P/228426

REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA: UP/I-034-01/25-01/4
URBROJ: 567-04-01/02-25-1
Zagreb, 27.2.2025.

Agencija za zaštitu osobnih podataka (OIB: 28454963989), na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 83. 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, članaka 36., 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), a postupajući po službenoj dužnosti protiv voditelja obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, (OIB: 13269963589) radi zaštite osobnih podataka, donosi sljedeće:

R J E Š E NJ E

1. Utvrđuje se da je nepoduzimanjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka u odnosu na osiguranje trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava, procesa za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, te uzimanja u obzir rizika koje predstavlja obrada, rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima, od strane voditelja obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, došlo do povrede članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti podataka.

2. Za kršenje opisano u točki 1. izreke ovog rješenja, u skladu s odredbama članka 83. stavka 2. i stavka 4. točke a) Opće uredbe o zaštiti podataka, izriče se voditelju obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, upravna novčana kazna u iznosu od:

25.000,00 EUR
(slovima: dvadesetpettisućaeura)

3. Voditelj obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet dužan 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 6092-25860-13269963589 s naznakom –"upravne novčane kazne koje izriče AZOP".

4. Ukoliko voditelj obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, 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.

5. Voditelj obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, je dužan 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

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je dana 15.04.2024. Izvješće o povredi osobnih podataka prema čl.33 Opće uredbe o zaštiti podataka voditelja obrade Istarski vodovod d.o.o. Buzet, kojim se Agenciju izvješćuje da je izvršen hakerski napad na računalne servere tvrtke u jutarnjim satima 11. travnja 2024., da su u trenutku spoznaje o incidentu svi serveri i potencijalno ugrožena oprema odspojeni sa mrežnih resursa te da je kontaktirana stručna podrška specijaliziranih tvrtki za poslove sigurnosti informacijskih sustava, da je plasirana informacija putem medija korisnicima i da je navedeno prijavljeno nadležnim tijelima (MUP, ZSIS, SOA).

Agencija je dopisom KLASA: 009-01/24-17/18, URBROJ: 567-04-01/02-24-2 od 8.5.2024. zatražila očitovanje i dokumentaciju od voditelja obrade Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet, i to, dostavu završnog izvješće o utvrđenjima i okolnostima predmetne povrede uključivo informacije koji je bio vektor ulaska u sustav voditelja obrade, opisati na koji način je ostvaren neovlašteni pristup, koji korisnički račun je kompromitiran/ koje računalo, poslužitelj (server) ili vatrozid (firewall), da navede da li je voditelj obrade zaprimio ucjenjivački email od nepoznate osobe u svezi predmetnog incidenta te dostaviti presliku istog ako je primjenjivo, da navede ukupan broj ispitanika čiji se osobni podaci obrađuju u sustavima pohrane voditelja obrade Istarski vodovod d.o.o. te koja je struktura osobnih podataka, da navede da li Istarski vodovod posjeduje vlastiti podatkovni centar/server sobu ili koristi usluge u oblaku, da navede da li Istarski vodovod sam održava informacijski sustav ili za tu svrhu koristi uslugu druge tvrtke, te dostavi presliku ugovora ako je primjenjivo, da navede organizacijske i tehničke mjere koje je voditelja obrade poduzeo nastavno na predmetnu

povredu, da dostavi preslike akata voditelja obrade, Istarski vodovod d.o.o. odnosnih na uređenje obrade osobnih podataka unutar istog, da dostavi preslike akata voditelja obrade, Istarski vodovod d.o.o. odnosnih na sigurnosti obrade osobnih podataka, odnosno tehničkih i organizacijskih mjera koje provodi predmetni voditelj obrade, posebice vezane uz informacijsku sigurnost.

Dana 22.05.2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane voditelja obrade Istarski vodovod d.o.o. u kojem se navodi da su tijekom ranog jutra u četvrtak 11. travnja primijećene na njihovim serverima određene automatske radnje inicirane napadom vrstom štetnog softvera (tzv. INC ransomware) koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja, da je uz to za rad bilo onemogućeno i dvadesetak osobnih računala na kojima su bile kriptirane datoteke a kod pojedinih je bilo onemogućeno i pokretanje operativnog sustava Windows.

Dalje se navodi da informacijski sustav istarskog vodovoda bilježi oko 90.000 podataka potrošača vodnih usluga i poslovnih partnera, te 300-tinjak podataka sadašnjih i bivših zaposlenika koji se Općom uredbom o zaštiti podataka (GDPR) smatraju osobnim podacima, da tijekom izvršenog napada međutim podaci pohranjeni u njihovim bazama podataka zbog svoje obimnosti i nemogućnosti jednostavnog i brzog kopiranja nisu kompromitirani, da su napadači na kompromitiranim računalima ostavili poruke u obliku txt i htmp datoteke, (očitovanju se prilaže preslika ucjenjivačke poruke na engleskom jeziku u kojoj se između ostalog navodi da su podaci ukradeni i kriptirani, da ako ne plate otkupninu da će biti objavljeni na TOR darknet stranicama, i da ako plate da će dostaviti dekripcijski ključ i uništiti ukradene podatke), da je brzom reakcijom djelatnika onemogućeno daljnje širenje štetnog softvera na način da su iz mreže i izvora napajanja odspojene sve serverske jedinice i uređaji za sigurnosno kopiranje podataka iako je on preko noći već napravio određenu štetu nad programskim rješenjima i podacima tvrtke na način da su određene datoteke i programska rješenja bili kriptirani te tako postali neupotrebljivi, da je razlog brze reakcije bila činjenica da Istarski vodovod posjeduje vlastitu serversku sobu/podatkovni centar te u većem dijelu samostalno održava informacijski sustav uz pomoć ovlaštenih tvrtki koji su proizvođači ili distributeri određenih softverskih rješenja, da se do kraja dana uspio povratiti sustav automatskog i daljinskog nadzora te djelomično upravljanje sustavom proizvodnje i distribucije vode pa opskrba vodom stanovništva i njihovih potrošača niti u jednom trenutku nije došla u pitanje, a zbog postavljenih redundantnih servera i sigurnosne zaštite od napada su bili izuzeti serveri na postrojenjima Butoniga i Gradole što je značajno olakšalo nesmetanu vodoopskrbu.

Dalje se navodi da su u narednim danima uz pomoć tvrtki koje su i inače angažirane na održavanju njihovog poslovnog informacijskog sustava i informatičkih rješenja gotovo sve funkcije vraćene u prvobitno stanje te je nakon tjedan dana normaliziran rad svih službi i djelatnika, da su radnje obuhvaćale povrat baze podataka sa uređaja za sigurnosno kopiranje i dekripciju određenih datoteka, da su povraćene sve serverske i mrežne funkcije a izvršene su i detaljne provjere svakog pojedinog računala te na onima koji su bili zahvaćeni malicioznim programskim rješenjima izvršena je potpuno nova instalacija Operativnog sustava i ostalih potrebnih programskih rješenja.

Istim očitovanjem se dalje pojašnjava da se prema dostupnim informacijama proboj u informacijski sustav dogodio tzv. „brute force“ napadom probijanjem zaporke korisnika s povećanim ovlastima na samom sustavu te upadom preko VPN aplikacije za udaljeni pristup računalima, da kako bi se pokušalo spriječiti daljnje pokušaje i napade, izvršene su određene promjene u sigurnosti informacijskog sustava, dok će za potpuno uklanjanje prijetnji biti potrebna dodatna financijska sredstva, da je u potpunosti zabranjen pristup računalima i serverima tvrtke aplikacijama za udaljeni pristup poput Teamviwera ili Anydeska, da su uz detaljni pregled svih računala i kontrole njihove moguće infekcije malicioznim programima ili samom njihovom posredovanju, svim korisnicima nanovo kreirane tzv. „jake lozinke“, da se trenutačno radi i na uvođenju sustava za dvostruku provjeru autentičnosti te izmjene „group policya“ za određene grupe korisnika na način da se njihova prava na sustavu dodatno ograniče, da je postavljeno i ograničenje broja neuspješnih pokušaja pristupa serveru kao i zabrana pristupa s IP adrese s koje su došli pokušaji neuspješnog pristupa, da se redovito ručno kontroliraju i pretražuju zapisi o neuspješnim pokušajima pristupa te analiziraju dnevnički zapisi i logovi.

Zaključno se navodi da je u svrhu zaštite informacijskih sustava tijekom veljače provedeno i penetracijsko testiranje ranjivosti računalne mreže i fizičkog pristupa ključnim objektima u svrhu prepoznavanja postojećih ranjivosti na sustavima ključnim za informacijsku sigurnost u poslovanju Istarskog vodovoda i u skladu s dostavljenim Izvješćem započeto je uklanjanje mogućih ranjivosti te je s tim u svezi u tijeku nadogradnja operativnih sustava Windows Server za poboljšano upravljanje virtualnim računalima kako bi se i na taj način poboljšala sigurnost i zaštita samih servera.

Očitovanju se prilaže dokument društva _ od 31.08.2018 „*Usluga analize stanje te usklađivanja procesa i dokumentacije s regulativom EU iz područja zaštite osobnih podataka*„ odnosna na Istarski vodovod d.o.o. Sv. Ivan 8, Buzet, odluka o imenovanju službenika za zaštitu osobnih podataka od 25.05.2018, interni akt „Temelj Analize“ od 10.07.2018., „Bibliografija zakona i standarda“ od 10.07.2018., „Ugovor o zaštiti poslovne tajne“ od 9.7.2018., „Završni izvještaj-GDPR“, *Ugovor o izvršenju usluge održavanja IS21 poslovnog sustava za 2023. godinu* sklopljen između Istarskog vodovoda d.o.o. i __ od 20. travnja 2023., *Ugovor o zaštiti osobnih podataka* sklopljen između Istarskog vodovoda d.o.o. i __ od 28. rujna 2018., *Ugovor o izvršenju usluge održavanja korisničkog portala za 2023. godinu* sklopljen između Istarskog vodovoda d.o.o. i __, od 10. veljače 2023., *Ugovor o usluzi održavanja aplikacije upravljanja imovinom i laboratorijem* sklopljen između Istarskog vodovoda d.o.o. i __ od 6. studenog 2023*., Ugovor o zaštiti i čuvanju povjerljivih podataka i osobnih podataka* sklopljen između Istarskog vodovoda d.o.o. i __ od 25. ožujka 2022., *Ugovor o izvršenju usluge održavanja aplikacije EBA za 2023. godinu* sklopljen između Istarskog vodovoda d.o.o. i __ od 10. veljače 2023., Ugovor o zaštiti i čuvanju povjerljivih podataka i osobnih podataka sklopljen između Istarskog vodovoda d.o.o. i __ od 21. ožujka 2023*., Ugovor o usluzi održavanja aplikacije upravljanja imovinom i laboratorijem* sklopljen između Istarskog vodovoda d.o.o. i __ od 6. studenog 2023., Ugovor o zaštiti i čuvanju osobnih podataka i povjerljivih poslovnih informacija sklopljen između Istarskog vodovoda d.o.o. i __ od 27. veljače 2020., *Ugovor o održavanju mobilnog sustava za očitanje vodomjera za 2024. godinu* sklopljen između Istarskog vodovoda d.o.o. i __ od 26. ožujka 2024., te dokument „*Edukacije i aktivnosti GDPR“.*

Agencija je dopisom KLASA: 009-01/24-17/18, URBROJ: 567-04-01/02-24-4 od 12.06.2024. zatražila od Ministarstva unutarnjih poslova RH, PU istarske, dostavu informacija da li su zaprimili prijavu društva Istarski vodovod d.o.o. u svezi predmetne povrede od 11.04.2024., da li su postupali po istoj, koja saznanja imaju o okolnostima povrede i dali je došlo do otuđenja osobnih podataka iz sustava pohrane istog društva.

Dana 16.07.2024. Agencija je zaprimila dopis Ministarstva unutarnjih poslova RH, PU istarske Broj: 511-08-32-K-43/2024 od 5.7.2024. kojim se izvješćuje da su policijski službenici PP Pazin s ispostavom Buzet 11.04.2024. zaprimili kaznenu prijavu odgovorne osobe __, voditelja informatičke službe Istarskog vodovoda d.o.o., podnesenu u ime trgovačkog društva Istarski vodovod d.o.o. Sveti Ivan broj 8, grad Buzet, protiv nepoznatog počinitelja koji je na njihovu štetu počinio kazneno djelo „Teška kaznena djela protiv računalnih sustava, programa i podataka“ iz čl. 273. KZ-a a u svezi kaznenog djela „Oštećenje računalnih podataka“ iz čl. 268. Kaznenog zakona, na način da je kriptirao datoteke na računalima unutar računalnog sustava, te da je o kaznenom djelu izvješteno Općinsko državno odvjetništvo u Pazinu.

Agencija je dopisom KLASA: 009-01/24-17/18, URBROJ: 567-04-01/02-24-6 od 20.08.2024. zatražila dodatno očitovanje i dokumentaciju od društva Istarski vodovod d.o.o., da navede naziv korisničkog računa ili više njih koji je/su bio/bili kompromitirani tj. korišteni od strane napadača na informacijski sustav Istarskog vodovoda za neovlašteni pristup istom, te navesti datum prvog neovlaštenog pristupa, da navede naziv servera (poslužitelja) i OS koji je bio postavljen na njemu a kojem je napadač pristupio, da navede naziv vatrozida (firewall-a) i njegov model, koji je bio implementiran u informacijskom sustavu u trenutku predmetnog incidenta, da navede IP adresu s koje je napadač izvršio neovlašteni pristup, da u odnosu na očitovanje od 20.5.2024. i navode sadržane u priloženom „Izvješću o kibernetičkom napadu nad informacijski sustav Istarskog vodovoda“ od 25.4.2024. da: „*podaci pohranjeni u našim bazama podataka zbog svoje obimnosti i nemogućnosti jednostavnog i brzog kopiranja nisu kompromitirani“,* dostaviti dokaze koji to potkrjepljuju, a imajući u vidu sadržaj ucjenjivačkog emaila kojim napadač navodi da je podatke ukrao i kriptirao te da će po izvršenom plaćanju uništiti ukradene podatke, da u odnosu na navode iz „Izvješću o kibernetičkom napadu nad informacijski sustav Istarskog vodovoda“, da je proboj u informacijski sustav ostvaren preko VPN aplikacije, navedu koliki je bio ukupan broj registriranih korisnika s ovlastima pristupa informacijskom sustavu Istarskog vodovoda d.o.o. putem VPN-a u vrijeme predmetne povrede.

Dana 04.09.2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane društva obrade Istarski vodovod d.o.o. u kojem se navodi da prema podacima dobivenih od voditelja službe elektronike i voditelja službe informatike Istarski vodovod d.o.o. nije bilo moguće utvrditi preko kojeg korisničkog računa ili više njih je izvršen neovlašteni pristup informacijskom sustavu Istarski vodovod d.o.o. no kompromitiran i korišten od napadača bio je administratorski korisnički račun pod nazivom „ADMINISTRATOR“, da u poslovanju Istarski vodovod d.o.o. koristi Servere __, a operativni sustavi su ___, da je u trenutku incidenta u informacijskom sustavu Istarski vodovod d.o.o. bio implementiran __, da vezano za upit o IP adresi s koje je napadač izvršio neovlašteni pristup navode da IP adresa napadača koji je izvršio

neovlašteni pristup nije poznata, da podaci pohranjeni u bazama Istarskog vodovoda d.o.o. zbog svoje obimnosti i nemogućnosti jednostavnog i brzog kopiranja nisu kompromitirani što je utvrđeno kontrolom firewall-a u prethodnom razdoblju, da je kontrolom firewall-a utvrđeno da nije zabilježen veliki promet, odnosno promet koji bi sugerirao da je napadač kopirao podatke iz baze podataka. Isto se navodi da je u trenutku pokušaja proboja u informacijski sustav Istarskog vodovoda d.o.o. bilo registrirano 250 korisnika s ovlastima pristupa informacijskom sustavu.

Agencija je dopisom KLASA: 009-01/24-17/18, URBROJ: 567-04-01/02-24-8 od 01.10.2024. zatražila očitovanje i dokumentaciju od društva Istarski vodovod d.o.o., da navede da li je i u kolikoj mjeri službenik za zaštitu podataka voditelja obrade Istarski vodovod d.o.o. bio informiran o stanju informacijskog sustava, poslužiteljima, računalima i implementiranim sigurnosnim rješenjima od strane Odjel IT-a, i je li o istome izvještavana uprava, te ako je, kada i kako, da s obzirom da u izvješću o povredi osobnih podataka od 12.04.2024., niti u naknadnim očitovanjima nije navedeno koje VPN rješenje (proizvođač, model) je voditelj obrade imao implementirano u trenutku predmetne povrede, potrebno je isto ovim putem iskazati, da uzimajući u obzir javno dostupne informacije o postojanju ranjivosti za VPN konekcije i njezinu iskoristivost od strane hakerskih skupina za neovlašteni pristup informacijskim sustavima tvrtki širom svijeta u periodu od gotovo godinu dana prije predmetne povrede, navedu razloge za ne poduzimanje preventivnih mjera za smanjenje rizika pojavnosti možebitne povrede iste ili slične predmetnoj.

Dana 14.10.2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane društva obrade Istarski vodovod d.o.o. u kojem se navodi da je Službenik za zaštitu podataka dio imenovanog tima za kibernetičku sigurnost, da je o tijeku implementacije mjera i postupaka vezanih uz kibernetičku sigurnost uprava bila izvještavana, a često i osobno sudjelovala na sastancima, da je tim za kibernetičku sigurnost i službenice za zaštitu osobnih podataka upravu izvijestile o konačnom penetracijskom testiranju, a sve iza provedbe istog. Dokumentacija kojom se potkrjepljuje isto dostavlja se u prilogu.
Po pitanju VPN rješenja (proizvođač, model) ističu kako su isto naveli u prethodnom očitovanju od 02.09.2024. i ponavljaju da je to proizvođač: __, model: __.
Po trećoj točki dopisa Agencije od 1.10.2024. isto demantiraju time što je Istarski vodovod d.o.o. obveznik NIS direktive po Zakonu o kibernetičkoj sigurnosti iz 2018. godine (NN 64/2018) od 18.7.2018.) upravo iz kojeg je razloga Društvo započelo sa implementacijom mjera vezanih uz procese kibernetičke sigurnosti te je za potporu istog angažiralo vanjsku tvrtku __ imenujući istovremeno i tim unutar kuće, da je u svrhu zaštite informacijskih sustava, između ostalog, tijekom veljače, provedeno penetracijsko testiranje ranjivosti računalne mreže i fizičkog pristupa ključnim objektima u svrhu prepoznavanja postojećih ranjivosti na sustavima ključnim za informacijsku sigurnost u poslovanju Istarskog vodovoda i u skladu s dostavljenim Izvješćem započeto je uklanjanje mogućih ranjivosti, da u svezi istog ističu kako prilikom penetracijskog testiranja nije iskazana ranjivost VPN konekcije i njezinu iskoristivost od strane hakerskih skupina za neovlašteni pristup, preko čega su u konačnici izvršili napad (Segment II – Penetracijsko testiranje - dostavljeno u prilogu).

Dalje se navodi da kako se u redovnim intervalima pristupa promjeni lozinka korisničkih računa aktiviranjem obaveznog postavljanja pravila (policy) na domenskom poslužitelju, da je također društvo u studenom 2023. godine dostavilo zahtjev za pristupanje sustavu SK@UT prema Sigurnosno-obavještajnoj agenciji te je u prosincu iste godine potpisan Sporazum o pristupanju sustavu SK@UT, bez obzira što Istarski vodovod d.o.o. nije bio dužan uvoditi navedeni sustav. U svezi dodatnog traženja iz dopisa od 1.10.2024. ističu kako je napadač uskratio pristup računalnim resursima napadom štetnog softvera no, kako su već ranije naveli, kontrolom firewall-a u razdoblju koji je prethodio napadu redovitim pregledima logova nije zabilježen veliki promet, odnosno promet koji bi sugerirao da je napadač kopirao podatke iz baze podataka, a čime je izrečena tvrdnja napadača dovedena u sumnju ali nažalost prilikom napada uništeni su logovi kojima bi isto mogli potkrijepiti.

Sukladno članku 4. stavku 1. točki 1. Opće uredbe o zaštiti podataka, osobni podaci su 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.

Članak 32. stavak 1. Opće uredbe o zaštiti podataka propisuje da 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: (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade i (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, dok je stavkom 2. istoga članka propisano da se prilikom procjene odgovarajuće razine sigurnosti u obzir 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 utvrđeno je da je nepoznata osoba/napadač došao u posjed pristupnih podataka (korisničko ime) korisnika/zaposlenika društva Istarski vodovod d.o.o. te putem VPN konekcije primjenom tehnike napada „brute-force“ (upisivanje velikog broja kombinacija zaporki do postizanja preklapanja) ostvario neovlašteni pristup informacijskom sustavu društva

Istarski vodovod d.o.o., te zatim zadobio ovlasti administratorskog korisničkog računa „ADMINISTRATOR“, nakon čega je provodio neovlaštene aktivnosti unutar sustava.

Utvrđeno je da je napadač pokrenuo ransomware napad kojim je zaključao (kriptirao) poslužitelje te ostavio datoteku s ucjenjivačkom porukom na više računala u kojoj je naveo da su podaci ukradeni i kriptirani te da traži plaćanje otkupnine za davanje dekripcijskog ključa, a da je uz to za rad bilo onemogućeno i dvadesetak osobnih računala na kojima su bile kriptirane datoteke a kod pojedinih je bilo onemogućeno i pokretanje operativnog sustava Windows, a o kojem činjeničnom stanju su zaposlenici informirani 11. travnja 2024.

U ovoj upravnoj stvari utvrđeno je da je društvo Istarski vodovod d.o.o., kao voditelj obrade učinio višestruke propuste kod implementacije odgovarajućih mjera sigurnosti obrade osobnih podataka. S tim u svezi, udaljeni pristup informacijskom sustavu Istarski vodovod d.o.o., putem VPN konekcije, unatoč postojanju javno dostupne informacije o kibernetičkoj ugrozi VPN konekcija na globalnoj razini više od godinu dana i trendova kibernetičkih kriminalnih skupina da iskorištavaju slabosti VPN konekcije uz primjenu različitih tehnika proboja u informacijske sustave voditelja obrade diljem svijeta, nije bio pravovremeno osnažen putem implementacije dodatne 2-faktorske autentifikacije (dalje u tekstu: 2-FA), a koja bi dodatnim korakom provjere identiteta korisnika možebitno spriječila napadača u ulasku u informacijski sustav Istarski vodovod d.o.o., odnosno osigurala viši nivo zaštite od neovlaštenog pristupa, uzimajući u obzir da je u trenutku predmetne povrede bilo aktivnih 250 korisnika koji imaju ovlasti spajanja putem VPN-a na informacijski sustav Istarski vodovod d.o.o., a što daje posebnu težinu obzirom da je isto predstavljalo rizik kojem je bilo potrebno posvetiti dužnu pažnju kod dizajniranja mjera informacijske sigurnosti.

Izvršenim uvidom u „I*zvještaj statusa provedbe penetracijskog testiranja ranjivosti računalne mreže i fizičkog pristupa ključnim štićenim objektima u svrhu prepoznavanja postojećih ranjivosti na sustavima ključnim za informacijsku sigurnost“* društva __ od 4. ožujka 2024. utvrđeno je da u trenutku predmetne povrede društvo Istarski vodovod d.o.o. nije imalo segmentiranu mrežu te je isto omogućilo napadaču da jednom kada je ostvario pristup informacijskom sustavu ima neometani pristup svim poslužiteljima, aplikacijama i servisima unutar mreže, te da su poslužitelji unutar istog sustava koristili operativne sustave za koje je prestala podrška proizvođača. Iz navedenog proizlazi da je voditelj obrade propustio pravovremeno provesti mjeru odnosnu na sigurnost obrade i nadograditi komponente informacijskog sustava što je imalo za posljedicu ranjivost sustava i utjecaj na predmetnu povredu.

Utvrđeno je da je društvo Istarski vodovod d.o.o. nakon utvrđenja okolnosti povrede pristupilo ograničavanju broja neuspješnih pokušaja pristupa serveru kao i zabranu pristupa s IP adrese s koje je došao napad iz čega proizlazi da je voditelj obrade, u vrijeme određivanja sredstava obrade i u vrijeme same obrade, nemarom propustio posvetiti pažnju, konfiguriranju sigurnosnih mjera udaljenog pristupa i ograničiti pristup svom informacijskom sustavu samo s IP adresa koje geolokacijski pripadaju Republici Hrvatskoj, dok je propust ograničenja broja neuspješnih pokušaja pristupa imalo za posljedicu da je napadač koristeći „brute-force“ tehniku

mogao neograničeno puta upisivati lozinku do postizanja preklapanja s ispravnom te zatim probojem u sustav dalje ostvariti svoje namjere.

Utvrđeno je da voditelj obrade nema usvojen interni akt odnosan na uređenje obrade osobnih podataka unutar istog, već iz dostavljene dokumentacije očitovanjem od 20.05.2024. proizlazi da je društvo __ provelo *analizu stanja te usklađivanja procesa i dokumentacije s regulativom EU iz područja zaštite osobnih podataka* Istarskog vodovoda d.o.o. 31. kolovoza 2018. i kreiralo dokumente u kojima se navode odredbe Opće uredbe o zaštiti podataka, konstatira stanje i navode preporuke a što ne predstavlja usvojeni interni akt društva Istarski vodovod d.o.o. koji odražava uređenje obrade osobnih podataka unutar istog.

U svezi tehničkih i organizacijskih mjera koje provodi predmetni voditelj obrade, posebice vezane uz informacijsku sigurnost, utvrđeno je da Istarski vodovod d.o.o. ima usvojen *Pravilnik o sigurnosti informacijskih sustava Istarskog vodovoda d.o.o. Buzet* od 21.ožujka 2022*.,* da isti sadrži u članku 22. odredbe o zaporkama da *minimalna dužina zaporke mora biti šest znakova, da u zaporci treba izmiješati mala i velika slova s brojevima i barem jednim specijalnim znakom*, ali isti pravilnik izrekom ne spominje pristup informacijskom sustavu sa strane Interneta putem VPN konekcije, a od svibnja 2018. od pune primjene Opće uredbe o zaštiti podataka takav Pravilnik nije bio niti usvojen do navedene 2022. godine.
Utvrđeno je da društvo Istarski vodovod d.o.o. nije izmijenio/revidirao navedeni akt, niti nakon pojave trendova novih kibernetičkih ugroza i pojavnosti kompromitacije informacijskih sustava voditelja obrade diljem svijeta, bilo u svezi slabih lozinki ili VPN konekcije bez 2-FA, te da je voditelj obrade propustio propisati obvezu korištenja kompleksne lozinke za korisnike sustava duljine najmanje 14 – 16 znakova kako to preporučuje između ostalih i Cybersecurity & Infrastructure Security Agency (CISA) SAD-a te implementaciju 2-FA, što je imalo za posljedicu smanjenja otpornosti njegovog sustava i omogućavanje napadaču lakši proboj u isti.

Uzimajući u obzir činjenicu da je voditelj obrade u trenutku predmetne povrede imao 250 VPN korisnika, da je napadač u njegovom informacijskom sustavu boravio neutvrđeni broj dana neprimijećeno, da je pokretao izvršne datoteke (.exe) za potrebe neovlaštenih aktivnosti, da sam voditelj obrade nije bio u stanju obrazložiti i dokumentirati sve okolnosti predmetne povrede, proizlazi da je voditelj obrade propustio prepoznati postojeće i predvidive rizike i implementirati odgovarajuće tehničko rješenje koje će u realnom vremenu pratiti aktivnosti unutar sustava/nadzirati, te pravovremeno putem predefiniranih mjera (alarma/automatskih akcija) onemogućiti neovlaštene aktivnosti unutar sustava i/ili izvijestiti odgovorne osobe za nadzor informacijskog sustava o istome. Takvo rješenje, Security Information and Event Management (SIEM) postoji dovoljno dugo na tržištu da je voditelj obrade mogao pravovremeno implementirati i dizajnirati isti za centralno prikupljanje i analizu logova te za izvještavanje sigurnosno operativnog centra za pravovremeno reagiranje i odgovarajuću reakciju na incident /povredu u realnom vremenu, a što je i već spomenuto društvo __ u svom dokumentu „Analiza rizika“ od 31.8.2018. Istarskom vodovodu d.o.o. na strani 12 navelo/predložilo poboljšanje: *„Kako bi se djelovalo proaktivno i spriječilo incidente u realizaciji te retroaktivno efikasno izvršila forenzička analiza potrebno je zapise o korištenju*

sa svih sustava povezanih sa korištenjem osobnih podataka prikupljati centralno kako bi se između zapisa mogla izvršiti korelacija te se predlaže implementacija SIEM rješenja.“

Iz prethodno navedenih odredbi Opće uredbe o zaštiti podataka proizlazi da je voditelj obrade prilikom obrade osobnih podataka dužan poduzeti odgovarajuće organizacijske i tehničke mjere sigurnosti, na način da treba osigurati trajnu povjerljivost sustava kao i proces redovnog testiranja, ocjenjivanja i procjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, a prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzeti rizike od, *inter alia*, neovlaštenog otkrivanja osobnih podataka.

Nakon utvrđenja činjeničnog stanja utvrđeno je da je voditelj obrade, iako obrađuje osobne podatke velikog broja ispitanika, zanemario veličinu i kompleksnost svog informacijskog sustava i nije poduzeo pravovremene i odgovarajuće tehničke mjere sigurnosti prije sigurnosnog incidenta/predmetne povrede osobnih podataka, a koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu, te učinio višestruke propuste prilikom dizajniranja sustava obrade, uključivo, ograničavanje pristupa, nadzor, izvješćivanje, pravovremeno reagiranje i uključivanje odgovarajućih korektivnih akcija u sustavu sukladno postojećim i predvidivim rizicima, čime je postupio protivno odredbama članka 32. stavka 1. točke b) i d) i stavka 2. Opće uredbe o zaštiti podataka.
Točnije, voditelj obrade je propustio implementirati 2-FA prilikom korištenja VPN konekcije, kompleksniju lozinku duljine 14-16 znakova, sustav nadzora logova aktivnosti korisnika prilikom spajanja na informacijski sustav i izvješćivanje o anomalijama u realnom vremenu, okidače (trigere) za „brute-force“ napad, tehniku koju je napadač koristio u predmetnoj povredi, podešenje zaključavanja VPN korisničkih računa nakon 3 kriva unosa, segmentirati mrežu i druga odgovarajuća sigurnosna rješenja nadzora mreže i korisnika.

I. 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 i/ili izvršitelju 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 ne može biti učinkovit ako nema značajan utjecaj na prihode voditelja obrade, načelo proporcionalnosti ne može se održati ako se povreda razmatra apstraktno bez obzira na utjecaj na voditelja ili izvršitelja obrade, a ista treba biti i odvraćajuća od budućih kršenja. Dakle, izrečena upravna novčana kazna ne može biti odvraćajuća ako nema financijskog utjecaja na predmetnog 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 izvršitelja/voditelja obrade koji obrađuju osobne podatke ispitanika u području informacijskih tehnologija. Izricanjem upravne novčane kazne treba se postići generalno odvraćanje (obeshrabriti druge u ponavljanju kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja kršenja).

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.;
(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. točki (a) Opće uredbe o zaštiti podataka je propisano da se za kršenja obveza voditelja i izvršitelja obrade u skladu s člankom 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.

Uvidom u dostupne informacije Agencija je utvrdila da je Istarski vodovod d.o.o. (MBS: 040004424, OIB: 13269963589) samostalni pravni subjekt.

Budući da ukupni godišnji prihodi u 2023. godini za Istarski vodovod d.o.o. iznosi 21.963.146,00 EUR, 2% tog iznosa je 439.262,92 EUR, isti ne predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju, jer je navedeni iznos manji od 10.000.000,00 EUR.

Agencija je radi kršenja članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti osobnih podataka izrekla voditelju obrade Istarski vodovod d.o.o. upravnu novčanu kaznu u iznosu od 25.000,00 EUR, a koji iznos čini 0,25 % 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 predmetnom slučaju, kako je utvrđeno u točki 1. izreke ovog rješenja, došlo je do kršenja obveza voditelja obrade iz članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti podataka, neprovođenjem odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka od strane voditelja obrade Istarski vodovod d.o.o. a za koje kršenje Opća uredba o zaštiti podataka propisuje izricanje upravne novčane kazne sukladno članku 83. stavku 4. točke a), odnosno, 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 što je veće.

Priroda kršenja

U predmetnoj povredi voditelj obrade je propustio pravovremeno implementirati odgovarajuće tehničke mjere sigurnosti obrade osobnih podataka u odnosu postojeće i predvidive rizike, a koje su mogle spriječiti predmetnu povredu ili svesti na najmanju moguću mjeru, odnosno, nepoduzimanjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka u odnosu na osiguranje trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava, procesa za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, te uzimanja u obzir rizika koje predstavlja obrada, rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima.
Pri tome se prvenstveno misli na implementaciju 2-FA prilikom korištenja VPN konekcije, kompleksniju lozinku duljine 14 - 16 znakova, sustav nadzora logova aktivnosti korisnika prilikom spajanja na informacijski sustav i izvješćivanje o anomalijama u realnom vremenu (SIEM), okidače (trigere) za „brute-force“ napad, tehniku koju je napadač koristio u predmetnoj povredi, podešenje zaključavanja VPN korisničkih računa nakon npr. 3 kriva unosa.

Težina povrede

Prilikom ocjenjivanja težine povrede u obzir su uzete činjenice da voditelj obrade u svom informacijskom sustavu obrađuje veliki broj osobnih podataka ispitanika, da je isti sustav kompleksan, da je u trenutku predmetne povrede bilo aktivno veliki broj korisnika VPN konekcije, točnije njih 250, da voditelj obrade nije uzeo u obzir recentne trendove kibernetičkih ugroza i pojavnosti kompromitacije informacijskih sustava voditelja obrade diljem svijeta i propisao i obvezu korištenja kompleksne lozinke duljine najmanje 14 – 16 znakova kako to preporučuje između ostalih i Cybersecurity & Infrastructure Security Agency (CISA) SAD-a umjesto postojeće duljine od minimalno 6 znakova, da je koristio operativne sustave na poslužiteljima za koje je prestala podrška proizvođača, te da mreža nije bila segmentirana što je omogućilo napadaču jednostavan pristup svim dijelovima sustava jednom kada je ušao u isti.

Neovisno o sadržaju poruke napadača u kojoj isti tvrdi da su podaci iz sustava ukradeni i kriptirani, voditelj obrade navodi da uvidom u sistemske zapise (logove) firewall-a nije zabilježen veliki izlazni promet te iz toga zaključuje da nije došlo do izvoza podataka ali istovremeno navodi da nije u mogućnosti to potkrijepiti dokazima jer su logovi u predmetnoj povredi obrisani. Navedena se izjava ne može uzeti kao relevantna jer se zaključci o prometu izvode iz logova firewall-a a ukoliko su isti obrisani od strane napadača onda ne postoje dokazi

za takve tvrdnje, dok o istom traženom podatku informaciju može imati i davatelj telekomunikacijskih usluga.

Isto tako očitovanjem od 02.09.2024. voditelj obrade navodi da im je „*nepoznata IP adresa napadača koji je izvršio neovlašteni pristup*“, no prethodnim očitovanjem od 20.05.2024. je naveo da su *„zabranili pristup s IP adrese s koje su došli pokušaji neuspješnog pristupa“* što također predstavlja nekonzistentnost u dostavljenim informacijama o utvrđenjima okolnosti predmetne povrede.

Iz navedenog proizlazi da voditelj obrade tijekom postupka nije u potpunosti transparentno artikulirao s činjenicama u svezi količine podataka koji su učinjeni dostupni napadaču i možebitno neovlašteno izvezeni iz njegovog informacijskog sustava, kao niti s podacima s koje IP adrese je neovlašteni pristup ostvaren i korištenjem kojeg korisničkog računa voditelja obrade.

Konačno, težina povrede se sagledava i iz činjenice da je voditelj obrade obveznik NIS 2 direktive i da je tek nakon njezinog usvajanja u studenom 2022. prepoznao potrebu implementacije složenih i naprednijih sigurnosnih rješenja zaštite informacijskog sustava i poduzeo korake u tom smjeru krajem 2023. godine i početkom 2024., dok su iste obveze koje proizlaze iz Opće uredbe o zaštiti podataka ostale zanemarene od 2018. godine unatoč činjenici da inicijalna analiza društva __ iz iste godine ukazuju na nedostatke sustava.

Trajanje povrede

Iako predmetna povreda može biti sagledana u vremenskom okviru od prvog uspješnog ulaska napadača u informacijski sustav voditelja obrade a što voditelj obrade nije definirao pa do dana kada je voditelj obrade postao svjestan povrede a što je 11.4.2024. i poduzeo mjere za rješavanje iste, kršenje odredbi Opće uredbe o zaštiti podataka voditelja obrade zapravo traje od 25. svibnja 2018. od pune primjene Opće uredbe o zaštiti podataka jer voditelj obrade nije implementirao odgovarajuće mjere sigurnosti koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu.

Broj ispitanika

U predmetnoj povredi je utvrđeno da voditelj obrade u svojim sustavima pohrane obrađuje osobne podatke 90.000 ispitanika/potrošača vodnih usluga i poslovnih partnera i 300-tinjak sadašnjih i bivših zaposlenika te su isti zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera zaštite informacijskog sustava voditelja obrade, učinjeni dostupnima neovlaštenoj osobi/napadaču.

Tijekom postupka nije utvrđeno da li su ispitanici pretrpjeli određenu štetu kao posljedicu predmetne povrede.

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

U ovoj upravnoj stvari utvrđeno je da je Istarski vodovod d.o.o. kao voditelj obrade propustio primijeniti odgovarajuće organizacijske i tehničke mjere zaštite kako bi zaštitio osobne podatke koje obrađuje, odnosno zaštitio osobne podatke od uništenja, izmjene, zabranjenog odavanja i neovlaštenog pristupa, što je za posljedicu imalo da je napadač jednom kada je ostvario pristup na sustav voditelja obrade, zadobivanjem privilegiranih administratorskih ovlasti, neometano i neopaženo mogao kretati cijelim informacijskim sustavom, čime je isti u cijelosti kompromitiran, te ostvario pristup osobnim podacima ispitanika na poslužitelju, a čime su ispunjeni svi elementi nepažnje u postupanju.

Kako tijekom postupka Istarski vodovod d.o.o. nije dostavio dokaze da je u periodu koji je prethodio predmetnoj povredi došlo do nadogradnje operativnih sustava servera kojima je prestala podrška proizvođača na novije verzije od onih koje su navedene u dostavljenom dokumentu društva __ d.o.o. od 04.03.2024., izveden je zaključak da je stanje bilo isto prethodnom, a informacija dostavljena očitovanjem od 20.05.2024. da je u „*tijeku nadogradnja operativnih sustava Windows Server",* ukazuje da je aktivnoj nadogradnji sustava pristupio tek nakon utvrđenja predmetne povrede a što potvrđuje i informacija dana očitovanjem od 02.09.2024. da koriste u poslovanju tri poslužitelja i da je na njima operativni sustav Windows Server 2018.

Također, *Pravilnik o sigurnosti informacijskih sustava Istarskog vodovoda d.o.o. Buzet* od 21.ožujka 2022. navodi da:" *Osoba čija je prvenstvena briga sigurnost informacijskih sustava je voditelj Službe elektronike. Briga voditelja je ukupna sigurnost informacijskog sustava. Voditelj piše pravilnike, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera, te sudjeluje u razvoju softvera, kako bi osigurao da se poštuju pravila iz sigurnosne politike.",* te iz navedenog proizlazi da je voditelj obrade propustio pravovremeno provesti propisanu organizacijsku mjeru odnosnu na sigurnost obrade i nadograditi komponente informacijskog sustava što je imalo za posljedicu ranjivost sustava i predmetnu povredu, te je isto ocijenjeno kao namjera.

Izvršenim uvidom u *Pravilnik o sigurnosti informacijskih sustava Istarskog vodovoda d.o.o. Buzet* od 21. ožujka 2022. utvrđeno je da isti, neovisno o navedenoj preporuci društva __ u Analizi rizika od 31.08.2018. o potrebi implementacije SIEM sustava, ne sadrži odredbe o navedenom rješenju, niti da je došlo do implementacije navedenog rješenja u sustavu po tom pitanju te posljedično do revizije istog Pravilnika, te je opisano ocjenjeno kako namjera.

Izvršenim uvidom u *Pravilnik o sigurnosti informacijskih sustava Istarskog vodovoda d.o.o. Buzet* od 21. ožujka 2022. koji navodi u članku 22. da *minimalna dužina zaporke mora biti šest znakova, da u zaporci treba izmiješati mala i velika slova s brojevima i barem jednim specijalnim znakom*, utvrđeno je da voditelj obrade nije revidirao sadržaj odnosan na pravila za zaporke u smislu duljine zaporke, kao i da nije implementirao rješenje vezano uz udaljeni pristup (VPN) u smislu uvođenja dvo-faktorske autentifikacije (2-FA) kao dodatne sigurnosne mjere a uzimajući u obzir činjenice postojanja trendova novih kibernetičkih ugroza i pojavnosti kompromitacije informacijskih sustava voditelja obrade diljem svijeta, bilo putem slabih

lozinki ili VPN konekcije bez 2-FA. Navedeno utvrđenje ocjenjeno je kao nepažnja u postupanju.

Konačno, iz očitovanja voditelja obrade od 10.10.2024. u odnosu na upit da li je i u kolikoj mjeri službenik za zaštitu podataka voditelja obrade Istarski vodovod d.o.o. bio informiran o stanju informacijskog sustava, poslužiteljima, računalima i implementiranim sigurnosnim rješenjima od strane Odjel IT-a, i je li o istome izvještavana uprava, te ako je, kada i kako, proizlazi da je službenik za zaštitu podataka dio imenovanog tima za kibernetičku sigurnost, da je o tijeku implementacije mjera i postupaka vezanih uz kibernetičku sigurnost uprava bila izvještavana, da je tim za kibernetičku sigurnost i službenice za zaštitu osobnih podataka upravu izvijestile o konačnom penetracijskom testiranju provedenom od strane društva __ zaključno s 4.3.2024. Navedeno predstavlja korake prema nadogradnji informacijskog sustava koji su poduzeti tek nakon usvajanja NIS 2 direktive kojom je Istarski vodovod d.o.o. obveznik primjene i slijedom koje je isto društvo podnijelo zahtjev za pristup SK@UT sustavu, a isto se ocjenjuje kao namjera.

- 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 predmetnom postupku nije utvrđeno da su ispitanici pretrpjeli štetu kao posljedicu predmetne povrede.

- 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);

Uzimajući u obzir odredbe članka 32. koje obvezuju voditelja obrade i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade; proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, da se prilikom procjene odgovarajućeg nivoa sigurnosti 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, utvrđeno je da Istarski vodovod d.o.o. provodi određene organizacijske i tehničke mjere zaštite pri obradi osobnih podataka, ali da u konkretnom slučaju nisu bile dovoljne čime je došlo do neovlaštenog pristupa i kompromitacije osobnih podataka ispitanika.
Naime, u ovoj upravnoj stvari utvrđeno je da je Istarski vodovod d.o.o. kao voditelj obrade učinio višestruke propuste prilikom dizajniranja sustava obrade, uključivo, ograničavanje pristupa, nadzor, izvješćivanje, pravovremeno reagiranje i uključivanje odgovarajućih korektivnih akcija u sustavu.

S obzirom na kompleksnost informacijskog sustava, velikog broja zaposlenika koji istom pristupaju lokalno i udaljeno, velikom broju osobnih podataka koje obrađuje, voditelj obrade je propustio implementirati odgovarajuće tehničko rješenje, kao što je npr. SIEM koje će u realnom vremenu pratiti aktivnosti unutar sustava te pravovremeno putem predefiniranih mjera (alarma/automatskih akcija) onemogućiti neovlaštene aktivnosti unutar sustava i/ili obavijestiti odgovorne osobe za nadzor informacijskog sustava o istome, a imajući u vidu da je napadač u informacijskom sustavu Istarski vodovod d.o.o. boravio neprimijećeno, da je pokretao izvršne datoteke (.exe) za potrebe neovlaštenih aktivnosti, te je njegova prisutnost primijećena tek kada je pokrenuo „ransomware“ napad, a što je navedenim tehničkim rješenjem moglo biti pravovremeno uočeno.

Uzimajući u obzir činjenicu da predmetni voditelj obrade u većem dijelu sam održava svoj informacijski sustav, uz podršku informatičkih društva s kojima ima sklopljen poslovni odnos, njegov stupanj odgovornosti time je veći u smislu praćenja komponenti sustava i održavanja, pravovremene zamjene zastarjelih i ranjivih operativnih sustava ili nadogradnja aplikativnih rješenja te pravovremena implementacija sigurnosnih rješenja sukladno postojećim i predvidivim rizicima. Stoga, navodi u očitovanjima da ne može pružiti sve tražene informacije o okolnostima povrede kao što su IP adresa napadača, dokazi u vidu sistemskih zapisa (logova) iz kojih je razvidan promet na firewall-u, te koji VPN korisnički račun ili više njih je bio kompromitiran u predmetnoj povredi, ukazuju na nedovoljne tehničke mjere implementirane u sustavu uz pomoć kojih je u mogućnosti u svakom trenutku utvrditi činjenično stanje vezane uz funkcioniranje istog sustava, utvrđenja nesukladnosti, anomalija, možebitnih ugroza i konačno uvida u sistemske zapise o svim aktivnostima unutar u istog.

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

Prema evidencijama kršenja koje vodi ova Agencija, voditelj obrade Istarski vodovod d.o.o. nije u prošlosti počinio istovjetno kršenje niti je prekršio Opću uredbu o zaštiti podataka na istovjetan način, a što je ocijenjeno kao neutralna okolnost jer se od svakog očekuje poštivanje pravnih obveza.

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

Voditelj obrade Istarski vodovod d.o.o. je tijekom ovog upravnog postupka pravovremeno odgovarao na zahtjeve nadzornog tijela. Međutim, iz informacija dobivenih u očitovanjima proizlaze kontradiktornosti oko utvrđenja činjeničnog stanje i neprecizni odgovori u pogledu okolnosti s koje IP adrese je napadač pristupio informacijskom sustavu voditelja obrade, da li su i u kojoj mjeri osobni podaci ispitanika izneseni iz informacijskog sustava, naziv kompromitiranog servera (poslužitelja) te struktura osobnih podataka koji se obrađuju u informacijskom sustavu.
Naime, na traženje dopisom Agencije od 08.05.2024. da navede *ukupan broj ispitanika čiji se osobni podaci obrađuju u sustavima pohrane voditelja obrade Istarski vodovod d.o.o. te koja*

je struktura osobnih podataka, očitovanjem od 20.05.2024. dostavljena je informacija o broju ispitanika ali ne i strukturi osobnih podataka.

Istim očitovanjem od 22.5.2024 se navodi „*da se redovito ručno kontroliraju i pretražuju zapisi o neuspješnim pokušajima pristupa te analiziraju dnevnički zapisi i logovi*“, dok se očitovanjem od 10.10. 2024. navodi *„kontrolom firewall-a u razdoblju koji je prethodio napadu redovitim pregledima logova nije zabilježen veliki promet, odnosno promet koji bi sugerirao da je napadač kopirao podatke iz baze podataka, ali da nažalost prilikom napada uništeni su logovi kojima bi isto mogli potkrijepiti“* što su kontradiktorne informacije jer ako su prilikom napada uništeni logovi kako je voditelj obrade onda „redovitom pregledom logova“ izveo zaključak da nije bilo velikog prometa koji bi sugerirao da je napadač kopirao podatke iz baze podataka.

Kada voditelj obrade navodi da „*provodi redovite kontrole dnevničkih zapisa i logova o pristupima sustavu“* iz istog proizlazi da je imao mogućnost detektiranja IP adrese s koje je neovlašteni pristup ostvaren, no na traženje Agencije o istome putem dopisa od 20.08.2024. očitovanjem od 02.09.2024. voditelj obrade paušalno navodi da *„IP adresa napadača koji je izvršio neovlašteni pristup nije poznata“.*
Isto tako, slijedom navedenog o provedbi redovitih kontrola dnevničkih zapisa i logova o pristupima sustavu, na traženje Agencije dopisom od 20.08.2024. da *„navede naziv korisničkog računa ili više njih koji je bio/bili kompromitirani tj. korišteni od strane napadača na informacijski sustav Istarskog vodovoda za neovlašteni pristup istom“,* voditelj obrade očitovanjem od 02.09.2024. navodi *„da nije bilo moguće utvrditi preko kojeg korisničkog računa ili više njih je izvršen neovlašteni pristup informacijskom sustavu Istarski vodovod d.o.o.“* što je u koliziji s prvotno izjavljenim.

Nadalje na traženje Agencije dopisom od 20.08.2024. „*da navede naziv servera (poslužitelja) i OS koji je bio postavljen na njemu a kojem je napadač pristupio*“ voditelj obrade očitovanjem od 02.09.2024. navodi da „*u poslovanju Istarski vodovod d.o.o. koristi __, a operativni sustavi su Windows Server 2018“,* što ne predstavlja zatraženu informaciju u kontekstu predmetne povrede, niti posredno s gledišta činjeničnog stanja u svezi sustava obrade jer iz spisa predmeta proizlazi da je društvo Istarski vodovod d.o.o. u svom informacijskom sustavu u trenutku povrede imalo znatno veći broj servera (poslužitelja) od navedenih tri te su svi imali operativne sustave kojima je prestala podrška proizvođača, slijedom čega se izvodi zaključak da je informacija o operativnom sustavu Windows Server 2018 na poslužiteljima odnosna na mjere poduzete nakon predmetne povrede i nije relevantna kod ocjenjivanja težine povrede.

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

Tijekom postupka na tražnje Agencije dopisom od 08.05.2024. da se očituje koja struktura osobnih podataka ispitanika se obrađuje u njihovom sustavima pohrane Istarski vodovod d.o.o. je očitovanjem od 20.05.2024. dostavio samo informaciju o broju ispitanika te naveo da se radi o potrošačima vodnih usluga i poslovnim partnerima te o sadašnjim i bivšim zaposlenicima,

bez navođenja strukture osobnih podataka, te je utvrđeno da se radi u najmanjem opsegu o imenu i prezimenu, OIB-u, adresi, te dodatno email adresi i broju telefona, dok za zaposlenike i o broju računa u banci, a u odnosu na sve povrede Opće uredbe o zaštiti podataka.

- 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);

Za predmetnu povredu nadzorno tijelo je saznalo putem dostavljenog Izvješća o povredi osobnih podataka sukladno članku 33. Opće uredbe o zaštiti podataka, te obavljanjem nadzornih aktivnosti po službenoj dužnosti.

- 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 Istarski vodovod d.o.o. 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);

Nastavno na saznanje o predmetnoj povredi Istarski vodovod d.o.o. navodi da je pristupio rješavanju nastalog sigurnosnog problema na način da je brzom reakcijom djelatnika onemogućeno daljnje širenje štetnog softvera na način da su iz mreže i izvora napajanja odspojene sve serverske jedinice i uređaji za sigurnosno kopiranje podataka, da se do kraja dana uspio povratiti sustav automatskog i daljinskog nadzora te djelomično upravljanje sustavom proizvodnje i distribucije vode, da je u narednim danima uz pomoć tvrtki koje su i inače angažirane na održavanju njihovog poslovnog informacijskog sustava i informatičkih rješenja gotovo sve funkcije vraćene u prvobitno stanje te je nakon tjedan dana normaliziran rad svih službi i djelatnika, da su radnje obuhvaćale povrat baze podataka sa uređaja za sigurnosno kopiranje i dekripciju određenih datoteka, da su povraćene sve serverske i mrežne funkcije a izvršene su i detaljne provjere svakog pojedinog računala te na onima koji su bili zahvaćeni malicioznim programskim rješenjima izvršena je potpuno nova instalacija Operativnog sustava i ostalih potrebnih programskih rješenja, te je prethodno navedeno uzeto u obzir kao olakotna okolnost prilikom ocjenjivanja težine kršenja odredbi Uredbe.

Istarski vodovod d.o.o je kao operater ključnih usluga i obveznik NIS 2 direktive nakon stupanja na snagu iste tek tada krenuo u planiranja jačanja svog informacijskog sustava tj. njegove

otpornosti, a što prethodno nije učinio iako je Opća uredba o zaštiti podataka u punoj primjeni od 25.05.2018. godine i kojom su jasno definirane odredbe odnosne na organizacijske i tehničke mjere zaštite koje su voditelji obrade dužni implementirati u obradi osobnih podatka, te je navedeno uzeto kao otegotna okolnost prilikom ocjenjivanja težine kršenja odredbi Uredbe.

Jednako tako, uzimajući u obzir sve prethodno navedeno, Agencija smatra da je upravo korektivna mjera u vidu upravne novčane kazne učinkovita, proporcionalna i odvraćajuća u ovoj upravnoj stvari, te da je njezin iznos u potpunosti primjeren okolnostima konkretnog slučaja zbog toga što voditelj obrade obrađuje osobne podatke velikog broja ispitanika, jer je došlo do kompromitacije njegovog informacijskog sustava, jer je povreda trajala šest godina, te konačno, voditelj obrade je prepoznao propuste u svom sustavu i izvršio korekcije te nije smisleno izricati druge mjere.

Temeljem svega navedenog 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 Rijeci u roku od 30 dana od dana dostave rješenja.

RAVNATELJ

Zdravko Vukić, univ. mag. oec.

DOSTAVITI:

1 Istarski vodovod d.o.o. Sv. Ivan 8, 52420 Buzet
2. Pismohrana, ovdje