POLITIKA ZAŠTITE OSOBNIH PODATAKA

Sadržaj

NAMJENA 3
OPSEG 3
DEFINICIJE 3
NAČELA 4
ODGOVORNOSTI 5
VOĐENJE EVIDENCIJE AKTIVNOSTI OBRADA OSOBNIH PODATAKA 6
PROCJENA UČINKA PREDVIĐENIH POSTUPAKA OBRADE NA ZAŠTITU OSOBNIH PODATAKA 7
PRAVA ISPITANIKA I VOĐENJE EVIDENCIJE ZAHTJEVA ISPITANIKA 7
UPRAVLJANJE PRIVOLAMA ISPITANIKA 7
UPRAVLJANJE POVREDAMA OSOBNIH PODATAKA 7
ZAVRŠNE I PRIJELAZNE ODREDBE 8

Namjena

Namjena ovog dokumenta je definiranje opće politike i pravila koja se primjenjuju za zaštitu svih osobnih podataka koji se odnose na fizičke osobe (dalje u tekstu: ispitanici), a do kojih dolazi Utilis d.o.o. (u nastavku: Utilis) tijekom svog redovnog poslovanja. Politikom se propisuju i odgovornosti za procese upravljanja evidencijama aktivnosti obrada osobnih podataka, registra zahtjeva ispitanika, registra povreda osobnih podataka (incidenata) i registra privola.

Politika se temelji na zahtjevima Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka - Opća uredba o zaštiti podataka (dalje u tekstu: GDPR).

Opseg

Ova politika primjenjuje se u cijeloj organizaciji Utilis na sve obrade u kojima se koriste osobni podaci pojedinaca (ispitanika). Usklađena je sa svim aktima koji u pojedinim svojim dijelovima dotiču zaštitu osobnih podataka ili podataka općenito (Politika sigurnosti informacijskog sustava, pravilnici i procedure).

Definicije

Pregled pojmova i njihovo značenje:

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

Ispitanik - Svaki pojedinac (fizička osoba) od kojeg prikupljamo i obrađujemo osobne podatke.

Izvršitelj obrade osobnih podataka – uloga ugovornog partnera (treće strane) Utilis-a kojemu je povjerena obrada (ili dio obrade) osobnih podataka u ime voditelja obrade osobnih podataka.

Obrada osobnih podataka – je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima.

Osobni podaci - Svi podaci o nekom ispitaniku (fizičkoj osobi) pomoću kojih se jednoznačno mogu identificirati iste te fizičke osobe/pojedinci – ispitanici. Osobni podaci su svi podaci koje u svojem poslovanju koristi Utilis koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (u daljnjem tekstu „ispitanik“). Pojedinac čiji se identitet može utvrditi je 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.

Privola ispitanika – slobodno dano i izričito očitovanje volje ispitanika kojom on izražava svoju suglasnost s obradom njegovih osobnih podataka u određene svrhe.

Voditelj obrade osobnih podataka – je uloga odgovorne osobe Utilis-a koja utvrđuje svrhu i način obrade osobnih podataka prikupljenih od ispitanika.

Načela

Sigurnost osobnih podataka - Utilis štiti osobne podatke od neovlaštenog pristupa, uporabe ili otkrivanja. Prikupljeni osobni podaci se čuvaju u elektroničkom obliku na koji su primjenjene odgovarajuće tehničke, organizacijske i proceduralne mjere kako bi se spriječilo da se osobnim podacima koji nisu dostupni ostalim korisnicima ne bi neovlašteno pristupalo te da bi osigurali da se koriste u skladu s našom Politikom i propisima koji se primjenjuju. Pri tome se Utilis služi dobrim praksama vezanim uz informacijsku sigurnost koje su propisane ostalim internim aktima počevši od Politike sigurnosti informacijskog sustava.

Svrha prikupljanja – Osobni podaci će se prikupljati prije svega radi osiguranja pružanja tražene usluge. Svaka obrada koja se radi nad osobnim podacima jasno će imati definiranu svrhu obrade. Osobne je podatke obrađivati dozvoljeno samo kada za to postoji jasno određena i dokumentirana zakonska osnova ili osnova temeljena na ugovornom odnosu, dok su sve ostale obrade osobnih podataka dozvoljene jedino uz jasnu dokumentiranu privolu njihovog vlasnika ili opunomoćenika.

Nužnost prikupljanja - Prilikom prikupljanja i obrade osobnih podataka, obavezna je primjena načela prema kojem se prikupljati smiju samo oni podaci koji su sa predmetnu obradu stvarno i potrebni. Svako prikupljanje suvišnih podataka je zabranjeno.

Ograničenje pohrane – Osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Iznimka su osobni podaci koji će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe koji se moraju adekvatno osigurati sukladno GDPR-u.

Točnost i ažurnost podataka – Utilis će osigurati sve potrebne mjere da osigura točnost i ažurnost osobnih podataka koje se koriste u obradama.

Pristup osobnim podacima – uvid u osobne podatke ispitanika smiju imati samo one osobe kojima je to nužno za obavljanje usluge koja je definirana svrhom obrade. Voditelj obrade, ako je to potrebno, može angažirati izvršitelja obrade s kojim će sklopiti ugovor i obvezati ga sigurnosnim mjerama u pogledu postupanja s osobnim podacima. Postupanje s izvršiteljima obrade propisana je i Pravilnikom o upravljanju s trećim stanama. Izvršitelj obrade, ako nije

siguran u to kome smije dati pristup osobnim podacima, savjetovat će se sa Voditeljem obrade osobnih podataka. Utilis može sklapati međunarodne ugovore koji uključuju prijenos osobnih podataka u treće zemlje ili međunarodne organizacije u onoj mjeri u kojoj takvi sporazumi ne utječu na GDPR Uredbu ili bilo koje druge odredbe prava Unije i koji uključuju odgovarajuću razinu zaštite temeljnih prava ispitanika.

Informiranost ispitanika - Prije prikupljanja osobnih podataka, ispitanicima se mora pružiti jasna informacija o razlogu prikupljanja, vrsti obrade u kojoj će se informacije koristiti, vremenu čuvanja podataka te eventualnim trećim osobama koje će informacijama pristupati. Ukoliko Utilis bude prikupljao osobne podatke putem web stranice Utilisa, detaljnije informacije za posjetitelje Utilis web stranice, koji ostavljaju svoje osobne podatke, propisat će se politikom privatnosti koja će se postaviti na web stranice Utilis-a.

Obrada osobnih podataka djece - Ako se podaci prikupljaju od djece, neophodno je uspostaviti posebne mehanizme koji će osigurati da su djeca dovoljno stara kako bi razumjela posljedice davanja informacija. Svakom prikupljanju i obradi informacija maloljetnika mora se pristupati sa posebnom pažnjom, te se pri tome mora voditi najvišim etičkim načelima. Za djecu mlađu od 16 godina potrebno je dobiti privolu roditelja.

Posebne kategorije osobnih podataka – Posebnu pažnju glede mjera zaštite treba posvetiti posebnim kategorijama osobnih podataka. Ovi podaci su primjerice podaci koji se odnose na rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca. Za obrade ovih podataka obavezno je provesti procjenu učinka na privatnost ispitanika.

„**Privacy by design**“ - Prilikom razvijanja, osmišljavanja, odabira i upotrebe aplikacija, usluga i proizvoda koji se temelje na obradi osobnih podataka ili obrađuju osobne podatke kako bi ispunili svoju zadaću, proizvođače proizvoda, usluga i aplikacija trebalo bi poticati da uzmu u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija i da uzimajući u obzir najnovija dostignuća osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka.

Odgovornosti

Pravila definiranih ovom politikom moraju se pridržavati **svi radnici Utilis-a**, kao i **treće strane** koje u okviru svoje suradnje sa Utilis-om ostvaruju pristup osobnim podacima ispitanika. S trećim stranama identificiranim kao izvršitelji obrada osobnih podataka će se potpisati izjave o tajnosti i povjerljivosti i ugovori koji osiguravaju sukladnost sa zahtjevima GDPR uredbe.

Za uspostavu i održavanje sustava upravljanja osobnim podacima, te koordinaciju svih aktivnosti vezanih uz upravljanje osobnim podacima odgovoran je **Voditelj obrade osobnih**

podataka (DPO). Za rad odgovara direktno upravi Utilis-a. Voditelj obrade osobnih podataka odgovoran je posebno za:

- obavještavanje i savjetovanje voditelja ili izvršitelja obrade, te radnika koji obrađuju osobne podatke o njihovim obavezama iz GDPR Uredbe,
- nadziranje poštivanja Uredbe i internih politika i ostale regulative vezane uz zaštitu osobnih podataka,
- uspostavu i održavanje registra obrada osobnih podataka,
- dodjela odgovornosti za zaštitu osobnih podataka radnicima i trećim stranama uključenim u prikupljanje i obradu osobnih podataka,
- podizanje svijesti i edukacija iz područja zaštite osobnih podataka,
- ugrađivanje zaštite privatnosti u poslovne procese i informacijske sustave,
- ugrađivanje zaštite privatnosti u revizijske procese,
- savjetovanje kod provedbe procjena učinka na zaštitu podataka (procjena rizika odnosno DPIA),
- suradnja sa nadzornim tijelima,
- nadziranje procesa upravljanja rizikom u obradama osobnih podataka (eng. DPIA),
- izvještavanje Uprave Utilis-a o učinkovitosti sustava upravljanja osobnim informacijama.

Voditelja obrade osobnih podataka imenuje uprava Utilis-a.

Razvojni odjel je odgovoran za operativnu uspostavu i održavanje tehničkih kontrola potrebnih za usklađivanje sa zahtjevima ove politike i podržavajućih akata pridržavajući se „privacy by design“ načela.

Uprava Utilisa je odgovorna za praćenje i tumačenje regulative iz područja privatnosti i pružanje pravne podrške radu sustava upravljanja osobnim podacima.

Voditelj sigurnosti informacijskog sustava zadužen je za nadzor primjene mjera zaštite osobnih podataka i pružanje stručne potpore iz svog područja radu sustava upravljanja osobnim podacima.

Vođenje evidencije aktivnosti obrada osobnih podataka

Utilis je dužan uspostaviti i održavati evidenciju aktivnosti obrada osobnih podataka i za svaku obradu i vrstu osobnih podataka imenovati odgovornu osobu. Odgovorna osoba je dužna osigurati da se u obradu uključuju isključivo osobni podaci za čiju obradu postoji odgovarajuća privola, zakonska osnova ili poslovna potreba.

Za izradu evidencije aktivnosti obrada osobnih podataka te ažuriranje u skladu s promjenama u poslovnim procesima i informacijskom sustavu Utilis odgovoran je voditelj obrade osobnih podataka (DPO).

Procjena učinka predviđenih postupaka obrade na zaštitu osobnih podataka

Ako je izvjesno da bi povreda osobnih podataka mogla prouzročiti visok rizik za ispitanika, voditelj obrade dužan je, uz savjetovanje sa Voditeljom obrade osobnih podataka (DPO), provesti procjenu učinka predviđenih postupaka za zaštitu osobnih podataka.

Procjena učinka predviđenih postupaka za zaštitu osobnih podataka (engl. DPIA – Data Protection Impact Analysis) provodi se sukladno metodologiji upravljanja rizicima.

Prava ispitanika i vođenje evidencije zahtjeva ispitanika

Ispitanicima (vlasnicima osobnih informacija) mora se omogućiti pravo na pristup informacijama o tome koje osobne podatke Utilis o njima posjeduje i koja je svrha obrade. Utilis ispitaniku mora omogućiti ispravak netočnih i nadopunu nedostajućih osobnih podataka, te mogućnost uskraćivanja prava na obradu njegovih podataka kada se obrada temelji na privoli ispitanika.

Na zahtjev ispitanika, osobne podatke koje su dane na temelju privole moraju se obrisati iz svih informacijskih sustava Utilis-a i informacijskih sustava trećih strana kojima je Utilis omogućio pristup ovim podacima. Ispitanik ima pravo na prenosivost svojih osobnih podataka. Na zahtjev ispitanika, njegovi se osobni podaci moraju isporučiti u elektroničkom obliku.

Proces upravljanja zahtjevima ispitanika sukladno njihovim pravima propisat će se posebnim internim aktom – procedurom. Odgovornost za provedbu procesa zahtjeva ispitanika je pri Voditelju obrade osobnih podataka (DPO).

Zahtjeve vezane uz prava ispitanika možete podnijeti na E-mail adresu: szop@utilis.biz

Upravljanje privolama ispitanika

Za sve obrade osobnih podataka ispitanika koje za svrhu obrade nemaju uporište u zakonskim ili regulatornim aktima, neposrednim ugovorima s ispitanicima ili legitimnom interesu Utilis-a, potrebno je osigurati proces upravljanja privolama ispitanika. Takve obrade se temelje na izričitoj privoli ispitanika čiji zapis se mora čuvati unutar informacijskog sustava Utilis-a. Ovo podrazumijeva vođenje registra privola za takve obrade.

Odgovornost za proces upravljanja privolama ispitanika je dodijeljena voditelju obrade osobnih podataka (DPO).

Upravljanje povredama osobnih podataka

Utilis će uspostaviti i održavati procedure odgovora na incidente (povrede) vezane uz narušavanje sigurnosti osobnih podataka unutar Utilis-a i kod trećih strana kojima je Utilis ustupila ili koje su Utilis-u ustupile osobne podatke.

Utilis će uspostaviti i održavati strukturu odgovornosti za izvještavanje o povredama vezanim uz sigurnost osobnih podataka.

Utilis će uspostaviti i održavati mjere za detekciju neovlaštenog pristupa osobnim podacima i curenja osobnih podataka iz informacijskog sustava.

U slučaju narušavanja sigurnosti osobnih podataka, Utilis će bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvijestiti nadležno tijelo (Agenciju za zaštitu osobnih podataka). U slučaju curenja osobnih podataka, Utilis će o tome obavijestiti i ispitanike čiji su podaci kompromitirani ukoliko to bude provedivo na razuman način.

Proces upravljanja povredama osobnih podataka (incidentima) ispitanika propisano je posebnim internim aktom – Pravilnik o upravljanju incidentima. Voditelj obrade osobnih podataka (DPO) odgovoran je za provedbu procesa upravljanja povredama osobnih podataka ispitanika u Utilis-u.

Završne i prijelazne odredbe

Politika stupa na snagu i primjenjuje se danom njezinog donošenja. Vlasnik ove politike je voditelju obrade osobnih podataka (DPO) te je odgovoran provjeriti je i po potrebi ažurirati minimalno jednom godišnje.