POLITIKA ZAŠTITE OSOBNIH PODATAKA

1. Uvod

Politika zaštite osobnih podataka (dalje u tekstu: Politika) uređuje način i opseg preporučljivog postupanja pri svakom prikupljanju, obradi i pohrani osobnih podataka od strane društva HOTEL LERO d.o.o., Iva Vojnovića 14, Dubrovnik, OIB: 97744396969, (dalje u tekstu: Društvo). Navedena Politika postavlja smjernice kojima se nastoji, u mjeri u kojoj je to moguće s obzirom na okolnosti svakog pojedinog slučaja, uspostaviti sukladnost s Uredbom EU 2016/679 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka od 27. travnja 2016. godine (Opća uredba o zaštiti podataka).

Svrha ove Politike je uspostaviti standarde za sve rukovoditelje, zaposlenike i druge djelatnike prilikom rada i profesionalnog djelovanja u Društvu, i to u odnosu na postupanje sa osobnim podacima. Krajnji cilj bi pritom bio minimalizirati rizik vezan uz potencijalne nesukladnosti s primjenjivim propisima, a o čemu dakako ovisi pravodobna i kvalitetna reakcija zaposlenika u svakom pojedinom slučaju. S tim u vezi se zaposlenici pozivaju da, u slučaju nerazumijevanja pojedinih odredbi ove Politike, nejasnoća prilikom njihovog implementiranja u poslovanje ili bilo kakve dvojbe vezane uz trenutno ili buduće prikupljanje, obradu ili pohranu osobnih podataka, zaustave svako postupanje te da se obvezno obrate nadležnom službeniku za zaštitu podataka radi daljnjeg savjetovanja i uputa.

Zaštita osobnih podataka jedno je od temeljnih ljudskih prava. Društvo je svjesno važnosti pouzdane i sigurne obrade osobnih podataka svojih gostiju, radnika i drugih fizičkih osoba čije osobne podatke prikuplja i dalje obrađuje.

Ovim Politikom Društvo stvara jedinstvenu i visoku razinu zaštite osobnih podataka koje obrađuje.

Društvo ostvaruje zaštitu osobnih podataka ponajprije na sljedeće načine:

a) usvajanjem ove Politike, kojom se reguliraju opća pravila vezana uz zaštitu osobnih podataka od strane Društva,
b) usvajanjem posebnih internih pravilnika ili protokola kojima se detaljnije regulira obrada osobnih podataka,
c) primjenom kadrovskih, organizacijskih i tehničkih mjera zaštite osobnih podataka,
d) imenovanjem službenika za zaštitu podataka,
e) ažurnim vođenjem evidencija o aktivnostima obrade osobnih podataka,
f) kontinuiranom edukacijom radnika o važnosti zaštite osobnih podataka.

2. Definiranje i razumijevanje ključnih pojmova

U svrhu boljeg razumijevanja pojmova koji će biti prisutni u brojnim odredbama Politike, u nastavku se navode sljedeće definicije:

2.1. Osobni podaci

Pod navedenim pojmom uzimaju se svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi izravno ili neizravno, odnosno 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.

2.2. Obrada i pohrana osobnih podataka

Obrada osobnih podataka označava svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim ili 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 osobnih podataka.

Prikupljanje, obrada ili pohrana osobnih podataka može biti izvršena nad osobnim podacima u u bilo kojem obliku, bilo neautomatiziranom (poput obrazaca, dokumenata priskrbljenih od strane klijenata, zaposlenika, ručno uvedenih zapisa o osobnim podacima), poluautomatiziranom (ručno unošenje u Excel tablice ili skeniranje, nakon čega se podaci šalju na daljnju obradu) i automatiziranom (bilo putem elektroničkih obrazaca ili pristupnih kartica, web stranica itd).

Obrađeni podaci, ili oni koji su u postupku obrade, pohranjuju se u određene sustave odnosno u strukturirani skup osobnih podataka, dostupnih i klasificiranih prema posebnim kriterijima (kategorijama osobnih podataka, bilo općih ili posebnih), te novisno jesu li centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi. Određena odstupanja u vezi obrade osobnih podataka pritom postoje pri obradi u znanstvene, javne ili statističke svrhe.

2.3. **Ispitanik i primatelj osobnih podataka**

Pojam ispitanika označava fizičku osobu čije osobne podatke Društvo prikuplja, odnosno koja osoba je Društvu podnijela navedene podatke ili čiji su osobni podaci Društvu iz zakonom predviđenih razloga dostavljeni (klijenti, sadašnji ili potencijalni zaposlenici Društva, vanjski suradnici itd).
Pojam primatelja osobnih podataka označava fizičku ili pravnu osobu, tijelo javne vlasti, agencija ili drugo tijelo kojem se iz određenih razloga otkrivaju osobni podaci

2.4. **Voditelj obrade i izvršitelj obrade**

Voditelj obrade je Društvo, koje samostalno ili zajedno s drugim voditeljem obrade (npr u slučaju prikupljanja osobnih podataka zajedno s drugim društvom partnerom) određuje svrhe i sredstva obrade osobnih podataka. Izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime Društva (npr vanjsko računovodstvo).

2.5. **Automatizirano donošenje odluka i izrada profila**

Automatizirano donošenje odluka označava situaciju kada računalni program Društva na temelju svojih tehničkih postavki i softvera obrađuje osobne podatke ispitanika bez ljudske intervencije, dakle isključivo na bazi nekog prethodno zadanog algoritma (primjera radi, program koji automatski prihvaća ili ne prihvaća određeni zahtjev ispitanika temeljem određenih pretpostavki).

Izrada profila označava svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca (primjera radi, program koji analizira potrošačke navike ispitanika i temeljem njih šalje određene ponude).

Radi izbjegavanja svake dvojbe, Društvo ne primjenjuje automatizirano pojedinačno donošenje odluka. Sve odluke koje proizvode pravne učinke koji se odnose na ispitanika ili na sličan način značajno na njega utječu donose se uz značajnu ljudsku intervenciju.

2.6. **Pseudonimizacija**

Navedeni pojam označava obradu pri kojoj se osobni podaci više ne mogu pripisati određenom pojedincu bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi

3. **Primjena Politike**

Politika se primjenjuje pri svakom prikupljanju i obradi osobnih podataka fizičkih osoba, neovisno u kojoj fazi, odnosno obavljaju li se tek inicijalne pripreme ili je postupak već u tijeku.

Osobni podaci koji su izuzeti od primjene ovog Politike su

a) podaci o pravnim osobama (primjer - trgovačka društva, udruge, javna tijela)
b) podaci o preminulim osobama, te
c) podaci temeljem kojih nije moguća identifikacija fizičke osobe, niti samostalno niti dovođenjem u vezu s nekim drugim podacima (primjera radi – pseudonimizacija).

Ova Politika temeljni je akt Društva primjenjiv na sve aktivnosti obrade osobnih podataka koje Društvo obavlja, a koje osobito uključuju:

a) obradu osobnih podataka radnika pri sklapanju, izvršavanju i obradi ugovora o radu i za kontaktiranje potencijalnih radnika u selekcijskim postupcima prije donošenja odluke o zapošljavanju,
b) obradu osobnih podataka fizičkih osoba koje Društvo angažira temeljem ugovora o djelu, autorskih ugovora i sličnih ugovora,
c) obradu osobnih podataka radnika zaposlenih kod dobavljača Društva,
d) obradu osobnih podataka učenika i studenata koji u Društvu obavljaju stručnu praksu ili su na povremenom učeničkom ili studentskom radu, te pri selektiranju, ugovaranju i provedbi postupaka stipendiranja učenika i/ili studenata od strane Društva,
e) obradu osobnih podataka članova obitelji zaposlenih radnika u dijelu koji je nužan za provedbu zakonskih obveza ili ostvarivanje nekog prava prema važećem kolektivnom ugovoru (npr. ostvarivanje prava na poreznu olakšicu, plaćeni dopust, nagradu za rođenje djeteta, pravo na prigodni dar za dijete i slično),
f) obradu osobnih podataka vezano za sklapanje, provedbu i obradu ugovora o hotelskim uslugama s poslovnim i privatnim korisnicima i provedbu prigodnih aktivnosti oglašavanja i ispitivanja tržišta s ciljem informiranja korisnika usluga i zainteresiranih trećih strana o uslugama koje Društvo nudi,
g) obradu osobnih podataka vezano za sklapanje, provedbu i obradu druge vrste ugovora čiji je predmet pružanje neke od usluga koje su u sadržaju registrirane djelatnosti Društva (kao npr. ugovor o pružanju usluga prehrane i točenja pića bez obzira na narav ugovora),
h) obradu podataka o udjeličarima ili dioničarima Društva, ovisno o pravnom ustroju Društva,
i) sve druge aktivnosti obrade osobnih podataka koje Društvo obavlja ili bi u budućnosti moglo obavljati bilo na povremenoj, bilo na kontinuiranoj osnovi.

Ova Politika obvezujuća za sve organizacijske jedinice Društva.
Ova Politika obvezujuća je i za sva ona društva od kojih Društvo može zahtijevati da je prihvate (npr. izvršitelje obrade).

Odredbe Politike namijenjene su osiguravanju visoke i jedinstvene razine zaštite osobnih podataka u Društvu. Ova Politika nema utjecaja na postojeće ili buduće obveze ustanovljene zakonima i drugim propisima koje Društvo mora poštovati u pogledu obrade i korištenja osobnih podataka, a koja su šireg opsega od načela utvrđenih ovim Politikom.

Odredbe ove Politike nemaju utjecaja na primjenjivost nacionalnog zakonodavstva donesenog u vezi s nacionalnom sigurnošću, obranom ili javnom sigurnošću ili za sprječavanje i istragu kaznenih djela i progon počinitelja kaznenih djela.

4. **Adresati**

Svi rukovoditelji, zaposlenici i djelatnici Društva (dalje u tekstu: Zaposlenici) adresati su primjene ove Politike, odnosno nositelji odgovornosti prilikom pravilnog prikupljanja, obrade i pohrane osobnih podataka. Navedena odgovornost pritom predstavlja i jednu od radnih obveza svakog pojedinog zaposlenika.

Navedeni adresati pri svim navedenim i/ili sličnim radnjama i/ili situacijama postupaju u dobroj vjeri i s dužnom pažnjom, imajući pri tome na umu najbolji interes svih ispitanika čiji se osobni podaci prikupljaju, obrađuju i pohranjuju, što je prije svega nužni preduvjet za ispravnu primjenu ove Politike.

Pravila primjenjiva na pojedina područja obrade osobnih podataka u Društvu detaljnije će se urediti pojedinačnim pravilima koja moraju biti u skladu sa svim relevantnim propisima iz područja zaštite osobnih podataka i ovom Politikom.

Radi detaljnijeg reguliranja pojedinih područja obrade osobnih podataka, Društvo može donijeti akte (*npr. Politiku sigurnosti informacijskog sustava, Pravilnik o obradi osobnih podataka radnika i drugih osoba koje Društvo angažira za rad, Pravilnik o video nadzoru, Pravilnik o zaštiti i obradi arhivskog i registraturnog gradiva i slično*). Društvo u svako doba može donijeti pravilnike koje smatra potrebnim radi postizanja veće razine zaštite osobnih podataka na pojedinom području poslovanja, pri čemu takvi pravilnici nadopunjuju odredbe ove Politike te joj ne smiju proturječiti.

5. **Načela**

Osnova svih postupanja iz predmetne Politike temelje se na sljedećim načelima kojih se treba pridržavati pri svakom ophođenju sa osobnim podacima.

5.1. **Načelo zakonitog, poštenog i transparentnog postupanja** određuje da svako postupanje mora biti u skladu sa zakonom odnosno drugim primjenjivim propisima te izvršeno na pošten i transparentan način.

Kako bi ispitanicima bilo jasno da se njihovi podaci prikupljaju i obrađuju te u koje svrhe se to čini, Društvo na odgovarajući način obavještava ispitanike između ostalog o svrsi obrade, što uključuje informiranje o tome koji se podaci prikupljaju, obrađuju i koriste, za koje namjene i koliko dugo se čuvaju te kojim se primateljima podaci otkrivaju. Obavijesti ispitanicima daju se putem različitih kanala, ovisno o tome što je prema okolnostima slučaja najprikladnije, a mogu uključivati: obavijesti putem web stranice Društva, pisane obavijesti u prostorijama Društva, pisane obavijesti na obrascima koje Društvo koristi, pisane obavijesti u

sklopu ugovora koje Društvo sklapa s ispitanikom, davanje obavijesti putem e-maila, usmeno davanje obavijesti od strane radnika Društva, a po potrebi i druge načine.

Društvo osobito obavještava ispitanike o njihovim pravima i o načinu na koji ih mogu ostvarivati. Kontakt podaci službenika za zaštitu podataka javno su dostupni.

5.2. **Načelo prikupljanja podataka isključivo temeljem zakonom dopuštenih razloga** određuje da se osobni podaci prikupljaju samo u posebne, izričite i zakonite svrhe te se ne smiju obrađivati na način koji nije u skladu s navedenim svrhama.

5.3. **Načelo ograničenja količine podataka i razmjernosti** određuje da se svako prikupljanje osobnih podataka mora svesti na najnužniju mjeru te da se prikupljaju samo oni podaci koji su relevantni i razmjerni svrsi temeljem koje se obrađuju.

5.4. **Načelo točnosti i ažurnosti** određuje potrebu da se pazi na točnost podataka koji se prikupljaju i unose u baze podataka te da je potrebno poduzeti svaku razumnu mjeru radi osiguravanja da se netočni osobni podaci bez odlaganja izbrišu ili isprave, uzimajući u obzir svrhe u koje se obrađuju.

5.5. **Načelo ograničenja pohrane** određuje da je potreba čuvanja podataka koji omogućuju identifikaciju fizičkih osoba ograničena svrhom radi koje se osobni podaci obrađuju. Osobni podaci moraju se čuvati u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. U slučajevima kada će to biti moguće, Društvo može primijeniti postupke za brisanje identifikacijskih obilježja ispitanika (anonimizacija) ili za zamjenu identifikacijskih obilježja drugim karakteristikama (pseudonimizacija).

Rokovi čuvanja različitih kategorija osobnih podataka navedeni su u evidenciji o aktivnostima obrade (ako se vode) zasebno za različite vrste osobnih podataka. Rokovi čuvanja određuju se uzimajući u obzir zakonske zahtjeve te potrebe zaštite interesa Društva.

Društvo može kroz Pravilnik o zaštiti i obradi arhivskog i registraturnog gradiva, regulirati rokove čuvanja dokumentacije po pojedinim poslovnim područjima Društva.

5.6. **Načelo sigurnosti osobnih podataka** određuje da svako ophođenje s osobnim podacima mora biti izvršeno na način koji osigurava najviši mogući stupanj sigurnosti tih podataka, uključujući zaštitu od neovlaštene i/ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovorajućih tehničkih ili organizacijskih mjera

6. Svrhe obrade osobnih podataka

Nužno je da svako prikupljanje ili obrada osobnih podataka ima svoju svrhu, odnosno razlog temeljem kojeg se određeni osobni podaci prikupljaju odnosno obrađuju. Navedeni razlozi su određeni, definirani i taksativno navedeni te tebaju biti jasno i nedvosmisleno naznačeni pri svakoj obradi osobnih podataka:

6.1. Privola ispitanika

Prikupljanje i obrada podataka temelji se na privoli/pristanku ispitanika, koja je dana u jednu ili više posebnih svrha.

6.2. Izvršenje ugovora

Prikupljanje i obrada podataka nužni su za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora (primjera radi - za sklapanje ugovora je potrebno definirati ugovorne stranke, koje se mogu identificirati samo putem osobnih podataka)

6.3. Pravna obveza Društva

Prikupljanje i obrada određenih podataka od strane Društva proizlazi iz zakonske obveze koja obvezuje društvo na navedene radnje i suradnju s tijelima javne vlasti (primjera radi – prikupljanje podataka o radnicima za zavod za mirovinsko i zdravstveno osiguranje, porezna uprava, carinska tijela, neovisna upravna tijela, hrvatska turistička zajednica)

6.4. Legitimni interesi Društva ili treće strane

Prikupljanje i obrada podataka je nužna za potrebe legitimnih interesa Društva ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, a osobito ako je ispitanik dijete (primjera radi – legitimni interes hotela da postavi sustav videonadzora, kako bi osigurao sigurnost nadziranog prostora).

U slučaju kada Društvo obrađuje osobne podatke na osnovi svog legitimnog interesa koji je očigledan, narav svog legitimnog interesa i okolnosti na temelju kojih je Društvo zaključilo da njegov legitimni interes prevladava na interesima, pravima i slobodama ispitanika navodi u evidenciji o aktivnostima obrade ukoliko ih je obvezan voditi. U slučajevima kad legitimni interes nije očigledan već zahtijeva primjenu detaljnijeg testa proporcionalnosti i dublju analizu, Društvo u pisanom obliku detaljnije dokumentira razloge na temelju kojih je utvrdilo da legitimni interes Društva prevladava.

6.4.1. Obrada u svrhe izravnog marketinga

Može se smatrati da postoji legitimni interes Društva za obradu osobnih podatka za svrhe izravnog marketinga. Pritom se treba raditi o osobnim podacima koje je Društvo prije toga zakonito prikupilo, a upotreba podataka u svrhe izravnog marketinga mora biti u okvirima onoga što ispitanik razumno može očekivati temeljem svog odnosa s Društvom kao voditeljem obrade. U protivnom, obrada osobnih podataka

u svrhe izravnog marketinga ne može se temeljiti na legitimnom interesu, već samo na izričitoj privoli ispitanika.

Ako se osobni podaci obrađuju za potrebe izravnog marketinga temeljem legitimnog interesa Društva, ispitanik u svakom trenutku ima pravo prigovoriti obradi osobnih podataka u svrhe izravnog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom. Najkasnije u trenutku prve komunikacije s ispitanikom, ispitanika se na ovo pravo upozorava na jasan način i odvojeno od bilo koje druge informacije. Ako se ispitanik usprotivi obradi za potrebe izravnog marketinga, njegovi osobni podaci više se ne smiju obrađivati u takve svrhe.

Radi izbjegavanja svake dvojbe, Društvo potvrđuje da je slanje različitih komunikacija (*npr. newslettera i novosti o pogodnostima i uslugama Društva*) moguće samo na temelju privole ispitanika, koju on izražava popunjavanjem odgovarajućih polja na web stranici Društva nakon što je obaviješten o obradi osobnih podataka te verifikacijom putem linka poslanog na e-mail kojeg je naveo za primanje obavijesti.

Osim od ispitanika, Društvo neće ni na koji drugi način prikupljati e-mail adrese ni druge podatke kako bi ispitanicima slalo newslettere. U svim takvim komunikacijama koje se upućuju ispitaniku, mogućnost odjave od daljnjeg primanja komunikacija (*unsubscribe*) jasno je istaknuta. Odjava predstavlja povlačenje privole. U slučaju odjave, Društvo briše osobne podatke ispitanika koje je prikupilo u svrhu izravnog marketinga.

6.5. **Zadaća od javnog interesa**

Prikupljanje i obrada podataka je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti.

6.6. **Zaštita ključnih interesa ispitanika ili druge fizičke osobe**

Prikupljanje i obrada podataka je nužna u svrhu zaštite ključnih interesa ispitanika ili druge fizičke osobe.

7. **Privola ispitanika**

Privola ispitanika je valjana osnova za prikupljanje osobnih podataka samo ako je Društvu iskomunicirana jasnom potvrdnom radnjom kojom se izražava dobrovoljan, izričit, informiran i nedvosmislen pristanak ispitanika, i to na način koji može biti u pisanom ili elektroničkom obliku te putem usmene izjave.

Važno je pritom imati u vidu činjenicu da Društvo nosi teret dokaza da je ispitanik doista dao svoju privolu za prikupljanje odnosno obradu osobnih podataka. Uzevši navedeno u obzir zaprimanje privole isključivo u usmenom obliku u pravilu nije preporučljivo.

Neovisno o obliku privole, komunikacija sa ispitanikom u vezi s navedenim mora biti u lako razumljivom obliku, uz uporabu jasnog i jednostavnog jezika i to bez ikakvih nepoštenih uvjeta.

7.1. **Privola ispitanika u pisanom obliku**

Ispitanik svoju privolu može dati u pisanom obliku, u kojem obliku je poželjno da se ispitanik na kraju potpiše te naznači datum davanja privole.

Isto tako, u slučaju da Društvo traži privolu u pisanom obliku u kojem se osim predmetnog zahtjeva traže i drugi podaci odnosno neke druge izjave i odgovori, potrebno je predmetni zahtjev predočiti na način da ga se može jasno razlučiti od tih drugih pitanja, odnosno da navedeno nije prezentirano na način koji bi mogao zbuniti ispitanika.

7.2. **Privola ispitanika u elektroničkom obliku**

Ispitanik svoju privolu može dati u elektroničkom obliku. Zahtjev Društva za davanjem privole pritom mora bit jasan, jezgrovit i ne smije nepotrebno ometati upotrebu usluge za koju se upotrebljava (*primjera radi – agresivni cookies od kojih nije moguće pristupiti sadržaju itd*).

Uzevši u obzir činjenicu da privola mora biti nedvosmislena i svojevoljna, potrebno je imati na umu da nije dozvoljeno „navoditi" na privolu, pogotovo na način da se polje kojim se daje privola unaprijed označi kvačicom, ili na neki drugi način koji bitno utječe na korištenje određene internetske stranice, odnosno biranjem tehničkih postavki, već je nužno da predmetni izbor bude „neutralan". Također se prilikom sastavljanja navedenog treba uzeti u obzir da se šutnja odnosno neaktivnost ispitanika ne smije ni u kojem slučaju tumačiti kao davanje privole.

7.3. **Dobrovoljnost privole**

U obrascima ili zahtjevima ispitaniku treba doista biti ponuđen slobodan izbor, pri kojem je moguće odbiti zahtjev odnosno povući danu privolu bez ikakvih posljedica.

U slučaju kada je obrazac ili zahtjev za otkrivanjem osobnih podataka usko povezan uz pružanje usluge ili izvršenje ponuđenog ugovora, Društvo zahtijeva samo podatke nužne za pružanje navedene usluge odnosno izvršenje ponuđenog ugovora.

7.4. **Postupak u slučaju povlačenja privole**

Ispitanik ima pravo povući danu privolu te Društvo omogućuje svakom ispitaniku da u bilo koje doba može na jednostavan način povući privolu, a o kojoj mogućnosti ispitanik mora biti prethodno obaviješten i što mu mora biti omogućeno jednostavnim kontaktiranjem Društva pisanim putem ili putem interneta. Nakon povlačenja privole zabranjena je svaka daljnja obrada osobnih podataka ispitanika. Potencijalno povlačenje privole pritom ne utječe na zakonitost obrade predmetnih podataka prije nego je privola povučena.

8. **<u>Ispunjenje prethodne obveze informiranja ispitanika</u>**

Osobne podatke ispitanika Društvo zaprima od samog ispitanika te iz drugog izvora. U oba slučaja Društvo daje obavijest ispitaniku o svim relevantnim informacijama u vezi prikupljanja i obrade osobnih podataka koji se na njega odnose.

Obvezu pružanja informacija ipak nije potrebno izvršiti
a) ako ispitanik već posjeduje tu informaciju,
b) ako je bilježenje ili otkrivanje osobnih podataka izrijekom propisano zakonom ili
c) ako je pružanje informacije ispitaniku nemoguće ili bi zahtijevalo nerazmjeran napor te ako

d) osobni podaci moraju ostati povjerljivi u skladu s obvezom čuvanja profesionalne tajne, koja obveza može biti propisana primjenjivim propisima ili statutom

8.1. **Informacije koje Društvo pruža ispitaniku u slučaju prikupljanja podataka direktno od ispitanika**

Prilikom prvog prikupljanja osobnih podataka od ispitanika Društvo ispitaniku pruža sljedeće podatke vezane uz samu obradu:

a) identitet i kontaktne podatke Društva, odnosno predstavnika Društva (odrediti zaposlenika koji će biti kontakt osoba)
b) kontaktne podatke službenika za zaštitu podataka, ako je imenovan
c) svrhu obrade osobnih podataka kao i pravnu osnovu za obradu, a ukoliko je svrha temeljena na legitimnim interesima Društva, definirati ih
d) primatelje predmetnih podataka, ako postoje, odnosno kome će se sve ti osobni podaci slati ako se planiraju prenositi izvan Društva;
e) ako je primjenjivo, činjenicu da Društvo namjerava osobne podatke ispitanika prenijeti trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Komisije o primjerenosti za tu zemlju odnosno upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje.
f) razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima bi se utvrdilo to razdoblje (ili dokle god traje pravna osnova za obradu ili interno ograničenje npr. 1 godina)
g) obznaniti ispitaniku njegova prava odnosno da ispitanik ima (I) pravo uvida u osobne podatke koji se obrađuju, (II) pravo na ispravak ili brisanje osobnih podataka, (III) pravo na ograničavanje obrade, (IV) pravo na ulaganje prigovora na obradu, (V) pravo prenijeti podatke drugom voditelju obrade, (VI) pravo povući privolu, (VII) pravo podnošenja prigovora nadzornom tijelu, te na koji način može ostvariti navedena prava (npr. pisanim putem, e-mailom, ispunjavanjem obrasca itd.)
h) informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže;
i) informaciju o tome postoji li sustav automatiziranog donošenja odluka, što uključuje izradu profila ispitanika

Nadalje, u situaciji kada se prikupljeni podaci naknadno obrađuju u svrhu koja je različita od one za koju su osobni podaci prvotno prikupljeni, Društvo je dužno ispitaniku navesti novu svrhu obrade te relevantne informacije navedene kao gore.

8.2. **Informacije koje Društvo pruža ispitaniku u slučaju prikupljanja podataka iz izvora različitog od ispitanika**

U predmetnom slučaju Društvo pruža iste informacije kao pod 8.1. izuzev one pod h), te uz navedeno naznačuje i izvor dobivenih osobnih podataka (ili ako je izvor javno dostupan).

Navedene informacije Društvo pruža u razumnom roku, a najkasnije mjesec dana od dana dobivanja predmetnih osobnih podataka ispitanika. Međutim, postoje dva slučaja koja odstupaju od navedenog pravila i pri kojima je postupanje drugačije, a to je:

a) ako se prikupljeni osobni podaci trebaju upotrijebiti za komunikaciju s ispitanikom, onda Društvo informacije pruža ispitaniku najkasnije u trenutku prve ostvarene komunikacije, te
b) ako je predviđeno otkrivanje podataka nekom drugom primatelju, onda Društvo informacije pruža najkasnije u trenutku kada su osobni podaci prvi put otkriveni

Nadalje, i u ovom slučaju Društvo nanovo navodi sve relevantne infomacije ukoliko se predmetni osobni podaci naknadno obrađuju temeljem svrhe koja je različita od one prvotne.

9. Vrijeme pohrane osobnih podataka

U odnosu na vrijeme pohrane određenih osobnih podataka, postoje osobni podaci čije je vrijeme pohrane zakonom propisano (*npr. posebni propisi o radnoj evidenciji za studente određuje da se podaci ne smiju brisati 6 godina od prestanka radnog odnosa ili u vezi računovodstvenih isprava određuju da se ne smiju brisati 11 godina od nastanka)* i osobni podaci čije vrijeme pohrane nije zakonom propisano.

Društvo u svakom slučaju podatke pohranjuje na minimalan period koji je zakonski dozvoljen i/ili potreban u odnosu na poslovne aktivnosti Društva te ih odmah nakon toga briše. Ukoliko ocijeni potrebnim, Društvo internim aktom može odlučiti koji će se podaci brisati ručno ili automatski nakon određenog perioda vremena (npr 1 godina, 2 godine itd) ili s obzirom na određeni događaj (npr kraj fiskalne godine).

10. Obrada posebnih kategorija osobnih podataka

Načelno se ne vrši obrada sljedećih tipova osobnih podataka: podaci koji se odnose na rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu, genetski podaci, biometrijski podaci u svrhu jedinstvene identifikacije pojedinca te podaci koji se odnose na zdravlje, spolni život i seksualnu orijentaciju pojedinca.

Gore navedene kategorije osobnih podataka Društvo ipak obrađuje u sljedećim situacijama:

a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka i to za jednu ili više određenih svrha, osim ako primjenjivi propisi navode da takva privola ne proizvodi učinak
b) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava Društva ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru primjenjivih propisa ili kolektivnog ugovora
c) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu;
d) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik
e) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;
f) obrada je nužna za potrebe značajnog javnog interesa na temelju primjenjivih propisa koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika;
g) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju primjenjivih propisa.

Svi zaposlenici moraju prilikom prikupljanja, obrade odnosno pohrane posebnih kategorija osobnih podataka postupati sa povećanom pažnjom.

Prisutna je mogućnost daljnjih promjena primjenjivih propisa u pogledu postupanja sa posebnim kategorijama osobnih podataka, te je s tim u vezi potrebno savjetovati se sa službenikom za zaštitu podataka.

10.1. **Posebnosti obrade podataka dobivenih videonadzorom**

Društvo obradu osobnih podataka putem video nadzora provodi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem video nadzora.

Društvo na vidljivom mjestu naznačuje da je objekt odnosno pojedina prostorija u njemu pod video nadzorom, zajedno sa kontakt podacima Društva putem kojih ispitanik može ostvariti svoja prava.

Obrada osobnih podataka zaposlenika putem sustava video nadzora provodi se samo ako su uz uvjete utvrđene ovim zakonom, ispunjeni i uvjeti utvrđeni propisima koji reguliraju zaštitu na radu i ako su zaposlenici bili pojedinačno unaprijed obaviješteni o takvoj mjeri i ako je Društvo informiralo zaposlenike prije donošenja odluke o postavljanju sustava video nadzora. Navedeni videonadzor pritom ne smije obuhvaćati prostorije za odmor, osobnu higijenu i presvlačenje.

Pravo pristupa osobnim podacima prikupljenim putem video nadzora imaju samo ovlaštene osobe te se snimke dobivene putem video nadzora mogu čuvati najviše 6 mjeseci, osim ako je drugim zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom ili drugom sličnom postupku.

10.2. **Posebnost obrade biometrijskih podataka i fotografija**

Društvo provodi obradu biometrijskih podataka samo ako je navedeno propisano zakonom ili ako je nužno za zaštitu osoba, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačno i sigurno identificiranje korisnika usluga, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom biometrijskih podataka iz ovog članka.

Pravni temelj za obradu biometrijskih podataka ispitanika radi sigurnog identificiranja je izričita privola takvog ispitanika.

Društvo provodi obradu biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija, ako je propisano zakonom ili ako se takva obrada provodi alternativno drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija uz uvjet da je zaposlenik dao izričitu privolu za takvu obradu biometrijskih podataka.

Obradu fotografija se ne bi trebalo smatrati obradom posebnih kategorija osobnih podataka jer su one biti obuhvaćene samo definicijom biometrijskih podataka pri obradi posebnim tehničkim sredstvima kojima se omogućuje jedinstvena identifikacija ili autentifikacija pojedinca te se takvi osobni podaci ne bi se smjeli obrađivati osim ako je obrada dopuštena u posebnim slučajevima.

10.3. **Posebnosti obrade osobnih podataka djeteta**

Primjenjivi propisi posebnu zaštitu daju osobnim podacima djece, i to one mlađe od 16 godina, iz razloga što navedena kategorija ispitanika može u pravilu biti manje svjesna potencijalnih rizika i posljedica.

Navedeno se posebno odnosi na upotrebu osobnih podataka djece u svrhu marketinga ili stvaranja osobnih ili korisničkih profila te prikupljanje osobnih podataka o djeci prilikom upotrebe usluga koje se izravno nude djetetu.

Obrada predmetnih podataka je u pravilu zakonita samo pod uvjetom da je privolu dao nositelj roditeljske odgovornosti nad djetetom (roditelj, skrbnik, staratelj itd). Društvo ulaže razumne napore kako bi se, uzimajući u obzir dostupnu tehnologiju, provjerilo odnosno utvrdilo postoji li navedeni pristanak roditelja (putem web obrazaca npr). Međutim, privola roditeljske odgovornosti ipak nije nužna u kontekstu preventivnih usluga ili usluga savjetovanja koje su ponuđene izravno djetetu.

11. **Postupanje prilikom ostvarivanja prava ispitanika**

Ispitanik u pogledu vlastitih osobnih podataka koje Društvo prikuplja i obrađuje ima određena prava koja se moraju ispoštovati u slučaju zahtijevanja njihovog ostvarivanja.

Društvo utvrđuje identitet osobe koja tvrdi da je ispitanik i zahtijeva uvid u osobne podatke odnosno ostvarenje drugih prava. Navedeno utvrđuje zahtijevanjem identifikacije putem službenih dokumenata poput osobne iskaznice, putovnice ili vozačke dozvole ili referentnog broja klijenta na drugačiji način web identifikacije. Društvo također, ukoliko ocijeni potrebnim, vodi evidenciju svih upita i aktivnosti provedenih u skladu s tim upitima. Navedeni postupak je na trošak Društva ali u slučaju brojnih upita istog ispitanika postoji mogućnost naplate administrativnih troškova.

11.1. **Ostvarivanje prava ispitanika na pristup osobnim podacima**

U slučaju predmetnog zahtjeva u pisanom ili elektroničkom obliku, Društvo izdaje potvrdu o tome obrađuju li se osobni podaci ispitanika, te navodi koji se točno podaci obrađuju odnosno omogućuje pristup tim podacima (i predaje presliku navedenih osobnih podataka, osim ako preslika sadrži i osobne podatke drugih ispitanika).

Uz to, Društvo također navodi i informacije o:

a) svrsi obrade;
b) kategorijama osobnih podataka o kojima je riječ
c) primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama;
d) ako je to moguće, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja;
e) postojanju prava da se od Društva zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika ili prava na prigovor na takvu obradu, odnosno prava na podnošenje prigovora nadzornom tijelu,
f) svakoj dostupnoj informaciji o izvoru osobnih podataka, ukoliko se oni ne prikupljaju od ispitanika;

g) informaciju o tome postoji li sustav automatiziranog donošenja odluka, što uključuje izradu profila ispitanika

11.2. **Način ostvarivanja prava**

Svoja prava ispitanik može ostvarivati slanjem pisanog zahtjeva službeniku za zaštitu podataka putem e-maila ili poštom. Kontakt podaci službenika za zaštitu podataka su javno dostupni na web stranici Društva.

Za pojedine kategorije ispitanika (npr. radnici) posebnim se pravilnikom mogu predvidjeti i druge, dodatne kontakt osobe kojima se ispitanici mogu obratiti radi što lakšeg ostvarivanja svojih prava.

U slučaju da bilo koji radnik Društva primi zahtjev ispitanika u bilo kojem obliku, isti će bez odgode proslijediti službeniku za zaštitu podataka, ili će o tome obavijestiti svog nadređenog, koji će ga proslijediti službeniku. Društvo je obvezno radnike upoznati s obvezom postupanja na ovaj način. Iznimno, službenika nije potrebno obavještavati u slučajevima kada ovlašteni radnik Društva na zahtjev radnika ili drugih ispitanika ažurira njihove osobne podatke u evidencijama koje Društvo vodi.

Po primitku pisanog zahtjeva ispitanika, službenik će isti razmotriti. Ovisno o složenosti zahtjeva, službenik može odlučiti da će sam izraditi odgovor na zahtjev, ili da će nacrt odgovora na zahtjev ispitanika pripremiti radnik društva uz čije je radne zadatke zahtjev ispitanika vezan. U potonjem slučaju, službenik je taj koji pregledava odgovor prije njegovog slanja ispitaniku.

11.3. **Ostvarivanje prava ispitanika na ispravak i brisanje osobnih podataka**

Društvo u slučaju predmetnog zahtjeva vrši ispravak netočnih osobnih podataka ispitanika bez nepotrebnog odgađanja, te nadopunjuje nepotpune osobne podatke na način da se zaprimi dodatna izjava ispitanika.
Uz gore navedeno, Društvo obaviještava sve primatelje predmetnih osobnih podataka o poduzetim ispravcima odnosno dopunama te obaviještava ispitanika o tim primateljima ukoliko ispitanik navedeno zatraži.

11.4. **Ostvarivanje prava na brisanje osobnih podataka**

Društvo briše osobne podatke ili na izričiti zahtjev ispitanika ili ukoliko je ispunjen barem jedan od sljedećih uvjeta:

a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;
b) ispitanik povuče privolu na kojoj se obrada temelji a pritom ne postoji druga pravna osnova za obradu;
c) ispitanik uloži prigovor na obradu osobnih podataka te ne postoje jači legitimni razlozi za obradu, ili ispitanik uloži prigovor na obradu podataka za potrebe izravnog marketinga
d) osobni podaci su obrađeni suprotno zakonskim odredbama;
e) osobni podaci moraju se brisati radi poštivanja pravne obveze temeljem primjenjivih propisa
f) osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva (društvenih mreža npr).

Društvo osobne podatke briše na način koji omogućuje trajno uklanjanje navedenih podataka iz glavnih sustava, te treba postojati određeni zapis o brisanju (*u potrebi potencijalnog dokazivanja da je brisanje doista provedeno*) i odrediti načine na koji će se određeni podaci uništiti (*npr podaci u pisanom obliku, USB-u, CD-u itd*).

U slučaju da je Društvo javno objavilo osobne podatke, dužno je uzimajući u obzir dostupnu tehnologiju i trošak provedbe poduzeti razumne tehničke mjere da se izbrišu sve poveznice do njih, odnosno kopije ili rekonstrukcije tih osobnih podataka, te je također dužno obavijestiti i druge povezane voditelje obrade koji obrađuju te podatke da je ispitanik tražio njihovo brisanje.

Društvo je dužno obavijestiti sve primatelje predmetnih osobnih podataka o brisanju navedenih te obavijestiti ispitanika o tim primateljima ukoliko ispitanik to zatraži.

Društvo određuje period u kojem će se preispitivati potreba obrade i pohrane osobnih podataka te izbrisati one za koje ne postoji više potreba da se obrađuju ili pohranjuju.

11.4.1. **Ograničenje izvršavanja zahtjeva za brisanjem osobnih podataka**

Društvo ipak ne provodi brisanje unatoč zahtjevu ispitanika ili postojanja razloga navedenih u 11.3., u mjeri u kojoj je obrada tih osobnih podataka nužna:

a) radi poštovanja pravne obveze kojom se zahtijeva obrada a kojoj obvezi Društvo podliježe, ili za izvršavanje zadaće od javnog interesa
b) radi ostvarivanja prava na slobodu izražavanja i informiranja;
c) zbog javnog interesa u području javnog zdravlja
d) u svrhe javnog interesa, povjesnog ili znanstvenog istraživanja ili u statističke svrhe odnosno radi ostvarivanja ili obrane pravnih zahtjeva.

11.5. **Ostvarivanje prava na ograničenje obrade**

Društvo na zahtjev ispitanika vrši ograničenje obrade osobnih podataka na način da se ti određeni osobnih podaci smiju obrađivati samo uz privolu ispitanika (uz iznimku potrebe za ostvarivanje ili obranu pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe ili zbog važnog javnog interesa) u slučaju ako:

a) ispitanik osporava točnost osobnih podataka, na razdoblje kojem se Društvu omogućuje provjera točnosti osobnih podataka;
b) obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe;
c) Društvo više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
d) ispitanik je uložio prigovor Društvu i u očekivianju je potvrde u vezi toga nadilaze li legitimni razlozi voditelja obrade razloge ispitanika za brisanjem
e) Društvo obaviještava ispitanika u slučaju kada je ishođeno ograničenje obrade, a takvo ograničenje bude ukinuto, te takva obavijest mora uslijediti neposredno prije samog ukidanja.

Društvo obaviještava sve primatelje predmetnih osobnih podataka o postavljenim ograničenjima obrade te obaviještava ispitanika o tim primateljima ukoliko ispitanik navedeno zatraži.

U praksi, predmetne metode kojima se ograničava obrada osobnih podataka bi uključivale privremeno premještanje odabranih osobnih podataka u drugi sustav obrade, činjenje odabranih podataka nedostupnima za korisnike ili privremeno uklanjanje objavljenih podataka s internetske stranice. U automatiziranim sustavima pohrane ograničavanje obrade bi trebalo osigurati tehničkim sredstvima na način da osobni podaci nisu predmet daljnjih obrada i da se ne mogu mijenjati te bi u sustavu trebalo biti jasno navedeno da je obrada predmetnih osobnih podataka ograničena.

11.6. **Ostvarivanje prava na prenosivost podataka**

Društvo ispitaniku na njegov zahtjev prenosi tražene osobne podatke u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, kako bi ispitanik predmetne podatke mogao neometano prenijeti drugom potencijalnom voditelju obrade (pritom ispitanik također odlučuje hoće li zajedno s prijenosom tražiti i brisanje podataka ili ne).

Ukoliko je tehnički izvedivo i ukoliko ispitanik navedeno traži, predmetni podaci se neposredno prenose drugom voditelju obrade kojeg je ispitanik izabrao, pod uvjetom da se obrada provodi automatiziranim putem i ako se temelji na privoli ispitanika odnosno ako je obrada nužna u vezi izvršenja nekog ugovora.

Pri navedenom treba uzeti u obzir da se prijenos podataka neće izvršiti ukoliko su pritom osobni podaci drugih ispitanika ugroženi.

12. Postupak povodom prigovora

12.1**. Prigovor na obradu osobnih podataka čija je svrha obrade legitimni interes Društva.**

Ispitanik može u svakom trenutku podnijeti prigovor na obradu osobnih podataka čija je svrha obrade očuvanje legitimnih interesa Društva. U tom slučaju Društvo zaustavlja svaku obradu osobnih podataka i provodi test razmjernosti interesa ispitanika i interesa Društva za obradom osobnih podataka.

Ukoliko legitimni interesi Društva prevladavaju interese ispitanika u konkretnom slučaju ili je obrada nužna radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva, obrada osobnih podataka se nastavlja. Ukoliko interesi ispitanika prevladavaju legitimne interese Društva, predmetni osobni podaci se više ne smiju obrađivati. Prilikom provođenja gore navedenog testa razmjernosti je svakako potrebno savjetovati se sa nadležnim službenikom za zaštitu podataka.

12.2. **Prigovor na obradu osobnih podataka u marketinške svrhe**

Ispitanik može u svakom trenutku podnijeti prigovor na obradu osobnih podataka u marketinške svrhe, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom. U tom slučaju Društvo prekida svaku obradu predmetnih osobnih podataka.

13. Posebnosti automatiziranog pojedinačnog donošenja odluka, uključujući izradu profila

Ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, a koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu. Navedeno je ispunjeno primjerice u situaciji kada računalni program Društva na temelju svojih tehničkih postavki i softvera izabire određene ispitanike u odnosu na njihove podatke bez ljudske intervencije.

Međutim, navedeno se neće primijeniti ukoliko je predmetna automatska odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka; dopuštena primjenjivim propisima ili je temeljena na izričitoj privoli ispitanika (u kojim slučajevima ispitanik ima pravo izraziti svoje stajalište i osporavati predmetnu odluku).

Predmetni način donošenja odluka nije dopušten u odnosu na posebne kategorije osobnih podataka, osim ako je dan izričit pristanak ispitanika i ako postoje odgovarajuće mjere zaštite prava i sloboda te legitimni interesa ispitanika.

Pri procjenjivanju radi li se u konkretnom slučaju o izradi profila ili ne, uzima se u obzir je li krajnji cilj prikupljanje podataka temeljem kojih se tvori određena slika o ispitaniku i njegovim preferencijama (pogotovo u slučaju praćenja web aktivnosti ispitanika) te šalje li se onda temeljem te slike ispitaniku određene ponude, sugestije i slično (npr radi se profil o tome koje usluge ispitanik u pravilu koristi i onda se temeljem toga šalju ponude usko vezane uz te usluge). Ukoliko je odgovor na prethodno pitanje potvrdan, Društvo ispitanika obaviještava o navedenom.

13.1. **Izrada i vođenje evidencije aktivnosti obrade osobnih podataka**

Ukoliko je obvezno po pozitivnim propisima, Društvo izrađuje i vodi evidenciju aktivnosti obrade podataka, u koju evidenciju je zapisuje odnosno naznačuje sve aktivnosti obrade osobnih podataka. Predmetni dokument je ili u pisanom ili elektroničkom obliku i sadrži sljedeće podatke:

a) naziv i kontaktne podatke Društva i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
b) svrhe obrade;
c) opis kategorija ispitanika i kategorija osobnih podataka;
d) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
e) ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te;
f) predviđene rokove za brisanje različitih kategorija podataka, ako je moguće;
g) opći opis tehničkih i organizacijskih sigurnosnih mjera

Društvo predmetnu evidenciju na zahtjev nadzornog tijela podnosi na uvid.

Predmetna evidencija se ne vodi ukoliko Društvo zapošljava manje od 250 zaposlenika, osim ako će obrada koju provodi vjerojatno prouzročiti visok rizik za prava i slobode ispitanika, ako obrada nije povremena ili obrada uključuje posebne kategorije podataka, ili je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima.

14. <u>Održavanje sigurnosti osobnih podataka</u>

Društvo u svakom trenutku posebnu pozornost pridaje zaštiti osobnih podataka koji se prikupljaju i obrađuju, a u smislu navedenog osobito provodi pseudonimizaciju i enkripciju osobnih podataka, osigurava trajnu povjerljivost, cjelovitosti, dostupnosti i otpornost sustava i usluga obrade, uspostavlja sustav ponovne dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta (back-up serveri

predmetnih podataka) te uspostavlja proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, zajedno sa potencijalnim rizicima kao što su slučajno uništenje ili gubitak osobnih podataka, njihovo neovlašteno otkrivanje ili neovlašteni pristup osobnim podacima koji su preneseni, pohranjeni ili na neki drugi način obrađeni.

14.1. **Enkripcija**

Društvo, ukoliko to ocijeni potrebnim, osobne podatke štiti enkripcijom, i to po mogućnosti tzv. asimetričnim enkripcijskim metodama, koji algoritmi bi se mogli dešifrirati samo preko ključa koji je poznat ovlaštenim osobama (primjera radi, preporuča se korištenje AES (Advanced Encryption Standard) ili TDEA (Triple Data Encryption Algorithm). Navedeno se pogotovo odnosi na sustavnu pohranu podataka, prijenos podataka izvan Društva, pohranjivanje podataka na prijenosnike poput USB itd ili na obradu posebnih kategorija osobnih podataka.

14.2. **Sigurnost pristupa osobnim podacima**

Osobni podaci u fizičkom obliku ili u elektronskom obliku pohranjeni na prijenosnike putem CD-a, USB- ili hard diskova Društvo čuva na sigurnom mjestu poput čuvanih arhiva ili sefa, a kojima je pristup dopušten samo ovlaštenim osobama. Ukoliko se radi o podacima u elektronskom obliku, navedeni se čuvaju računalnim programima kojima je pristup omogućen samo putem sigurnog log-in, lozinke i sustava koji zahtijeva strogu identifikaciju ovlaštenika (pogotovo u slučaju ako se radi o posebnim kategorijama osobnih podataka).

Preporučljivo je voditi evidenciju o svim prijenosima ili otpremama osobnih podataka kako bi se mogla detektirati potencijalna neovlaštena uporaba ili slanje osobnih podataka, putem sustava koji bi automatski naznačio ovlaštenika koji je izvršio predmetnu otpremu, mjesto gdje su se predmetni podaci nalazili, datum i sat otpreme i sadržaj predmetnih podataka.

Osobni podaci koji se šalju elektronskim putem trebali bi biti isključivo putem sigurnih HTTPS poveznica, a preporučljivo je pristup podacima preko weba odrediti putem OUATH informatičkog određenja pristupa.

14.3. **Data Backup sustav**

Društvo će, ukoliko ocijeni potrebnim, očuvati sigurnost osobnih podataka od potencijalnog uništenja u slučaju pada računalnog sustava ili sličnog razloga, i to na način da se sastavi i pusti u funkciju određeni back-up sistem koji bi spriječio navedeno (npr rezervni server ili hard disk).

15. **Revizija obrade i sigurnosti osobnih podataka**

Društvo će, ukoliko ocijeni potrebnim, vršiti internu reviziju zaštite osobnih podataka, u svrhu lociranja potencijalniih propusta i rizika u vezi sigurnosti, te kako bi se obrisali osobni podaci za kojima nema potrebe da više budu pohranjeni.

Navedenu internu reviziju izvršavaju ovlaštene osobe u Društvu, i to u suradnji sa Službenikom za zaštitu podataka.

Društvo će u slučaju potrebe također provesti i neovisnu reviziju od strane treće osobe, a u koju reviziju ne bi trebale biti uključene osobe koje su sudjelovale u implementaciji mjera sigurnosti i obrade osobnih

podataka, i kojom metodologijom će se također utvrditi mogući propusti pri svakom aspektu prikupljanja, obrade i pohrane osobnih podataka zajedno sa savjetovanjem kako poboljšati sigurnost navedenih

16. Postupak u slučaju povrede osobnih podataka

16.1. Općenito o povredama

Unatoč odgovarajućim mjerama zaštite osobnih podataka koje Društvo poduzima kako bi se spriječile povrede osobnih podataka, nije isključena mogućnost da ipak dođe do povrede osobnih podataka. Pored mjera zaštite koje bi trebale osigurati da do povrede ne dođe, Društvo poduzima i tehničke mjere kojima je cilj otkriti je li do povrede došlo.

Povreda osobnih podataka može imati niz štetnih posljedica za ispitanike te je stoga od iznimne važnosti da Društvo na povrede što prije reagira.

Povreda osobnih podataka znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

O **uništenju** osobnih podataka riječ je kad osobni podaci više ne postoje ili ne postoje u obliku u kojem su Društvu potrebni za svrhe u koje ih obrađuje.

O **gubitku** je riječ kada osobni podaci postoje, ali je Društvo izgubio kontrolu nad njima ili mogućnost pristupa, ili podaci na drugi način više nisu u posjedu Društva. Gubitak može biti privremenog ili trajnog karaktera.

O **izmjeni** je riječ kada zbog promjena izvršenih na njima osobni podaci više nisu potpuni, točni ili ažurni.

O **neovlaštenom otkrivanju ili pristupu osobnim podacima** radi se kada je došlo do njihovog otkrivanja osobama koje za to nisu ovlaštene.

16.2. Podnošenje izvještaja Agenciji za zaštitu osobnih podataka

Ukoliko Društvo otkrije povredu zaštite osobnih podatka, a za koju povredu je vjerojatno da će prouzročiti rizik za prava i slobode ispitanika, Društvo mora odmah i bez odgađanja podnijeti izvještaj Agenciji za zaštitu osobnih podataka i to najkasnije u roku 72 sata (*ukoliko se obavijest dostavi kasnije, mora se obrazložiti zakašnjenje*).

Predmetni izvještaj mora sadržavati

a) opis prirode povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
b) ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
c) opis vjerojatnih posljedica povrede osobnih podataka;
d) opis mjera koje je Društvo poduzelo ili predložilo poduzeti za rješavanje potencijalne povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Ukoliko Društvo navedene informacije iz nekog razloga nije u mogućnosti pružiti u jednom izvještaju, može ih pružati postepeno, ali bez nepotrebnog odgađanja.

Društvo će dokumentirati svaku povredu osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, posljedice i mjere poduzete za popravljanje štete.

Nakon obavijesti Agenciji, Društvo slijedi sve daljnje naloge koje Agencija odredi, te je u navedenom postupku također nužno savjetovanje sa nadležnim službenikom za zaštitu podataka.

16.3. **Podnošenje izvještaja ispitaniku čiji se podaci obrađuju**

Društvo će ispitanika odmah i bez odgađanja izvijestiti o povredi, ako je vjerojatno da predstavlja visok rizik za prava i slobode ispitanika kojeg se ti osobni podaci tiču. Pri navedenoj obavijesti Društvo dostavlja opis povrede zajedno sa informacijama b), c) i d) iz prethodnog članka, i to uporabom jasnog i jednostavnog jezika.

Međutim, obavijest se ipak ne dostavlja ispitaniku ukoliko je ispunjen barem jedan od sljedećih uvjeta:

a) poduzete su odgovarajuće tehničke i organizacijske mjere zaštite, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;
b) poduzete su naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika
c) za obavijest ispitaniku je potreban nerazmjeran napor. U takvom slučaju mora postojati neki vid javne obavijesti ili slične mjere kojom se ispitanici obavješćuju na jednako djelotvoran način.

16.4. **Postupanje radnika u slučaju povrede**

Zadaća svih radnika Društva je da bez odgode obavijeste službenika za zaštitu podataka o povredi koja se dogodila, odnosno o sumnji da je do povrede došlo i okolnostima iz kojih takva sumnja proizlazi.
U slučaju da je službenik odsutan, o povredi treba obavijestiti odgovornu osobu za ljudske potencijale i/ili pravne poslove koji preuzimaju zadatke službenika dok isti ne preuzme postupanje ili da izričite upute.

16.5. **Postupanje službenika u slučaju povrede**

Zadatak službenika za zaštitu podataka je da u roku od najviše 48 sati istraži okolnosti pod kojima je došlo do povrede, odnosno okolnosti vezane uz navodnu povredu. U tu svrhu, službenik za zaštitu podataka ovlašten je i dužan poduzeti potrebne provjere koje uključuju razgovore sa relevantnim zaposlenicima i drugim osobama koje bi mogle imati saznanja o povredi te se konzultirati s pravnicima i IT stručnjacima zaposlenim u Društvu.
O poduzetim radnjama, službenik za zaštitu podataka sastavlja pisano izvješće koje podnosi Upravi Društva, a koje će između ostalog sadržavati:

a) opis i rezultat radnji i provjera koje je službenik poduzeo,
b) prirodu povrede osobnih podataka uključujući, ako je moguće, kategorije i približan broj ispitanika te kategorije i približan broj evidencija osobnih podataka zahvaćenih povredom,
c) opisati rizik i vjerojatne posljedice povrede osobnih podataka,
d) opisati mjere koje predlaže poduzeti za rješavanje problema povrede osobnih podataka, uključujući mjere umanjivanja njezinih mogućih štetnih posljedica,

e) izvješće treba zaključiti prijedlogom Upravi o tome je smatra li potrebnim obavijestiti nadzorno tijelo - AZOP (pri čemu obavijest AZOP-u nije potrebna ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca), odnosno potrebi informiranja ispitanika (što je potrebno ako je vjerojatno da će povreda prouzročiti visoki rizik za prava i slobode pojedinaca).

Radi osiguravanja veće razine konzistentnosti, Društvo može pripremiti obrazac koji će se koristiti za izvještavanje o povredama.

17. Provođenje procjene učinka na zaštitu podataka

Društvo će procjenu učinka na zaštitu podataka provesti ako je vjerojatno da će se uvođenjem neke nove tehnike i vrste obrade, a osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca. Pritom se jedna procjena može odnositi na niz sličnih postupaka obrade koji predstavljaju podjednake visoke rizike. Društvo će se pri provođenju predmetne procjen savjetovati sa službenikom za zaštitu podataka.

Predmetna procjena se obvezatno provodi u sljedećim situacijama:

a) u slučaju sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na njega značajno utječu
b) u slučaju opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima ili
c) u slučaju sustavnog praćenja javno dostupnog područja u velikoj mjeri.

Agencija za zaštitu osobnih podataka odnosno druga nadzorna tijela također uspostavljaju i javno objavljuju popis vrste postupaka za koji je potrebno provesti predmetnu procjenu.

17.1. Sadržaj procjene

Procjena mora sadržavati sljedeće informacije:

a) sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes Društva;
b) procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama;
c) procjenu rizika za prava i slobode ispitanika odnosno procjena vjerojatnosti da bi predmetna povreda mogla prouzročiti fizičku, materijalnu ili nematerijalnu štetu, ili dovesti do diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, štete za ugled, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije, ili bilo koje druge znatne gospodarske ili društvene štete; ili ako ispitanici mogu biti uskraćeni za svoja prava i slobode ili spriječeni u obavljanju nadzora nad svojim osobnim podacima; ako se obrađuju posebne kategorije podataka; ako se procjenjuju osobni aspekti, osobito analiza ili predviđanje aspekata u vezi s učinkom na poslu, ekonomskim stanjem, zdravljem, osobnim preferencijama ili interesima, pouzdanošću ili ponašanjem, lokacijom ili kretanjem kako bi se izradili ili upotrebljavali osobni profili; ako se obrađuju osobni podaci osjetljivih pojedinaca, osobito djece; ili ako obrada uključuje veliku količinu osobnih podataka i utječe na velik broj ispitanika

d) mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba.

Društvo ipak ne treba provesti procjenu ako je svrha predmetne obrade u pravnoj obvezi Društva te ako ti propisi na kojima se obveza temelji uređuju posebne postupke obrade ili skupina dotičnih postupaka te je procjena učinka na zaštitu podataka već provedena, osim ako primjenjivi propisi ne određuju drukčije.

17.2. **Postupak savjetovanja sa nadzornim tijelom**

Društvo se savjetuje s nadzornim tijelom prije potencijalno rizične obrade ukoliko prethodno provedena procjena učinka na zaštitu podataka navodi na to da bi obrada mogla predstavljati visoki rizik ukoliko se ne donesu određene sigurnosne mjere.

Prilikom savjetovanja nadzornom tijelu potrebno je dostaviti:

a) odgovarajuće podatke Društva, zajedničkih voditelja obrade i izvršitelja obrade uključenih u obradu, osobito za obrade unutar grupe poduzetnika;
b) svrhu i sredstva namjeravane obrade;
c) zaštitne mjere i druge mjere za zaštitu prava i sloboda ispitanika;
d) kontaktne podatke službenika za zaštitu podataka;
e) procjenu učinka na zaštitu podataka
f) sve druge informacije koje nadzorno tijelo zatraži.

Ukoliko nadzorno tijelo smatra da bi se namjeravanom obradom kršili primjenjivi propisi, a osobito ukoliko nije u dovoljnoj mjeri utvrđen ili umanjen rizik, nadzorno tijelo u roku od najviše osam tjedana od zaprimanja zahtjeva za savjetovanje (navedeni rok može biti produžen za daljnjih šest tjedana) pisanim putem savjetuje Društvo, pri čemu može koristiti bilo koje od svojih zakonom ustanovljenih ovlasti, poput obveznih naredbi, ishođenje pristupa osobnim podacima ili provođenja revizije zaštite osobnih podataka.

18. **<u>Postupak u slučaju prijenosa osobnih podataka u treće zemlje</u>**

Ukoliko se osobni podaci koji se prikupljaju i obrađuju prenose izvan EU u treću zemlju ili međunarodnu organizaciju (npr udruženje ugostitelja iz inozemstva), Društvo provjerava postoji li za tu određenu zemlju u koju će se predmetni podaci slati dozvola za slanje u vidu tzv. Odluke o primjerenosti, a koju Odluku izdaje Europska Komisija te koje odluke se izdaju u *Službenom listu Europske Unije.* U odnosu na navedeno, daljnje postupanje se diferencira s obzirom na tri potencijalne situacije:

a) ukoliko takva Odluka postoji, prijenos je dozvoljen.
b) ukoliko takva Odluka ne postoji, prijenos u načelu nije dozvoljen ali je ipak moguć pod uvjetom da je Društvo ili izvršitelj obrade predvidilo odgovarajuće zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkovita sudska zaštita. Pod navedene mjere se osobito uzimaju standardne klauzule za zaštitu podataka
c) čak i u slučaju da takva Odluka ne postoji, a niti postoje odgovarajuće mjere iz b), prijenos je ipak moguć ukoliko je ispitanik dao izričiti pristanak na takav prijenos nakon što je obaviješten o potencijalnimi rizicima, ili ukoliko je prijenos nužan u sklopu ugovorne obveze odnosno u vezi

postavljanja, ostvarivanja ili obrane pravnih zahtjeva te ukoliko postoji neki drugi bitni javni interes ili važan interes ispitanika.

U smislu toč. b) iz prethodnog stavka, Društvo će nastojati da se prednost dade onoj zaštitnoj mjeri koja osigurava veću razinu zaštite (npr. primjena standardnih ugovornih klauzula koje je usvojila Europska komisija ili posebnim ugovornim klauzulama odobrenim od strane nadležnog tijela), osim ako je prema okolnostima slučaja očito prikladnija primjena nekog od odstupanja za posebne slučajeve iz članka 49. Opće Uredbe.

Predmet poslovanja Društva je takav da ima goste iz različitih zemalja, pri čemu Društvo osobne podatke gostiju može dobiti od stranih turističkih agencija ili stranih operatora online booking platformi. U odnosu na Društvo, navedeni subjekti djeluju kao zasebni voditelji obrade te za njihove radnje Društvo nije i ne može biti odgovorno. Takvi subjekti mogu imati sjedište u zemljama koje ne osiguravaju adekvatnu razinu zaštite. Društvo s takvim partnerima može povratno razmjenjivati određene osobne podatke gostiju potrebne radi naplate pruženih usluga, kao npr. razdoblje boravka određenog gosta i podatke o potrošnji gosta. Takve povratne razmjene osobnih podataka s navedenim partnerima temelje se na članku 49. stavku 1. točki c) Opće Uredbe (prijenos koji je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe; kao gore pod c)).

U slučaju postojanja sumnje je li prijenos osobnih podataka u zemlju koja ne osigurava adekvatnu razinu zaštite dozvoljen, potrebno je prethodno tražiti savjet i mišljenje službenika za zaštitu podataka.

19. <u>Izvršitelj obrade</u>

Društvo može dio obrade osobnih podataka povjeriti izvršitelju obrade (*primjera radi – revizori, odvjetnici i slično*).

Izvršitelj obrade mora u dovoljnoj mjeri jamčiti provedbu odgovarajućih tehničkih i organizacijskih mjera koje su sukladne primjenjivim propisima o zaštiti osobnih podataka, te treba djelovati samo u skladu s uputama Društva. Odnosi sa Izvršiteljima glede zaštite osobnih podataka reguliraju se posebnim sporazumima ili u okviru osnovnih ugovora.

19.1. **Sklapanje ugovora s izvršiteljima obrade**

Društvo može odlučiti da će pojedine aspekte obrade osobnih podataka povjeriti izvršiteljima obrade, koji će osobne podatke obrađivati u ime i po uputama Društva. Društvo može angažirati jedino one izvršitelje obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka.

S izvršiteljem obrade Društvo obvezno sklapa sporazum u pisanom obliku kojim se regulira predmet i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka i kategorija ispitanika te prava i obveze Društva i izvršitelja obrade. U sklopu takvog sporazuma, izvršitelj obrade daje Društvu određena jamstva u pogledu zaštite osobnih podataka.

Ovisno o okolnostima slučaja, a prema vrsti i opsegu obrade koju izvršitelj obrade obavlja, Društvo može prije angažiranja određenog izvršitelja obrade izvršiti provjere koje smatra razumnim i prikladnim, kao na primjer:

a) tražiti informaciju je li izvršitelj obrade imenovao službenika za zaštitu podataka,
b) tražiti informaciju o tome angažira li izvršitelj obrade podizvršitelje, koga sve i u kojim se zemljama oni nalaze,
c) provjeriti s izvršiteljem vodi li evidenciju o aktivnostima obrade,
provjeriti s izvršiteljem ima li i kakve interne politike i procedure glede zaštite osobnih podataka,
d) obaviti razgovore o načinu na koji su organizirani relevantni procesi izvršitelja obrade,
e) tražiti informaciju ima li izvršitelj certifikat da je usklađen s GDPR-om (certificiranje nije obvezno, ali je korisno navesti ako ima),
f) tražiti informaciju ima li izvršitelj kakve ISO certifikate na području IT sigurnosti,
g) razmotriti u kojoj mjeri Društvo ima mogućnost nadzora nad izvršiteljem obrade,
h) posjetiti poslovne prostorije izvršitelja obrade,
i) ako se radi o izvršitelju obrade s kojim Društvo surađuje već duže vrijeme, u obzir se može uzeti njihova savjesnost i urednost u dosadašnjem izvršavanju ugovornih obveza.

U svrhu kontinuirane provjere izvršitelja obrade, Društvo može na godišnjoj razini, a po potrebi i češće, od izvršitelja obrade tražiti dostavljanje potpisane izjave kojom izvršitelj obrade potvrđuje svoju sukladnost. Nacrt takve izjave može biti prilog ugovoru kojeg Društvo potpisuje s izvršiteljem obrade.

Izvršitelje obrade društvo navodi u evidenciji o aktivnosti obrade (ukoliko je istu obvezno voditi), zajedno sa svim provjerama koje je Društvo poduzelo prije njihovog angažiranja. Sektor ljudskih potencijala i pravnih poslova vodi popis izvršitelja obrade i čuva ugovore s izvršiteljima obrade.

Društvo će u pravilu izbjegavati suradnju s izvršiteljima obrade kod kojih bi trebalo doći do prijenosa osobnih podataka u treću zemlju (izvan EU). Do suradnje s takvim izvršiteljima može doći ako su primijenjene odgovarajuće zaštitne mjere sukladno Poglavlju V. Opće Uredbe.

19.2. **Ugovori koji uključuju razmjenu podataka s drugim primateljima**

Društvo u svom poslovanju može ulaziti u pravne odnose s drugim pravnim i fizičkim osobama s kojima ne djeluje kao zajednički voditelj obrade niti ih angažira kao svoje izvršitelje obrade. U takvim pravnim odnosima može doći do razmjene određenih osobnih podataka. Isto tako, do razmjene osobnih podataka može doći prema državnim tijelima.

U svim takvim slučajevima, ovisno o okolnostima, Društvo procjenjuje je li potrebno sklopiti pisani ugovor kojim se pobliže definiraju prava i obveze ugovornih strana, te je li i u kojoj mjeri u takav pisani ugovor, osim opće odredbe o obvezi obiju ugovornih strana da čuvaju povjerljivost svih informacija i osobnih podataka koje jedna od druge prime radi izvršavanja ugovornih obveza, potrebno uključiti dodatne odredbe o razmjeni osobnih podataka.

Takve dodatne odredbe o razmjeni osobnih podataka osobito mogu uključivati odredbe kojima se precizira svrha razmjene osobnih podataka, vrsta osobnih podataka koji se prenose, pravna osnova za prijenos podataka, ograničenje u pogledu daljnjih primatelja osobnih podataka, obveza čuvanja povjerljivosti, razdoblje tijekom kojeg će primatelj čuvati osobne podatke, posljedice povrede i slično.

Osobni podaci koji se razmjenjuju s primateljima u svakom će slučaju biti ograničeni na ono što je nužno kako bi se ostvarila svrha radi koje se prijenos odvija.

20. Upotreba kolačića (cookies)

Web stranica Društva koristi kolačiće (cookies). Kolačići su malene tekstualne datoteke koje web stranice pohranjuju na računalo posjetitelja prilikom posjete web stranici. Kolačići služe tome da web stranica zapamti posjetitelja i prepozna ga prilikom sljedeće posjete te da zapamti njegove preferencije.

Kolačići mogu prikupljati podatak o IP adresi, gradu i državi iz koje je posjetitelj web stranice, dobi i spolu posjetitelja, te druge podatke. Uvodna odredba (30) GDPR-a izričito propisuje da se mrežni identifikatori kao što su npr. kolačići mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju. Društvo stoga obavještava posjetitelje web stranice o logici automatske obrade i o posljedicama koje profiliranje na osnovi kolačića ima za pojedince.

Radi izbjegavanja svake dvojbe, Društvo ne ide za time da pomoću kolačića utvrđuje identitet pojedinaca, već koristi kolačiće jedino u svrhe kontrole podataka. Društvo prikuplja i obrađuje osobne podatke za potrebe rezervacija i upravljanja gostima, računima i naplatom, marketinških akcija i ispitivanja zadovoljstva. Podaci su namijenjeni Društvu i njegovim pružateljima usluga. Ispitanik ima pravo ispitati, pristupiti, ispraviti ili prigovoriti takvoj obradi pisanim putem našem službeniku za zaštitu podataka.

Korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup već pohranjenim podacima u terminalnoj opremi korisnika dopušteno je samo u slučaju kada je korisnik/ispitanik dao svoju privolu, i to nakon što je dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade osobnih podataka. U skladu s navedenom odredbom, Društvo prije instalacije kolačića traži privolu posjetitelja.

Prilikom posjete web stranici Društva, posjetitelju se daju informacije o vrsti kolačića koje web stranica koristi i njihovoj svrsi. Posjetitelj pritom može odabrati kolačiće čiju će instalaciju dopustiti, a koje će kolačiće odbiti.

Posjetitelju su na web stranici Društva dostupne detaljnije informacije o kolačićima, kao i o načinu na koji posjetitelj može promijeniti svoje postavke kolačića i brisati ranije instalirane kolačiće.

Iznad opisano postupanje u svezi korištenja kolačića Društvo će pravovremeno preispitati, a po potrebi i revidirati nakon što se na razini Europske unije donese uredba koja će regulirati predmetno područje (e-privacy Regulation).

21. Prava i dužnosti službenika za zaštitu podataka

Službenik za zaštitu podataka samostalan je i neovisan u svom radu i ovlašten je poduzimati sve potrebne aktivnosti i mjere kako bi se osigurala usklađenost poslovanja Društva s propisima o zaštiti osobnih podataka.

Službenik za zaštitu podataka za svoj rad odgovara izravno Upravi Društva.

Pri donošenju odluke o imenovanju službenika za zaštitu podataka Društvo će voditi računa da imenovana osoba ima odgovarajuća stručna znanja za provedbu svih mjera i aktivnosti za zaštitu osobnih podataka.

Službenik mora imati potrebne stručne kvalifikacije, a osobito stručno znanje o pravu i praksama u području zaštite osobnih podataka. Iako certifikati koje je službenik ishodio mogu biti od pomoći, od veće je važnosti za obavljanje funkcije službenika kontinuirana edukacija, poznavanje procesa i razumijevanje IT sustava Društva, kao i zakonskog okvira poslovanja Društva te njegovih potreba sigurnosti i zaštite osobnih podataka.

Uprava odlučuje hoće li službenik za zaštitu podataka biti u radnom odnosu s Društvom ili će se za službenika ugovorno angažirati vanjski pružatelj usluga.

U slučaju radnog odnosa, službenik za zaštitu podataka može biti zaposlen na puno ili na nepuno radno vrijeme. Pored radnih zadataka koje ima kao službenik može obavljati i druge zadatke koji ne dovode do sukoba interesa s obavljanjem zadataka koji proizlaze iz funkcije službenika.

Službenik za zaštitu podataka je osoba koja u svakom trenutku mora biti na primjeren i pravodoban način uključena u sva pitanja u pogledu zaštite osobnih podataka u Društvu, te se preporučuje svim radnicima i trećim osobama da se obrate navedenom u slučaju ikakve dvojbe vezano uz pitanje osobnih podataka. Društvo osigurava da sve organizacijske jedinice Društva, počevši od njihovih rukovoditelja pa naniže, budu upoznate s postojanjem Službenika u Društvu i njegovim zadacima te s važnošću obavještavanja službenika pri razvoju novih usluga, namjeravanoj upotrebi novih tehnologija, novim vrstama obrade osobnih podataka, povredama osobnih podataka i zahtjevima za ostvarivanjem prava ispitanika.

Društvo je dužno osigurati kako slijedi:

a) u slučaju namjeravane nove vrste obrade osobnih podataka ili namjeravane obrade osobnih podataka u drugu svrhu od postojeće te upotrebe novih tehnologija, službenik treba biti uključen na relevantne sastanke u što ranijoj fazi, kako bi mogao izraziti svoje mišljenje i pomoći svojim savjetom,
b) Društvo će nastojati da službenik bude prisutan na redovitim sastancima uprave i višeg menadžmenta kako bi mogao dati korisne doprinose zaštiti osobnih podataka, osobito na onim sastancima koji bi mogli imati utjecaja na obradu osobnih podataka,
c) osiguravanjem da službenik na raspolaganju ima odgovarajuće kadrovske, organizacijske i tehničke resurse na raspolaganju kako bi mogao obavljati svoje zadatke,
d) sve organizacijske jedinice Društva dužne su, bez odgode, obavještavati službenika za zaštitu podataka o svim kretanjima i promjenama vezanim uz poslovanje Društva, a koje bi mogle imati utjecaja na zaštitu osobnih podataka,
e) prije izmjene bilo kakvih politika i pravilnika koji se odnose na zaštitu osobnih podataka, Uprava će tražiti mišljenje Službenika
f) službenik ne smije biti razriješen dužnosti niti kažnjen zbog obavljanja njegovih zadataka.

Pri obnašanju dužnosti službenik za zaštitu podataka ne smije primati nikakve upute u pogledu izvršavanja svojih dužnosti te ne smije biti razriješen dužnosti ili kažnjen zbog izvršavanja navedenih.

Službenik je svoje zadatke dužan obavljati osobno, uredno i savjesno. Službenik za zaštitu podataka odgovoran je za provođenje svih mjera i aktivnosti usmjerenih na ostvarivanje ciljeva politike zaštite privatnosti i osobnih podataka Društva, provedbu zakonskih, podzakonskih i drugih obvezujućih akata na području zaštite osobnih podataka.

Obveze i zadaće službenika za zaštitu podataka osobito uključuju sljedeće:

a) informiranje i savjetovanje Uprave i radnika Društva o obvezama iz Opće Uredbe i drugih primjenjivih zakona i propisa o zaštiti osobnih podataka,

b) održavanje redovitih edukacija radnika zaposlenih u Društvu na području zaštite osobnih podataka kako bi ih se upoznalo sa zakonskim zahtjevima i internim zahtjevima Društva glede zaštite osobnih podataka,
c) provođenje internih revizija radi provjere usklađenosti poslovanja i prakse pojedinih organizacijskih jedinica sa zahtjevima Opće Uredbe i internih akata Društva. O provedenim revizijama službenik će sastaviti pisano izvješće u kojem mora opisati rezultate svog pregleda i eventualne uočene nedostatke,
d) provođenje povremenih revizija politika i pravilnika Društva o zaštiti osobnih podataka,
e) izrada i pregled dokumentacije vezane uz zaštitu osobnih podataka (npr. ugovori s izvršiteljima obrade, ugovori sa zajedničkim voditeljima obrade, ugovori temeljem kojih dolazi do razmjene osobnih podataka s primateljima, obavijesti ispitanicima, interne politike i procedure i slično),
f) pregledavanje svih izmjena u evidencijama o aktivnosti obrade i pomoć nadležnim zaposlenicima pri njihovom popunjavanju,
g) priprema, odnosno pregledavanje odgovora na zahtjeve za ostvarivanje prava ispitanika iz dijela trećeg ove Politike te vodi evidenciju primljenih zahtjeva za ostvarivanje prava ispitanika i odgovora na njihove zahtjeve,
h) vođenje evidencije o povredama osobnih podataka i postupanje u skladu s odredbama šestog dijela ove Politike u slučaju kada dođe do povrede, te se aktivno uključuje u istraživanje i izvještavanje o povredama osobnih podataka do kojih može doći,
i) izrada procjene učinka na zaštitu osobnih podataka iz članka 35. Opće Uredbe (kada postoji obveza izrade procjene učinaka),
j) redovito se usavršava pohađanjem edukacija namijenjenih službenicima za zaštitu podataka u dogovoru s Upravom, ali i samostalno prati promjene i praksu na području zaštite osobnih podataka, a osobito smjernice i mišljenja AZOP-a, smjernice Radne skupine osnovane na temelju članka 29. Direktive 95/46/EC i Odbora za zaštitu podataka osnovanog na temelju Opće Uredbe,
k) surađuje s nadzornim tijelom i djeluje kao kontakt točka za nadzorno tijelo u pogledu obrade,
l) obavljanje drugih aktivnosti koje doprinose podizanju razine zaštite osobnih podataka.

Službenik je ovlašten usmeno upozoravati radnike kod kojih uoči postupanje koje nije u skladu s Općom Uredbom ili ovom Politikom te im davati upute o načinu ispravljanja uočenih nesukladnosti.

O svim uočenim neusklađenostima na području zaštite osobnih podataka Službenik za zaštitu podataka upozorava Upravu Društva. Uprava Društva odlučuje o mjerama koje će se poduzeti kako bi se otklonile eventualne neusklađenosti.

Dođe li uslijed propusta u radu službenika za zaštitu podataka do štete za ispitanike, Društvo ili druge osobe, službenik za zaštitu podataka može biti izravno odgovoran za štetu, što će se prosuđivati prema primjenjivim zakonskim propisima ukoliko je do istoga došlo namjerom ili krajnjom nepažnjom službenika.

Službenik je dužan trajno čuvati povjerljivost svih informacija i osobnih podataka koje je saznao vezano uz obnašanje svoje funkcije.

22. **Edukacija radnika**

Svi radnici potpisuju posebne izjave o povjerljivosti ili ugovorom o radu preuzimaju obvezu trajnog čuvanja tajnosti osobnih podataka. Međutim, kako bi se radnike što bolje osvijestilo o važnosti zaštite podataka, Društvo je dužno obrazovati sve svoje radnike o značaju i načinima zaštite osobnih podataka unutar prvog

mjeseca rada. Edukaciju organizira odgovorna osoba ustrojstvene jedinice za ljudske potencijale, za planiranje i provođenje edukacija i treninga.

Sukladno analizi stanja zaštite osobnih podataka, promjenama u zakonskim propisima ili internim politikama, broju povreda ili inače na prijedlog službenika za zaštitu osobnih podataka, Društvo provodi povremene edukacije radnika tijekom trajanja ugovora o radu s ciljem podizanja razine zaštite osobnih podataka i svijesti radnika o potrebi zaštite njihove tajnosti. Ove edukacije održavaju se najmanje jednom godišnje.

Održavanje edukacija potrebno je evidentirati.

Program obrazovanja utvrđuje službenik za zaštitu podataka u dogovoru s Upravom Društva, vodeći računa o razini rizika za pojedina radna mjesta tako da sadržaj programa bude prilagođen radnim zadacima radnika i opsegu u kojem oni dolaze u dodir s osobnim podacima.

Radnike će se na edukacijama informirati o tome da sve uočene nedostatke i nesukladnosti na području zaštite osobnih podataka mogu priopćiti službeniku ili svojim rukovoditeljima.

23. **Odgovornost**

Društvo je odgovorno za usklađenost sa primjenjivim propisima vezanim uz zaštitu osobnih podataka te treba biti u mogućnosti dokazati predmetnu usklađenost odnosno zakonito postupanje.

24. **Zaključak**

Predmetna Politika predstavlja kodificiranu dobru praksu u vezi zaštite osobnih podataka te služi kao svojevrsni putokaz. Navedena Politika nastoji pokriti većinu predvidljivih situacija koje bi mogle nastati ali to dakako nije moguće, tako da će svaku situaciju trebati procjenjivati po okolnostima koje su jedinstvene u svakom pojedinom slučaju.

Ovaj Politika tumači se sukladno Općoj Uredbi i primjenjivom zakonodavstvu Republike Hrvatske na području zaštite osobnih podataka. Sva pitanja ispitanika u svezi ove Politike mogu se podnijeti službeniku za zaštitu osobnih podataka, koji će na upit podnositelja odgovoriti u što kraćem roku, a najkasnije u roku od mjesec dana.

Za sve eventualne sporove proizašle iz povrede osobnih podataka koju bi počinilo Društvo primjenjuju se zakoni i drugi propisi primjenjivi u Republici Hrvatskoj, a sud nadležan za rješavanje u sporu je stvarno nadležni sud prema sjedištu Društva.

Ova Politika prestaje važiti ako Društvo o tome donese odluku, odnosno ako dođe do likvidacije Društva ili do druge statusne promjene koja bi rezultirala prestankom postojanja Društva. Međutim, prestanak važenja ove Politike ne oslobađa radnike Društva obveza zaštite osobnih podataka u pogledu onih podataka koji su do tada prikupljeni i/ili obrađeni.

Predmetna tematika zaštite osobnih podataka je opsežne i složene naravi te je ključno da svi radnici navedenom pristupe ozbiljno, pažljivo i staloženo, jer se jedino na taj način može odgovoriti na sve izazove koje ovo dinamično područje nameće svakodnevnom poslovanju Društva.

HOTEL LERO d.o.o.

_____

Srđan Pujo
Član Uprave