_____,sa sjedištem u Zagrebu, _____, osobni identifikacijski broj (OIB):_____ kao voditelj obrade, zastupan po_____

i

_____**NAZIV DRUŠTVA,** Adresa_____, osobni identifikacijski broj (OIB):_____ kao izvršitelj obrade, zastupan po_____

(zajedno u tekstu: **Ugovorne stranke)**

sklapaju sljedeći

UGOVOR O OBRADI OSOBNIH PODATAKA

Ovaj Ugovor o obradi i dijeljenju osobnih podataka je dodatak postojećem Ugovoru _____, između _____ (dalje u tekstu: Voditelj obrade) i _____ (dalje u tekstu: Izvršitelj obrade), zajedno u tekstu Ugovorne strane, kako bi se utvrdili odnosi između Voditelja obrade i Izvršitelja u kontekstu obrade osobnih podataka, a u sklopu pružanja usluga temeljem Ugovora te zahtjeva primjenjivih propisa i pravne stečevine EU o zaštiti osobnih podataka.

Izvršitelj obrade u ime i za račun Voditelja obrade, na temelju glavnog Ugovora pruža usluge _____ za _____.

Svi pojmovi koji nisu eksplicitno definirani unutar ovog Ugovora imaju značenje definirano u Ugovoru i Uredbi (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).

I. PRIMJENA UGOVORA

Članak 1.

(1) Ovaj Ugovor dodatak je postojećem Ugovoru.

(2) Ugovor sadrži priloge koji su njegov sastavni dio, a kojima se pobliže utvrđuju priroda i uvjeti obrade podataka:

- Prilog 1. Detalji o obradi osobnih podataka,
- Prilog 2. Tehničke i organizacijske mjere koje mora ispuniti Izvršitelj obrade
- Prilog 3. Tehničke i organizacijske mjere koje zahtjeva Voditelj obrade

(3) Ugovor je dodatak temeljnom Ugovoru te ne isključuje odredbe, prava i obveze Ugovornih strana koji su definirani istim.

Komentirano [JV1]: Tvrtka ovlaštenog inženjera geodezije, odnosno u kojoj je isti zaposlen

Komentirano [JV2]: Tvrtka s kojom se dijele osobni podaci

II. DEFINICIJA POJMOVA

Članak 2.

(1) „**Voditelj obrade**“ je pravna ili fizička osoba koja određuje svrhu i način obrade podataka.

(2) **„Ispitanik**“ je osoba čiji je identitet utvrđen ili se može utvrditi; 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.

(3) „**Izvršitelj obrade**“ je pravna ili fizička osoba koja obrađuje podatke u ime voditelja obrade.

(4) „**Podizvršitelj obrade**“ je pravna ili fizička osoba angažirana od strane izvršitelja obrade kao sudionik u obradi podataka u ime voditelja obrade.

(5) „**GDPR**“ je 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 (Opća uredba o zaštiti podataka).

(6) „**Osobni podatak**“ su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”).

(7) „**Obrada osobnih podataka**“ je 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.

III. UVODNE ODREDBE I OBRADA OSOBNIH PODATAKA

Članak 3.

(1) Ugovorne strane suglasno utvrđuju da su sklopile glavni Ugovor _____(datum), a temeljem kojeg je _____ Voditelj obrade, a _____ Izvršitelj obrade te sudjeluje u obradi osobnih podataka u ime i za račun Voditelja obrade.

(2) Ovim Ugovorom Ugovorne strane uređuju svoja prava i obveze kada u izvršavanju glavnog Ugovora nastupaju kao Voditelj obrade i Izvršitelj obrade te se na svaku ugovornu stranu primjenjuju prava i obveze u skladu s njihovom ovdje navedenom ulogom u obradi osobnih podataka. U slučaju neslaganja odredbi glavnoga Ugovora i ovog Ugovora u dijelu u kojem se uređuje obrada osobnih podataka, prednost će imati odredbe ovog Ugovora.

(3) Predmet ovog Ugovora je obrada osobnih podataka, a koja se vrši na temelju glavnog Ugovora. Voditelj obrade ovlašćuje Izvršitelja obrade da obrađuje osobne podatke

ispitanika, s prirodom i svrhom obrade koje su isključivo povezane s izvršenjem obveza Izvršitelja obrade koje proizlaze iz glavnog Ugovora odnosno da ih obrađuje kada i u mjeri u kojoj je to nužno kako bi mogao uredno pružiti ugovorene usluge. Detalji obrade osobnih podataka i kategorije osobnih podataka navedeni su u Prilogu 1. ovog Ugovora.

IV. OBVEZE VODITELJA OBRADE

Članak 4.

Obrada osobnih podataka po nalogu Voditelja obrade

(1) Voditelj obrade izjavljuje kako su njegovi nalozi za obradu osobnih podataka prema Izvršitelju obrade u skladu s primjenjivim propisima i cjelokupnom pravnom stečevinom EU o zaštiti osobnih podataka. Voditelj obrade zadržava odgovornost za točnost, cjelovitost i zakonitost osobnih podataka koje će isporučiti Izvršitelju obrade u svrhu obrade, kao i za usklađenost pravnih temelja obrade osobnih podataka s Općom uredbom o zaštiti podataka, primjenjivim propisima i cjelokupnom pravnom stečevinom EU o zaštiti osobnih podataka.

V. OBVEZE IZVRŠITELJA

Članak 5.

Obrada podataka od strane Izvršitelja obrade

(1) Izvršitelj obrade se obvezuje da će osobne podatke tretirati kao povjerljive te da će osobne podatke obrađivati isključivo u skladu s uputama Voditelja obrade. Ukoliko Voditelj obrade ne dostavi upute za provedbu obrada, Izvršitelj obrade će, prema svojoj diskrecijskoj ocjeni, provoditi obrade u skladu s interno propisanim politikama i procedurama. Izvršitelj obrade jamči Voditelju obrade kako je nositelj ISO 27001 certifikata te da je organizirao svoje postupanje i procedure sa zahtjevima sigurnosti i navedenog ISO 27001 certifikata. Izvršitelj obrade se obvezuje poduzimati mjere kako bi za trajanja Ugovora zadržao isti certifikat.

(2) Izvršitelj obrade jamči da su njegovi zaposlenici:

- upoznati s povjerljivom prirodom osobnih podataka definiranih Ugovorom te načinom na koji se može postupati s podacima povjerljive prirode (sigurnosno prihvatljivo postupanje),
- educirani za primjereno korištenje informacijskog sustava i rukovanje osobnim podacima te
- temeljem internih akata obvezni čuvati povjerljivost osobnih podataka.

(3) Izvršitelj obrade se obvezuje da će pristup svojih zaposlenika osobnim podacima koji se obrađuju na njegovom informacijskom sustavu dopuštati isključivo ukoliko za to postoji poslovna potreba, vodeći se pritom načelom minimalnih privilegija.

(4) Izvršitelj obrade se obvezuje da će odmah, ali u svakom slučaju u roku od 24 sata od identifikacije incidenta odnosno sumnje na incident, izvijestiti Voditelja obrade ukoliko dođe do incidenta s povredom sigurnosti ili privatnosti osobnih podataka koje Izvršitelj

obrade ili treće strane angažirane od strane Izvršitelja obrade obrađuju u ime Voditelja obrade. Pritom, Izvršitelj obrade se obvezuje dostaviti sljedeće informacije u mjeri u kojoj su te informacije dostupne u trenutku obavijesti (prvi prioritet je upozoriti Voditelja obrade o incidentu, a tek zatim pružiti mu punu informaciju o incidentu; Izvršitelj obrade će iste informacije o incidentu dostavljati Voditelju obrade kako mu postanu dostupne/potvrđene):

- tip incidenta, datum i vrijeme nastanka incidenta kao i period njegova trajanja; način identifikacije incidenta; uzroci i utjecaj incidenta na osobne podatke Voditelja obrade,
- kategorija i količina osobnih podataka obuhvaćenih incidentom/povredom,
- kategorije i broj ispitanika obuhvaćenih incidentom/povredom,
- mjere poduzete u cilju kontrole i umanjivanja štete te prevenciji sličnih incidenata u budućnosti,
- kontakt osoba Izvršitelja od koje Voditelj obrade može zatražiti dodatne informacije o prirodi incidenta.

(5) Izvršitelj obrade nije dužan postupiti po uputama Voditelja obrade, ako prema svojim saznanjima smatra da određene upute krše primjenjive propise, o čemu će izvijestiti Voditelja obrade.

(6) Izvršitelj obrade se obvezuje da će pružiti pomoć Voditelju obrade, u skladu s prirodom i svrhom obrade osobnih podataka, u izvršenju zahtjeva ispitanika ili nadzornih tijela postavljenih prema Voditelju obrade.

VI. TREĆE STRANE KOJE SUDJELUJU U OBRADI OSOBNIH PODATAKA

Članak 6.

(1) Izvršitelj obrade može angažirati podizvršitelje kao sudionike u izvršenju obrada osobnih podataka koji su predmet ovog Ugovora. Izvršitelj obrade je dužan osigurati da podizvršitelji osobne podatke obrađuju isključivo u svrhu i na način definiranima temeljnim Ugovorom i ovim Ugovorom. Popis podizvršitelja koje sudjeluju u obradi osobnih podataka mora biti sastavni dio ovoga Ugovora.

(2) Ukoliko Izvršitelj obrade uslijed vlastitih poslovnih potreba želi angažirati podizvršitelje, obvezuje se prethodno o tome izvijestiti Voditelja obrade i to najmanje deset (10) radnih dana prije sklapanja ugovora sa poizvršiteljem odnosno angažmana podizvršitelja. Voditelj obrade se obvezuje izvijestiti Izvršitelja obrade o eventualnom prigovoru za promjenu angažmana podizvršitelja u roku od deset (10) radnih dana od zaprimanja obavijesti Izvršitelja obrade. Voditelj obrade može izjaviti prigovor samo radi neusklađenosti postupanja podizvršitelja sa primjenjivim propisima o zaštiti osobnih podataka ili iz razloga što predloženi podizvršitelj predstavlja povećani rizik kod obrade osobnih podataka. U slučaju da Voditelj obrade uloži prigovor na promjenu angažmana podizvršitelja, Ugovorne strane će bez odgode dogovoriti korake kako bi se otklonili razlozi prigovora ili izmijenila priroda ovoga Ugovora. U slučaju nemogućnosti postizanja

dogovora u periodu od 30 dana računajući od dana kada je predložen podizvršitelj, isto se smatra opravdanim razlogom za raskid Ugovora od strane Voditelja obrade.

(3) Izvršitelj obrade će osigurati da su tehničke i organizacijske mjere zaštite osobnih podataka podizvršitelja, po svrsi i učinkovitosti jednake ili naprednije kao tehničke i organizacijske mjere zaštite Izvršitelja obrade.

VII. PRIJENOS PODATAKA, TRAJANJE OBRADE I SIGURNOSNE KOPIJE

Članak 7.

Prijenos podataka u zemlje i institucije izvan Europske Unije

(1) Izvršitelj obrade izjavljuje da ne prenosi osobne podatke koje obrađuje po nalogu Voditelja obrade u zemlje i organizacije koje su izvan Europske Unije.

(2) Izvršitelj obrade se obvezuje da će obradu osobnih podataka po nalogu Voditelja obrade vršiti do prestanka važenja Ugovora, osim ukoliko Ugovorom ili drugim primjenjivim propisima nije utvrđeno drugačije. Po isteku osnove za obradu podataka po nalogu Voditelja obrade, Izvršitelj obrade se obvezuje po izboru Voditelja obrade podatke obrisati ili vratiti Voditelju obrade.

(3) Voditelj obrade u sklopu organizacijskih i tehničkih mjera zaštite provodi sigurnosno kopiranje (backup) podataka. Trenutno brisanje podataka iz sigurnosnih kopija može biti neizvedivo uslijed tehničkih ograničenja, zbog čega podaci Voditelja obrade mogu ostati pohranjeni u sigurnosnim kopijama u periodu do najviše 60 dana nakon predviđenog trajanja obrade ili izvršenja naloga za brisanjem. Ako Voditelj obrade zahtijeva čuvanje sigurnosnih kopija duže od 60 dana, sam snosi odgovornost za povredu primjenjivih propisa o zaštiti osobnih podataka, npr. pravo ispitanika na brisanje. Ukoliko dođe do potrebe da se izvrši operacija povrata (restore) podataka iz sigurnosne kopije u produkcijski informacijski sustav Izvršitelja obrade, postoji mogućnost da se prethodno brisani podaci Voditelja obrade vrate u produkcijske informacijske sustave Izvršitelja obrade. Radi toga će u slučaju provedbe operacije povrata Izvršitelj obrade o tome bez odgode obavijestiti Voditelja obrade, koji će mu dati upute za daljnje postupanje sa osobnim podacima Voditelja obrade koji su vraćeni u produkcijski informacijski sustav.

VIII. TEHNIČKE I ORGANIZACIJSKE MJERE

Članak 8.

Primjena tehničkih i organizacijskih mjera Izvršitelja obrade

(1) U okviru svog sustava upravljanja informacijskom sigurnošću temeljenog na procjeni rizika, Izvršitelj obrade je uspostavio tehničke i organizacijske mjere u cilju zaštite osobnih podataka u obradi, sukladno članku 32. Opće uredbe o zaštiti podataka. Popis tehničkih i organizacijskih mjera primijenjenih u cilju zaštite osobnih podataka nalazi se

u Prilogu 2. ovog Ugovora. Izvršitelj obrade jamči Voditelju obrade kako su te tehničke i organizacijske mjere primjerene za tip usluga, uzimajući u obzir uobičajene rizike koji iz njih proizlaze, koje Izvršitelj obrade pruža Voditelju obrade.

(2) U slučaju potrebe Voditelja obrade za dodatnim tehničkim i organizacijskim mjerama zaštite koje nisu obuhvaćene ovim Ugovorom, Voditelj obrade će uputiti pisani zahtjev Izvršitelju obrade s prijedlogom i obrazloženjem implementacije dodatnih mjera. Izvršitelj obrade će zahtjev za dodatnim mjerama razmotriti i provesti analizu primjenjivosti i isplativosti, o čemu će u najkraćem mogućem roku izvijestiti Voditelja obrade.

(3) Izvršitelj obrade će na zahtjev Voditelja obrade dostaviti Voditelju obrade certifikate i izvješća neovisnih revizora kojima se dokazuje implementacija i učinkovitost implementiranih tehničkih i organizacijskih mjera zaštite osobnih podataka.

IX. OSTALE ODREDBE

Članak 9.

(1) Izvršitelj obrade se obvezuje, uzimajući u obzir prirodu obrade, dostupne informacije i primjerenost zahtjeva Voditelju obrade, pomagati voditelju obrade u ispunjavanju obveza koje ima kao Voditelj obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika koja su utvrđena u poglavlju III. Opće uredbe o zaštiti podataka te člancima od 32. do 36. Opće uredbe o zaštiti podataka. Ugovorna strana čijim je radnjama uzrokovana šteta, odgovorna je za nastalu štetu, bez obzira kojoj je od Ugovornih strana zahtjev za naknadu štete podnesen. Sukladno tome, ako je Ugovorna strana koja nije odgovorna za povredu osobnih podataka zaprimila zahtjev ispitanika za naknadu štete, druga Ugovorna strana dužna je nadoknaditi iznos štete i nastale dodatne troškove.

(2) Komunikacija između Voditelja obrade i Izvršitelja obrade o svim pitanjima vezanima uz ovaj Ugovor odvijat će se putem elektroničke pošte, sa sljedećim kontakt adresama na strani Voditelja obrade i Izvršitelja obrade:

Kontakt Voditelja obrade/DPO:

_____

Kontakt Izvršitelja/DPO:

_____

(3) Ugovorne strane su dužne obavijestiti drugu stranu o zamjeni odgovorne osobe iz stavka 2. ovog članka, u pisanom obliku u roku od 3 dana od nastale promjene.

(4) Odgovornost Voditelja obrade i Izvršitelja obrade za štetu prouzročenu obradom osobnih podataka te pravo na naknadu tako prouzročene štete uređeni su odredbama

Opće uredbe o zaštiti podataka s tim da je Izvršitelj obrade odgovoran za štetu prouzročenu obradom osobnih podataka samo ako nije poštovao obveze iz Opće uredbe o zaštiti podataka koje su posebno namijenjene Izvršiteljima obrade ili je djelovao izvan zakonitih uputa Voditelja obrade ili protivno njima. Izvršitelj obrade ne odgovara za štetu koju u ispunjavanju ovog ugovora prouzroči Voditelj obrade. Ugovorna strana, koja je odgovorna za postupanje ili propuštanje postupanja koje je rezultiralo novčanom kaznom nadzornih tijela, bit će odgovorna, bez obzira na to kome je kazna službeno izrečena. Sukladno tome, ako je Ugovornoj strani koja nije počinila povredu osobnih podataka izrečena kazna, druga Ugovorna strana dužna je nadoknaditi iznos novčane kazna i nastale dodatne troškove.

(5) U slučaju spora vezano za zaštitu osobnih podataka, odredbe ovog Ugovora imaju prednost pred odredbama drugih ugovora između Voditelja obrade i Izvršitelja obrade te se Ugovorne strane obvezuju eventualni spor najprije pokušati riješiti mirnim putem. Na ovaj Ugovor primjenjuje se hrvatsko pravo. Za sporove iz ovog Ugovora mjesno je nadležan Trgovački sud u Zagrebu.

(6) Ugovorne strane suglasne su da će sve naknadne izmjene i dopune ovog Ugovora biti sklopljene u pisanom obliku, kao dodatak ovom Ugovoru.

(7) Ukoliko pojedinačne odredbe ovog Ugovora postanu ništetne, to ne utječe na valjanost preostalih odredbi iz ovog Ugovora.

(8) Ugovorne strane suglasne su da se prava i obveze iz ovog Ugovora primjenjuju od dana potpisa ovog Ugovora.

(9) Ugovorne strane suglasne su da prestankom važenja temeljnog Ugovora ne prestaje i važenje ovog Ugovora. Odredbe iz ovog Ugovora primjenjuju se u roku od 5 godina od raskida temeljnog Ugovora.

Članak 10.

(1) Ugovorne stranke su suglasne da će eventualne sporove iz ovog Ugovora rješavati sporazumno. Ako sporazum nije moguć za rješavanje je nadležan sud prema sjedištu Voditelja obrade.

Članak 11.

(1) Ugovor stupa na snagu danom potpisivanja obiju ugovornih stranaka.

(2) Ugovor je sklopljen u dva (2) istovjetna primjeraka, od kojih svaka ugovorna stranka prima po jedan (1) primjerak.

U Zagrebu, _____	U Zagrebu, _____
NAZIV DRUŠTVA	NAZIV DRUŠTVA
ODGOVORNA OSOBA	ODGOVORNA OSOBA

PRILOG UGOVORU O OBRADI I DIJELJENJU OSOBNIH PODATAKA

Komentirano [ab3]: Popunjava izvršitelj obrade

PRILOG 1. DETALJI O OBRADI OSOBNIH PODATAKA

Naziv aktivnosti obrade osobnih podataka	Svrha obrade	Kategorija ispitanika	Vrsta osobnih podataka	Osnova prikupljanja	Tehničke i organizacijske mjere	Navesti podizvršitelja u slučaju da postoji a vezani su uz obradu osobnih podataka	Mjesto obrade podataka, način pohrane I vrijeme čuvanja

PRILOG 2. TEHNIČKE I ORGANIZACIJSKE MJERE KOJE MORA ISPUNITI IZVRŠITELJ OBRADE

Komentirano [ab4]: Popunjava izvršitelj obrade

Izvršitelj obrade mora ispuniti i mjere navedene kao minimalne od strane Voditelja obrade u Prilogu 3.

Naziv kontrole	Ključne mjere u primjeni
Politika sigurnosti informacijskog sustava	
Organizacija informacijske sigurnosti	
Sigurnost ljudskih resursa	
Upravljanje imovinom	
Kontrola pristupa	
Kriptografija	
Fizička i okolišna sigurnost	
Sigurnost operacija	
Sigurnost komunikacija	
Nabava, razvoj i održavanje sustava	
Odnosi s dobavljačima	
Upravljanje incidentima	
Upravljanje kontinuitetom poslovanja	

Upravljanje usklađenošću	

Izvršitelj obrade ispunio je ˝GDPR- Self assessment questionnaire˝ u kojem je naveo mjere koje poduzima te se potpisom ovoga Ugovora obvezuje ispuniti mjere koje mu nalaže Voditelj obrade u Prilogu 1.

˝GDPR- Self assessment questionnaire˝ prilaže se ovom Ugovoru te Izvršitelj obrade jamči za njegovu točnost.

Paraf Izvršitelja obrade

_____

PRILOG 3. TEHNIČKE I ORGANIZACIJSKE MJERE KOJE ZAHTJEVA VODITELJ OBRADE

OPĆENITE MJERE

1. Povjerljivost (članak 32. stavak 1. točka (b) Opće uredbe o zaštiti podataka)

- Kontrola fizičkog pristupa
  Zabranjen je neovlašteni pristup objektima za obradu podataka, npr.: pametne kartice, ključevi, elektronički sustavi za otvaranje vrata, službe za zaštitu objekata i/ili osoblje za sigurnosnu kontrolu na ulazu, sustavi alarma, video/CCTV sustavi
- Kontrola elektroničkog pristupa
  Zabranjena je neovlaštena uporaba sustava za obradu podataka i pohranu podataka, npr.: (sigurne) lozinke, mehanizmi za automatsko blokiranje/zaključavanje, dvostruka provjera autentičnosti, enkripcija nosača podataka / medija za pohranu podataka
- Kontrola internog pristupa (dopuštenja za korisnička prava na pristup i izmjenu podataka)
  Nije dopušteno neovlašteno čitanje, kopiranje, mijenjanje ili brisanje podataka unutar sustava, npr. koncept odobrenja prava, prava pristupa ovisno o potrebi, zapisivanje događaja pristupa sustavu
- Kontrola izolacije
  Izolirana obrada podataka koji se prikupljaju u različite svrhe, npr. višestruka podrška Naručitelju, testno okruženje
- Pseudonimizacija (članak 32. stavak 1. točka (a) Opće uredbe o zaštiti podataka; članak 25. stavak 1. Opće uredbe o zaštiti podataka)
  Obrada osobnih podataka na način da se podaci ne mogu povezati s određenim subjektom podataka bez uporabe dodatnih informacija, uz uvjet da su te dodatne informacije pohranjene odvojeno; podliježe odgovarajućim tehničkim i organizacijskim mjerama.

2. Cjelovitost (članak 32. stavak 1. točka (b) Opće uredbe o zaštiti podataka)

- Kontrola prijenosa podataka
  Zabranjeno je neovlašteno čitanje, kopiranje, mijenjanje ili brisanje podataka elektroničkim prijenosom ili prijevozom, npr.: enkripcija, virtualne privatne mreže (VPN), elektronički potpis
- Kontrola unosa podataka
  Provjera jesu li osobni podaci uneseni u sustav za obradu podataka, izmijenjeni ili izbrisani te tko je to učinio, npr.: zapisivanje, upravljanje dokumentima

3. Dostupnost i otpornost (članak 32. stavak 1. točka (b) Opće uredbe o zaštiti podataka)

- Kontrola dostupnosti
  Sprječavanje slučajnog ili namjernog uništavanja ili gubitka, npr.: strategija izrade sigurnosnih kopija (na mreži / izvanmrežno; na lokaciji / izvan lokacije), neprekidni izvor napajanja (UPS), zaštita od virusa, vatrozid, postupci izvještavanja i plan za izvanredne situacije
- Brzi oporavak (članak 32. stavak 1. točka (c) Opće uredbe o zaštiti podataka)

4. Postupci za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti (članak 32. stavak 1. točka (d) Opće uredbe o zaštiti podataka; članak 25. stavak 1. Opće uredbe o zaštiti podataka)
- Upravljanje zaštitom podataka
- Upravljanje odgovorom na incidente
- Tehnička i integrirana zaštita podataka (članak 25. stavak 2. Opće uredbe o zaštiti podataka)
- Kontrola narudžbe
  U skladu s člankom 28. Opće uredbe o zaštiti podataka treće osobe ne smiju izvoditi obradu podataka bez odgovarajućih uputa Naručitelja, npr.: jasnih i nedvosmislenih ugovora, službenog upravljanja narudžbom, strogih kontrola pri odabiru pružatelja usluga, dužnosti prethodne ocjene, nadzorne kontrole.

Minimalni sigurnosni uvjeti (Verzija 1.0) koje zahtjeva Voditelj obrade od Izvođača

Ova točka opisuje minimalne sigurnosne mjere koje je potrebno usvojiti u svrhu zaštite osobnih podataka i informacija ispitanika koji se dijele kao posljedica sklopljenog Ugovora između _____ d.o.o. i Izvođača.

Pridržavanje ovih minimalnih sigurnosnih mjera ne jamči pružanje odgovarajućeg stupnja zaštite, holistička i sveobuhvatna procjena sigurnosti mora se provesti ovisno o okolnostima, vrsti podataka i obradi koja se provodi.

Tehnike informacijske sigurnosti, kao i prijetnje za sigurnosti neprestano se razvijaju. Sigurnost je stoga potrebno kontinuirano procjenjivati u svjetlu posebnih konkretnih okolnosti kako bi se utvrdio odgovarajući stupanj zaštite.

Ove uvjete primjenjivat će fizička ili pravna osoba koja obrađuje osobne podatke u ime društva _____(UNIJETI PODATKE DRUGE UGOVORNE STRANE), a takva fizička ili pravna osoba spominje se kao ″Voditelj obrade″ ili ″Podizvođač″.

Ovi se uvjeti također trebaju čitati zajedno s ostalim općim sigurnosnim uvjetima kao što su svi sigurnosni uvjeti utvrđeni u sigurnosnoj procjeni prije i poslije sklapanja ugovora.

Mnogi od ovih uvjeta nisu namijenjeni da budu specifično prilagođeni za poslove obrade koji se provode specifično u ime _____ d.o.o. Očekuje se od društva _____(UNIJETI PODATKE DRUGE UGOVORNE STRANE) i s njim povezanih društava da usvoje ove standarde kao odgovarajuće standarde kako bi se osiguralo sigurno radno okruženje za postupanje s osobnim podacima ispitanika _____ d.o.o.

Ovaj Prilog će biti predmetom godišnje revizije. Do takve revizije može također doći i u slučaju bitnijih izmjena okolnosti, osobito u slučaju incidenta u koji je uključeno i društvo _____(navesti društvo, drugu stranu potpisnika ovog Ugovora). Obje Ugovorne strane će pisanim putem odobriti takve izmjene. Izmjene se prate u svakoj verziji dokumenta i dokumentiraju se u povijesti revizije.

1. Standardne sigurnosne mjere

1.1 Organizacijske mjere

Sigurnost zaposlenika

Samo oni zaposlenici koji su dokazali poštenje, integritet i diskreciju mogu biti ovlašteni korisnici (˝Ovlašteni korisnici˝) ili imati pristup prostorima gdje se nalaze informacijski sustavi ili mediji s osobnim podacima _____ d.o.o. Zaposlenici trebaju biti vezani obvezom povjerljivosti u odnosu na svaki pristup osobnim podacima _____ d.o.o.

Izvršitelj obrade obvezuje se usvojiti potrebne mjere kako bi svi zaposlenici bili osposobljeni i upoznati s ovim minimalnim sigurnosnim uvjetima, svim odgovarajućim politikama i primjenjivim propisima u vezi s obavljanjem njihovih funkcija i dužnosti u odnosu na obradu osobnih podataka, kao i s posljedicama svakog kršenja ovih uvjeta.

Funkcije i obveze zaposlenika koji imaju pristup osobnim podacima i informacijskim sustavima bit će jasno utvrđene i dokumentirane. Za potonje je odgovoran Izvršitelj obrade.

Ovlašteni korisnici dobit će upute da elektronička oprema ne smije biti ostavljena bez nadzora i dostupna za vrijeme postupka obrade. Izvršitelj obrade je zadužen i odgovoran za navedeno u odnosu na svoje zaposlenike ili vanjske suradnike ili druge fizičke osobe koje se smatraju ovlaštenim korisnicima.

Fizički pristup prostorima gdje su pohranjeni osobni podaci bit će ograničen na ovlaštene korisnike.

Disciplinske mjere za kršenje sigurnosnog plana bit će jasno utvrđene i dokumentirane te priopćene zaposlenicima i ovlaštenim korisnicima.

Dodatno: Standard sigurnosti zaposlenika uključuje dva poglavlja:

- u prvom su sažeti ključni koraci koje svi ovlašteni korisnici moraju poduzeti kako bi se zaštitile osobne radne stanice, a osmišljeni su kako bi se zaštitile radne stanice od zlonamjernih kodova (npr. zaštita Symantec Endpoint Protection),
- u drugom su sažete odgovornosti zaposlenika u pogledu zaštite informacija, i navedeni su sigurnosni uvjeti i uvjeti korištenja u ostalim okolnostima s kojima će se zaposlenici vjerojatno susresti.

Redovito će se provjeravati jesu li radne stanice u skladu sa sigurnosnim standardima obrade u pogledu sljedećih elemenata:

- Hard Drive Passwords, Screen Saver, Antivirus Software, Firewall Software, Unauthenticated
- File Sharing, Peer-to-Peer File Sharing Applications, Lotus Notes Database Encryption,
- Microsoft Windows User Account Passwords i odgovarajuće razine sigurnosnih zakrpa.
- Proceduralne i tehničke kontrole provode se kako bi se otkrila i popravila odstupanja usklađenosti radnih stanica i radnih mjesta zaposlenika. Mobilne radne stanice (npr. Mobilni uređaji) nisu dozvoljene. Izvođač se obvezuje

provoditi tehničke mjere kako bi se spriječilo ispisivanje ili lokalno pohranjivanje osobnih podataka od strane zaposlenika.

- Lozinke se trebaju primjenjivati prema određenim uvjetima za radne stanice ili tehnologijom koja je slijednik iste s najmanje istom funkcionalnošću i razinom zaštite, ukoliko drugačije nije odredio _____ d.o.o. U tom slučaju _____ d.o.o. će biti dužan isto primijeniti.
- Izmjene lozinki provode se svakih 30 dana. Lozinke:
  - moraju imati najmanje 8 znakova
  - moraju sadržavati kombinaciju slovnih i ne-slovnih znakova (broj, interpunkcija ili posebnih znakova) ili kombinaciju najmanje dvije vrste ne-slovnih znakova
  - ne smiju sadržavati korisnički identifikator kao dio lozinke.
- Izvođač se obvezuje osigurati da se korisničko ime, lozinke (računi) ne smiju dijeliti/razmjenjivati između zaposlenika, tj. jedan račun koristi samo jedan pojedinačni zaposlenik odnosno ovlašteni korisnik.
- Izvođač se obvezuje osigurati odgovarajuće provjere podobnosti budućih zaposlenika/ovlaštenih korisnika.

Osposobljavanje u pogledu zaštite podataka i privatnosti

Svi zaposlenici društva _____(NAVESTI PODATKE DRUGE UGOVORNE STRANE) i s njim povezanih društava prolaze osposobljavanje u pogledu zaštite podataka i privatnosti u vezi s odgovarajućim postupanjem s osobnim podacima i zaštitom osobnih podataka _____ d.o.o.

_____(NAVESTI PODATKE DRUGE UGOVORNE STRANE) će _____ d.o.o. dostaviti dokaz o izvršenim edukacijama zaposlenika koji su zaduženi za provedbu ovog i temeljnog Ugovora s društvom _____(NAVESTI PODATKE DRUGE UGOVORNE STRANE) i _____ d.o.o.

Klasifikacija informacija

Posebno osposobljavanje provodi se za stručnjake koji sudjeluju u izvršavanju poslova vezanih uz Ugovorne strane, a biti će minimalno upoznati s vrstama podatka koje će obrađivati kao i s rizicima povezanim s njima.

Kako bi se osiguralo neotkrivanje povjerljivih i osjetljivih osobnih podataka neovlaštenim pojedincima; sve takve informacije bit će klasificirane kao povjerljive.

Korištenje operativnih podataka koji sadrže osobne identifikacijske podatke ili bilo koje druge povjerljive informacije u svrhe testiranja potrebno je izbjegavati. Ukoliko se osobni identifikacijski podaci ili na drugi način povjerljive informacije koriste u svrhe testiranja, sve osjetljive pojedinosti i sadržaji trebaju biti zaštićeni uklanjanjem ili modifikacijom.

1.2 Sigurnosni koncept

_____(NAVESTI PODATKE DRUGE UGOVORNE STRANE) obvezan je osigurati sigurnosni koncept kojim će pokriti:

i. Sigurnosne mjere u vezi s modifikacijom i održavanjem sustava koji se koristi za obradu osobnih podataka, uključujući razvoj i održavanje aplikacija, odgovarajuću podršku

dobavljača, popis hardvera i softvera, fizičke zaštite, uključujući zaštitu zgrada ili prostorija gdje se odvija obrada podataka, zaštita opreme za obradu podataka i telekomunikacijske infrastrukture te kontrole sigurnosti radnog okružja;

ii. Mehanizme za zaštitu sigurnosti podataka za osiguravanje integriteta i povjerljivosti podataka, klasifikaciju podataka;

iii. Zaštitu računala i telekomunikacijskih sustava uključujući postupke upravljanja sigurnosnim kopijama, postupke rješavanja računalnih virusa, postupke upravljanja signalom/kodovima, sigurnost implementacije softvera, zaštitu baze podataka, zaštitu sustava spajanja na internet, kontrolu zaobilaženja sustava za zaštitu podataka, mehanizme za vođenje evidencije o pokušajima probijanja sigurnosne zaštite sustava ili neovlaštenom pristupu.

Sigurnosni koncept uključuje obvezno no ne ograničava se samo na:

i. Plan oporavka od kriznih situacija kojim se utvrđuje: mjere za minimiziranje prekida u normalnom funkcioniranju sustava; ograničenje opsega svake štete i krizne situacije; osiguranje neometanog prijenosa osobnih podataka s jednog računalnog sustava na drugi; ako je potrebno pružanje alternativnih načina korištenja računalnog sustava; edukacija, obučavanje i upoznavanje zaposlenika s postupcima u slučaju izvanrednih situacija; omogućavanje brzog i neometanog oporavka sustava, te minimiziranje ekonomski posljedica bilo kojeg slučaja krizne situacije.

ii. Krizni plan kojim se moraju pokriti sljedeće moguće opasnosti za sustav i odgovarajući kriteriji kako bi se utvrdilo kada je potrebno pokrenuti plan: kritične funkcije i sustavi, strategija za zaštitu sustava i prioriteti u slučaju aktiviranja Plana; popis odgovarajućih zaposlenika koji će se pozvati u hitnim slučajevima, kao i telefonski brojevi ostalih relevantnih strana; skup postupaka za obračun nastale štete; realistični planovi upravljanja vremenom u pogledu oporavka sustava; jasna raspodjela dužnosti zaposlenika; moguće korištenje alarmnih sustava i posebnih uređaja (npr. filtara zraka, filtara buke); u slučaju požara treba biti dostupna posebna oprema (npr. protupožarni aparati, pumpe za vodu, itd.); uređaji ili metode za mjerenje temperature, vlažnosti i drugih faktora okoliša (npr. klimatizacija, termometri, itd.); posebni sigurnosni softver za otkrivanje sigurnosnih povreda; posebni generatori u slučaju nestanka struje; zadržavanje kopija softvera ili materijala u drugim zaštićenim objektima kako bi se izbjegao nenamjerni gubitak.

Dokumenti o sigurnosti bit će dostupni zaposlenicima koji imaju pristup osobnim podacima i sustavima koji se koriste za pristup, pohranjivanje ili obradu, na drugi način, osobnih podataka uključujući privremene datoteke (˝Informacijski sustavi˝), a moraju pokrivati minimalno sljedeće aspekte:

- opseg, s detaljnom specifikacijom zaštićenih resursa;

- mjere, standarde, postupke, kodeks ponašanja, pravila i norme kako bi se jamčila sigurnost, uključujući kontrolu, inspekciju i nadzor Informacijskih sustava;

- funkcije i obveze zaposlenika;

- strukturu datoteka u kojima su sadržani osobni podaci i opis informacijskih sustava u kojima se obrađuju;

- svrhe u koje se Informacijski sustavi mogu koristiti;

-postupke za izvješćivanje o incidentima, upravljanje incidentima i reagiranje na incidente;

- postupke za izradu sigurnosnih kopija i obnavljanje podataka uključujući osobu koja je provela postupak, obnovljene podatke i, kada je primjenjivo, one podatke je bilo potrebno unijeti ručno u postupak obnavljanja.

Sigurnosni dokument i sve povezane evidencije i dokumentacija čuvat će se najmanje 15 godina od završetka obrade.

1.3 Tehničke mjere

Odobrenje

Odobrenje se izdaje isključivo zaposlenicima koji imaju opravdanu poslovnu potrebu za pristupom informacijskim sustavima ili za provođenjem bilo kakve obrade osobnih podataka (˝Ovlašteni korisnici˝).

Sustav izdavanja odobrenja primjenjuje se kada se koriste različiti profili odobrenja za različite namjene.

Logička sigurnost

Izvođač će s osobnim podacima koje obrađuje u ime _____ d.o.o. postupati u skladu s uputama tako što će ispunjavati obveze vezane za obradu i zaštitu sigurnosti koje su navedene u ovom Ugovoru.

Osobni podaci pohranjuju se isključivo na mjesta koje je odobrio _____ d.o.o. _____(NAVESTI PODATKE DRUGE UGOVORNE STRANE) obvezuje se tražiti odobrenje od _____ d.o.o. mjestu pohrane podataka.

Pristup sustavima _____ d.o.o. na temelju identifikacijskih podataka korisnika i poslovne uloge korisnika dodjeljuju se na osnovu dokumentiranog zahtjeva kojeg _____ d.o.o. mora odobriti. Projektni tim ima pristup osobnim podacima koji su dio testnih podataka koje _____ d.o.o. osigurava u razvojnim i proizvodnim okruženjima i odobrava u skladu s dogovorenim procesima.

Samo Ovlašteni korisnici mogu zatražiti logički pristup okruženju _____ d.o.o. i pristupiti traženom okruženju na temelju odobrenja _____ d.o.o.

_____ d.o.o. nadgleda provjeru identiteta i upravljanje identitetom za pristup određenom okruženju, što uključuje učestalost promjene lozinke za korisnička imena i druge mehanizme provedbe.

Zahtjev za opozivom korisničkog imena i pristupa zaposlenika šalje se _____ d.o.o. na opoziv nakon prestanka zaposlenja.

Autentikacija na temelju dva čimbenika mora se provesti kod pristupanja povjerljivim podacima.

Dnevnički zapisi (Logovi)

Opremu za bilježenje dnevničkih zapisa i podatke logova treba se zaštititi od krivotvorenja i neovlaštenog pristupa.

- Centralno zapisivanje dnevničkih zapisa:

- prijava (uspješna/neuspješna) i odjava
- bilježenje promjena na korisničkim računima, pravima i poslovnim ulogama
- bilježenje vraćanja izvorne lozinke (resetiranja)
- bilježenje promjena u konfiguraciji komponenata
- zabilježeni podaci moraju se pohraniti u skladu sa zakonskim i internim zahtjevima.

- Zabilježeni podaci moraju sadržavati najmanje sljedeće informacije:
- datum i vrijeme, naziv računala / IP adresu, korisnički račun, aplikaciju/uslugu

- Mora biti moguće izvesti dnevničke zapise u format koji je općenito moguće uređivati (npr.CSV, XML, syslog).

Fizička zaštita

Kako bi se ublažio rizik za sredstva obrade podataka, rizik od neovlaštenog otkrivanja ili brisanja podataka te rizik od prekida podrške poslovnim procesima, a što može proizaći iz neovlaštenog fizičkog pristupa sredstvima za obradu podataka moraju biti implementirane sljedeće mjere:

- Uspostavljene su nadzorne mjere kako bi se fizički zaštitila područja u kojima se nalaze računalni sustavi i komponente mrežne infrastrukture od neovlaštenog pristupa i štete.

Fizička zaštita provedena u prostorijama Izvođača uključuje:

- Pristup zgradama i unutarnjim prostorima kontroliran iskaznicom.
- Posjetiteljima je dopušten ulaz isključivo u pratnji nadležne osobe i uz upis u Registar
- posjetitelja.
- Zaštitari su prisutni u svim zgradama, a ondje gdje je potrebno osigurana je 24-satna
- prisutnost zaštitara.
- Nadzorne kamere u velikoj mjeri se koriste u zgradama na vratima za Ulaz/Izlaz.
- Postoje procedure za izvanredne situacije kao što su požar, poplava i slično.

Informacije o lokacijama Izvođača potrebne za pružanje usluge moraju biti dostupne _____ d.o.o.

Arhitektura

- Aplikacije i drugi sustavi koji se koriste moraju biti organizirane u nekoliko razina koje su međusobno sigurnosno odvojene.

Nijedna razina ne smije biti preskočena tijekom pristupa.

- Pristup s jedne razine drugoj mora biti moguć isključivo putem određenih protokola (portova).
- Testni, integracijski i produkcijski sustavi moraju biti odvojeni. Zaposlenici ne smiju pristupiti produkcijskim sustavima bez izričitog pisanog dopuštenja koje izdaju odgovorne osobe.
- Uporaba SNMP-a (Jednostavni protokol za upravljanje mrežom) nije podržan iz sigurnosnih razloga.

Testne podatke pažljivo se izabire, štiti i nadzire.

2. Visoke sigurnosne mjere u pogledu ključnih podataka

U skladu s gore navedenim mjerama Izvođač (Izvršitelj) se pridržava sljedećih mjera ako se npr., podaci o klijentu, prometu, lokaciji ili drugi osjetljivi podaci (uključujući podatke o zaposlenicima, dužnosnicima, istaknutim osobama društva, marketinškim aktivnostima i poslovnim planovima, poznatim ličnostima (influencerima), političkoj opredijeljenosti, podacima o zdravlju, suradnicima (˝Ključni podaci društva˝) obrađuju ili pohranjuju u proizvodima ili kroz usluge ili sustave ili ako postoje sučelja za te podatke:

Dnevnički zapisi (Logovi)

- Bilježenje podataka o pristupu/izvozu ključnih podataka društva,
- Dnevnički zapisi moraju se pohraniti u skladu s važećim zahtjevima _____ d.o.o. U bilo kojem slučaju mora biti omogućeno postavljanje parametara za dnevničke zapise.
- Bilježenje podataka neophodno je kako bi se mogla osigurati sljedivost transakcija u sustavima, osobito u slučajevima zlouporabe. Pristup dnevničkim zapisima smije biti odobren isključivo ovlaštenim osobama i mora biti zaštićen od naknadnih izmjena.
- Unutar Izvođača napravit će se zapisnici o posebnim podacima (važne transakcije, sigurnosni podacima (sigurnosni parametri koji se zapisuju) i o podacima o mrežnom poslužitelju (učitane mrežne stranice, potpuni URL). Pristup podacima o prometu i osobnim podacima također mora biti zabilježen.
- Minimalni zahtjevi za bilježenje podataka su sljedeći: korisničko ime, IP adresa ili naziv računala, datum i vrijeme.
- Zabilježeni podaci moraju biti pohranjeni u skladu sa zakonskim obvezama: ICS (sustav interne kontrole) logovi u trajanju od 18 mjeseci i logovi o sigurnosti u trajanju od 3 mjeseca.

Brisanje podataka

Ključni podaci moraju se brisati redovito i automatski u skladu sa zakonskim zahtjevima i zahtjevima _____ d.o.o.

Izvođač je dužan proaktivno nabaviti potrebne informacije od _____ d.o.o. ukoliko se za to ukaže potreba. Izvođač mora u svakom slučaju obrisati podatke ako mu više nisu potrebni za ispunjavanje ugovornih obveza te mora upotrijebiti pažnju profesionalca u svom poslu.

Enkripcija

- Ključni podaci _____ d.o.o. moraju biti kriptirani tijekom prijenosa u podatkovnoj mreži i kada se pohranjuju na uređaje za spremanje podataka.

Penetracijsko testiranje

- Tehnike penetracijskog testiranja primijenit će se kako bi se ispitala razina zaštite; pristup će se simulirati uporabom testova crne ili bijele kutije (eng. black or white box tests).

Izvođač mora bez odgode ispraviti bilo kakve sigurnosne nedostatke koji su pronađeni tijekom testiranja. Rezultate testiranja nužno je napraviti prije sklapanja ugovora i o istima obavijestiti odgovorne osobe _____ d.o.o.

Provjera ranjivosti

- Proizvodi i sustavi ili aplikacije moraju biti isporučeni i implementirani u sigurnom, ojačanom stanju i s instaliranim svim sigurnosnim zakrpama. Prije stavljanja u uporabu mora ih se osigurati provjerama ranjivosti. Izvođač mora osigurati potrebno ažuriranje bez naplate za bilo koje slabe točke otkrivene nakon izvođenja testiranja.

Posebni zahtjevi za sigurnost podataka

Ako sustav obrađuje podatke iz različitih poslovnih i drugih područja djelovanja _____ d.o.o., mora biti omogućeno razdvajanje tih područja putem utvrđenih prava pristupa.

3. Certifikacija

Izvođač mora biti u mogućnosti predočiti certifikat za uslugu koji obavlja (SSAE 16, ISAE 3402 ili ISO 27001).

Barem jednom godišnje Izvođač mora _____ d.o.o. podnijeti izvješće o trenutačnom stanju sustava koji sudjeluju u pružanju usluge. Ukoliko temeljni Ugovor nema važenje više od 12 mjeseci navedeno se mora napraviti protekom roka navedenog u temeljnog Ugovoru

4. Prijenos podataka u treće zemlje

- Zabranjuje se Izvođaču prijenos podataka u SAD.
- Izvođač mora dostaviti popise zemalja u koje se prenose podaci koji se vežu uz temeljni i ovaj Ugovor.

Paraf Voditelja obrade

_____

Prilog 4. Uputa Izvršitelju obrade

Voditelj obrade nalaže izvršitelju obrade dostavu sljedeće dokumentacije na pregled:

VRSTA DOKUMENTA
Pravilnik o zaštiti osobnih podataka- molimo dostaviti.
Smjernice za postupanje uslijed COVID 19/ smjernice za rad od kuće- molimo dostaviti.
Pravilnik o tehničkim, organizacijskim i sigurnosnim mjerama- molimo dostaviti.
Interni akt u kojem se jasno vide procedure postupanja tijekom incidenta /povrede osobnih podataka
RADNI ODNOSI
Ugovor o radu- dostaviti primjerak.
Izjava o povjerljivosti za radnike- dostaviti primjerak potpisane izjave.
Obavijest radnicima- dostaviti primjerak.
Smjernice za zaštitu osobnih podatak u radnim odnosima- jeste li ih donijeli ili ste radnike upoznali s njihovim pravima na drugi način? Opišite.
UGOVORI O OBRADI I DJELJENJU PODATAKA
Molimo Vas da nam se dostavi popis podizvršitelja ili izvršitelja s kojima se dijele podaci vezani uz ovaj Ugovor. Priložite i preslike Ugovora o obradi i dijeljenju podataka. U slučaju da se podaci ne dijele s podizvršiteljima molimo pisanu potvrdu odgovorne osobe o navedenom.
EVIDENCIJE AKTIVNOSTI OBRADE
Vidjeti Prilog 3.
OBRASCI
Obrazac 1: Zahtjev za dopunu ili ispravak
Obrazac Z2: Zahtjev za ispravak ili dopunu osobnih podataka
Obrazac Z3: Zahtjev za brisanje osobnih podataka
Obrazac Z4: Zahtjev za ograničenje obrade osobnih podataka
Obrazac Z5: Zahtjev za prenošenje osobnih podataka
Obrazac Z6: Prigovor na obradu osobnih podataka
Ukoliko ne ostvarujete prava ispitanika sukladno određenim obrascima, molimo Vas da nam detaljno opišete procedure ostvarivanja prava? Kako legitimirate ispitanike?
TESTOVI PROCJENE UČINKA
Test procjene učinka (DPIA) Internet stranica, sustavi pohrane podataka, e mail sustvai, i sl.? Kada ste proveli zadnji test procjene učinka i za koje obrade ste ih proveli? Molimo dostaviti primjerak.
SLUŽBENIK ZA ZAŠTITU PODATAKA

Odluka o imenovanju službenika za zaštitu podataka- dostaviti ukoliko ste imenovali službenika.
OSTALO
Prava ispitanika, kako ostvarujete prava i koje procedure ste uspostavili?
Razduživanje opreme prilikom odlaska zaposlenika, jeste li uredili i uspostavili procedure?
Odluka ovlaštenje pristupa osobnim podacima- jeste li ih donijeli?
Procjena legitimnog interesa- obrađujete li podatke na temelju legitimnog interesa? Ukoliko da jeste li provodili test legitimnosti? Molimo primjerak. Također, molimo potvrdu odgovorne osobe da se podaci koji se dijele s Voditeljem obrade ne koriste u druge svrhe.

Paraf Voditelja obrade

_____

Prilog 5. Popis podizvođača

Naziv podizvođača	Adresa sjedišta	Kategorije podataka koje se dijele s podizvođačem/ pravni osnov i rokovi čuvanja	Stvarna lokacija obrade

(*Uputa: Popunjava Izvođač odnosno Izvršitelj obrade*)

Paraf Izvršitelja obrade

_____

_____

_____

_____

_____

_____

(Uputa: Ovaj dio popunjava Voditelj obrade s obrazloženjem i potvrdom odobrava li popis Podizvođača ili ne. U slučaju da nema podizvođača isto se konstatira).

Paraf Voditelja obrade

_____