to samo u mjeri i za razdoblje koje je propisano primjenjivim zakonima i uvijek pod uvjetom da će osigurati povjerljivost svih takvih osobnih podataka Naručitelja.

10. Pravo na reviziju

Ponuditelj je dužan Naručitelju staviti na raspolaganje sve informacije potrebne za dokazivanje sukladnosti s ovim Dodatkom, te omogućiti reviziju.

11. Ostale odredbe

Ako bilo koja odredba ovog Dodatka bude nevažeća ili neprovediva, ostatak ovog Dodatka ostaje na snazi. Neispravna ili neprovediva odredba bit će izmijenjena kako bi se osigurala njezina valjanost i provedivost, ili, ako to nije moguće, tumačiti će se na način kao da nevažeći ili neprovedivi dio ovog Ugovora nikad nije bio njegov sastavni dio.

Ovaj Dodatak je sklopljen i postaje obvezujući dio Glavnog ugovora datumom njegova potpisivanja.

[Naručitelj]

Potpis _____

Odgovorna osoba _____

Datum potpisivanja _____

[Ponuditelj]

Potpis _____

Odgovorna osoba _____

Datum potpisivanja _____

PRILOG 1: DETALJI OBRADE OSOBNIH PODATAKA

Ovaj Prilog 1 sadrži pojedinosti o obradi osobnih podataka sukladno članak 28. stavku 3. GDPR-a.

- Predmet i trajanje obrade osobnih podataka
Predmet i trajanje obrade osobnih podataka Društva navedeni su u glavnom ugovoru i ovom Dodatku.
- Priroda i svrha obrade osobnih podataka
[Ovdje uključite opis]
- Vrste osobnih podataka koje treba obrađivati
[Ovdje uključite popis vrsta podataka]
- Kategorije ispitanika
[Ovdje uključite kategorije podataka podataka]
- Prava i obveze Naručitelja
Prava i obveze Naručitelja utvrđeni su u glavnom ugovoru i ovom Dopunom.

ZAKLJUČAK

Predlošci i komentari su prijedlozi elemenata ugovora te se mogu usklađivati s obzirom na okolnosti svakog pojedinog ugovornog odnosa. U slučaju bilo kakvih dvojbi preporuča se da tvrtka traži pravni savjet vezano uz sklapanje ugovora bez obzira da li je u poziciji Ponuditelja ili Naručitelja.

U slučaju sklapanja ugovora s podizvođačima svakako treba jasno definirati i njihova prava i obveze.

U postojeće ugovore potrebno je ugraditi elemente vezane uz zaštitu osobnih podataka kako bi bili sukladni s GDPR-om.

Ključni zahtjevi GDPR-a u pogledu uvjeta obrade podataka su:

- imati ugovor u pisanom obliku pri imenovanju izvršitelja obrade (bilo kao voditelj obrade ili izvršitelj obrade koji imenuje podizvršitelja);
- ugovor mora odrediti:
 - predmet i trajanje obrade;
 - prirodu i svrhu obrade;
 - vrstu osobnih podataka i kategoriju ispitanika;
 - prava i obveze voditelja obrade.

Ugovor mora sadržavati sljedeće minimalne uvjete, koji zahtijevaju od izvršitelja obrade da:

- djeluje samo prema pisanim uputama voditelja obrade;
- osigurati da osobe koje obrađuju podatke podliježu obvezi povjerenja;
- poduzeti odgovarajuće mjere kako bi se osigurala sigurnost obrade;
- uključiti samo podizvršitelje uz prethodnu suglasnost voditelja obrade i temeljem ugovora u pisanom obliku;
- pomažu voditelju obrade i ispitanicima da ostvaruju svoja prava prema GDPR-u;

GDPR je složeno zakonodavstvo koje je otvoreno za dodatna tumačenja. Trenutno postoje vrlo ograničene smjernice i komentari GDPR-a vezano uz sklapanje ugovora a svakako se prilikom sklapanja ugovora treba voditi odredbama članka 28. GDPR-a kako bi se zadovoljili osnovni propisani uvjeti.

Dodatak 1 – Odredbe Opće uredbe o zaštiti podataka Europske unije

A. Definicije

Pojmovi koji se koriste, ali nisu definirani u ovim Odredbama, primjerice „povreda osobnih podataka“, „obrada“, „voditelj obrade“, „izvršitelj obrade“ i „ispitanik“ imat će isto značenje kakvo je navedeno u članku 4. Opće uredbe o zaštiti podataka.

Sljedeća se definicija također koristi u ovim Odredbama:

„Podizvođači obrade podataka“ znači drugi izvođač obrade podataka kojeg izvršitelj obrade koristi za obradu osobnih podataka.

B. Uloge i opseg

1. Ove odredbe primjenjuju se na izvršitelja obrade, u opsegu koji definira Opća uredba.
2. U svrhu ovih odredbi voditelj i izvršitelj obrade suglasni su da je voditelj obrade _____, a _____ je vršitelj obrade takvih podataka, osim kada _____ nastupa kao izvršitelj obrade osobnih podataka, u kojem je slučaju _____ podizvođač obrade podataka.
3. Ove Odredbe ne ograničavaju niti smanjuju obveze zaštite osobnih podataka na koje se izvršitelj obrade obvezao.

C. Relevantne obveze koje proizlaze iz GDPR-a: članci 28, 32 i 33

1. Izvršitelj obrade neće angažirati drugog izvođača obrade podataka prije preciznog ili općenitog ovlaštenja voditelja obrade u pisanom obliku. U slučaju općenitog ovlaštenja u pisanom obliku, izvršitelj obrade će informirati voditelja obrade o eventualnim nenamjernim promjenama u vezi s dodavanjem ili zamjenom drugih izvođača obrade podataka, dajući tako voditelju obrade priliku da prigovori na takve promjene. (Članak 28(2))
2. Obradu koju izvodi izvršitelj obrade regulirat će ove odredbe na temelju zakona Europske unije (u daljnjem tekstu: „Unija“) ili države članice i obvezujuće su za izvršitelja obrade u odnosu na voditelja obrade. Tema i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka, kategorije ispitanika te obveze i prava navedeni su u Ugovoru, uključujući i ove odredbe. Konkretno, izvršitelj obrade će:
 - (a) obrađivati osobne podatke samo prema dokumentiranim uputama voditelja obrade; uključujući u vezi s prijenosima osobnih podataka u treću zemlju ili međunarodnu tvrtku ili ustanovu, osim ako to zahtijeva zakon Unije ili države članice koji se primjenjuje na izvršitelja obrade; u tom slučaju izvršitelj obrade izvješćuje voditelja obrade o tom pravnom zahtjevu prije obrade, osim ako se tim pravom zabranjuje takvo izvješćivanje zbog važnih razloga od javnog interesa;
 - (b) osigurati da su se osobe ovlaštene za obradu osobnih podataka obvezale na povjerljivost ili ih na to obvezuje odgovarajuća zakonska obveza;
 - (c) poduzeti sve mjere koje proizlaze iz Članka 32 GDPR-a;

- (d) poštovati odredbe na koje se ukazuje u stavcima 2 i 3 za angažiranje drugog izvođača obrade podataka;
- (e) uzimajući u obzir prirodu obrade, pomoći voditelju obrade odgovarajućim tehničkim i organizacijskim mjerama, onoliko koliko je moguće, radi ispunjavanja obveze voditelja obrade odgovaranja na zahtjev za raspolaganjem pravima ispitanika navedenim u Poglavlju III GDPR-a;
- (f) pomoći voditelju obrade u osiguravanju usklađenosti s obvezama koje proizlaze iz članaka 32 do 36 GDPR-a, uzimajući u obzir prirodu obrade i informacije dostupne izvršitelju obrade;
- (g) po izboru voditelja obrade, izbrisati ili vratiti sve osobne podatke voditelju obrade nakon kraja pružanja usluga koje se odnose na obradu i izbrisati postojeće kopije osim ako zakon Unije ili države članice zahtijeva pohranu osobnih podataka;
- (h) učiniti voditelju obrade sve informacije potrebne za dokazivanje usklađenosti s obvezama navedenim u članku 28 GDPR-a dostupnim i omogućiti revizije te im doprinositi, uključujući inspekcije pod vodstvom voditelja obrade ili drugog revizora kojeg ovlasti voditelj obrade.

Izvršitelj obrade će odmah informirati voditelja obrade ako, po njegovu mišljenju, uputa povrjeđuje GDPR ili druge odredbe zaštite osobnih podataka Unije ili države članice. (Članak 28(3))

3. Kada izvršitelj obrade angažira drugog izvođača obrade podataka za provođenje određenih aktivnosti obrade u ime voditelja, iste obveze zaštite osobnih podataka kakve su navedene u ovim Odredbama GDPR-a nametnut će se tom drugom izvođaču obrade podataka u vidu ugovora ili drugog pravnog akta u skladu sa zakonom Unije ili države članice, osobito u smislu pružanja dostatnih jamstava za implementaciju odgovarajućih tehničkih i organizacijskih mjera tako da obrada zadovolji zahtjeve GDPR-a. Kada taj drugi izvođač obrade podataka ne izvrši svoje obveze zaštite osobnih podataka, izvršitelj obrade ostaje u cijelosti odgovoran voditelju obrade za izvršenje obveza tog drugog izvođača obrade podataka. (Članak 28(4))

4. Uzimajući u obzir suvremene trendove, troškove implementacije i prirodu, opseg, kontekst i svrhu obrade, kao i promjenjivu vjerojatnost i ozbiljnost rizika za prava i slobode stvarnih osoba, voditelj i izvršitelj obrade implementirat će odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti koja odgovara riziku, uključujući, između ostalog, kako je prikladno:

- (a) pseudonimizaciju i enkripciju osobnih podataka;
- (b) mogućnost osiguravanja kontinuirane povjerljivosti, integriteta, dostupnosti i otpornosti sustava i usluga obrade;
- (c) mogućnost pravovremenog oporavka dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta;
- (d) proces za redovito testiranje i procjenu učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade. (Članak 32(1))

5. Pri procjeni odgovarajuće razine sigurnosti, račun će se izuzeti iz rizika koje predstavlja obrada, osobito od slučajnog ili protupravnog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili pristupa osobnim podacima koji se prenose, pohranjuju ili obrađuju na drugi način. (Članak 32(2))

6. Voditelj i izvršitelj obrade poduzet će korake za osiguravanje da svaka stvarna osoba koja nastupa s ovlaštenjem voditelja ili izvršitelja obrade, a ima pristup osobnim podacima, ne obrađuje osobne podatke ni na koji drugi način osim prema uputama voditelja obrade, osim ako je ta osoba dužna napraviti to po zakonu Unije ili države članice. (Članak 32(4))

7. Izvršitelj obrade će obavijestiti voditelja obrade bez nepotrebnog odgađanja kad sazna za povredu osobnih podataka. (Članak 33(2)).

U takvoj obavijesti mora se barem:

- (a)** opisati prirodu povrede osobnih podataka, uključujući, kada je to moguće, kategorije i približan broj pogođenih ispitanika i kategorija te približan broj zahvaćenih evidencija osobnih podataka;
- (b)** prenijeti ime i podatke za kontakt službenika za zaštitu osobnih podataka ili druge kontakt-osobe od koje se može dobiti više informacija;
- (c)** opisati izgledne posljedice povrede osobnih podataka i
- (d)** opisati mjere koje su poduzete u vezi s povredom Osobnih podataka ili njihovo poduzimanje predloži nadzornik, uključujući, gdje je to primjereno, mjere za ublažavanje mogućih štetnih posljedica. (Članak 33(3))

Dodatak 2 – Dodatne Odredbe GDPR-a - PODIZVOĐAČI

A. Podizvođači

1. Voditelj obrade je suglasan s tim da izvršitelj obrade angažira Podizvođače za obradu Osobnih podataka, u skladu s odredbama GDPR-a.

2. Izvršitelj obrade će se pobrinuti da podizvođači budu obvezani ugovorima u pisanom obliku koji od njih zahtijevaju da pruže razinu zaštite osobnih podataka najmanje jednaku onoj koju od izvršitelja obrade zahtijevaju odredbe GDPR-a.

3. Tamo gdje je _____ izvršitelj obrade primjenjuju se sljedeće odredbe:

- (a)** Ako voditelj obrade nije suglasan s novim Podizvođačem, voditelj obrade može prekinuti ugovorni odnos bez sankcija slanjem, prije završetka otkaznog roka, obavijesti o prekidu u pisanom obliku koja uključuje objašnjenje razloga za neodobravanje.

B. Pomoć voditelju obrade za odgovore na zahtjeve ispitanika

1. Izvršitelj obrade će voditelju obrade učiniti dostupnim osobne podatke njegovih ispitanika, kao i omogućiti ispunjavanje zahtjeva ispitanika radi raspolaganjem jednim ili više njihovih prava na temelju GDPR-a Izvršitelj obrade će postupati u skladu s razumnim zahtjevima voditelja obrade kako bi pomogao voditelju obrade da odgovori na takav zahtjev ispitanika.

2. Ako izvršitelj obrade dobije zahtjev od ispitanika radi raspolaganja jednim ili više njegovih prava na temelju GDPR-a, izvršitelj obrade će preusmjeriti ispitanika da zahtjev uputi izravno voditelju obrade.

C. Obrada osobnih podataka

1. Izvršitelj obrade također može prenijeti osobne podatke ako to zahtijeva mjerodavno pravo.
2. Izvršitelj obrade će se pobrinuti da njegovi zaposlenici angažirani u obradi osobnih podataka
 - (i) obrađuje Osobne podatke samo prema uputama voditelja obrade, osim ako je to dužno napraviti prema zakonu Unije, države članice ili drugom mjerodavnom pravu i
 - (ii) budu obvezani održavati povjerljivost bilo kojih osobnih podataka čak i nakon završetka svojeg angažmana.
4. Predmet obrade ograničen je na osobne podatke u okviru GDPR-a, a obrada će trajati koliko i angažman izvršitelja obrade.
5. Kod isteka ili prekida ugovora izvršitelj obrade će izbrisati ili vratiti osobne podatke u skladu s odredbama i vremenskim sljedovima za svaku uslugu kako je navedeno u ugovoru, osim ako zakon Unije, države članice ili drugo mjerodavno pravo zahtijeva pohranu osobnih podataka.

D. Sigurnost

Izvršitelj obrade će:

- (i) održavati sigurnosne postupke i pravila za zaštitu osobnih podataka, kako je navedeno u pisanim pravilima o sigurnosti podataka i,
- (ii) podložno obvezama ne otkrivanja, učiniti Pravila o sigurnosti informacija dostupnim voditelju obrade, zajedno s opisima prisutnih sigurnosnih kontrola i druge informacije koje voditelj obrade zahtijeva u vezi s sigurnosnim postupcima i pravilima izvršitelja obrade.

E. Povreda Osobnih podataka

Izvršitelj obrade će u razumnoj mjeri pomoći voditelju obrade u ispunjavanju obveze izvršitelja obrade obavješćivanja relevantnog nadzornog nadležnog tijela i ispitanika o povredi osobnih podataka prema člancima 33 i 34 GDPR-a.

F. Evidencija aktivnosti obrade

Izvršitelj obrade će voditi svu evidenciju koju zahtijeva Članak 30(2) GDPR-a i, u mjeri primjenjivoj na obradu osobnih podataka u ime voditelja obrade, učiniti je na zahtjev dostupnom voditelju obrade.

G. Izmjene, dopune i trajanje

1. Izvršitelj obrade može izmijeniti ili nadopuniti ove Odredbe, uz obavijest voditelju obrade,

(i) ako ga na to obveže nadležno nadzorno tijelo ili drugi državni ili regulatorni subjekt,

(ii) ako je potrebno radi pridržavanja mjerodavnog prava,

(iii) radi implementiranja standardnih ugovornih klauzula koje je propisala Europska komisija ili

(iv) radi pridržavanja odobrenog kodeksa ponašanja ili mehanizma certificiranja odobrenog ili certificiranog u skladu s člancima 40, 42 i 43 GDPR-a.

2. Ne prejudicirajući ove odredbe, izvršitelj obrade može povremeno pružiti dodatne informacije i pojedinosti o tome kako će izvršiti ove odredbe u svojoj tehničkoj dokumentaciji, dokumentaciji o zaštiti privatnosti ili pravilima.

3. Ove Odredbe GDPR-a stupaju na snagu nakon

(a) početka primjene GDPR-a ili

(b) početka korištenja Proizvoda ili pružanja Profesionalnih usluga za koje je izvršitelj obrade izvođač ili podizvođač, ovisno o tome što nastupi kasnije.