Na temelju čl. ___ Izjave o osnivanju SEDRA CONSULTING d.o.o., Dragan Šekrija, direktor donosi

POLITIKU ZAŠTITE OSOBNIH PODATAKA

Uvod

Članak 1.

Društvo je predano obavljanju vršenju svog poslovanja u skladu sa svim važećim zakonima i regulativom zaštite podataka te u skladu s dobrim praksama.

Članak 2.

Uprava Društva je u potpunosti predana osiguranju kontinuirane i efektivne uspostave ove politike, te isto očekuje od svojih zaposlenika i poslovnih partnera. Svako kršenje ove politike može rezultirati disciplinskim mjerama ili poslovnim sankcijama.

Članak 3.

Ova politika određuje očekivano ponašanje Društva i trećih strana Društva u odnosu na prikupljanje, korištenje, čuvanje, prijenos, otkrivanje ili uništavanje svih osobnih podataka koji se obrađuju.

Opseg

Članak 4.

Ova politika se odnosi na sve dijelove Društva gdje se obrađuju osobni podaci, na procesiranje svih osobnih podataka u elektronskom ili papirnatom obliku.

Definicije

Članak 5.

- **osobni podaci** su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („Ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;

- **obrada** 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;

- **ograničavanje obrade** je označivanje pohranjenih osobnih podataka s ciljem ograničavanja njihove obrade u budućnosti;

- **izrada profila** je svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;

- **pseudonimizacija** je obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom Ispitaniku 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;

- **sustav pohrane** je svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;

- **voditelj obrade** je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

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

- **primatelj** je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;

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

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

- **povreda osobnih podataka** je 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;

- **genetski podaci** su osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca;

- **biometrijski podaci** su osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci;

- **podaci koji se odnose na zdravlje** su osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu;

Zaštita podataka

Članak 6.

U svrhu osiguranja da su svi zahtjevi zaštite osobnih podataka identificirani i obrađeni tijekom dizajna novih sustava, usluga i procesa, svaki mora proći kroz proces odobrenja.

Društvo vrši procjenu rizika za sve nove ili izmijenjene sustave, usluge i procese u svojoj nadležnosti u suradnji s IT odjelom Društva. Nalaze analizira Službenik za zaštitu osobnih podataka u suradnji s Voditeljem informacijske sigurnosti i Voditeljem obrade osobnih podataka.

Službenik za zaštitu osobnih podataka (DPO- Data protection officer)

Članak 7.

Službenika za zaštitu osobnih podataka (data protection officer – DPO) imenuje Uprava Društva. DPO mora biti imenovan imenom i prezimenom, ali ne mora biti zaposlenik. Ova se funkcija može eksternalizirati.

Odgovornosti i aktivnosti istoga uključuju, ali nisu ograničene na:

- informiranje, izvještavanje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu, o njihovim obvezama vezanim uz zaštitu podataka,
- revizija Politike zaštite osobnih informacija,
- upravljanje procjenom rizika osobnih podataka,
- suradnja s ostalim poslovnim jedinicama u rješavanju incidenata vezanih uz osobne podatke,
- praćenje poštovanja politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu, osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade, te povezane revizije,
- pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja,
- suradnja s nadzornim tijelom,
- djelovanje kao kontaktna točka za nadzorno tijelo vezano uz pitanja o obradi, što uključuje i prethodno savjetovanje, te savjetovanje o svim drugim pitanjima,
- vođenje računa o riziku povezanom s postupcima obrade uz uzimanje u obzir prirodu, opseg, kontekst i svrhe obrade.

Praćenje sukladnosti

Članak 8.

U svrhu potvrde slijeđenja prihvatljive razine sukladnosti od strane Društva, Službenik za zaštitu osobnih podataka će, na godišnjoj razini, izvršiti reviziju sukladnosti slijeđenja i usklađenosti cijelog Društva i vezanih trećih strana koje vrše obradu podataka za društvo.

Sukladnost s politikom će se minimalno mjeriti u pogledu na:

- Usklađenost s politikom u skladu s zaštitom osobnih podataka, uključujući:
- Dodjelu odgovornosti
- Podizanje osviještenosti
- Edukaciju
- Efektivnost operativnih praksi zaštite podataka, uključujući:
- Prava Ispitanika
- Prijenos osobnih podataka
- Upravljanje incidentima vezanim uz osobne podatke
- Upravljanje pritužbama vezanim uz osobne podatke
- Razinu razumijevanja internih akata zaštite podataka i vezanih obavijesti
- Ažurnost internih akata zaštite podataka
- Točnost pohranjenih osobnih podataka
- Usklađenost aktivnosti izvršitelja obrade
- Adekvatnost procedura vezanih uz djelovanje u slučaju povrede osobnih podataka

Službenik za zaštitu osobnih podataka, u suradnji s voditeljima poslovnih jedinica, izraditi će plan s jasno definiranim rokovima u svrhu ispravljanja svih identificiranih nesukladnosti.

Načela zaštite podataka

Članak 9.

Društvo je prihvatilo slijedeća načela vezano uz prikupljanje, korištenje, čuvanje, transfer, otkrivanje i uništavanje osobnih podataka:

Osobni podaci moraju biti:

- zakonito, pošteno i transparentno obrađivani s obzirom na Ispitanika („zakonitost, poštenost i transparentnost");
- prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 89. stavkom 1. GDPR-a, ne smatra se neusklađenom s prvotnim svrhama („ograničavanje svrhe");
- primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka");
- točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave („točnost");
- čuvani u obliku koji omogućuje identifikaciju Ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1., što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih ovom Uredbom radi zaštite prava i sloboda Ispitanika („ograničenje pohrane");
- obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („cjelovitost i povjerljivost");

Prikupljanje podataka

Izvori podataka

Članak 10.

Osobni podaci se prikupljaju direktno od Ispitanika osim ako:

- Poslovni proces mora prikupljati osobne podatke od drugih osoba ili organizacija.

Ako se podaci prikupljaju od treće strane, Ispitanik mora biti obaviješten o prikupljanju, osim ako:

- Ispitanik je već obaviješten na neki drugi način
- Informacija mora ostati tajna zbog profesionalnih obaveza čuvanja tajne

Gdje se utvrdi da je obavijest prema Ispitaniku potrebna, obavijest se mora odmah proslijediti, ali ne kasnije od:

- Mjesec dana od prikupljanja osobnih podataka
- Za vrijeme prve komunikacije s Ispitanikom

Privola Ispitanika

Članak 11.

Društvo će dobiti privolu kroz zakonske i poštene načine, te uz potpuno znanje i razumijevanje Ispitanika.

Članak 12.

Društvo mora dobiti privolu Ispitanika za obradu osobnih podataka (osim u slučajevima kad je obrada zakonski utemeljena). Privola mora biti precizna, dobro informirajuća i nedvosmislena te mora biti jasno za što će se Ispitanikovi podaci koristiti. Ispitanik mora biti obaviješten o tome i biti slobodan donijeti odluku hoće li dati privolu.

Članak 13.

Privola se traži u situacijama:

- Kada se traži unos (novih) osobnih podataka
- Kod promjene ili davanja nove svrhe obrade već prikupljenih podataka

Traženje privola se primjenjuje na:

- Zaposlenike
- Poslovne partnere / pružatelje usluga
- Klijente (korisnike) / građane / treće pravne osobe

Članak 14.

Traženje privole se ne mora primjenjivati u slučaju da je obrada utemeljena na jednom od slijedećih slučajeva:

- obrada je nužna za izvršavanje ugovora u kojem je Ispitanik stranka ili kako bi se poduzele radnje na zahtjev Ispitanika prije sklapanja ugovora;
- obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- obrada je nužna kako bi se zaštitili ključni interesi Ispitanika ili druge fizičke osobe;
- obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode Ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je Ispitanik dijete.

Članak 15.

Ispitanik privolu mora dati svojevoljno te mu moraju biti jasni ciljevi, odnosno svrha prikupljanja njegovih osobnih podataka. Isto tako, Ispitanik mora biti obaviješten o tome da u svakom trenu može povući privolu, osim ako obrada podataka nema drugačiju zakonsku podlogu.

Članak 16.

Voditelj obrade mora moći dokazati da je Ispitanik dao privolu za obradu njegovih podataka, da je zahtjev za privolu bio razumljiv i pisan jednostavnim jezikom, da Ispitanik privolu može povući jednako jednostavno kao što ju je i dao.

Članak 17.

Privola se treba dati jasnom potvrdnom radnjom poput pisane izjave (uključujući i elektroničku) ili usmene izjave. Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih. Ako Ispitanik nema slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica, onda se ne može smatrati da je privola dana dobrovoljno.

Članak 18.

Ukoliko postojeći osobni podaci i njihova obrada nisu usklađeni s zahtjevima regulative GDPR i zahtijevaju privolu, istu je potrebno zatražiti od Ispitanika.

Društvo kroz privolu obavještava korisnika o tome:

- Koje podatke prikuplja?

- U koju svrhu prikuplja podatke?
- Kako ih obrađuje?
- Kome ih šalje?
- Koja su prava Ispitanika?
- U kojem slučaju može zatražiti pravo na zaborav?
- Tko je Službenik za zaštitu osobnih podataka i njegove kontakt informacije?

Članak 19.

Društvo vodi evidenciju privola korisnika na slijedeći način:

- Evidencija će biti papirnata i skenirana u elektroničko obliku. Ista se čuva u zaključanoj arhivi.

Obavijesti o privatnosti

Članak 20.

Internet stranica Društva uključivati će informacije o privatnosti i informacije o Internet kolačićima (Cookies) slijedeći prikladne zakonske odredbe. Svaku izjavu o privatnosti mora odobriti Uprava organizacije.

Korištenje podataka

Obrada podataka

Članak 21.

Društvo koristi osobne podatke za slijedeće svrhe:

- Generalne aktivnosti i administraciju korisnika usluga
- Pružanje usluga korisnicima
- Administraciju i upravljanje uslugama

Posebne kategorije osobnih podataka

Članak 22.

Društvo obrađuje slijedeće posebne kategorije osobnih podataka:

- Podaci o bolovanju zaposlenika
- Podaci o djeci zaposlenika
- Zapisi video nadzora na ulazu

Članak 23.

U slijedećim slučajevima se ne traži izričita privola:

- obrada se odnosi na osobne podatke koje je već javno objavio Ispitanik
- obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili Ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava države članice ili kolektivnog ugovora u skladu s pravom države članice koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese Ispitanika;
- obrada je nužna za zaštitu životno važnih interesa Ispitanika ili drugog pojedinca ako Ispitanik fizički ili pravno nije u mogućnosti dati privolu;
- obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;

Članak 24.

U svakoj situaciji gdje se obrađuju Posebne kategorije osobnih podataka potrebno je zatražiti odobrenje obrade od Uprave Društva, te osnova za obradu treba biti jasno definirana.

Društvo će u slučaju obrade Posebnih kategorije osobnih podataka uspostaviti posebne mjere zaštite sukladno dobrim praksama i očekivanjima Ispitanika.

Kvaliteta podataka

Članak 25.

Društvo će usvojiti sve potrebne i moguće mjere kako bi osiguralo da su prikupljeni osobni podaci potpuni i točni, te ažurirani na način da odražavaju trenutačnu situaciju Ispitanika.

Mjere usvojene od strane Društva, kako bi se osigurala kvaliteta podataka, uključuju:

- Ispravljanje osobnih podataka za koje se zna da su netočni, nepotpuni, dvosmisleni, stvaraju zabludu ili su zastarjeli, čak i ako Ispitanik ne traži ispravak.
- Čuvanje osobnih podataka samo za razdoblje potrebno za zadovoljavanje dopuštenih uporaba ili primjenjivog zakonskog razdoblja zadržavanja.
- Uklanjanje osobnih podataka ako krši bilo koji od načela zaštite podataka ili ako više nisu potrebni.
- Ograničenje obrade, umjesto brisanja osobnih podataka, ukoliko zakon zabranjuje brisanje ili bi brisanje ugrozilo legitimne interese Ispitanika
- Ispitanik osporava da su njihovi osobni podaci točni i ne može se jasno utvrditi jesu li njihovi podaci točni ili netočni.
- Profiliranje i automatizirano odlučivanje

Članak 26.

Društvo će koristiti profiliranje i automatizirano odlučivanje gdje je potrebno sklopiti ili izvršiti ugovor s Ispitanikom ili gdje je to zakonom dopušteno.

Tamo gdje Društvo koristi profiliranje i automatizirano odlučivanje, to će biti otkriveno relevantnim ispitanicima. U takvim će slučajevima Ispitanik imati priliku:

- Izraziti svoje stajalište
- Dobiti objašnjenje za automatsku odluku
- Pregledati logiku koja se koristi automatiziranim sustavom
- Nadopuniti automatizirani sustav s dodatnim podacima
- Pregled automatske odluke u suradnji s zaposlenikom Društva
- Osporiti automatsku odluku
- Društvo također mora osigurati da se profiliranje i automatizirano odlučivanje koje se odnosi na Ispitanika temelji na točnim podacima
- Digitalni marketing

Članak 27.

Kao opće pravilo Društvo neće slati promotivni ili izravni marketinški materijal kontaktu tvrtke putem digitalnih kanala kao što su mobilni telefoni, e-mail i internet, bez prethodnog pribavljanja suglasnosti. Slanje digitalne marketinške kampanje bez prethodnog odobrenja Ispitanika mora odobriti Uprava.

Gdje je obrada osobnih podataka odobrena u svrhu digitalnog marketinga, Ispitanik mora biti obaviješten u trenutku prvog kontakta da imaju pravo prigovoriti, u bilo kojoj fazi, da se njegovi podaci obrađuju u takve svrhe. Ako Ispitanik podnese prigovor, obrada odluka o isključivanju se mora čuvati, umjesto da bude potpuno izbrisana.

Treba napomenuti da tamo gdje se digitalni marketing provodi u kontekstu "B2B", ne postoji zakonski zahtjev da se dobije naznaku suglasnosti za obavljanje digitalnog marketinga pojedincima pod uvjetom da im se pruži prilika za isključivanje.

Zadržavanje podataka

Članak 28.

Da bi se osigurala poštena obrada, Društvo neće zadržati osobne podatke duže nego što je to neophodno u odnosu na svrhe za koje je izvorno prikupljeno ili za koje je dalje obrađivano.

Duljina vremena u kojem Društvo treba zadržati osobne podatke definirano je zakonom. Svi osobni podaci trebaju biti izbrisani ili uništeni što je prije moguće ako je potvrđeno da više nema potrebe za zadržavanjem.

Zaštita podataka

Članak 29.

Društvo će usvojiti fizičke, tehničke i organizacijske mjere kako bi osigurala sigurnost osobnih podataka. To uključuje prevenciju gubitka ili oštećenja, neovlaštene izmjene, pristupa ili obrade i drugih rizika kojima može biti izložena ljudskim djelovanjem, fizičkim ili prirodnim okruženjem.

U nastavku je naveden sažetak sigurnosnih mjera povezanih s osobnim podacima:

- Spriječiti neovlaštene osobe da dobiju pristup sustavu obrade podataka u kojima se obrađuju osobni podaci
- Spriječiti osobe koje imaju pravo koristiti sustav obrade podataka od pristupa osobnim podacima koji su izvan njihovih potreba i ovlaštenja
- Osigurati da se osobni podaci tijekom elektronskog prijenosa ili tijekom transporta ne mogu čitati, kopirati, mijenjati ili ukloniti bez odobrenja
- Osigurati dostupnost zapisa sustava u svrhu utvrđivanja od koga su uneseni, mijenjani ili uklonjeni Osobni podaci iz sustava obrade podataka
- Osigurati da u slučaju kada obradu obavlja izvršitelj obrade, podaci se mogu obrađivati samo u skladu s uputama voditelja obrade
- Osigurati da su osobni podaci zaštićeni od neželjenog uništavanja ili gubitka
- Osigurati da osobni podaci prikupljeni za različite svrhe mogu biti obrađeni odvojeno
- Osigurati da se osobni podaci ne drže duže nego što je potrebno

Zahtjevi Ispitanika

Članak 30.

Tvrtka će uspostaviti sustav koji će omogućiti i olakšati ostvarivanje prava Ispitanika u odnosu na:

- Pristup informacijama
- Prigovor na obradu
- Prigovor na automatizirano odlučivanje i profiliranje
- Ograničenje obrade
- Prijenos podataka
- ispravljanje podataka
- Brisanje podataka

Ako pojedinac podnese zahtjev koji se odnosi na bilo koje gore navedeno pravo, Društvo će razmotriti svaki takav zahtjev u skladu sa svim primjenjivim zakonima i propisima o zaštiti

podataka. Neće se naplaćivati nikakva administrativna naknada za razmatranje i / ili pridržavanje takvog zahtjeva, osim ako se zahtjev ne smatra nepotrebnim ili prekomjernim poslom.

Članak 31.

Ispitanici imaju pravo na pribavljanje, na temelju pisanog zahtjeva tvrtke i nakon uspješne provjere njihovog identiteta, informacije o sljedećim informacijama o vlastitim osobnim podacima:

- Svrha prikupljanja, obrade, korištenja i čuvanja njihovih osobnih podataka
- Izvor osobnih podataka, ako nije dobiven od Ispitanika
- Kategorije osobnih podataka Ispitanika
- Primatelje ili kategorije primatelja kojima su ili mogu biti preneseni Osobni podaci, zajedno s lokacijom tih primatelja
- Predviđeno razdoblje skladištenja za osobne podatke ili obrazloženje za određivanje razdoblja skladištenja
- Upotreba bilo kakvog automatiziranog odlučivanja, uključujući profiliranje

Pravo Ispitanika da:

- se usprotivi obradi njihovih osobnih podataka
- može podnijeti žalbu nadležnom tijelu za zaštitu podataka
- može zatražiti ispravak ili brisanje njihovih osobnih podataka
- može zatražiti ograničenje obrade njihovih osobnih podataka

Članak 32.

Svi zahtjevi za pristup ili ispravak osobnih podataka moraju biti upućeni Službeniku za zaštitu osobnih podataka koji će prijaviti svaki zahtjev po primitku. Odgovor na svaki zahtjev bit će dostavljen u roku od 30 dana od primitka pismenog zahtjeva od Ispitanika. Društvo mora potvrditi da je podnositelj zahtjeva Ispitanik ili njegov ovlašteni pravni zastupnik. Ispitanici imaju pravo zahtijevati da Društvo ispravlja ili dopuni pogrešne, obmanjujuće, zastarjele ili nepotpune osobne podatke.

Ako Društvo ne može potpuno odgovoriti na zahtjev u roku od 30 dana, isto će ipak dostaviti sljedeće podatke Ispitaniku ili njihovom ovlaštenom pravnom zastupniku u navedenom roku:

- Potvrdu o primitku zahtjeva
- Sve informacije do sada
- Pojedinosti o bilo kojoj traženoj informaciji ili izmjenama koje neće biti dostavljene ispitaniku, razlogu za odbijanje te o svim mogućim postupcima za žalbu na odluku
- Procijenjeni datum do kojeg će biti dostavljeni preostali odgovori
- Procjena troškova koje mora platiti Ispitanik (npr. Ako je zahtjev prekomjeran)
- Ime i kontakt informacije pojedinca tvrtke koje bi Ispitanik trebao kontaktirati za daljnje informacije

Treba napomenuti da se mogu pojaviti situacije u kojima pružanje informacija koje je zatražio Ispitanik otkriva osobne podatke o drugoj osobi. U takvim slučajevima informacije moraju biti ispravljene ili uskraćene kako je potrebno ili prikladno za zaštitu prava te osobe.

Zahtjevi od strane pravosudnih tijela

Članak 33.

U određenim okolnostima, dopušteno je da se osobni podaci dijele bez znanja ili suglasnosti Ispitanika. I to kada je otkrivanje osobnih podataka potrebno u bilo kojoj od sljedećih svrha:

- Sprječavanje ili otkrivanje zločina
- Uhićenje ili progon prekršitelja
- Procjena ili naplata poreza ili pristojbi

- Po nalogu suda ili bilo kojeg zakona
- Edukacija i osvješćivanje

Članak 34.

Svi zaposlenici Društva koji imaju pristup osobnim podacima imati će svoje odgovornosti, prema ovoj politici, predstavljene kao dio njihove obuke. Osim toga, Društvo će pružiti obuku za zaštitu podataka i proceduralne smjernice za zaposlenike.

Obuka i osvješćivanje sastojati će se, barem, od sljedećih elemenata:

- Načela zaštite podataka navedena u ovom dokumentu
- Svaka obveza zaposlenika da koristi i dopusti korištenje osobnih podataka samo ovlaštenim osobama i za ovlaštene svrhe
- Potreba i pravilna upotreba oblika i postupaka usvojenih za provedbu ove politike
- Točna upotreba zaporki, oznaka sigurnosti i drugih pristupnih mehanizama
- Važnost ograničavanja pristupa osobnim podacima, poput korištenja čuvara zaslona zaštićenih lozinkom i prijave kad sustavima ne pristupa ovlaštena osoba
- Sigurno pohranjivanje datoteka, ispisa i elektroničkih medija za pohranu
- Potreba za dobivanjem odgovarajućeg odobrenja i korištenje odgovarajućih zaštitnih mjera za sve prijenose osobnih podataka izvan mreže i prostorija Društva
- Pravilno uništavanje papira korištenjem rezača papira
- Svaki poseban rizik povezan s određenim aktivnostima ili dužnostima odjela

Prijenos podataka

Članak 35.

Tvrtka može prenijeti osobne podatke primateljima interne ili treće strane koji se nalaze u drugoj zemlji ukoliko je ta država ima odgovarajuću razinu pravne zaštite za prava i slobode Ispitanika. Tamo gdje se trebaju izvršiti transferi zemljama koje nemaju odgovarajuću razinu pravne zaštite (tj. Trećih zemalja), one se moraju izvršiti u skladu s odobrenim metodama prijenosa.

Tvrtka može prenositi samo osobne podatke u kojima se primjenjuje jedan od dolje navedenih scenarija prijenosa:

- Ispitanik je dao suglasnost za predloženi prijenos
- Prijenos je neophodan za izvedbu ugovornih obveza
- Prijenos je neophodan za provedbu predugovornih mjera koje se poduzimaju kao odgovor na zahtjev Ispitanika
- Prijenos je neophodan za zaključivanje ili izvršenje ugovora sklopljenog s trećom stranom u interesu Ispitanika
- Prijenos je zakonski obvezan na temelju važnih javnih interesa
- Prijenos je neophodan za osnivanje, vršenje ili obranu pravnih zahtjev
- Prijenos je neophodan kako bi se zaštitili vitalni interesi Ispitanika
- Prijenosi između poslovnica Društva

Članak 36.

Da bi Društvo moglo učinkovito obavljati svoje poslovanje, može doći do slučajeva kada je potrebno prenositi osobne podatke iz jedne poslovnice u drugu ili omogućiti pristup osobnim podacima međunarodnih lokacija. Ako se to dogodi, Društvo je odgovorno za zaštitu tih osobnih podataka.

Tvrtka upravlja prijenosom osobnih podataka između poslovnica, gdje je mjesto primatelja entiteta treća zemlja, koristeći jasno definirane sigurnosne mjere. Obvezujuća korporativna pravila pružaju pravno obvezujuća, provediva prava na ispitanicima u pogledu obrade njihovih osobnih podataka i mora ih provoditi svaka poslovnica, uključujući i njihove zaposlenike.

Prilikom prijenosa osobnih podataka drugoj tvrtki koja se nalazi u trećoj zemlji, moramo:

- Dostaviti samo minimalnu količinu osobnih podataka potrebnih za određenu svrhu prijenosa (na primjer, ispuniti transakciju ili izvršiti određenu uslugu)
- Osigurati odgovarajuće sigurnosne mjere za zaštitu osobnih podataka tijekom prijenosa (uključujući zaštitu lozinkom i šifriranje, ako je potrebno)

Prijenos na treće strane

Članak 37.

Društvo će prenijeti Osobne podatke na treće strane samo ako je zajamčeno da će informacije biti pravovremeno obrađene i prikladno zaštićene od primatelja. Tamo gdje se obavlja obrada treće strane, Društvo će najprije utvrditi da li se, prema mjerodavnom zakonu, treća strana smatra voditeljem obrade ili izvršiteljem obrade osobnih podataka koji se prenose.

Ako se Treća strana smatra voditeljem obrade, Društvo će u suradnji s trećom stranom sklopiti odgovarajući ugovor kako bi se pojasnile odgovornosti svake strane u odnosu na prenesene Osobne podatke.

Ako se Treća strana smatra izvršiteljem obrade, Društvo će u suradnji s trećom stranom sklopiti odgovarajući ugovor o obradi podataka. Ugovor mora zahtijevati od izvršitelja obrade podataka zaštitu osobnih podataka od daljnjeg objavljivanja i samo obradu osobnih podataka u skladu s uputama Društva. Osim toga, sporazum će zahtijevati od izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere za zaštitu osobnih podataka, kao i postupke za obavještavanje o povredama sigurnosti osobnih podataka.

Članak 38.

Kada Društvo vrši usluge eksternalizacije trećoj strani (uključujući usluge „cloud computinga"), oni će utvrditi hoće li treća strana obraditi osobne podatke u njihovo ime i hoće li eksternaliziranje značiti prijenos bilo kojeg osobnog podatka u treće zemlje. U oba će slučaja osigurati da, u suradnji s tvrtkom, uključe odgovarajuće odredbe u ugovoru o eksternalizaciji za takve transakcije i transfere u područja trećih zemalja.

Društvo će redovito provoditi reviziju Obrade osobnih podataka koje obavljaju treće strane, osobito u pogledu tehničkih i organizacijskih mjera koje imaju. Identificirat će se i pratiti od strane zaposlenika odgovornog za treću stranu.

Pravo na prenosivost osobnih podataka

Članak 39.

Ispitanik ima pravo na dobivanje osobnih podataka o njemu, koje je on dostavio Društvu, u strukturiranom obliku koji se može računalno čitati i koji ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja Društva, u slučajevima kad:

- obrada se temelji na privoli Ispitanika ili ugovornoj obvezi
- obrada se vrši automatiziranim putem

Društvo će prenijeti osobne podatke izravno drugom voditelju obrade, gdje je to tehnički izvedivo.

Utvrđivanje metode prijenosa će se izvršiti direktno s drugim voditeljem obrade.

Rukovanje pritužbama

Članak 40.

Ispitanici bi prigovor u vezi s obradom njihovih osobnih podataka trebali pismeno uputiti Društvu. Istraga o pritužbi provest će se u mjeri koja je prikladna temeljem opsega konkretnog slučaja. Društvo će u razumnom roku obavijestiti Ispitanika o napretku i ishodu prigovora.

Ako se problem ne može riješiti putem konzultacija između Ispitanika i Društva, Ispitanik može, po vlastitom izboru, zatražiti naknadu putem posredovanja, obvezujuće arbitraže, parnice ili putem pritužbe nadležnom tijelu za zaštitu podataka.

Izvješćivanje o povredi zaštite osobnih podataka

Članak 41.

Svaki zaposlenik koji sumnja da je došlo do kršenja zaštite osobnih podataka zbog krađe ili izloženosti osobnih podataka, mora odmah prijaviti incident s opisom događaja. Obavijest o incidentu može poslati putem službenih kontakata Društva (mail, fax, telefon, kontakt obrazac).

Društvo će istražiti sve prijavljene incidente kako bi potvrdio je li došlo do kršenja osobnih podataka. Ako je potvrđena povreda zaštite osobnih podataka, Društvo će slijediti odgovarajući autorizirani postupak na temelju kritičnosti i količine uključenih osobnih podataka. Za teške povrede osobnih podataka, Uprava tvrtke pokrenut će i predsjedat će timom za hitne slučajeve koji će koordinirati i upravljati reakcijom na incident.

Završne odredbe

Odgovornost

Članak 42.

Svi sudionici poslovnog procesa Društva odnosno informacijskog sustava dužni su se pridržavati odredbi ove procedure u dijelu koji se na njih odnosi i na način koji je istima propisan.

Nepridržavanje ili ponašanje (djelovanje) suprotno ovim odredbama smatra se povredom radne obveze za koju se može dati otkaz ugovora o radu.

Valjanost

Članak 43.

Ovaj Pravilnik se primjenjuje i stupa na snagu danom donošenja.

DIREKTOR

Dragan Šekerija, struč.spec.ing.aedif.

SEDRA CONSULTING d.o.o.
Ulica 11
OIB 09177957072