P/233265

REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA: UP/I-034-01/25-01/11
URBROJ: 567-05-02/02-25-1
Zagreb, 13.6.2025.

Agencija za zaštitu osobnih podataka, OIB: 28454963989, na temelju članka 57. stavka 1. i 58. stavka 1. i 2. 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 te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Službeni list Europske unije L119/1, 4.5.2016.) i članaka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj: 42/2018; dalje u tekstu: Zakon o provedbi Opće uredbe o zaštiti podataka), postupajući po službenoj dužnosti protiv voditelja obrade društva HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, OIB: 15907062900, zastupano po Tomislavu Brnadiću, direktoru, OIB: 12671789249, donosi sljedeće

R J E Š E N J E

I. Utvrđuje se da je nepoduzimanjem odgovarajućih tehničkih i organizacijskih mjera zaštite kod obrade osobnih podataka u sklopu aplikacije „Moj račun“ od strane društva HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, kao voditelja obrade, protivno članku 32. stavku 1. i 2. Opće uredbe o zaštiti podataka, došlo do kršenja sigurnosti osobnih podataka ispitanika društva HEP-Toplinarstvo d.o.o. Miševečka ulica 15A, Zagreb.

II. Utvrđuje se da društvo HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, kao voditelj obrade nije surađivalo s nadzornim tijelom i nije mu omogućilo pristup svim informacijama koje su mu potrebne za obavljanje zadaća, uslijed čega je došlo do kršenja članka 31. u vezi s člankom 58. stavkom 1. točkom e) Opće uredbe o zaštiti podataka.

III. Uslijed utvrđenih povreda iz Opće uredbe o zaštiti podataka iz točke I. i II. izreke ovog rješenja, društvu HEP-Toplinarstvo d.o.o, Miševečka ulica 15A, Zagreb, izriče se upravna novčana kazna u iznosu od

320.000,00 eura (slovima: tristodvadesettisuća eura)

IV. Društvo HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, dužno je platiti izrečenu upravnu novčanu kaznu u korist državnog proračuna u roku od 15 dana od dana pravomoćnosti ovog rješenja u korist računa broj: **HR1210010051863000160, model HR64 i poziv na broj odobrenja 6092-25860-15907062900** s naznakom – "upravne novčane kazne koje izriče AZOP".

V. Ukoliko društvo HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija će sukladno članku 46. stavku 2. Zakona o provedbi Opće uredbe o zaštiti podataka obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području sjedište navedenog društva radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza.

VI. Društvo HEP-Toplinarstvo d.o.o., Miševečka ulica 15A, Zagreb, je dužno u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati na uvid ovoj Agenciji.

O b r a z l o ž e nj e

I. UTVRĐENJE POVREDE PRAVA NA ZAŠTITU OSOBNIH PODATAKA

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je dana 18. listopada 2024. predstavku ispitanika u kojoj je u bitnom navedeno kako je prilikom korištenja korisničkog portala društva HEP-Toplinarstvo d.o.o., sa sjedištem u Zagrebu, Miševečka ulica 15A (dalje u tekstu: Voditelj obrade) https://mojracun.hep.hr primijećen nesiguran način promjene zaboravljene lozinke, na način da je privremena lozinka zapravo zadnja lozinka koju je korisnik postavio i ista se prikazivala u jednostavnom (čistom odnosno neformatiranom) tekstu (prileži spisu predmeta). Agencija je dopisom od 28. listopada 2024. od podnositelja predstavke zatražila dopunu predstavke od 18. listopada 2024. i dostavu dodatnih informacija i dokaza kojima se potkrepljuju tvrdnje iz dostavljene predstavke te je podnositelj predstavke, postupajući po zahtjevu Agencije, traženu dopunu dostavio dopisom dana 28. listopada 2024. (prileži spisu predmeta).

Slijedom navedene predstavke i dostavljene dokumentacije, Agencija je na temelju ovlaštenja iz članka 58. Opće uredbe o zaštiti podataka i odredaba članka 36. i članka 37. Zakona o provedbi Opće uredbe o zaštiti podataka provela nenajavljeni nadzor dana 6. studenog 2025. u prostorijama društva HEP – Toplinarstvo d.o.o., o čemu je sastavljen Zapisnik o provedenom nadzoru KLASA: 009-01/24-01/14, URBROJ: 567-02/06-24-6 od 6. studenog 2024. (prileži spisu predmeta). Navedeno nadzorno postupanje provedeno je u prisutnosti predstavnika Voditelja obrade, i to: X, u svojstvu osobe ovlaštene za zastupanje i predstavnika Voditelja obrade, Direktor pogona posebne toplane, HEP-Toplinarstvo d.o.o.; X, u svojstvu službenika za zaštitu podataka Voditelja obrade: X, u svojstvu voditeljice Odjela za obračun i naplatu potraživanja kod Voditelja obrade; X u svojstvu službenika za zaštitu podataka društva HEP

d.d.; X, pomoćnika direktora, Sektor za informacijsko-komunikacijske tehnologije društva HEP d.d.

Na upit ovlaštenih službenika Agencije da li Voditelj obrade vodi evidenciju aktivnosti obrade osobnih podataka, a osobito u dijelu korištenja programskog rješenja „Moj račun“, X u bitnome je izjavio kako je u koordinaciji s kolegom X iz društva HEP d.d. te je naveo kako je društvo HEP d.d. nadležno za Voditelja obrade kao vodeći voditelj zaštite podataka za cijelu HEP grupu. Nadalje, izjavio je kako je nakon utvrđenja da je zaprimljen upit vezan za funkcionalnost aplikacije „Moj računa“ kontaktirao društvo HEP d.d. te kako nije nastala šteta za potrošača niti u jednom opsegu osobnih podataka.

Na upit ovlaštenih službenika Agencije zašto Agenciji nije prijavljen sigurnosni propust u smislu članka 33. Opće uredbe o zaštiti podataka u roku od 72 sata, X je izjavio kako predmetni incident nije u nadležnosti društva HEP-Toplinarstvo d.o.o., već je isti u nadležnosti posebne jedinice unutar HEP grupe. U vezi navedenog, X je izjavio kako je dana 6. studenog 2024. saznao za predmetni incident.

Na upit ovlaštenih službenika Agencije koji se set osobnih podataka koristi prilikom izrade korisničkog računa ispitanika (dalje u tekstu: ispitanika ili korisnika), X je u bitnom izjavio kako mu je poznato da u predmetnoj aplikaciji postoje podaci o krajnjem kupcu, OIB-u, mjernom mjestu, e-mail-u i adresi kupca. U vezi navedenog, X je dodatno izjavila kako je za registraciju računa korisnika potreban broj obračunskog mjernog mjesta, ime i prezime stranke i poziv na broj iz zadnja tri računa koji je potreban radi sigurnosti i provjere vlasnika mjernog mjesta i lozinku koju si korisnici sami zadaju. U vezi navedenog, X je priložila fotografiju zaslona koja sadrži set informacija potrebnih za registraciju računa (prileži spisu predmeta).

Na upit ovlaštenih službenika Agencije koje podatke korisnik može vidjeti prilikom korištenja aplikacije „Moj račun“, pristupilo se aplikaciji „Moj račun“ u svojstvu korisnika sustava te je izvršen uvid u osobne podatke korisnika koji su vidljivi korisniku aplikacije. Prilikom provođenja navedene radnje utvrđeno je kako aplikacija „Moj račun“ omogućuje uvid u sljedeća polja:

- „Moj račun“ – sadržava osobne podatke vlasnika računa i to: šifru korisnika, ime i prezime, adresu i adresu elektroničke pošte.
- „Krajnji kupac“ – sadržava osobne podatke vlasnika računa i to: šifru, naziv, adresu, OIB, adresu i grad SUC, oznaku krajnjeg kupca.
- „Računi“ – sadržava osobne podatke vlasnika računa i to: šifru korisnika, ime i prezime, adresu i adresu elektroničke pošte te sadržava zadnjih 12 izdanih (mjesečnih) računa i iznos računa te se isti mogu preuzeti u obliku pdf dokumenta, a ujedno se u ovom polju omogućuje i deaktivacija računa.
- „Zaduženja i uplate“ – sadržava osobne podatke vlasnika računa i to: šifru korisnika, ime i prezime, adresu i adresu elektroničke pošte te su ujedno vidljive informacije o uplatama i zaduženjima, odnosno datumu, datumu dospijeća zaduženja, broju računa te o opisu radi li se o računu ili uplati, a ujedno je vidljiv i računovodstveni prikaz duguje odnosno potražuje.

- „Izvješća“ – sadržava informacije o vlasniku računa i to: šifru korisnika, ime i prezime, adresu i adresu elektroničke pošte te podatke o energetskom certifikatu SUC-a i godišnje izvješće o poslovanju.

Ujedno je priložena fotografija s prikazom zaslona svakog od navedenih polja u kojem su vidljivi osobni podaci ispitanika (prileži spisu predmeta), ispis Izvješća o poslovanju kupca toplinske energije u 2023. (prileži spisu predmeta), prijepis obračuna toplinske energije za kategoriju krajnjih kupaca „KUĆANSTVO“ (prileži spisu predmeta).

Na upit ovlaštenih službenika Agencije u koje osobne podatke zaposlenici Voditelja obrade imaju uvid u aplikaciji „Moj račun“, X je izjavila kako zaposlenici Voditelja obrade imaju uvid u podatke o šifri kupca, OIB-u, nazivu krajnjeg kupca, adresu SUC-a, obračunskom mjernom mjestu, građevini, grupi, da li je račun aktivan te o e-mail adresi krajnjeg kupca. Ovlašteni službenici Agencije izvršili su uvid u poslovno računalo X te je izrađen ispis zaslona aplikacije „Moj račun“ namijenjen za zaposlenike Voditelja obrade (prileži spisu predmeta).

Na upit ovlaštenih službenika Agencije vezano za razdoblje implementacije aplikacije „Moj račun“ i razdoblje od kada je omogućeno korištenje iste korisnicima, X je priložila elektroničku poštu od 1. ožujka 2019. kao dokaz kada je aplikacija implementirana (prileži spisu predmeta) te je uz isto priložila interne informacije o aplikaciji od 1. ožujka 2019. (prileži spisu predmeta), ispis elektroničke pošte od 1. ožujka 2024. (prileži spisu predmeta) te dokument naziva „APLIKACIJA MOJ RAČUN“ od 1. ožujka 2019. (prileži spisu predmeta).

Na upit ovlaštenih službenika Agencije o implementiranim tehničkim mjerama, odnosno kojim je aktom uređeno funkcioniranje aplikacije, gdje je ista pohranjena te vezano za postojanje akta kojim se uređuje duljina lozinke potrebne za pristup krajnjeg korisnika korisničkom računu, X je izjavio kako ne postoji akt kojim bi postavljanje lozinke bilo uređeno i kako krajnji kupci ne moraju mijenjati lozinku kada je jednom postave, a duljina lozinka je postavljena za minimalno 6 znakova, ali nisu postavljena pravila u odnosu na vrstu slova, brojeve ili sl.

Na upit ovlaštenih službenika Agencije u vezi načina pohrane lozinke korisnika i jesu li iste kriptirane, X je izjavio kako se lozinke pohranjuju u „X“ bazu u čitljivom ne kriptiranom obliku. Potom je radi uvida ovlaštenih službenika Agencije u navedeno od strane predstavnika Voditelja obrade izvršen pristup administratorskom dijelu baze podataka u kojoj su pohranjeni podaci aplikacije „Moj račun“. X je ujedno izjavio kako je ime produkcijske baze …, verzija 11, a naziv tablice u predmetnoj bazi u kojoj su sadržani podaci o korisničkim imenima i lozinkama korisnika je „Korisnici“ te ista sadrži sljedeća polja: MAIL, STATUS, IME, PREZIME, PWD, ATIV_CODE, LAST_LOGIN, LAST_ADDRESS, KORISNIK_id. U vezi navedene nadzorne aktivnosti sačinjena je fotografija s prikazom navedenih podataka (prileži spisu predmeta).
Ovlašteni službenici Agencije su izvršili uvid u naprijed navedena polja i utvrdili kako polje „MAIL“ sadrži korisnička imena korisnika, dok polje „PWD“ sadrži lozinke korisnika spremljene u čitljivom nekriptiranom obliku.

Na upit ovlaštenih službenika Agencije o broju korisnika koji upisanu lozinku u polju „PWD“, X je izjavio kako oko 15.900 korisnika ima upisanu lozinku u polju „PWD“. Ovlašteni službenici Agencije su potom neposrednim uvidom i pristupom utvrdili kako baza podataka u polju „PWD“ sadrži upisane lozinke za 16.530 korisnika te je prilikom provođenja navedene radnje sačinjena fotografija zaslona s prikazom broja korisnika koji imaju upisan podatak u koloni polja „PWD“ (prileži spisu predmeta).

U vezi navedenog X je dodatno izjavio kako se radi o svim korisnicima koji su kreirali račun, a da od tog broja od 15.900 korisnika ima aktivirani korisnički račun u aplikaciji „Moj račun“. U prisutnosti ovlaštenih službenika Agencije utvrdilo se kako „SQL“ upit u bazu podataka rezultira brojem od 15.908 korisnika te je o provedenoj radnji sačinjena fotografija zaslona s prikazom broja korisnika koji imaju upisan status „aktivni“ (prileži spisu predmeta).

Na zahtjev ovlaštenih službenika Agencije izvršena je demonstracija funkcionalnosti aplikacije „Moj račun“ prilikom izmjene lozinke i predaje zahtjeva za izdavanje nove lozinke te je tom prilikom svaki korak zaslona zabilježen fotografijom zaslona računala na kojem je provedena predmetna radnja (fotografije zaslona prileže spisu predmeta). Prilikom provođenja navedene radnje, ovlašteni službenici Agencije su utvrdili sljedeće korake tijekom izmjene lozinke:

1. Iniciranje oporavka lozinke započinje unosom korisničkog imena i odabirom polja „Zaboravljena lozinka“.
2. Zaslon za iniciranje oporavka lozinke sadrži polje „Korisnik“ u kojemu se unosi elektronička pošta korisnika te polje „Promjena lozinka“ u kojem se unosi „Nova lozinka“ i polje „Ponovni unos“. Postavlja se nova lozinka kojom se željelo testirati funkcionalnost izmjene lozinke.
3. Uvidom u bazu podataka utvrđeno je da je nova lozinka upisana u bazu, odnosno u tablicu „Korisnici“ u polje „PWD“.
4. Iniciran je ponovni oporavak lozinke unosom korisničkog imena i odabirom polja „Zaboravljena lozinka“ te je utvrđeno kako se ista šalje na elektroničku poštu korisnika.
5. Utvrđeno je da je na elektroničku poštu korisnika kao privremena lozinka zaprimljena ista lozinka koja je upisana u bazi u polje „PWD“ za tog korisnika.

Na upit ovlaštenih službenika Agencije o tome zašto se kod promjene lozinke korisnika, nakon predaje zahtjeva u polju „Zaboravljena lozinka“ korisniku vraća postojeća lozinka kao privremena, X je izjavio kako je takav način promjene lozinke uspostavljen prilikom izrade idejnog rješenja aplikacije „Moj račun“ te da se od tada isti nije mijenjao.

Na upit ovlaštenih službenika Agencije u vezi broja korisnika koji imaju pristup administrativnom dijelu baze i je li isto propisano internim aktom, X je izjavio kako prava pristupa administrativnom dijelu baze podataka nisu propisana internim aktom, a da pristup navedenoj bazi trenutno imaju djelatnici razvojnog dijela web sučelja, određeni developeri koji rade na …, a pristup podacima ima vlasnik baze kroz DBA (eng. *Database Administrator*) te je ujedno izjavio kako administratora ima petero ili šestero, a da će točan podataka dostaviti naknadno.

Na upit ovlaštenih službenika Agencije o tome da li je Voditelj obrade zaprimio zahtjev ispitanika vezano za korištenje programskog rješenja „Moj račun“, X je izjavio kako je Voditelj obrade 19. listopada 2024. zaprimio obavijest X u kojem isti upozorava na sigurnosni propust web aplikacije „Moj račun“ te je ujedno izjavio kako je predmetnu obavijest proslijedio 4. studenog 2024. službeniku za zaštitu podataka društva HEP d.d., X putem elektroničke pošte (spisu predmeta prileži dio korespondencije od 4. studenog 2024. s email adrese: sluzbenikzazastitu.toplinarstvo@hep.hr na adresu elektroničke pošte X@hep.hr i odgovor s adrese elektroničke pošte naziva: Službenik za zaštitu podataka HEP d.d. na adresu elektroničke pošte naziva: Službenik za zaštitu osobnih podataka Toplinarstvo). X je ujedno izjavio kako su određeni zaposlenici društva HEP d.d. zaprimili predmetnu obavijest 31. listopada 2024. s adrese elektroničke pošte X (X@hep.hr) proslijeđene na adresu elektroničke pošte naziva: X (X@hep.hr), X (X@hep.hr); X (X@hep.hr) i X (X@hep.hr) te je dodatno izjavio kako je njemu obavijest dostavljena 4. studenog 2024. s adrese elektroničke pošte naziva: X (X@hep.hr) na adresu X (sve prileži spisu predmeta).

Na upit ovlaštenih službenika Agencije o mogućim dodatnim zahtjevima ispitanika vezanim za funkcioniranje aplikacije „Moj račun“, X je izjavio kako se ne sjeća da je došao upit ovakve vrste, ali da on ima samo pristup informacijama odnosnim na društvo HEP d.d., a nema informacije za društvo HEP-Toplinarstvo d.o.o.

Na upit ovlaštenih službenika Agencije o poduzetim radnjama nakon obavijesti korisnika, X je izjavio kako su promijenili proceduru promjene lozinke danas (6. studenog 2024.) ujutro te u prilog navedenom prilaže prijepis elektroničke pošte u kojoj X s adrese elektroničke pošte poslane na adrese elektroničke pošte naziva X Toplinarstvo, X, X, X, X, X, X, od 6. studenog 2024., dostavlja informaciju kako je završena prva faza dorade web aplikacije „Moj račun“ HEP Toplinarstva te kako su pripremljene promjene u aplikaciji „Moj račun“ (prileži spisu predmeta).

U svrhu zakonitog i pravilnog rješavanja ove upravne stvari, ovlašteni službenici Agencije su po provedenom nadzoru naložili Voditelju obrade da u roku od osam dana od dana zaprimanja zapisnika o provedenom nadzoru Agenciji dostavi:

- Evidenciju aktivnosti obrade osobnih podataka.
- Odluku o imenovanju službenika za zaštitu podataka od 17.11.2023., broj Odluke 1/2023.
- Interne akte kojima se uređuje funkcioniranje i način korištenja aplikacije „Moj račun“.
- Interni akt kojim se uređuje način kreiranja lozinke korisnika prilikom otvaranja korisničkog računa.
- Akt kojim je uređen način pristupa administratorskom dijelu baze te popis osoba ovlaštenih za pristup administratorskom dijelu baze s pripadajućim ovlastima (zajedno s dokazima koji potvrđuju navedeno).
- Očitovanje o drugim incidentima koji su prijavljeni vezano za uslugu „Moj račun“, ako su prijavljeni.
- Cjelokupnu korespondenciju elektroničkom poštom od 4. studenog 2024. s adrese elektroničke pošte naziva sluzbenikzazastitu.toplinarstvo@hep.hr na adresu elektroničke pošte X@hep.hr i odgovor a adrese elektroničke pošte naziva „Službenik za zaštitu

podataka HEP d.d.“ na adresu elektroničke pošte naziva „Službenik za zaštitu osobnih podataka Toplinarstvo“.

Postupajući u skladu s naprijed navedenim zahtjevom Agencije, Voditelj obrade je dopisom od dana 10. prosinca 2024. dostavio Agenciji sljedeću dokumentaciju:

- Evidencija aktivnosti obrade osobnih podataka (prileži spisu predmeta)
- Tehničke i organizacijske mjere (prileži spisu predmeta)
- Odluka o imenovanju službenika za zaštitu podataka od 17.11.2023., broj Odluke 1/2023 (prileži spisu predmeta)
- Pravilnik o korištenju informacijskog sustava/Pravilnik o korištenju interneta (Bilten br. 187) (prileži spisu predmeta)
- Očitovanje Voditelja obrade od 10. prosinca 2024. na upit Agencije o postupanju vezano za prijavu incidenta/potencijalne povrede (prileži spisu predmeta)
- Cjelokupna korespondencija elektroničkom poštom od 4. studenog s adrese elektroničke pošte naziva sluzbenikzazastitu.toplinarstvo@hep.hr, na adresu elektroničke pošte X@hep.hr i odgovor a adrese elektroničke pošte naziva „Službenik za zaštitu podataka HEP d.d.“ na adresu elektroničke pošte naziva „Službenik za zaštitu osobnih podataka Toplinarstvo“ uključivo uz korespodenciju vidljivu unutar predmete a razmijenjene između korisnika adrese e-pošte X@gmail.com i toplinarstvo @hep.hr od 18. i 31.10.2024. (prileži spisu predmeta)
- Uvjeti korištenja WEB aplikacije „Moj račun“ (prileži spisu predmeta)
- Dopis društva HEP d.d. upućen Voditelju obrade (br. 08-5328/24) od 9. prosinca 2024. vezano uz administratorske ovlasti za aplikaciju „Moj račun“ (prileži spisu predmeta).

U dostavljenom očitovanju Voditelja obrade od 10. prosinca 2024. na upit Agencije o postupanju vezano za prijavu incidenta/potencijalne prijetnje, Voditelj obrade je u navedenom podnesku u bitnom naveo kako su nadzorne aktivnosti Agencije započele 6. studenog 2024., a službenici za zaštitu podataka su bili upoznati s predmetnom situacijom dana 4. studenog 2024., a iz čega je razvidno kako je rok za prijavu od 72 sata od saznanja službenika bio još u tijeku, a Agencija je već pokrenula nadzorne aktivnosti. S tim u vezi, Voditelj obrade je naveo kako službenici za zaštitu podataka nisu imali saznanja o predmetnoj prijavi korisnika sve do 4. studenog 2024. Kako je postupanje Agencije započelo unutar roka od 72 sata od saznanja službenika, Voditelj obrade je naveo kako je već konzumiran bio rok od strane Agencije za prijavu jer su nadzorne aktivnosti već bile pokrenute uživo, osobnim prisustvom u službenim prostorijama Voditelja obrade te su slijedom navedenog službenik za zaštitu podataka Voditelja obrade i službenik za zaštitu podataka društva HEP d.d. smatrali kako zbog početka nadzornih aktivnosti od strane Agencije nije postojala potreba daljnje prijave incidenta/potencijalne povrede s njihove strane kao niti za obavještavanjem Agencije pisanim putem.
U svrhu zakonitog i pravilnog rješavanja ove upravne stvari, Agencija je zahtjevom od 6. svibnja 2025. (prileži spisu predmeta) koji je Voditelju obrade dostavljen putem elektroničke pošte 6. svibnja 2025. zatražila od Voditelja obrade dostavu dopune očitovanja u roku od tri dana od dana primitka navedenog dopisa, na način da dostavi Agenciji sljedeću dokumentaciju:

- Relevantne dokaze u vidu nabavne dokumentacije web aplikacije „Moj račun“ posebice preslike dokumentacije društva HEP d.d. kojom su definirane tehničke specifikacije

tražene aplikacije te dokumentacije kojom su definirane sigurnosne specifikacije aplikacije.
- Cjelokupnu dokumentaciju idejnog i izvedbenog projektnog rješenja dobavljača web aplikacije „Moj račun“.
- Cjelokupnu relevantnu korespondenciju između društva HEP d.d. i dobavljača web aplikacije „Moj račun“ kojom su se definirali sigurnosni aspekti pohrane lozinki korisničkih računa u bazi podataka.
- Cjelokupnu internu i vanjsku (od i prema dobavljaču web aplikacije „Moj račun“) relevantnu korespondenciju kojom se je definirala procedura promjene korisničke lozinke, posebice sigurnosnih aspekata iste.
- Popis svih sigurnosnih incidenata od 25 svibnja 2018. do danas, u skladu s člankom 33. Opće uredbe o zaštiti podataka.

Postupajući u skladu s naprijed navedenim zahtjevom Agencije od 6, svibnja 2025., Voditelj obrade je dana 13. svibnja 2025. putem elektroničke pošte dostavio Agenciji sljedeću dokumentaciju: Dopuna očitovanja Sektora za informacijsko-komunikacijske tehnologije HEP-d.d.-a - 8/2252/25KA od 9. svibnja 2025. (prileži spisu predmeta); Odgovor krajnjem kupcu g. X od službenika za zaštitu podataka Voditelja obrade od 16. prosinca 2024. (prileži spisu predmeta); Odgovor krajnjem kupcu g. X od Voditelja obrade od 31. prosinca 2024. (prileži spisu predmeta).

U podnesku od 9. svibnja 2025. - Dopuna očitovanja Sektora za informacijsko-komunikacijske tehnologije HEP-d.d.-a - 8/2252/25KA, Voditelj obrade u bitnom navodi kako su sukladno važećem „Pravilniku o organizaciji i sistematizaciji HEP-a d.d.“ odnosno Ugovorima o međusobnim odnosima između HEP-a d.d. i ovisnih društava (npr. HEP – Toplinarstvo d.o.o.) definirane obveze i odgovornosti vezane uz izgradnju i upravljanje zajedničkim informacijskim sustavom HEP-a. Ovim dokumentima definirana je obveza Sektora za informacijsko-komunikacijske tehnologije HEP-a d.d. (dalje u tekstu: SIT) da u suradnji s ovisnim društvima izgrađuje i daje na korištenje zajednički informaciji sustav HEP-a s ciljem osiguravanja aplikativne podrške provođenju poslovnih procesa ovisnih društava. Nadalje, navodi kako je aplikacija „Moj Račun – HEP Toplinarstva“ razvijena vlastitim snagama, bez angažmana vanjskih dobavljača IT usluga. Uobičajeni postupak razvoja ovakvih aplikativnih rješenja je visoko iterativan uz intenzivnu suradnju IT stručnjaka i poslovnih korisnika, gdje se kroz niz internih radionica definiraju stvarne poslovne potrebe i testiraju predložena tehnička rješenja, a nakon završetka razvojnog procesa i prihvaćanja završnog testa, aplikativno rješenje ulazi u produkcijsko korištenje u kojem SIT osigurava infrastrukturu i tehničku podršku za neometano korištenje i po potrebi i na zahtjev korisnika neophodne prilagodbe i nadogradnje. Nadalje, Voditelj obrade navodi kako s obzirom na ovakav način rada, u slučaju aplikacije „Moj račun – HEP Toplinarstva“ nije provođen postupak nabave web aplikacije niti su korištene usluge vanjskih dobavljača web aplikacija pa stoga nije u mogućnosti dostaviti tražene dokumente i korespondenciju.

Nastavno na navedeno, ističe se kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, u području zaštite osobnih podataka izravno i

obvezujuće primjenjuje Opća uredba o zaštiti podataka, a odgovornost za praćenje primjene i provedbe Opće uredbe o zaštiti podataka na području Republike Hrvatske je u nadležnosti Agencije za zaštitu osobnih podataka.

Članak 2. Opće uredbe o zaštiti podataka propisuje kako se ista primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

Opća uredba o zaštiti podataka u članku 4. stavku 1. točki 1. propisuje da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a 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.

Sukladno članku 4. stavku 1. točki 2. Opće uredbe o zaštiti podatka, obrada znači 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.

Sukladno članku 4. stavku 1. točki 7. Opće uredbe o zaštiti podataka, voditelj obrade znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.

Sukladno članku 5. stavku 1. Opće uredbe o zaštiti podataka osobni podaci moraju biti: a) zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); b) prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama (načelo ograničavanja svrhe); c) primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koju se obrađuju (načelo smanjenje količine podataka); d) točni i prema potrebi ažurni (načelo točnosti); e) čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju (načelo ograničenja pohrane); f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Sukladno članku 31. Opće uredbe o zaštiti podataka, voditelj obrade i izvršitelj obrade te, ako je to primjenjivo, njihovi predstavnici, na zahtjev surađuju s nadzornim tijelom u ispunjavanju njegovih zadaća.

Sukladno članku 58. stavku 1. točki e) Opće uredbe o zaštiti podataka, svako nadzorno tijelo ima istražne ovlasti, među kojima je i ovlast ishoditi, od voditelja obrade i izvršitelja obrade, pristup svim osobnim podacima i svim informacijama potrebnim za obavljanje svojih zadaća.

Sukladno članku 32. stavku 1. Opće uredbe o zaštiti podataka, uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

a) pseudonimizaciju i enkripciju osobnih podataka;
b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Sukladno članku 32. stavku 2. Opće uredbe o zaštiti podataka, prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

U ovoj upravnoj stvari je kao nesporna činjenica utvrđeno kako je Voditelj obrade obrađivao osobne podatke korisnika svojih usluga putem korisničkog portala aplikacije „Moj račun“ dostupnog na poveznici internet stranice: https://mojracun.hep.hr

U ovoj upravnoj stvari je utvrđeno kako se prilikom korištenja aplikacije „Moj račun“, u postupku izmjene korisničke lozinke, odnosno prilikom podnošenja zahtjeva za izdavanje nove lozinke putem opcije „Zaboravljena lozinka“, korisniku putem elektroničke poste dostavljala privremena lozinka koja je identična lozinki spremljenoj u bazi podataka u polju „PWD“ za tog korisnika, a koja se vodi kod Voditelja obrade. Navedeno je utvrđeno tijekom neposrednog nadzora koji je 6. studenog 2024. proveden u prostorijama Voditelja obrade od strane ovlaštenih službenika Agencije.

U ovoj upravnoj stvari je utvrđeno je kako je predmetni postupak promjene lozinke implementiran već prilikom izrade idejnog rješenja aplikacije „Moj račun“ te do dana provođenja nadzora (6. studenog 2024.) nije bio mijenjan. Ovu okolnost je svojim iskazom potvrdio X, kako je sadržano u Zapisniku o provedenom nadzoru od 6. studenog 2024.

Na temelju utvrđenih činjenica u ovoj upravnoj stvari, jasno je kako Voditelj obrade nije osigurao odgovarajuću razinu sigurnosti osobnih podataka korisnika aplikacije „Moj račun“, sukladno članku 32. stavcima 1. i 2. Opće uredbe o zaštiti podataka.
Prvenstveno, način izmjene korisničke lozinke u kojem se ista lozinka koja je prethodno pohranjena u bazi podataka Voditelja obrade (u polju „PWD“) šalje korisniku putem elektroničke pošte kao „privremena lozinka“, predstavlja ozbiljan sigurnosni propust i rizik za neovlašteno otkrivanje i zlouporabu osobnih podataka korisnika aplikacije „Moj račun“. Ovako uspostavljeni mehanizam promjene lozinke ne uključuje osnovne sigurnosne mjere, kao što su primjerice generiranje jednokratne privremene lozinke, čime se povećava rizik neovlaštenog pristupa osobnim podacima korisnika.

S obzirom da su lozinke korisnika pohranjene u bazi podataka Voditelja obrade u čitljivom obliku te se bez dodatne zaštite prilikom postupka izmjene lozinke bez poduzimanja mjera zaštite osobnih podataka šalju elektroničkom poštom, time se osobni podaci korisnika aplikacije „Moj račun“ izlažu riziku neovlaštenog otkrivanja i zlouporabe, a što sve prema članku 32. stavku 2. Opće uredbe o zaštiti podataka predstavlja jedan od ključnih sigurnosnih rizika koje je Voditelj obrade bio dužan prethodno procijeniti i suzbiti poduzimanjem odgovarajućih mjera sigurnosti osobnih podataka.

S obzirom na prirodu obrade osobnih podataka koji uključuju osobne podatke velikog broja korisnika koji se obrađuju putem internetske aplikacije, svrhu obrade te rizike po prava i slobode ispitanika, a koji uključuju rizik od neovlaštenog pristupa korisničkim računima i podacima, jasno je da su tehničke i organizacijske mjere zaštite koje je Voditelj obrade poduzeo bile neadekvatne i nesrazmjerne s obzirom na obveze iz Opće uredbe o zaštiti podataka.

Temeljem izjave X tijekom provođenja izravnog nadzornog postupanja (str. 3. Zapisnika o provedenom nadzoru od 6. studenog 2024.), u ovoj upravnoj stvari utvrđeno je kako Voditelj obrade nije pisanim aktom uredio postavljanje lozinke krajnjih korisnika, kao niti akt kojim bi se propisala obveza redovite promjene lozinke. Nadalje, Voditelj obrade je uredio minimalnu duljinu lozinke (6 znakova), ali nije definirao pravila o sadržaju lozinke (poput primjerice obveznog korištenja velikih i malih slova ili posebnih znakova i sl..). Voditelj obrade je u prilogu podneska od 10. prosinca 2024. dostavio Agenciji dokument „Uvjeti korištenja web aplikacije „Moj račun““ , ažurirano: prosinac 2024. (prileži spisu predmeta) te je čitanjem istoga utvrđeno kako je Voditelj obrade naknadno (nakon provedenog nadzora od strane Agencije 6. studenog 2024.) donio pisani akt kojim je uređeno postavljanje lozinke krajnjih korisnika i sadržaj predmetnih lozinki.

Slijedom navedenoga, utvrđeno je da je Voditelj obrade povrijedio članak 32. stavke 1. i 2. Opće uredbe o zaštiti podataka jer nije osigurao odgovarajuću razinu sigurnosti osobnih podataka korisnika aplikacije „Moja račun“.

U cilju zakonitog i pravilnog rješavanja ove upravne stvari, Agencija je zatražila od Voditelja obrade dopisom od 6. svibnja 2025. koji je istome upućen putem elektroničke pošte dostavu dopune očitovanja i dostavu dokumentacije. Voditelj obrade nije postupio po navedenom zahtjevu Agencije, a slijedom čega nije nadzornom tijelu omogućio pristup svim informacijama potrebnim za obavljanje njegovih zadaća u okviru njegovih istražnih ovlasti sukladno članku 58. stavku 1. točki e) Opće uredbe o zaštiti podataka. Ovakvo postupanje Voditelja obrade predstavlja nesuradnju istoga s Agencijom kao nadzornim tijelom, a što je protivno članku 31. Opće uredbe o zaštiti podataka.

Voditelj obrade nije na traženje agencije dostavio traženu dokumentaciju, uključujući i dokumentaciju kojom su definirane tehničke specifikacije aplikacije „Moj račun“ te dokumentaciju kojom su definirane sigurnosne specifikacije aplikacije. Voditelj obrade je u svom očitovanju u podnesku od 9. svibnja 2025. (prileži spisu predmeta) naveo kako prilikom

izrade aplikacije nisu angažirani vanjski izvođači te da zbog navedenoga nije u mogućnosti dostaviti traženu dokumentaciju. Agencija smatra kako je Voditelj obrade, neovisno o činjenici što prilikom izrade aplikacije nisu angažirani vanjski izvođači, bio u mogućnosti, a samim time i u obvezi dostaviti Agenciji informacije o tehničkim specifikacijama aplikacije, kao i očitovanje u pogledu definiranim sigurnosnim specifikacijama predmetne aplikacije. Također, Voditelj obrade nije dostavio dokumentaciju niti očitovanje vezano za traženje Agencije u pogledu dostave popisa sigurnosnih incidenata od 25. svibnja 2018. pa do danas, u skladu s člankom 33. Opće uredbe o zaštiti podataka, a što upućuje na nesuradnju, a time i povredu članka 31. Opće uredbe o zaštiti podataka.

II. UTVRĐENJE UPRAVNE NOVČANE KAZNE

Člankom 44. Zakona o provedbi Opće uredbe o zaštiti podataka je propisano da Agencija izriče upravne novčane kazne za povrede odredaba ovoga Zakona i Opće uredbe o zaštiti podataka, sukladno članku 83. Opće uredbe o zaštiti podataka.

Člankom 45. stavkom 1. navedenog Zakona je propisano da se upravne novčane kazne izriču odlukom. Temeljem stavka 2. istoga članka, odlukom će se utvrditi iznos i način uplate upravne novčane kazne. Odlukom se može utvrditi da se upravna novčana kazna plaća u obrocima. Temeljem stavka 4. istoga članka, protiv odluke nije dopuštena žalba, ali se može pokrenuti upravni spor pred nadležnim upravnim sudom.

Temeljem članka 46. istoga Zakona, upravna novčana kazna uplaćuje se u roku od 15 dana od dana pravomoćnosti odluke kojom je izrečena. Ako stranka u propisanom roku ne uplati upravnu novčanu kaznu odnosno po dospijeću zadnjeg obroka ako je odobreno obročno plaćanje, Agencija će obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području prebivalište odnosno sjedište stranke kojoj je izrečena upravna novčana kazna, radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza. Upravne novčane kazne uplaćuju se u korist državnog proračuna. Iznimno od stavka 2. ovoga članka, na dospjelu, a neplaćenu upravnu novčanu kaznu ne obračunava se kamata.

S obzirom na utvrđene okolnosti u konkretnom slučaju Agencija je sukladno svojim ovlastima iz članka 58. stavka 2. točke (i) Opće uredbe o zaštiti podataka izrekla upravnu novčanu kaznu umjesto drugih korektivnih mjera iz predmetnog članka, a sve u skladu s uvjetima za njezino izricanje iz članka 83. Opće uredbe o zaštiti podataka i članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka. Nakon detaljnog razmatranja raspoloživih korektivnih mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, a koje nadzorno tijelo ima ovlasti izreći voditelju obrade, u slučaju kršenja odredbi Opće uredbe o zaštiti podataka, te cijeneći sve okolnosti predmetnog slučaja, a posebno da odabrana korektivna mjera mora biti učinkovita, proporcionalna i odvraćajuća u svakom pojedinom slučaju, Agencija je odlučila izreći upravnu novčanu kaznu posvećujući dužnu pozornost kriterijima propisanim člankom 83. stavkom 2. Opće uredbe o zaštiti podataka.

Naime, člankom 83. stavkom 1. Opće uredbe o zaštiti podataka propisano je da svako nadzorno tijelo osigurava da je izricanje upravnih novčanih kazni u skladu s ovim člankom u pogledu kršenja ove Uredbe iz stavaka 4., 5. i 6. u svakom pojedinačnom slučaju učinkovito, proporcionalno i odvraćajuće.

Agencija smatra da iznos izrečene upravne novčane kazne može biti učinkovit jedino ako ima stvaran i značajan financijski utjecaj na prihode voditelja obrade. Načelo proporcionalnosti ne može se primjenjivati u apstrakciji, odnosno bez uzimanja u obzir konkretnih okolnosti i stvarnog učinka kazne na voditelja obrade. Kazna mora služiti svojoj svrsi, ne samo kao sankcija za počinjenu povredu, već i kao sredstvo odvraćanja od budućih nezakonitih postupanja. Slijedom navedenog, upravna novčana kazna ne može biti učinkovita niti odvraćajuća ako ne ostavlja mjerljiv financijski trag na poslovanje voditelja obrade.

Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog voditelja obrade tako i od svih drugih voditelja/izvršitelja obrade koji obrađuju osobne podatke u usporedivim situacijama putem sustava videonadzora. Svrha takve sankcije je postići opće odvraćanje (obeshrabriti druge od ponavljanja sličnih povreda u budućnosti), kao i posebno odvraćanje (spriječiti samog adresata ove odluke da ponovno povrijedi propise o zaštiti osobnih podataka).

Sukladno uvodnoj izjavi 10. Opće uredbe o zaštiti podataka, kako bi se osigurala postojana i visoka razina zaštite pojedinaca te uklonile prepreke protoku osobnih podataka unutar Unije, razina zaštite trebala bi biti jednaka u svim državama članicama. Sukladno uvodnoj izjavi 11. Opće uredbe o zaštiti podataka, djelotvorna zaštita osobnih podataka širom Unije zahtijeva jačanje i detaljno određivanje prava ispitanika i obveza onih koji obrađuju i određuju obradu osobnih podataka, kao i jednake ovlasti praćenja i osiguravanja poštivanja pravila za zaštitu osobnih podataka i jednake sankcije za kršenja u državama članicama. Sukladno uvodnoj izjavi 13. Opće uredbe o zaštiti podataka, jednake sankcije u svim državama članicama te učinkovita suradnja među nadzornim tijelima različitih država članica potrebni su da bi se "spriječila razilaženja koja ometaju slobodno kretanje osobnih podataka na unutarnjem tržištu".

Temeljem članka 83. stavka 2. Opće uredbe o zaštiti podataka, upravne novčane kazne izriču se uz mjere ili umjesto mjera iz članka 58. stavka 2. točaka od (a) do (h) i članka 58. stavka 2. točke (j), ovisno o okolnostima svakog pojedinog slučaja. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna se pozornost posvećuje sljedećem:
(a) prirodi, težini i trajanju kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli;
(b) ima li kršenje obilježje namjere ili nepažnje;
(c) svakoj radnji koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici;
(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32.;
(e) svim relevantnim prijašnjim kršenjima voditelja obrade ili izvršitelja obrade;

(f) stupnju suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja;
(g) kategorijama osobnih podataka na koje kršenje utječe;
(h) načinu na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju;
(i) ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera;
(j) poštovanju odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42.; i
(k) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

U članku 83. stavku 4. Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člancima 31. i 32. Opće uredbe o zaštiti podataka mogu izreći upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Uvodnom izjavom 150. Opće uredbe o zaštiti podataka navodi se da u slučaju kada se upravne novčane kazne izriču poduzetniku, poduzetnik bi se u te svrhe trebao tumačiti u skladu s člankom 101. i 102. Ugovora o funkcioniranju Europske unije.

Sukladno Smjernicama Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017. godine (WP 253), a koje je Europski odbor za zaštitu podataka podržao na svojoj prvoj plenarnoj sjednici 25. svibnja 2018. godine, kako bi nadzorno tijelo izreklo novčanu kaznu koja je učinkovita, proporcionalna i odvraćajuća, ono primjenjuje definiciju pojma poduzetnika kako ju je naveo Sud Europske unije za potrebe primjene članaka 101. i 102. UFEU-a, to jest smatra se da koncept poduzetnika znači gospodarsku jedinicu koju mogu osnovati matično društvo i sva uključena društva kćeri. U skladu s pravom EU-a i sudskom praksom, pojam poduzetnika treba shvatiti kao gospodarsku jedinicu koja se bavi komercijalnim/gospodarskim djelatnostima bez obzira na uključenu pravnu osobu.

U navedenim Smjernicama navode se i definicije pojma "poduzetnik" iz odluka Suda Europske Unije: Pojam "poduzetnik" obuhvaća svaki subjekt "koji obavlja gospodarsku djelatnost, neovisno o pravnom statusu tog subjekta i načinu njegova financiranja". Pojam poduzetnika "mora se smatrati izrazom kojim se označava gospodarska jedinica čak i ako se u pravu ta gospodarska jedinica sastoji od nekoliko osoba, bilo fizičkih ili pravnih.".

Uvidom u sudski registar Trgovačkog suda u Zagrebu Agencija je utvrdila da je osnivač i jedini član Voditelja obrade – društva HEP-Toplinarstvo d.o.o. društvo Hrvatska elektroprivreda d.d. (MBS: 080004306, OIB: 28921978587). U ovoj upravnoj stvari ujedno je utvrđeno kako društvo HEP d.d. utječe na donošenje odluka u pogledu obrade osobnih podataka putem

aplikacije „Moj račun“, odnosno ima stvarni utjecaj na donošenje odluka o obradi osobnih podataka kod Voditelja obrade, a što je utvrđeno temeljem izjave X (str. 2. Zapisnika o provedenom nadzoru od 6. studenog 2025. – prileži spisu predmeta) koji je tijekom provođenja neposrednog nadzora kod Voditelja obrade izjavio kako je u pogledu programskog rješenja aplikacije „Moj račun“ nadležno društvo HEP d.d., budući da je predmetno društvo nadležno za cijelu HEP grupu te kako predmetni incident u pogledu obrade osobnih podataka putem aplikacije „Moj račun“ nije u nadležnosti Voditelja obrade već je isti u nadležnosti posebne jedinice unutar HEP grupe.

Sukladno praksi suda Europske unije (presuda od 13. veljače 2025., Anklagemyndigheden protiv ILVA A/S, C- 383/23, ECLI:EU:C:2024:752), članak 83. stavke 4.,5. i 6. Opće uredbe o zaštiti podataka, u vezi s uvodnom izjavom 150. Opće uredbe o zaštiti podataka, treba tumačiti na način da pojam „poduzetnik“ iz tih odredbi odgovara pojmu „poduzetnik“ u smislu članaka 101. i 102. Ugovora o funkcioniranju Europske, tako da se, kada se novčana kazna zbog kršenja Opće uredbe o zaštiti podataka izriče voditelju obrade osobnih podataka koji je poduzetnik ili dio poduzetnika, najveći iznos novčane kazne određuje na temelju postotka poduzetnikova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.

Stoga se u obzir uzima ukupni godišnji promet na svjetskoj razini poduzetnika čiji je voditelj obrade dio, odnosno uzima se u obzir ukupni godišnji promet grupe čiji je poduzetnik dio.

Čitanjem financijskog izvješća za 2024. društva Hrvatska elektroprivreda d.d. koje prileži spisu predmeta ukupni godišnji promet na svjetskoj razini za grupu HEP za 2023. (podaci dostupni u dokumentu „HRVATSKA ELEKTROPRIVREDA d.d. – Godišnji konsolidirani financijski izvještaji i Izvješća neovisnih revizora za 2023.“ –putem poveznice internet stranice: https://www.hep.hr/UserDocsImages//dokumenti/fin-izvj/konsolidirana/2023//HEP_grupa_revizorsko_2023_konsolidirano.pdf; prileži spisu predmeta) iznosi 4.636.776.000,00 eura. Obzirom na navedeno, utvrđeno je kako je 2% od tog iznosa 92.735.520,00 eura te budući da isti iznosi više od 20.000.000,00 eura, gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju predstavlja iznos od 92.735.520,00 eura.

Agencija je radi kršenja članka 31. u vezi s člankom 58. stavkom 1. toč. e) Opće uredbe o zaštiti podataka, članaka 32. stavaka 1. i 2. Opće uredbe o zaštiti podataka, izrekla Voditelju obrade upravnu novčanu kaznu u iznosu od 320.000,00 eura, a koji iznos čini 0,34% u odnosu na maksimalni iznos upravne novčane kazne koju je u konkretnom slučaju Agencija mogla, odnosno bila ovlaštena izreći.

Na temelju odredbe članka 83. stavka 2. Opće uredbe o zaštiti podataka, pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne, Agencija je u ovom slučaju dužnu pozornost posvetila sljedećem:

- Priroda, težina i trajanje kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli (članak 83. stavak 2, točka a);

U ovoj upravnoj stvari, kako je utvrđeno u točki I. izreke ovog rješenja, došlo je do povrede obveze iz članka 32. Opće uredbe o zaštiti podataka u pogledu sigurnosti osobnih podataka, budući da voditelj obrade nije poduzeo odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti s obzirom na rizik obrade osobnih podataka, a sve u odnosu na osobne podatke korisnika aplikacije „Moj račun“.

U ovoj upravnoj stvari, kako je utvrđeno u točki II. Izreke ovog rješenja, također je došlo do povrede obveze iz članka 31. u vezi s člankom 58. stavkom 1. točkom e) Opće uredbe o zaštiti podataka, budući da Voditelj obrade nije surađivao s Agencijom tijekom provođenja istražnih ovlasti Agencije, a sve jer nije Agenciji omogućio pristup svim informacijama potrebnim za obavljanje zadaće Agencije kao nadzornog tijela za zaštitu osobnih podataka.

Sukladno Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679, pokazatelj težine kršenja može biti ne samo priroda kršenja, već i opseg, svrha predmetne obrade kao i broj ispitanika i razina štete koju su pretrpjeli.

U pogledu trajanja povrede uzet je datum 1. ožujka 2019. kao početak trajanja povrede, kada se počela koristiti aplikacija „Moj račun“, a što je utvrđeno čitanjem e-mail korespondencije naslova „Obavijest o početku primjene aplikacije MOJ RAČUN HEP-TOPLINARSTVA“ od 1. ožujka 2019. pošiljatelja X. Kao datum prestanka povrede Agencija nije uzela u obzir datum 6. studenog 2024. i dostavljenu e-mail korespondenciju (e-mail upućen od strane pošiljatelja X u 9:12 sati primateljima X Toplinarstvo, X, X, X, X, X, X; prileži spisu predmeta) u kojoj se navodi kako je navedenog datuma promijenjena procedura izmjene lozinke. Naime, 6. studenog 2024. u 9:00 sati započelo je nenajavljeno izravno nadzorno postupanje Agencije koje je završeno u 13:00 sati, a tijekom kojega su ovlašteni službenici Agencije prilikom demonstracije funkcionalnosti aplikacije „Moj račun“ prilikom izmjene lozinke korisnika i predaje zahtjeva za izdavanjem nove lozinke, utvrdili kako se na elektroničku poštu korisnika kao privremena lozinka i dalje zaprima ista lozinka koja je upisana u bazi u polje „PWD“ za tog korisnika. Voditelj obrade nije naknadno Agenciji dostavio dokaz o izmjeni funkcionalnosti aplikacije. Slijedom navedenog, za potrebe određivanja trajanja povrede glede naprijed opisanog postupanja uzima se razdoblje od 1. ožujka 2019. do dana donošenja ovog rješenja, što čini vremenski okvir od više od šest godina.

U odnosu na povredu odnosnu na nepoduzimanje mjera sigurnosti glede donošenja pisanog akta kojim je uređeno postupanje korisnika u pogledu izmjene lozinke i njenog sadržaja, utvrđeno je kako Voditelj obrade od 1. ožujka 2019. pa sve do prosinca 2024. nije donio predmetni akt niti je uredio proceduru izmjene lozinke od strane krajnjih korisnika, stoga je u pogledu navedenog kao trajanje povrede uzeto razdoblje od 1. ožujka 2019. pa do prosinca 2024., što čini vremenski period od više od pet godina.

Prilikom utvrđenja težine povrede u obzir je uzet broj ispitanika čiji su se osobni podaci obrađivali putem aplikacije „Moj račun“ i čiji su osobni podaci bili pohranjeni u običnom ili čistom tekstu unutar iste, a koji iznosi 15.908 osoba (ispitanika), a što je utvrđeno od strane

ovlaštenih službenika Agencije tijekom provođenja izravnog nadzornog postupanja (str. 4. Zapisnika o provedenom nadzoru od 6. studenog 2025. – prileži spisu predmeta; fotografije zaslona računala s prikazima radnji u aplikaciji „Moj račun“ sačinjene prilikom provođenja izravnog nadzora – prileže spisu predmeta).

U ovoj upravnoj stvari nije utvrđen nastanak konkretne materijalne ili nematerijalne štete za ispitanike uslijed predmetne povrede, no s obzirom na prirodu povrede i broj pogođenih osoba, rizik za prava i slobode ispitanike je u ovoj upravnoj stvari ocijenjen kao značajan.

- Ima li kršenje obilježje namjere ili nepažnje (članak 83. stavak 2, točka b);

Radna skupina iz članka 29 navodi u Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 da “namjera” u pravilu uključuje znanje i nakanu u pogledu značajki prekršaja, dok “nenamjerno” znači da nije postojala namjera da se prouzroči kršenje iako je voditelj obrade/izvršitelj obrade prekršio svoju obvezu dužne pažnje propisanu zakonom. Iste Smjernice dakle naglašavaju razliku između okolnosti koje su indikativne ili „namjerne povrede“ i onih koje ukazuju na kršenja koja su prouzročena „nenamjerno“ ili “nemarom“. U tom smislu Smjernice navode "nedonošenje politika" i "ljudsku pogrešku" kao primjere ponašanja koji mogu ukazivati na nepažnju.

U ovoj upravnoj stvari utvrđeno je postojanje namjere u vezi s postupkom izmjene lozinke korisnika, budući da je postupak u kojem se korisniku, nakon iniciranja zahtjeva za izmjenu lozinke, na njegovu elektroničku poštu šalje ista lozinka koja je pohranjena u bazi podataka (polje „PWD“) uspostavljen već prilikom izrade idejnog rješenja aplikacije „Moj račun“. Obzirom na navedeno, zaključuje se kako je Voditelj obrade svjesno odabrao rješenje koje nije sadržavalo osnovne mjere sigurnosti zaštite podataka, poput generiranja privremene lozinke ili korištenja metoda kriptiranja podataka, te nije uzeo u obzir rizike za sigurnost osobnih podataka niti je proveo procjenu rizika obrade osobnih podataka korisnika. budući da je način promjene lozinke korisnika na način da se korisniku prilikom pokretanja izmjene lozinke na elektroničku poštu korisnika kao privremena lozinka dostavlja ista lozinka koja je upisana u bazi podataka aplikacije za tog korisnika, uspostavljen prilikom izrade idejnog rješenja aplikacije „Moj račun“. Voditelj obrade čak niti prilikom izrade idejnog rješenja predmetne aplikacije nije takav postupak smatrao spornim s aspekta zaštite sigurnosti osobnih podataka.

Tijekom provođenja nadzora, X je izjavio da se takav način izmjene lozinke primjenjuje od samog početka rada aplikacije „Moj račun“ te da isti nije mijenjan (str. 4. Zapisnika o provedenom nadzoru od 6. studenog 2024. – prileži spisu predmeta).

Ovakvo postupanje Voditelja obrade ukazuje na postojanje namjere na strani Voditelja obrade u odnosu na postupanje protivno obvezama iz članka 32. Opće uredbe o zaštiti podataka, odnosno na namjerno zanemarivanje sigurnosnih standarda koje je Voditelj obrade dužan poznavati, osobito s obzirom da se radi o sustavu koji obrađuje osobne podatke više od 15.000 ispitanika.

U odnosu na postupanje Voditelja obrade protivno članku 31. Opće uredbe o zaštiti podataka, također je utvrđeno postojanje namjere Voditelja obrade, budući da je Voditelj obrade znao za zahtjev Agencije u pogledu dostave svih relevantnih informacija i dokumentacije odnosne na aplikaciju „Moj račun“.

- Svaka radnja koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici (članak 83. stavak 2., točka c);

U ovoj upravnoj stvari nije utvrđeno da su ispitanici pretrpjeli konkretnu materijalnu ili nematerijalnu štetu kao izravnu posljedicu povrede osobnih podataka. Međutim, s obzirom na prirodu i način na koji su osobni podaci korisnika bili obrađivani (pohranjivanje korisničkih lozinki u čitljivom tekstualnom obliku te njihovo slanje putem elektroničke pošte), rizik za prava i slobode ispitanika ocijenjen je kao vrlo visok.

Unatoč navedenome, tijekom postupka nije utvrđeno da je Voditelj obrade poduzeo bilo kakve konkretne ili učinkovite mjere radi ublažavanja mogućih štetnih posljedica po ispitanike poput npr. obavješćivanja ispitanika, privremene obustave funkcionalnosti aplikacije, slanja upozorenja korisnicima i sl.

Izostanak proaktivnog pristupa Voditelja obrade u otklanjanju ili ublažavanju rizika po ispitanike predstavlja otegotnu okolnost koja se uzima u obzir pri odmjeravanju visine upravne novčane kazne.

- Stupanj odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32. (članak 83. stavak 2 točka d);

Voditelj obrade u obvezi je sukladno članku 32. primijeniti odgovarajuće tehničke i organizacijske mjere kako bi osigurao razinu sigurnosti primjerenu rizicima obrade osobnih podataka, osobito uzimajući u obzir narav, opseg, kontekst i svrhu obrade.

U ovoj upravnoj stvari utvrđeno je da Voditelj obrade nije poduzeo odgovarajuće mjere sigurnosti zaštite podataka u odnosu na obradu osobnih podataka putem aplikacije „Moj račun“. Naime, korisničke lozinke bile su pohranjene u bazi podataka u nešifriranom odnosno čitljivom obliku; ista lozinka bila je dostavljana korisniku kao „privremena lozinka“ pute elektroničke pošte, bez ikakve izmjene ili primjerice generiranja jednokratne privremene lozinke; Voditelj obrade ne posjeduje dokumentiranu procjenu rizika niti ima uspostavljene sigurnosne politike koje bi prethodile razvoju aplikacije „Moj račun“.

Naprijed opisano postupanje Voditelja obrade ukazuje na sustavno zanemarivanje obveza iz članka 32. Opće uredbe o zaštiti podataka, osobito u pogledu sigurnosti pohrane i prijenosa osobnih podataka. Izostanak primjene osnovnih mjera sigurnosti predstavlja ozbiljan propust Voditelja obrade koji se uzima u obzir kao otegotna okolnost prilikom odmjeravanja visine upravne novčane kazne.

U upravnoj stvari utvrđeno je kako Voditelj obrade nije angažirao izvršitelja obrade te je stoga stupanj odgovornosti Voditelja obrade u odnosu na predmetno kršenje naprijed navedenih obveza Opće uredbe o zaštiti podataka maksimalan.

- Relevantna prijašnja kršenja voditelja obrade ili izvršitelja obrade (članak 83. stavak 2. točka e);

Prema službenim evidencijama o upravnim postupanjima koje vodi Agencija, nije evidentirano ranije istovrsno kršenje Opće uredbe o zaštiti podataka od strane Voditelja obrade. Stoga se ova okolnost uzima u obzir kao neutralna prilikom odmjeravanja visine upravne novčane kazne, budući da se od svakog voditelja obrade i izvršitelja obrade očekuje poštivanje važećih propisa.

- Stupanj suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja (članak 83. stavak 2. točka f);

Tijekom upravnog postupka, Voditelj obrade nije pokazao odgovarajući stupanj suradnje kako bi se otklonilo kršenje i ublažili mogući štetni učinci. Voditelj obrade nije Agenciji dostavio dokaze o izmjeni funkcionalnosti aplikacije, a niti je nakon saznanja za sigurnosni propust poduzeo mjere kako bi se ublažili mogući štetni učinci kršenja članka 32. Opće uredbe o zaštiti podataka, poput primjerice obavješćivanja ispitanika.

Voditelj obrade tijekom upravnog postupka nije na odgovarajući način odgovarao na zahtjeve Agencije kao nadzornog tijela, budući da isti nije dostavio tražena očitovanja i dokumentaciju radi utvrđenja svih činjenica i radi rješavanja ove upravne stvari, ali navedena okolnost nije dodatno uzeta u obzir kao otegotna prilikom utvrđivanja visine upravne novčane kazne jer je u ovoj upravnoj stvari utvrđeno kršenje članka 31. Opće uredbe o zaštiti podataka u vezi s člankom 58. stavkom 1. toč. e) Opće uredbe o zaštiti podataka.

Voditelj obrade je u prilogu podneska od 10. prosinca 2024. dostavio dokument Uvjeti korištenja web aplikacije „Moj račun“ – ažuriran u prosincu 2024., kojim je uredio upute za korisnike u pogledu kreiranja lozinke i sadržajem znakova iste, a čime je Voditelj obrade u jednom dijelu poduzeo radnje kako bi se otklonile daljnje štetne posljedice, a što je prilikom odmjeravanja visine upravne novčane kazne uzeto kao olakotna okolnost.

- Kategorije osobnih podataka na koje kršenje utječe (članak 83. stavak 2. točka g);

U ovoj upravnoj stvari utvrđena je obrada osobnih podataka korisnika aplikacije „Moj račun“ i to kategorija koje se odnose na identifikacijske podatke korisnika aplikacije, kategorija koje se odnose na autentifikaciju korisnika (lozinke korisnika), podatke koji se odnose na kontakt korisnika aplikacije, podatke o korištenju usluge, kao i osjetljive podatke (podaci o potrošnji, podaci o financijskim transakcijama i sl.).

Budući da su u pitanju osobni podaci – lozinke korisnika, njihovo neovlašteno otkrivanje ili prijenos predstavlja visoki rizik za prava i slobode ispitanika jer omogućuje neovlašteni pristup korisničkim računima i svim povezanim osobnim podacima koji su sadržani u istima te je stoga navedena okolnost prilikom odmjeravanja visine upravne novčane kazne uzeta kao otegotna.

- Način na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju (članak 83. stavak 2. točka h);

Agencija je za predmetno kršenje saznala na temelju predstavke ispitanika zaprimljene dana 18. listopada 2024. koji je obavijestio Agenciju o postojanju sigurnosnog propusta prilikom korištenja aplikacije „Moj račun“ od strane Voditelja obrade, a o istome je navedenog dana i ispitanik putem elektroničke pošte upozorio i Voditelja obrade.

Povodom zaprimljene predstavke, Agencija je 6. studenog 2024. provela nenajavljeno izravno nadzorno postupanje u prostorijama Voditelja obrade, tijekom kojega su utvrđeni elementi povrede iz članka 32. Opće uredbe o zaštiti podataka.

- Ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera (članak 83. stavak 2. točka i);

Voditelju obrade u vezi s istim predmetom nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka.

- Poštovanje odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42. (članak 83. stavak 2. točka j);

Nije primjenjivo u predmetnom slučaju.

- Svi ostali otegotni ili olakotni čimbenici koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem (članak 83. stavak 2. točka k);

Potrebno je ukazati kako će predmetnim iznosom kazne od 320.000,00 eura biti postignuta, osim generalne, i specijalna prevencija na način da će se predmetni Voditelj obrade odvratiti od sličnog kršenja Opće uredbe o zaštiti podataka u budućnosti te će ujedno i svi izravni i neizravni adresati postati svjesni nužnosti poštivanja propisa o zaštiti osobnih podataka, a osobito u dijelu poštivanja obveze poduzimanja odgovarajućih mjera sigurnosti i zaštite osobnih podataka. Isto tako, svaka kazna mora biti i efikasna u pogledu utjecaja na konkretnog voditelja obrade osobnih podataka, a kojemu se ne smije „isplatiti“ kršenje odredbi Opće uredbe o zaštiti podataka, već mu se mora kaznom koja je primjerena njegovim financijskim prilikama (gore objašnjeno), kao i povredi u pitanju (proporcionalnost) jasno dati do znanja da je neprihvatljivo kršenje Opće uredbe o zaštiti podataka koje je bilo predmetom ovog upravnog postupka.

Agencija smatra kako se radi o financijski dobro stojećem Voditelju obrade koji je u predmetnom slučaju učinio tešku povredu Opće uredbe o zaštiti podataka u pogledu članka 32. Opće uredbe o zaštiti podataka, a koji članak predstavlja kamen temeljac normativnog dijela Opće uredbe o zaštiti podataka.

Nadalje, u odnosu na povredu obveze suradnje s nadzornim tijelom iz članka 31. Opće uredbe o zaštiti podataka, Agencija smatra kako će se izrečenom upravnom novčanom kaznom i u pogledu navedene obveze postići generalna i specijalna prevencija na način da će se predmetni Voditelj obrade odvratiti od sličnog kršenja u budućnosti, a ujedno će i svi izravni i neizravni adresati postati svjesni nužnosti poštivanja propisa o zaštiti osobnih podataka u pogledu obveze suradnje s nadzornim tijelom za zaštitu podataka.

Uzimajući u obzir sve gore navedene parametre te otegotne i olakotne okolnosti utvrđivanja pojedine upravne novčane kazne, kao i poštujući kazne koje su u sličnim činjeničnim stanjima izrekla druga nadzorna tijela u okviru mehanizma konzistentnosti, Agencija smatra kako je utvrđeni iznos kazne od 320.000,00 eura prikladan za postizanje svrhe kažnjavanja u ovom slučaju, odnosno da je kazna učinkovita, proporcionalna i odvraćajuća u ovoj upravnoj stvari, te da je njezin iznos u potpunosti primjeren okolnostima konkretnog slučaja.

U ovoj upravnoj stvari Agencija nije mogla primijeniti blažu mjeru u skladu s člankom 58. stavkom 2. Opće uredbe o zaštiti podataka (poput primjerice službene opomene), budući da se radi o težem i dugotrajnijem kršenju obveza iz članka 32. stavka 1. i 2. Opće uredbe o zaštiti podataka, koje je trajalo više od šest godina, obuhvatilo je velik broj ispitanika te je uključivalo nedostatak osnovnih sigurnosnih mjera zaštite osobnih podataka (poput primjerice enkripcije lozinki), budući da su se lozinke ispitanika pohranjivale u datotekama Voditelja obrade u običnom ili čistom tekstu te da je na strani Voditelja obrade postojala namjera kršenja članaka 31. u vezi s člankom 58. stavkom 1. točkom e) Opće uredbe o zaštiti podataka te namjera kršenja obvezi iz članka 32. stavka 1. i 2. Opće uredbe o zaštiti podataka.

Nadalje, izostanak suradnje Voditelja obrade tijekom upravnog postupka, kao i činjenica da Voditelj obrade nije poduzeo radnje za ublažavanje mogućih štetnih posljedica povrede, okolnosti su koje su utjecale na ocjenu kako u konkretnom slučaju nije moguće primijeniti blaže korektivne mjere.

S obzirom na visok rizik za prava i slobode ispitanika, dugotrajnost i sustavnost propusta te nepostojanje ublažavajućih mjera sa strane Voditelja obrade, Agencija smatra da je izricanje novčane kazne jedina odgovarajuća mjera kojom se ostvaruje svrha prevencije, odvraćanja i kažnjavanja u skladu s člankom 83. Opće uredbe o zaštiti podataka.

Agencija smatra da će izricanje iste dovesti do toga da Voditelj obrade pravovremeno ispunjava svoje obveze u području zaštite osobnih podataka u budućnosti, a osobito u pogledu implementiranja odgovarajućih tehničkih i organizacijskih mjere koje omogućavaju učinkovitu primjenu načela zaštite podataka.

Temeljem članka 42. i članka 96. Zakona o općem upravnom postupku („Narodne novine“, broj 47/2009, 110/2021) odlučeno je kao u izreci rješenja.

UPUTA O PRAVNOM LIJEKU

Protiv ovog rješenja nije dopuštena žalba, ali se može pokrenuti upravni spor pred Upravnim sudom u Zagrebu roku od 30 dana od dana dostave rješenja.

RAVNATELJ

Zdravko Vukić, univ.mag.oec.

DOSTAVITI :

1. HEP-Toplinarstvo d.o.o, Miševečka ulica 15A, 10 000 Zagreb
2. Pismohrana, ovdje