



Ulica grada Vukovara 37, 10000 Zagreb

POLITIKA UPRAVLJANJA ZAŠTITOM OSOBNIH PODATAKA U HEP GRUPI

SADRŽAJ

Politika upravljanja zaštitom osobnih podataka u HEP grupi	3
Preambula	3
Svrha dokumenta	3
Vrijednost osobnih podataka i odgovornost za njihovu zaštitu.....	4
Prikupljanje i obrada osobnih podataka.....	4
Prava ispitanika	4
Tehnička integrirana zaštita osobnih podataka.....	5
Minimizacija i zaštita osobnih podataka.....	5
Upravljanje incidentima	6
Certifikacija.....	6
Iznimke	6
Odgovornosti Uprava društava HEP grupe.....	7
Odgovornosti radnika i trećih strana	7
Odgovornosti Službenika za zaštitu podataka u HEP-u d.d. i Službenika za zaštitu podataka u društvima HEP grupe.....	7
Odgovornosti Sektora za informacijsko komunikacijske tehnologije u HEP-u d.d.	8
Odgovornosti Ureda za korporativnu sigurnost u HEP-u d.d.....	8
Odgovornosti Sektora za internu reviziju u HEP-u d.d.	8
Odgovornosti za održavanje ovog dokumenta	9

Na temelju članka 26. Statuta Hrvatske elektroprivrede d.d., a u vezi s Odlukom broj 15-3.1/2018. od dana 11. travnja 2018. godine, Uprava HEP-a d.d. dana 7. svibnja 2018. godine donijela je:

POLITIKU UPRAVLJANJA ZAŠTITOM OSOBNIH PODATAKA U HEP GRUPI

PREAMBULA

Zaštita osobnih podataka u Republici Hrvatskoj te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj, uređena je Zakonom o zaštiti osobnih podataka. Društva HEP grupe su u vremenu od stupanja na snagu predmetnog Zakona poduzela sve potrebne mjere zaštite osobnih podataka.

Uredbom Europskog parlamenta i Vijeća Europske Unije (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka od dana 27. travnja 2016. godine, a koja započinje s primjenom dana 25. svibnja 2018. godine, (dalje u tekstu: Uredba) značajno su proširene obveze pravnih osoba koje obrađuju osobne podatke te je definirana zaštita pojedinaca s obzirom na takvu obradu osobnih podataka kao temeljno pravo.

Time je svrha zaštite osobnih podataka definirana kao zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka, a prikupljanje i obrada osobnih podataka se smiju odvijati isključivo pod strogim i kontroliranim procesima u skladu s Uredbom.

SVRHA DOKUMENTA

Ovom politikom HEP d.d. definira odnos prema osobnim podacima, definira pravila postupanja, dodjeljuje odgovornosti i daje punu podršku sustavnom upravljanju osobnim podacima i njihovoj zaštiti u svim društvima HEP grupe.

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

Pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

VRIJEDNOST OSOBNIH PODATAKA I ODGOVORNOST ZA NJIHOVU ZAŠTITU

Osobni podaci koje društva HEP grupe prikupljaju i obrađuju u svom radu smatraju se povjerljivom, nematerijalnom, informacijskom imovinom čiji su vlasnici fizičke osobe na koje se podaci odnose (u daljnjem tekstu ispitanici). S ovim podacima mora se postupati s posebnom pažnjom, a koristiti se smiju isključivo u skladu s razlogom iz kojeg su prikupljeni.

Sva društva HEP grupe odgovorna su za uspostavu i održavanje adekvatnih organizacijskih, pravnih i tehničkih mjera za zaštitu osobnih podataka koji su im ustupljeni, bez obzira obrađuju li podatke samostalno ili ih na obradu ustupaju trećim stranama (izvršiteljima obrade).

PRIKUPLJANJE I OBRADA OSOBNIH PODATAKA

Prikupljanje osobnih podataka smije se provoditi isključivo u skladu sa zakonskim propisima i etičkim načelima. Dopušteno je obrađivati osobne podatke samo kad za to postoji jasno određena i dokumentirana zakonska osnova ili osnova temeljena na ugovornom odnosu, dok su sve ostale obrade osobnih podataka dopuštene jedino uz jasnu dokumentiranu privolu njihovog vlasnika ili njegovog opunomoćenika.

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

Prije prikupljanja osobnih podataka, vlasnicima se mora pružiti jasna informacija o razlogu i osnovi prikupljanja, vrsti obrade u kojoj će se informacije koristiti te eventualnim trećim osobama koje će informacijama pristupiti.

Ako se podaci prikupljaju od djece, odnosno maloljetnih osoba, neophodno je uspostaviti posebne mehanizme koji će osigurati da su oni dovoljne životne dobi 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.

PRAVA ISPITANIKA

Ispitanicima se mora omogućiti pravo na pristup informacijama o tome koje osobne informacije društva HEP grupe o njima posjeduju, temeljem koje pravne osnove su prikupljeni, za koje se svrhe koriste i koliko dugo će se čuvati.

Društva HEP grupe moraju ispitaniku omogućiti ispravak netočnih i dopunu nedostajućih osobnih podataka te mogućnost uskraćivanja prava na obradu njegovih osobnih podataka kada se predmetna obrada temelji na privoli ispitanika.

Na zahtjev ispitanika, osobne informacije koje su dane na temelju privole moraju se obrisati iz svih informacijskih sustava društava HEP grupe, kao i informacijskih sustava trećih strana kojima su društva HEP grupe omogućila pristup ovim podacima.

Ispitanik ima pravo na prenosivost svojih osobnih podataka. Na zahtjev, njegovi se osobni podaci moraju isporučiti u elektronskom obliku.

TEHNIČKA INTEGRIRANA ZAŠTITA OSOBNIH PODATAKA

Kod izgradnje informacijskih sustava i dizajna poslovnih procesa koji mogu utjecati na sigurnost osobnih podataka ili mogućnost ostvarivanja prava ispitanika, društva HEP grupe moraju provoditi procjenu učinka na sigurnost te osigurati primjerene zaštitne mjere.

Ako se procjenom ustanovi da zaštitne mjere koje društva HEP grupe mogu implementirati nisu dovoljne, o tome bez odlaganja mora biti obaviješten Službenik za zaštitu podataka HEP-a d.d. i Službenik za zaštitu podataka društva HEP grupe

na koje se procjena odnosi, a koji će pokrenuti postupak prethodnog savjetovanja s Agencijom za zaštitu osobnih podataka (u daljem tekstu „nadležno nadzorno tijelo“).

Svi novi procesi i informacijski sustavi u društvima HEP grupe moraju se dizajnirati tako da ispunjavaju sve zahtjeve ove Politike.

MINIMIZACIJA I ZAŠTITA OSOBNIH PODATAKA

Društva HEP grupe prikupljat će osobne podatke i pohranjivati ih isključivo u mjeri u kojoj je to potrebno za pružanje usluge. Prilikom pohrane podataka osobni podaci pohranjivat će se na najmanjem mogućem broju mjesta na kojima moraju biti adekvatno zaštićeni. Pristup osobnim podacima smije biti omogućen isključivo na temelju poslovne potrebe.

Zabranjeno je koristiti osobne podatke radi razvoja ili testiranja IT sustava. Gdje god je to moguće, osobni podaci moraju biti zaštićeni enkripcijom, pseudonimizacijom ili anonimizacijom.

UPRAVLJANJE INCIDENTIMA

Društva HEP grupe moraju uspostaviti i održavati procedure odgovora na incidente vezane uz narušavanje sigurnosti osobnih podataka unutar društva u njihovom vlasništvu, kao i kod trećih strana kojima su ustupile ili koje su njima ustupile osobne podatke.

Društva HEP grupe moraju uspostaviti i održavati strukturu odgovornosti za izvještavanje o incidentima vezanim uz sigurnost osobnih podataka na razini grupe. Društva HEP grupe moraju uspostaviti i održavati učinkovite mjere za detekciju neovlaštenog pristupa osobnim podacima i osigurati primjerenu razinu zaštite osobnih podataka od neovlaštenog pristupa, izmjene, uništenja te otkrivanja.

U slučaju narušavanja sigurnosti osobnih podataka, društva HEP grupe moraju bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvijestiti nadležno nadzorno tijelo. U slučaju narušavanja sigurnosti osobnih podataka koje bi moglo prouzročiti znatnu štetu ispitanicima, društva HEP grupe uložiti će razumne napore kako bi ih se o tome obavijestilo i time umanjilo nastalu štetu.

CERTIFIKACIJA

Upravljanje osobnim podacima, društva HEP grupe uspostaviti će i održavati sukladno primjenjivim standardima iz područja zaštite privatnosti i informacijske sigurnosti.

Gdje je to moguće, društva HEP grupe će upravljanje osobnim podacima i njihovom zaštitom integrirati sa postojećim sustavima upravljanja.

IZNIMKE

Iznimno, u vrlo ograničenom opsegu i uz postojanje opravdanog razloga, društva HEP grupe mogu odobriti privremeno postupanje s osobnim podacima koje nije u skladu s ovom Politikom. Prije donošenja takve odluke, Službenici za zaštitu podataka u tim društvima HEP grupe moraju biti obaviješteni i konzultirani. Službenici za zaštitu podataka društava HEP grupe informirat će Službenika za zaštitu podataka HEP-a d.d. i Upravu društva HEP grupe na koje se odnosi ako ocijene da bi zaštita osobnih podataka u društvu HEP grupe mogla utjecati na sigurnost zaštite osobnih podataka na razini grupe. Službenik za zaštitu podataka u HEP-u d.d. dužan je voditi evidenciju ovakvih odobrenja, odgovornosti i rokova za usklađivanje te o tome izvještavati Upravu HEP-a d.d. i Upravu društva HEP grupe koje je donijelo takvu odluku.

ODGOVORNOSTI UPRAVA DRUŠTAVA HEP GRUPE

Uprava HEP-a d.d., i Uprave svih društava HEP grupe koje svoje proizvode ili usluge prodaju fizičkim osobama ili u svom radu sustavno obrađuju osobne podatke kupaca – fizičkih osoba i drugih fizičkih osoba (radnika, vanjskih izvođača i dr.) dužne su imenovati Službenike za zaštitu podataka, u skladu s ovom Politikom i dokumentom „Prava i obveze službenika za zaštitu podataka u društvima HEP grupe“, koji dokument čini Prilog 1. i sastavni je dio ove Politike.

ODGOVORNOSTI RADNIKA I TREĆIH STRANA

Mjera zaštite osobnih podataka definiranih ovom Politikom moraju se pridržavati svi radnici društava HEP grupe, kao i treće strane koje ostvaruju pristup osobnim podacima povjerenim društvu HEP grupe.

ODGOVORNOSTI SLUŽBENIKA ZA ZAŠTITU PODATAKA U HEP-u d.d. I SLUŽBENIKA ZA ZAŠTITU PODATAKA U DRUŠTVIMA HEP GRUPE

Službenika za zaštitu podataka u HEP-u d.d. i Službenika za zaštitu podataka u društvima HEP grupe imenuje Uprava HEP-a d.d., odnosno Uprava društva HEP grupe kojoj je izravno odgovoran za svoj rad.

Službenik za zaštitu osobnih podataka odgovoran je za savjetovanje u uspostavi i održavanju sustavnog upravljanja osobnim podacima i njihovom sigurnošću na način usklađen s primjenjivom zakonskom regulativom, etičkim načelima i najboljim svjetskim praksama.

Službenik za zaštitu podataka odgovoran je posebno za:

- praćenje i tumačenje regulative iz područja privatnosti i zaštite osobnih podataka
- savjetovanje Uprave HEP-a d.d., odnosno Uprave društva HEP grupe u području usklađenosti i dobrih praksi u zaštiti osobnih podataka
- obavještanje i savjetovanje voditelja ili izvršitelja obrada te radnika koji obrađuju osobne podatke o njihovim obavezama iz Uredbe iz ostale zakonske regulative
- nadziranje poštivanja regulative i internih politika vezanih uz zaštitu osobnih podataka
- savjetovanje u uspostavi i održavanju evidencije obrada osobnih podataka

- savjetovanje u dodjeli odgovornosti za zaštitu osobnih podataka radnicima i trećim stranama uključenim u prikupljanje i obradu osobnih podataka
- podizanje svijesti i edukaciju iz područja zaštite osobnih podataka
- savjetovanje u ugrađivanju zaštite privatnosti u poslovne procese i informacijske sustave,
- savjetovanje u ugrađivanju zaštite privatnosti u revizijske procese
- savjetovanje kod provedbe procjena učinka na zaštitu osobnih podataka,
- suradnju s nadležnim nadzornim tijelom
- nadziranje učinkovitosti procesa upravljanja rizikom u obradama osobnih podataka
- izvještavanje Uprave o učinkovitosti sustava upravljanja osobnim podacima.

ODGOVORNOSTI SEKTORA ZA INFORMACIJSKO KOMUNIKACIJSKE TEHNOLOGIJE U HEP-u d.d.

Sektor za informacijsko komunikacijske tehnologije odgovoran je za operativnu uspostavu i održavanje tehničkih kontrola potrebnih za usklađivanje sa zahtjevima ove politike, a posebice mjera za:

- identifikaciju i zaštitu osobnih podataka
- mehanizama za ispunjavanje prava vlasnika osobnih podataka.

ODGOVORNOSTI UREDA ZA KORPORATIVNU SIGURNOST U HEP-u d.d.

Ured za korporativnu sigurnost zadužen je za nadzor primjene aktivnosti i mjera identifikacije i zaštite osobnih podataka i pružanje stručne potpore iz svog područja u upravljanju zaštitom osobnih podataka.

ODGOVORNOSTI SEKTORA ZA INTERNU REVIZIJU U HEP-u d.d.

Sektor za internu reviziju zadužen je za reviziju primjene i učinkovitosti ove politike, a posebice mjera i postupka za ispunjavanje prava ispitanika i upravljanje zaštitom osobnih podataka.

ODGOVORNOSTI ZA ODRŽAVANJE OVOG DOKUMENTA

Ova se politika revidira najmanje jednom godišnje ili nakon svake izmjene u pravnom okruženju ili okruženju rizika koja bi mogla imati učinak na njenu učinkovitost.

Za donošenje ove Politike i njene izmjene i dopune nadležna je Uprava HEP-a d.d. Za provedbu ove Politike zadužen je Službenik za zaštitu podataka u HEP-u d.d. odnosno Službenik za zaštitu podataka u društvima HEP grupe.

Ovaj akt stupa na snagu i primjenjuje se danom donošenja, a objavit će se u Biltenu Vjesnika HEP-a.

Sva društva u sastavu HEP grupe, obvezna su na odgovarajući način preuzeti i primjenjivati odredbe ove Politike.

U Zagrebu, dana 7. svibnja 2018. godine.

HEP d.d.

Predsjednik Uprave
Frane Barbarić, dipl. iur.
(v. r.)