REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA: UP/I-034-01/21-01/02
URBROJ: 567-12/07-21-01
Zagreb, 12. svibnja 2021.

Agencija za zaštitu osobnih podataka na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 83. stavka 2. i 4. 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 (dalje u tekstu: Opća uredba o zaštiti podataka) SL EU L119, članka 44. i 45. Zakona o provedbi Opće uredbe o zaštiti podataka ("Narodne novine" br. 42/18) te članka 42. stavka 1. i 2. i članka 96. Zakona o općem upravnom postupku ("Narodne novine" br. 47/09) po službenoj dužnosti donosi sljedeće

R J E Š E NJ E

1. Utvrđuje se da je nepoduzimanjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka od strane društva xy d.o.o. iz Zagreba, izvršitelja obrade, društva xx d.o.o., kao pravnog prednika društva__, kao voditelja obrade, protivno članku 32. stavku 1. točke b) i d) te stavku 2. Opće uredbe o zaštiti podataka, došlo do kršenja sigurnosti koje je dovelo do neovlaštene obrade osobnih podataka 28085 ispitanika.

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 društvu xy, kao izvršitelju obrade, upravna novčana kazna u iznosu od:

230.000,00 kuna
(slovima: dvijestotinetridesettisućakuna)

Društvo xy 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: 6092-25860-03401210102, s naznakom – "upravne novčane kazne koje izriče AZOP".

3. Ukoliko društvo 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.

4. Društvo xy 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

Agenciji za zaštitu osobnih podataka (dalje u tekstu: Agencija) obratio se voditelj obrade, dana 03. srpnja 2020. godine sukladno članku 33. stavku 1. Opće uredbe o zaštiti podataka s prijavom povrede osobnih podataka u kojoj navodi da procjenjuje da je dana 29.04. i 07.05.2020. godine došlo do sigurnosnog incidenta uzrokovanog iskorištavanjem ranjivosti softvera treće strane koji je korišten u razvoju aplikacije web shopa, da je prilikom analize i rješavanja sigurnosnog incidenta na kompromitiranom sustavu za pretpostaviti da su na istome smješteni određeni dokumenti koji sadržavaju osobne podatke nekih korisnika, te da je po otkrivanju sigurnosnog incidenta pokrenuo procedure za zaštitu poslovanja i korisničkih podataka kao i detaljne analize utjecaja sigurnosnog incidenta na poslovanje.

U svrhu utvrđenja točnog i potpunog činjeničnog stanja vezanog uz predmetnu povredu osobnih podataka Agencija je dana 18. rujna 2020. provela nadzor u prostorijama društva voditelja obrade, o tome sastavila zapisnik KLASA:042-03/20-01/55, URBROJ:567-12/07-20-22 od 12. listopada 2020., a kojom prilikom je iz priložene dokumentacije i izjava predstavnika predmetnog voditelja obrade utvrđeno da je 26. lipnja 2020. godine iz centrale društva smještenog u___ javljeno društvu u Hrvatskoj da sumnjaju na ostatke „pen-test-a“ (penetration test) na web poslužiteljima koji se fizički nalaze u ___. Na antivirusnoj konzoli__, centrala u ___primijetila je maliciozni “kod“ i javila društvu u Hrvatskoj da provode analizu na svojoj opremi. Prema prikupljenim informacijama najranije maliciozne aktivnosti, vezane uz ovaj incident, pojavljuju se 29.04.2020. i ustanovljeno je da su kod predmetnog incidenta napadači ostvarili pristup na kompromitirane javno dostupne front-end poslužitelje ___ koji podržavaju sljedeće procese odnosno usluge: ___ web stranicu, ___ web shop, proces beskontaktnog plaćanja u kanalima udaljene prodaje i samostalnu dostavu robe. Napadači su ušli kroz Telerik UI aplikaciju, tj. poslužitelji su kompromitirani iskorištavanjem ranjivosti (*Remote Code Execution via insecure Deserialization in Telerik UI)* za koju je javno dostupan sigurnosni propust (*„exploit“)* koji omogućava iskorištavanje ranjivosti.

Voditelj obrade dalje navodi da je uvidom u logove predmetnih poslužitelja ustanovljeno da su napadači postavili tzv. *web shell* aplikaciju (shell.aspx na poslužitelju), koja im je omogućila daljnje izvršenje komandi pod privilegijama IIS korisnika pod kojim je bila pokrenuta i web aplikacija. Napadači su između ostalog, dohvatili i glavnu konfiguracijsku datoteku u kojoj su pohranjeni višestruki parovi aplikativnih kredencijala (korisničkih imena i zaporki), te enkripcijskih ključeva koje su tijekom rada koristile aplikacije voditelja obrade. Ovi podaci su između ostalog uključivali i podatke za spajanje web aplikacije na MS SQL bazu podataka. Identificirane su višestruke datoteke koje sadrže osobne podatke te su iste bile dostupne korisničkom računu pod kojim je pokrenut IIS web poslužitelj, odnosno korisničkom računu pod kojim je napadač bio u mogućnosti pokretati komande te dohvaćati datoteke.

Voditelj obrade dalje navodi da je nastavno na predmetni incident, društvo (voditelj obrade= iz Hrvatske izvršilo udaljeno spajanje na poslužitelje __u ---, kopiralo sadržaj memorijske slike i slike tvrdog diska poslužitelja i dobiveno predalo društvu____, na forenzičku analizu, napadnuti poslužitelji su izolirani te je onemogućen daljnji pristup istima, pokrenuta je procedura za zaštitu poslovanja i korisničkih podataka kao i detaljne analize utjecaja sigurnosnog incidenta na poslovanje. Voditelj obrade je iz ukupnog opsega osobnih podataka sadržanih na kompromitiranim poslužiteljima pretragom svih datoteka utvrdio točan broj identificiranih korisnika i to njih 28085.

Predstavnica predmetnog voditelja obrade tijekom nadzora na upit tko je bio odgovoran za praćenje stanja poslužitelja na kojima su se nalazili osobnih podaci ispitanika zahvaćeni predmetnim incidentom te postavljanje sigurnosnih nadogradnji na iste, navodi: „*da je za to bio zaduženo društvo___ u dijelu održavanja operativnog sustava i baza podataka, a izvršitelj obrade društvo d.o.o. za održavanje softvera web aplikacije koji je u konkretnom slučaju koristio softver treće strane Telerik UI koju koristi web aplikacija i koji nije imao sigurnosnu nadogradnju i napadači su iskoristivši ranjivost iste, zaobišli kredencijale (korisničko ime i zaporka) i ušli u poslužitelj.“*.
Ista prilaže pisano očitovanje o incidentu koje navodi, između ostalog, ključne nalaze provedene forenzike da: *“Poslužitelji SEWP-HRWSFR01 i SEWP-HRWSFR02 su kompromitirani iskorištavanjem CVE-2019-18935 ranjivosti (Remote Code Execution via Insecure Deserialization in Telerik UI) za koju je javno dostupan exploit koji omogućava iskorištavanje ranjivosti, da je provedenom analizom najranija maliciozna aktivnost identificirana 20.04.2020. 18:48:36 kada je napadač na ranjive poslužitelje postavio tzv. web shell aplikaciju (shell.aspx na poslužitelju), koja mu je omogućila daljnje izvršavanje komandi pod privilegijama IIS korisnika pod kojima su bile pokrenute i web aplikacije, da provedenom analizom nisu identificirani nikakvi dokazi koji bi ukazivali na eskalaciju privilegija od strane napadača (npr. dokaz do administratorskih privilegija), da je nakon identificiranog inicijalnog napada detektirano i nekoliko naknadnih pristupa od strane napadača, a zbog nepostojanja odgovarajućih log zapisa nije bilo moguće ustanoviti da li je bilo ikakvih naknadnih malicioznih aktivnosti, da je 29.04.2020. u 16:52:41 napadač uspješno dohvatio Web.config i Web.config.bak konfiguracijske datoteke sa SEW-HRSFR02 poslužitelja, da su dodatne maliciozne aktivnosti koje su rezultirale u dohvaćanju navedenih datoteka identificirane i 30.04.2020. i 01.05.2020, da se napadač uspješno spojio na MS SQL bazu koju koristi*

kompromitirana web aplikacija, da su identificirane višestruke datoteke koje sadrže osobne podatke koje su bile dostupne korisničkom računu pod kojim je pokrenut IIS web poslužitelj, odnosno korisničkom računu pod kojim je napadač bio u mogućnosti pokretati komande te dohvaćati datoteke, da nisu pronađeni dokazi o eksfiltraciji datoteka, da direktoriji u kojima su identificirane datoteke s osobnim podacima sadrže ugovore za zasnivanje pretplatničkog odnosa za maksimalno 25032 korisnika, skenove/fotografije osobnih iskaznica za maksimalno 44236 korisnika, HTM datoteke s ugovornom dokumentacijom za zasnivanje pretplatničkog odnosa maksimalno 12116 datoteka.

Uvidom u dostavljeni *Ugovor o obradi podataka* između voditelja obrade i xy d.o.o. kao izvršitelja obrade od 24. svibnja 2018. navodi se u poglavlju 5. Sigurnosne mjere, točka 5.1. da: *„Izvršitelj obrade osigurava da ima odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke koji se obrađuju. Izvršitelj obrade će, između ostalog, poštivati sigurnosne zahtjeve navedene u Ugovoru i njegovim Aneksima kako i posebne sigurnosne mjere i upute navedene u ovom Ugovoru o obradi.“*, točka 5.2. navodi: „*Izvršitelj obrade će zaštititi osobne podatke od uništenja, izmjene, zabranjenog odavanja i neovlaštenog pristupa“,* točka 5.3. navodi da*: „Izvršitelj obrade osigurava da osobe ovlaštene za obradu osobnih podataka (sve osobe koje rade na temelju uputa izvršitelja obrade) slijede i poštuju ovaj Ugovor o obradi podataka i svaku uputu danu od strane Voditelja obrade, te da ovlaštene osobe prime točne i redovite informacije i obuku o europskom zakonodavstvu o zaštiti podataka.“*. Također, točka 5.4. navodi da*: “Izvršitelj obrade potvrđuje da je primijenio tehnička i praktična rješenja za istraživanje bilo koje sumnje na neovlaštenu obradu ili pristup osobnim podacima. U slučaju bilo kojeg incidenta ili pokušaja, neovlaštene obrade, neovlaštenog pristupa, brisanje ili izmjena osobnih podataka, izvršitelj obrade će bez odgode pisanim putem obavijestiti voditelja obrade.“.*

Uvidom u dostavljeni *Ugovor o održavanju i kontinuiranom razvoju programskih rješenja,* br. T-1/2017 od 17. travnja 2017. između voditelja obrade kao naručitelja i xy d.o.o. kao pružatelja usluge, u poglavlju XIV. ZAŠTITA PODATAKA, u članku 20. točki 6. navodi se da: *“Pružatelj usluge jamči ispunjavanje uvjeta određenih važećim propisima o zaštiti osobnih podataka za izvršitelje obrade osobnih podataka, a osobito da će osigurati mjere zaštite podataka sukladno važećim propisima i ovom Ugovoru, te se obvezuje držati u tajnosti bilo koji podatak koji se odnosi na korisnike usluga Naručitelja ili na radnike Naručitelja uključivo njihove osobne i predmetne podatke.“*, točka 8. navodi da:“ „*U svrhu ispunjavanja obveze zaštite podataka o korisnicima Pružatelj usluge je dužan poduzimati sve potrebne tehničke, organizacijske, sigurnosne te kadrovske mjere*.“, članak 21. točka 1. navodi*: „U slučaju kršenja svojih obveza zaštite podataka o korisnicima Pružatelj usluge se obvezuje poduzimati sve potrebne radnje i aktivnosti kako bi zaštitio Naručitelja od mogućih pravnih zahtjeva trećih osoba i postupaka nadležnih tijela. Pružatelj usluga je dužan bez odlaganja obavijestiti ovlaštenu osobu Naručitelja u slučaju sumnje o nastupu incidenta koji se odnosi na bilo koji podatak o korisnicima*.“, a Prilog 4, Tehničke, organizacijske i kadrovske mjere zaštite osobnih podataka točka 6. Razvoj programskih rješenja stavak a) navodi: „*Sigurnosni zahtjevi trebaju biti sastavni dio procesa programskih rješenja“*, stavak b) navodi: *„Najbolja sigurnosna praksa u razvoju programskih rješenja mora biti slijeđena. Prilikom razvoja Web aplikacija*

moraju se slijediti OWASP zahtjevi najbolje prakse.", stavak c) navodi: *„Prilikom testiranja razvoja programskih rješenja posebna pozornost treba biti stavljena na provjeru postojanja poznatih sigurnosnih ranjivosti/rizika kao što je primjerice OWASP Top 10.“*, stavak d) navodi: „*Moraju postojati pisani zapisi o implementiranim mjerama, testiranjima vezano za sigurnost i kvalitetu programskih rješenja.“*, točka 7. Tehnička sigurnost, stavak *a) navodi: „Kontrole za detekciju, prevenciju i oporavak od malicioznog softvera moraju biti implementirane“.“*

Uvidom u dostavljeni *Pravilnik o upravljanju ranjivostima* voditelja obrade od 03.12.2018. u poglavlju III. Uloge i odgovornosti članak 3. navodi: „*Treće strane (pružatelji usluga razvoja poslovnih aplikacija) odgovorne su za: - prikupljanje informacija i uklanjanje ranjivosti u poslovnim aplikacijama za čiji su razvoj i održavanje nadležni, - klasifikacija otkrivenih ranjivosti u poslovnim aplikacijama za čiji su razvoj i održavanje nadležni, - informiranje voditelja odjela za sigurnost o otkrivenim ranjivostima u poslovnim aplikacijama za čiji su razvoj i održavanje nadležni,“*, poglavlje IV. Cilj i opseg, točka 4. Prikupljanje informacija i otkrivanje ranjivosti, članak 9. navodi*: „Nadležnost za prikupljanje informacija i otkrivanje ranjivosti na pojedinim IT sustavima imaju iste osobe koje su nadležne i za razvoj i održavanje tih sustava te za uklanjanje otkrivenih ranjivosti: - vanjski dobavljači za poslove aplikacije, primjerice ResellerTool, xy, CQ,“*, zatim: *„za prikupljanje informacija o ranjivostima moguće je koristiti slijedeće metode: - praćenje službenih informacija i obavijesti proizvođača putem Internet stranica, obavijesti putem elektroničke pošte te sistemskih obavijesti, - praćenje informacija i obavijesti neovisnih organizacija u domeni informacijske sigurnosti putem Internet stranica te obavijesti putem elektroničke pošte“, - zapisi specijaliziranih alata za upravljanje instalacijom sigurnosnih zakrpa, - izvještaji alata za automatiziranu provjeru ranjivosti, - izvještaji o provedenim penetracijskim testovima te – revizijski i drugi izvještaji u domeni testiranja sigurnosnih kontrola.“*, članak 10. navodi: *„Osobe nadležne za prikupljanje informacija i uklanjanje ranjivosti dužne su otkrivene ranjivosti prijaviti Voditelju Odjela za sigurnost te s njim koordinirati načine i rokove njihovog otklanjanja. Prijava se vrši putem elektroničke pošte. Od ove obveze izuzet je SO.“,* točka 5. Prioritizacija i uklanjanje ranjivosti, članak 13. navodi: *„Za svaku ranjivost, sukladno utvrđenom prioritetu rješavanja, Voditelj Odjela za sigurnost, u konzultacijama s osobama nadležnim za prikupljanje informacija i uklanjanje ranjivosti, definira rok i način uklanjanja.“*, članak 14. navodi: „*Načini uklanjanja ranjivosti mogu biti: - instalacija sigurnosne zakrpe, - izmjene konfiguracije sustava, - izmjene programskog koda, - uklanjanje ranjive komponente IT sustava.“, članak 16. navodi: „Ukoliko određene ranjivosti nije moguće ukloniti iz tehničkih ili poslovnih razloga, potrebno je u planu za otklanjanje naznačiti razlog tome te predvidjeti primjerene kompenzirajuće mjere kojima će se rizik uslijed otvorene ranjivosti svesti na prihvatljivu mjeru.“,* članak 17. navodi*: „Mjere uklanjanja ranjivosti moraju biti primjereno testirane prije primjene u produkcijskim sustavima kako bi se osiguralo da njihova primjena neće narušiti stabilnost i funkcionalnost IT sustava. Testiranje promjena izvodi se sukladno Proceduri za upravljanje promjenama.“,* i konačno točka 6. Ponovljeno ispitivanje, članak 19. navodi: „*Voditelj Odjela za sigurnost ovlašten je zahtijevati ponovljeno ispitivanje specifične ranjivosti kako bi se steklo razumno uvjerenje da je ranjivost uklonjena i rizik sveden na prihvatljivu razinu.“.*

U odnosu na mjere koje je poduzeo voditelj obrade nakon predmetnog incidenta, predstavnica predmetnog voditelja obrade navodi: „*da je postavljen dodatni softverski alat za detekciju i sprječavanje lateralnog kretanja napadača na sustavu (Microsft APT), angažiran je dobavljač sustava web trgovine radi podizanja sigurnosnih zakrpa na svim dijelovima sustava, napravljen je deploy cjelokupne nove platforme za implementaciju sustava web trgovine uz postavljanje dodatnih mjera zaštite (promijenjene IP adrese, postojeći poslužitelji su zamijenjeni novim koji su ponovo instalirani i očvrsnuti posljednjim sigurnosnim nadogradnjama, instalirana je nova verzija aplikacije s važećim zakrpama softvera treće strane (Telerik UI), aktivirano je skupljanje log zapisa na svim relevantnim komponentama sustava s koje se pruža usluga web trgovine), u aplikaciju web trgovine ugrađene su dodatne mjere koje onemogućuju iskorištavanje ranjivosti udaljenog izvršavanja koda (eng. remote code execution), promijenjena su korisnička imena i zaporke koje sustav web trgovine koristi za povezivanje s ostalim sustavima s kojima komunicira u svrhu pružanja servisa web trgovine.“*.

Tijekom nadzora društvo voditelj obrade priložilo je Izvješće koje sadrži preslike ekrana i sistemske zapise, te navodi poduzete mjere zaštite nakon otklanjanja sigurnosnog incidenta, a koje je implementiralo društvo xy. na novim poslužiteljima koji su ponovo instalirani i očvrsnuti sigurnosnim zakrpama i koje navodi; „*Kupljena je najnovija verzija Progress Telerik Web UI komponenti 2020.2.617.40 (R2 2020 SP1) za koju je forenzičkom istragom od strane voditelj obrade u suradnji s tvrtkom __ otkriveno da je inicijalni vektor napada tj. da je iskorišten security propust CVE-2019-18935 koji omogućuje upload exacutable datoteka kroz bug u deserijalizaciji koji je prisutan unutar komponente za asinkroni upload, - proširen je scope IIS logova, uključene su dodatni parametri o veličinama payloada (incoming/outgoing bytes kao i custom server varijable za forwarding IP adresa kroz laod-balancing (x-forwarded-for)), - implementirana su dodatna IIS rewrite pravila za ograničavanje izvršavanja active server pages s lokacija koje nisu „whitelisted“, - Izmjena logike managementa user-uploaded sadržaja kroz automatsku migraciju na private lokacije izvan DFSR volume-a, - implementirana su dodatna IIS rewrite pravila za web aplikaciju, - provedena je interna revizija koda aplikacije i uklonjene su legacy stranice i nekorišteni kod koji je sadržavao mogućnost uploada ili form post-a s ---..hr web aplikacije, - implementirana su dodatna IIS pravila za preusmjeravanje URL-ova koja će onemogućiti daljinsko izvršavanje .as(p|h) x datoteka s mjesta na kojima se takva izvedba ne očekuje kako redovan rad web aplikacije ---.hr, - promijenjena je poslovna logika same aplikacije na način da se datoteke krajnjeg korisnika s CMS servera koji je smješten u DMZu automatski, istog trenutka po unosu, prenose u privatnu mapu gdje je pristup ograničen samo na back-office zaposlenike, pa se tako potencijalna mogućnost kompromitacije osobnih podataka umanjuje na još manju moguću mjeru, tj. batch skripta automatski se izvršava svakih 60 sekundi na razini CMS servera kojoj je zadatak da user-uploaded sadržaj preseli u private folder koji nije dostupan kroz browser, - dodan je i IIS rewrite rule kojim je spriječeno preuzimanje dotičnih datoteka (koje se ionako automatski premještaju) iz konteksta ---web aplikacije, - promijenjena su korisnička imena i zaporke koje sustav web shopa koristi za povezivanje s ostalim sustavima s kojima sustav komunicira u svrhu pružanja servisa web shopa, te novi više nisu pohranjeni u plain text formatu, već su enkriptirani s X509 certifikatom, - komunkacija s AIWS-om (Aduro web servisi*

za provizioniranje između sustava) je prebačen na drugi HTTPS endpoint za koji je potreban dodatan client X509 certifikat, dok su svi credentialsi u web.config datoteci enkriptirani drugim X509 certifikatom čiji thumbprint je embedded unutar binary datoteke web aplikacije. Oba certifikata instalirana su u certificate store na svim serverima.

Xy d.o.o. dodatno navodi da je: *"U suradnji s ---započeta integracija --- Digitalne Arhive kao jednog mjesta pohrane datoteka koje sadrže podatke o korisnicima (osobna iskaznica, ZZPO obrazac, maloprodajni račun, sales audit log, MNP obrazac, OSX prijevoznice). Svaki dokument ima određene triggere za pohranu i update ovisno o poslovnom procesu, a svaka pohrana se vrši uz postavljeni expiration date čime je ujedno inkorporirana i politika pravila čuvanja istih. Uz pravila čuvanja, za svaki dokument postoji i pravilo pristupa od strane a) samih korisnika, b) back-office agenata i administratora sustava, ukoliko to poslovni proces zahtjeva – npr. provjera ispravnosti osobne iskaznice. Projekt je trenutno u fazi testiranja s obzirom na kompleksnost poslovnih procesa.*

Nastavno na provedeni nadzor kod društva voditelj obrade d.o.o. 18. rujna 2020., isto društvo je dostavilo Agenciji 06. listopada 2020. dopunu informacija o predmetnoj povredi/sigurnosnom incidentu, a koje između ostalog sadrži očitovanje društva __d.o.o. od 25. rujna 2020. koje je provelo forenzičku analizu poslužitelja i koje navodi da su: „*analizom datoteka na kompromitiranom poslužitelju pronađene datoteke s potpisima hackerske skupine (tzv. defacement datoteke). Hackerske skupine često ostavljaju ovakve datoteke kako bi označile kompromitirane poslužitelje. Primjer jedne datoteke s potpisom dan je u nastavku. Prikazana datoteka potpis je VLS3C hackerske grupe iz Vijetnama. Dodatnom analizom materijala dostupnih na Internetu identificiran je i facebook kanal grupe (https://www.facebook.com/pg/Krzambie/videos/) gdje se, između ostalih, nalazi i video zapis s uputama kako napasti ranjive Telerik instalacije, što odgovara analiziranom napadu. U svrhu identifikacije brojeva korisnika na poslužitelju analizirane su sve dostupne datoteke u nekoliko koraka. Analiza je napravljena specijalnim skriptama i programima razvijenim od strane Infiga, a čiji je cilj bio identificiranje datoteka koje sadrže korisničke podatke. Analizom tipova datoteka prvo su uklonjeni duplikati u slučaju kada je datoteka istog naziva i vremenske značke imala različite rezolucije i formate (sve datoteke su bile pohranjene u dvije rezolucije, identičnog sadržaja). Nakon ovog koraka provedeno je uklanjanje identičnih datoteka korištenjem izračuna SHA1 kriptografskog sažetka. Dvije datoteke, neovisno o nazivu i vremenskoj znački, ako imaju isti SHA1 kriptografski sažetak su identične te je riječ o duplikatu koji je uklonjen. Nakon ovih koraka dobiven je konačan broj od 44236 datoteka u direktoriju s najvećim brojem datoteka, dok su ostali direktoriji sadržavali podskup ovih datoteka, gdje je riječ o različitim direktorijima korištenim tijekom rada aplikacije. Voditelj obrade je nad ovim skupom datoteka u svrhu točne identifikacije broja korisnika proveo obradu sadržaja datoteka."*.
Istom izvješću kao dokaz prilažu preslike osobnih iskaznica za nekoliko ispitanika, a koje su dobivene forenzičkom analizom.

Agencija je dopisom KLASA:042-03/20-01/55, URBROJ:567-12/07-20-24 od 17. prosinca 2020. zatražila društvo xy d.o.o. očitovanje o predmetnoj povredi i dostavu relevantne

dokumentacije i informacija o tome kada je društvo xy d.o.o. saznalo tj. postalo svjesno sigurnosnog incidenta navedenog u izvješću od 03.srpnja 2020., pri tome navesti datum, da li je o tome izvijestilo voditelja obrade temeljem članka 33. stavka 2. Opće uredbe o zaštiti podataka, je li društvo d.o.o. o predmetnom incidentu obaviješteno od strane društva d.o.o., društva iz ___ili iz vlastitih izvora, ima li društvo d.o.o. ima implementirano tehničko rješenje putem kojeg može primijetiti pojavu malicioznog "koda" na poslužitelju kojem ima pristup temeljem ugovornog odnosa s društvom (voditelj obrade).

Uvidom u zaprimljeno očitovanje xy d.o.o. od 11. siječnja 2021. isti, između ostalog, navodi se da je*: "Društvo xy d.o.o. "25. lipnja 2020. u 13:45 primio e-mail obavijest od tima IT infrastrukture ___o pojavi potencijalno maliciozne datoteke na jednom od web poslužitelja te upit za provjerom je li navedena datoteka legitimni dio aplikacije. Email obavijest uključuje screenshot s putanjom datoteke na poslužitelju koji su zaprimili od ___. Odmah po primitku obavijesti od ____ izvršene su provjere kompletne IT infrastrukture unutar društva d.o.o. uključujući sva računala zaposlenika društva d.o.o. sva terminalna oprema te pregled svog izvornog koda na kojima nisu pronađene nikakve ranjivosti. Svi poslužitelji na kojima se nalazi web aplikacija razvijena od strane društva d.o.o. za nalaze se na infrastrukturi koju je omogućila i konfigurirala te koju održava xy. Društvo xy d.o.o. ima usko ograničene korisničke račune na tim poslužiteljima te nema mogućnost administracije poslužitelja na razini operativnog sustava, niti mogućnost instalacija aplikacija na servisnoj razini ili izmjene konfiguracije operativnog sustava, već isključivo prava za administraciju web aplikacija za potrebe funkcionalnih nadogradnji.*

Isti dodatno navode: „*U nastavku je opis akcija koje su učinjene od strane društva d.o.o. u suradnji s xy odmah po potvrdi vektora napada s ciljem otklanjanja konkretnog sigurnosnog propusta te prevencijom eventualnih budućih napada koji se baziraju sličnoj mehanici kao i CVE-2019-18935; - izvršena je kupovina najnovije verzije Telerik UI komponenti – 2020.2.617.40 (R2 2020 SP1–koje ne sadrže navedeni propust, instalacija i prilagodba web aplikacija), - promijenjeni su X509 certifikati koji se koriste za enkripciju konfiguracijskih postavki aplikacija i autentifikaciju klijenata te svi hash i enkripcijski ključevi, - postavljeni su dodatni filteri i pravila za sve resurse koji na poslužitelj dospijeva putem web aplikacije, kao i za pristup istima s ciljem smanjenja površine, - dodani su url-redirect pravila na razini HTTP modula koje onemogućuju izvršavanje aplikativnog koda osim na lokacijama gdje je to zaista potrebno, tj. gdje je to neophodno za normalan rad aplikacije.*

Isti također navode: *„Nastavno na akcije izvedene neposredno nakon sigurnosnog incidenta, učinjen je niz mjera u suradnji s ___kako bi se dodatno povećala sigurnost aplikacije te smanjila ranjiva površina (surface area) za eventualne buduće napade: - od strane ___pokrenut je proces migracije kompletne hosting platforme u data centar koji će biti pod kontrolom ___a ne pod kontrolom___. Nakon migracije ___d.o.o. imat će mogućnost bolje administracije poslužitelja iz svih aspekata pa tako i sigurnosnog te će biti u mogućnosti i društvu d.o.o. osigurati alate za monitoring performans i health-checking aplikacija, - paralelno s navedenom tehničkom migracijom pokrenut je proces i restrukturiranje samih aplikacija s ciljem smanjenja odgovornosti pojedine aplikacije kroz razdvajanje u mikro-*

servise s naglaskom na odvajanje prezentacijske i poslovne logike, kao i uvođenje procesa automatiziranog postavljanja promjena u produkcijsko okruženje. Osim funkcionalnih benefita, iz sigurnosne perspektive bitno za naglasiti jest da će svi servisi koji imaju pristup bilo kojoj bazi podataka biti uvijek smješteni u privatnu mrežu te da će im front-end aplikacije koje su izložene prema internetu, odnosno krajnjim korisnicima, uvijek pristupati putem specijaliziranih web servisa s precizno definiranim upitima, - u skladu s pripremama za novu hosting platformu započet je i proces migracije svih aplikacija na .net core platformu kako bi se iskoristili svi benefiti nove platforme u smislu i sigurnosti i performansi te kako bi ih bilo moguće instalirati i na Linux poslužitelje ili kao docker containers, gdje bi se Windows kao operativni sustav u potpunosti izbjegao, - završen je projekt integracije ___digitalne arhive putem kojeg se u potpunosti izbjegava pohrana svih datoteka koje se putem web aplikacije poslužuju krajnjim korisnicima ili krajnji korisnici dostavljaju ___ d.o.o. osim naravno za vrijeme samog transfera koji se odvija iza HTTPS-a.".

Agencija je dopisom KLASA: 042-03/20-01/55 URBROJ: 567-12/07-21-27 od 08. veljače 2021. zatražila od __Hrvatska d.o.o. (kao pravnog sljednika društva ___d.o.o.) dodatno očitovanje i dostavu preslike sistemskih zapisa/operativnih zapisa (log files) i drugih zapisa s poslužitelja zahvaćenih predmetnom povredom iz kojih je razvidno da u nadnevke navedene u izvješću o povredi osobnih podataka od 03. srpnja 2020. (29.04. i 07.05.2020.) nije došlo do izvoza osobnih podataka ispitanika od strane napadača kako se navodi u istom izvješću, te preslike podatkovnog sustava (datoteka) iz kojih je razvidan navod da su napadači iz predmetne povrede ostavili na poslužitelju/ima datoteke s potpisima (tzv. defacement datoteke).

Uvidom u zaprimljeno dodatno očitovanje ___Hrvatska d.o.o. od 19. veljače 2021. isti prilažu preslike sistemskih zapisa/operativnih zapisa (log files) za nadnevke 29.04. i 07.05.2020., presliku datoteke s potpisom hakerske skupine VLS3C iz Vijetnama (tzv. defacement datoteke) te navode da se iz dostavljenih preslika zapisa ne može utvrditi da je dana 29.04. i 07.05.2020. došlo do takvog prometa podataka iz kojih proizlazi izvoz osobnih podataka ispitanika od strane napadača, da su iz dostavljenih preslika zapisa vidljive samo one radnje odnosno aktivnosti iz kojih proizlazi svakodnevna i uobičajena korisnička aktivnost na Web shopu. Dodatno ističu da je __Hrvatska d.o.o. pisanim putem izvijestio korisnike usluga i/ili druge fizičke osobe o potencijalnoj povredi osobnih podataka, da su putem email komunikacije zaprimili sedamdesetak upita glede obavijesti koje su poslali navedenim korisnicima, te da do nadnevka očitovanja nisu zaprimili niti jednu prijavu zlouporabe osobnih podataka zahvaćenih korisnika odnosno trećih fizičkih osoba, niti su protiv ___isti korisnici odnosno druge fizičke osobe temeljem članka 82. stavak 6. Opće uredbe o zaštiti podataka pokrenule sudski postupak za ostvarivanje prava na naknadu štete.
Agencija je izvršila uvid u dostavljene preslike sistemskih zapisa/operativnih zapisa (log files) od 29.04. i 07.05.2020. i presliku datoteke s potpisom hakerske skupine VLS3C iz Vijetnama (.aspx) te potvrdila navode ___Hrvatska d.o.o. iz njihovog očitovanja od 19. veljače 2021.

Agencija ističe da se od 25. svibnja 2018. godine u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno i obvezujuće primjenjuje Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom

osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (SL EU L119).

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.

Člankom 5. stavkom 1. Opće uredbe o zaštiti podataka propisano je da osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); 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); primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju (načelo smanjenja količine podataka); točni i prema potrebi ažurni (načelo točnosti); čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju (načelo ograničenja pohrane) i obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neodgovarajuće ili nezakonite obrade te od slučajnog gubitka ili uništenja, primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Člankom 28. stavkom 1. Opće uredbe o zaštiti podataka propisano je da ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika. Temeljem stavka 3. istoga članaka, obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. Tim se ugovorom ili drugim pravnim aktom osobitom određuje da izvršitelj obrade, između ostalog temeljem točke c) istoga stavka, poduzima sve potrebe mjere u skladu s člankom 32.

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 društvo d.o.o. kao izvršitelj obrade, koji temeljem *Ugovora o održavanju i kontinuiranom razvoju programskih rješenja* od 17. travnja 2017. voditelju obrade pruža usluge zaštite obrade osobnih podataka poduzimajući sve potrebne tehničke, organizacijske, sigurnosne i kadrovske mjere, kao i razvoj i implementaciju programskih rješenja, provodi kontrole za detekciju, prevenciju i oporavak od malicioznih softvera, te temeljem *Ugovora o obradi podataka* od 24. svibnja 2018. osigurava da ima odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke koje obrađuje od uništenja, izmjene, zabranjenog odavanja i neovlaštenog pristupa, propustio izvršiti sigurnosnu nadogradnju aplikacije Telerik UI, za koju je postojala javno dostupna ranjivost CVE-2019-18935 i koju su iskoristili napadači te u nadnevke 29.04.2020. i 07.05.2020. ostvarili pristup na kompromitirane javno dostupne front-end poslužitelje ___koji podržavaju procese odnosno usluge; web stranicu, web shop, proces beskontaktnog plaćanja u kanalima udaljene prodaje (sales) i samostalnu dostavu robe, postavili tzv. *web shell* aplikaciju (shell.aspx na poslužitelju), koja im je omogućila daljnje izvršenje komandi pod privilegijama IIS korisnika pod kojim je bila pokrenuta i web aplikacija.
Napadači su između ostalog, dohvatili i glavnu konfiguracijsku datoteku u kojoj su pohranjeni višestruki parovi aplikativnih kredencijala (korisničkih imena i zaporki), te enkripcijskih ključeva koje su tijekom rada koristile ___aplikacije. Ovi podaci su između ostalog uključivali i podatke za spajanje web aplikacije na MS SQL bazu podataka. Identificirane su višestruke datoteke koje sadrže osobne podatke te su iste bile dostupne korisničkom računu pod kojim je pokrenut IIS web poslužitelj, odnosno korisničkom računu pod kojim je napadač bio u mogućnosti pokretati komande te dohvaćati datoteke. Forenzičkom analizom kompromitiranih poslužitelja utvrđeno je da su napadačima učinjene dostupne datoteke koje sadrže osobne podatke 28085 ispitanika.

Agencija je utvrdila da jed.o.o. koji je bio zadužen da temeljem *Pravilnika o upravljanju ranjivostima* od 03. prosinca 2018. usvojenog od strane___. prikuplja informacije i otkriva ranjivosti za poslovne aplikacije i o tome izvješćuje Voditelja Odjela za sigurnost___., te zbog ne poduzimanja mjera zaštite obrade osobnih podataka temeljem *Ugovora o održavanju i kontinuiranom razvoju programskih rješenja* od 17. travnja 2017. a koje između ostalog uključuju i provjeru postojanja poznatih sigurnosnih ranjivosti/rizika kao primjerice putem OWASP Top 10 (web stranica s top 10 sigurnosnih rizika za web aplikacije) i uklanjanja istih, propustom provođenja obveza izvršitelja obrade omogućio napadačima/vijetnamskim hakerima pristup podatkovnom sustavu/datotekama na poslužiteljima voditelja obrade koje sadrže osobne podatke 28085 ispitanika.

Također je utvrđeno da je d.o.o. omogućio napadačima pristup osobnim podacima 28085 ispitanika zbog nepoduzimanja odgovarajućih tehničkih mjera sigurnosti, uslijed čega su napadači postavili maliciozni „kod“ na __web aplikaciju, a čime im je omogućeno daljinsko izvršavanje naredbi nad datotekama s mjesta na kojima se takva aktivnost ne očekuje odnosno ne predstavlja redovan rad web aplikacije ___.

d.o.o. navodi da je osim redovnih sigurnosnih mjera koje poduzima prilikom izrade aplikacija (Privacy & Security by Design), prije predmetne povrede (sigurnosnog incidenta) u suradnji s ___Hrvatska d.o.o. poduzeo i određene mjere bitne u smislu zaštite podataka krajnjih korisnika aplikacija; da je definirana politika čuvanja svakog osobnog transakcijskog podatka unutar baza i aplikacija, kao i pravilo pristupa u smislu potrebnih ovlasti i trajanja pristupa i pohrane podataka, da se svi upiti na baze podataka vrše isključivo kroz *stored procedures* i da u kodu aplikacija pa samim time niti u assembly-u koji završi na samim poslužiteljima ne postoji niti jedan inline upit na bazu što ima za cilj eliminiranje mogućnosti ubacivanja malicioznog koda u same baze podataka i kontrolirano čitanje podataka, te mogućnost pseudonimizacije osobnih podataka već na samom izvoru podataka u skladu s politikom čuvanja osobnih podataka. d.o.o. navodi da je u 2018. godini izvršeno penetracijsko testiranje od strane tvrtke __ d.o.o. unutar kojeg nisu uočeni kritični nedostaci, a svi manji nedostaci su promptno otklonjeni.

Međutim, pored navedenih mjera sigurnosti na podatkovnom nivou (baze podataka), iz spisa predmeta je razvidno da izvršitelj obrade nije poduzeo dovoljne, odnosno, odgovarajuće tehničke mjere sigurnosti na aplikativnom nivou prije sigurnosnog incidenta/predmetne povrede osobnih podataka, a koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu. Pri tom je ključno uzeti u obzir da se u predmetnom slučaju radi o izvršitelju obrade koji je prema javno dostupnim informacijama društvo koje pruža informatičke usluge i drugim mobilnim operaterima, bankama i državnim institucijama u Republici Hrvatskoj, da obrada osobnih podataka kod navedenih voditelja obrade obuhvaća veliki broj ispitanika i time bi predmetni izvršitelj obrade trebao posvećivati veću pozornost tehničkim mjerama zaštite implementiranim kroz informacijsku tehnologiju imajući u vidu opseg osobnih podataka koji mogu biti kompromitirani uslijed možebitnog sigurnosnog incidenta, i da isto tako navedeni izvršitelj obrade pruža informatičke usluge i tvrtkama u SAD-u, Velikoj Britaniji, Nizozemskoj, Švedskoj, Rusiji, Sloveniji i dr.

Iz prethodno navedenih odredbi Opće uredbe o zaštiti podataka proizlazi da je izvršitelj obrade prilikom obrade osobnih podataka dužan poduzeti odgovarajuće 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 točno i potpuno utvrđenog činjeničnog stanja razvidno je da je izvršitelj obrade propustio provesti odgovarajuće tehničke mjere sigurnosti 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.

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 upravno 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 upravno 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 izvršitelja 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 izvršitelja obrade.

Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog izvršitelja 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 istog kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja istog kršenja).

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 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 (uvodna izjava 10 Opće uredbe o zaštiti podataka). U uvodnoj izjavi 11 pojašnjava se činjenica da su za jednaku razinu zaštite osobnih podataka diljem Unije potrebne, među ostalim, "jednake ovlasti praćenja i osiguravanja poštovanja pravila za zaštitu osobnih podataka i jednake sankcije za kršenja u državama članicama". Nadalje, kako je navedeno u uvodnoj izjavi 13, 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. 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.

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 Agencija je utvrdila da su osnivači i ujedno i članovi društva d.o.o.

Budući da ukupni godišnji promet na svjetskoj razini u 2019. godini za društvo B d.o.o. iznosi 3 943 292,06 kn, 2% tog iznosa je 78 865,84 kn, isti ne predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju, jer je navedeni iznos manji od 10 000 000 EUR. Navedeni podaci su javno dostupni na mrežnim stranicama Financijske Agencije (Fina).

Agencija je radi kršenja članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti osobnih podataka izrekla izvršitelju obrade društvu

d.o.o. upravnu novčanu kaznu u iznosu od 230.000,00 kn, a koji iznos čini 0,30 % 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 izvršitelja obrade iz članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti podataka, neprovođenjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka od strane društva d.o.o. kao izvršitelja obrade za društvo__. (pravni prednik društva __Hrvatska d.o.o.) kao voditelja obrade, 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.

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 ovoj upravnoj stvari utvrđeno je da je d.o.o. propustio izvršiti sigurnosnu nadogradnju aplikacije Telerik UI, za koju je postojala javno dostupna ranjivost CVE-2019-18935 i koju su iskoristili napadači te u nadnevke 29.04.2020. i 07.05.2020. ostvarili pristup na kompromitirane javno dostupne front-end poslužitelje ___koji podržavaju procese odnosno usluge; web stranicu, web shop, proces beskontaktnog plaćanja u kanalima udaljene prodaje (sales) i samostalnu dostavu robe, postavili tzv. *web shell* aplikaciju (shell.aspx na poslužitelju), koja im je omogućila daljnje izvršenje komandi pod privilegijama IIS korisnika pod kojim je bila pokrenuta i web aplikacija.
Napadači su između ostalog, dohvatili i glavnu konfiguracijsku datoteku u kojoj su pohranjeni višestruki parovi aplikativnih kredencijala (korisničkih imena i zaporki), te enkripcijskih ključeva koje su tijekom rada koristile aplikacije. Ovi podaci su između ostalog uključivali i podatke za spajanje web aplikacije na MS SQL bazu podataka. Identificirane su višestruke datoteke koje sadrže osobne podatke te su iste bile dostupne korisničkom računu pod kojim je pokrenut IIS web poslužitelj, odnosno korisničkom računu pod kojim je napadač bio u mogućnosti pokretati komande te dohvaćati datoteke. Forenzičkom analizom kompromitiranih poslužitelja utvrđeno je da su napadačima učinjene dostupne datoteke koje sadrže osobne podatke 28085 ispitanika.

U predmetnoj povredi osobni podaci 28085 ispitanika su zbog nepoduzimanja odgovarajućih tehničkih mjera zaštite web aplikacije koja je korištena u poslovnim procesima voditelja obrade društva xx učinjeni dostupni neovlaštenim osobama. Nadalje, ista povreda ne može se iskazati u vremenskom kontinuitetu jer se radilo o neovlaštenom pristupu osobnim podacima u dva navrata, no navedeno u bitnome ne utječe na težinu predmetne povrede jer su napadači/vijetnamski hakeri, kada su ostvarili pristup datotekama na kompromitirane poslužitelje, bili u mogućnosti izvesti osobne podatke ispitanika u kratkom vremenu.

- 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 "ne donošenje politika" i "ljudsku pogrešku" kao primjere ponašanja koji mogu ukazivati na nepažnju.

U odnosu na navedeno, u predmetnom slučaju nije utvrđeno da je bilo izravne namjere kršenja odredbi Opće uredbe o zaštiti podataka od strane d.o.o., ali je utvrđen nemar i nedostatak radnji koje bi prevenirale povredu. Naime, u ovoj upravnoj stvari utvrđeno je da je d.o.o. kao izvršitelj obrade propustio prikupljati informacije i otkrivati ranjivosti dijela IT sustava voditelja obrade za koje je nadležan za razvoj i održavanje a koje je bio dužan temeljem *Pravilnika o upravljanju ranjivosti od 03. prosinca 2018.,* zatim provjeravati postojanje poznatih sigurnosnih ranjivosti/rizika putem javno dostupnih informacija kao što je web stranica OWASP Top 10, a kako je isto navedeno u *Ugovoru o održavanju i kontinuiranom razvoju programskih rješenja* od 17. travnja.2017., te konačno temeljem *Ugovora o obradi podataka* od 24. svibnja 2018. osigurati da ima odgovarajuće tehničke i organizacijske mjere 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 su javno dostupnu ranjivost CVE-2019-18935 aplikacije Telerik UI koju je koristio d.o.o. u IT sustavu voditelja obrade, iskoristili napadači/vijetnamski hakeri te ostvarili pristup osobnim podacima 28085 ispitanika pohranjenim na kompromitiranim poslužiteljima voditelja obrade, a čime su ispunjeni svi elementi grube nepažnje u postupanju.

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

Nastavno na predmetnu povredu od 29.04.2020. i 07.05.2020. i saznanja o istoj na nadnevak 25. lipnja 2020., d.o.o. je odmah pristupio rješavanju nastalog sigurnosnog problema na način da je 30. lipnja 2020. izvršio kupovinu najnovije verzije Telerik UI komponenti – 2020.2.617.40 (R2 2020 SP1–koje ne sadrže navedeni propust vezan uz prethodnu verziju), promijenjeni su X509 certifikati koji se koriste za enkripciju konfiguracijskih postavki

aplikacija i autentifikaciju klijenata te svi hash i enkripcijski ključevi, postavljeni su dodatni filteri i pravila za sve resurse koji na poslužitelj dospijevaju putem web aplikacije, kao i za pristup istima, dodani su url-redirect pravila na razini HTTP modula koje onemogućuju izvršavanje aplikativnog koda osim na lokacijama gdje je to zaista potrebno, tj. gdje je to neophodno za normalan rad aplikacije.

Isto društvo je naknadno poduzelo i druge radnje u suradnji s voditeljem obrade kako bi mogućnost incidenta iste ili slične prirode sveo na najmanju moguću mjeru na način da je voditelj obrade pokrenuo proces migracije kompletne hosting platforme u data centar koji će biti pod kontrolom istog, a ne pod kontrolom___, te će nakon migracije imat mogućnost bolje administracije poslužitelja iz svih aspekata pa tako i sigurnosnog te će biti u mogućnosti i društvu d.o.o. osigurati alate za monitoring performans i health-checking aplikacija, da je paralelno s navedenom tehničkom migracijom pokrenut proces i restrukturiranje samih aplikacija s ciljem smanjenja odgovornosti pojedine aplikacije kroz razdvajanje u mikro-servise s naglaskom na odvajanje prezentacijske i poslovne logike, kao i uvođenje procesa automatiziranog postavljanja promjena u produkcijsko okruženje, da će svi servisi koji imaju pristup bilo kojoj bazi podataka biti uvijek smješteni u privatnu mrežu te da će im front-end aplikacije koje su izložene prema internetu, odnosno krajnjim korisnicima, uvijek pristupati putem specijaliziranih web servisa s precizno definiranim upitima, da je u skladu s pripremama za novu hosting platformu započet i proces migracije svih aplikacija na .net core platformu kako bi se iskoristili svi benefiti nove platforme u smislu i sigurnosti i performansi te kako bi ih bilo moguće instalirati i na Linux poslužitelje ili kao docker containers, gdje bi se Windows kao operativni sustav u potpunosti izbjegao, da je završen projekt integracije digitalne arhive voditelja obrade putem kojeg se u potpunosti izbjegava pohrana svih datoteka koje se putem web aplikacije poslužuju krajnjim korisnicima ili krajnji korisnici dostavljaju voditelju obrade osim naravno za vrijeme samog transfera koji se odvija iza HTTPS-a.“.

- 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 d.o.o. provodi određene tehničke mjere zaštite pri obradi osobnih podataka, ali da u konkretnom slučaju nisu prikupljali informacije i uklanjali ranjivosti u poslovnim aplikacijama za čiji su razvoj i održavanje bili nadležni, čime je došlo do neovlaštenog pristupa osobnim podacima 28085 ispitanika. Naime, u ovoj upravnoj stvari utvrđeno je da je d.o.o. kao

izvršitelj obrade propustio prikupljati informacije i otkrivati ranjivosti dijela IT sustava voditelja obrade za koje je nadležan za razvoj i održavanje a koje je bio dužan temeljem *Pravilnika o upravljanju ranjivosti od 03. prosinca 2018.,* zatim provjeravati postojanje poznatih sigurnosnih ranjivosti/rizika putem javno dostupnih informacija kao što je web stranica OWASP Top 10, a kako je isto navedeno u *Ugovoru o održavanju i kontinuiranom razvoju programskih rješenja* od 17. travnja.2017., te konačno temeljem *Ugovora o obradi podataka* od 24. svibnja 2018. osigurati da ima odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke koje obrađuje, odnosno zaštitio osobne podatke od uništenja, izmjene, zabranjenog odavanja i neovlaštenog pristupa

Odgovornost izvršitelja obrade tim je veća što je društvo xx kao voditelj obrade, za provođenje zaštite obrade osobnih podataka ispitanika sadržanih u njegovim evidencijama, angažirao izvršitelja obrade - društvo specijalizirano za pružanje informatičkih usluga. d.o.o., prema javno dostupnim informacijama, ujedno pruža usluge i drugim mobilnim operaterima, bankama i državnim institucijama u Republici Hrvatskoj. Isto tako, navedeni izvršitelj obrade pruža informatičke usluge i tvrtkama u SAD-u, Velikoj Britaniji, Nizozemskoj, Švedskoj, Rusiji, Sloveniji i drugima, te je stoga voditelj obrade mogao opravdano očekivati visoki stupanj stručnog znanja u pogledu osiguranja odgovarajućih tehničkih mjera zaštite sigurnosti obrade osobnih podataka.

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

Prema evidencijama kršenja koje vodi ova Agencija, društvo d.o.o. nije u prošlosti počinilo istovjetno kršenje niti je prekršilo Opću uredbu o zaštiti podataka na istovjetan način.

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

Društvo d.o.o. je tijekom ovog upravnog postupka na odgovarajući način odgovaralo na zahtjeve nadzornog tijela.

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

Datoteke na kompromitiranim poslužiteljima predmetne povrede sadrže ugovore za zasnivanje pretplatničkog odnosa, skenove/fotografije osobnih iskaznica i datoteke s ugovornom dokumentacijom za zasnivanje pretplatničkog odnosa ispitanika, a iz kojih je moguće utvrditi sljedeće kategorije osobnih podataka: ime i prezime, datum rođenja, adresa, potpis, OIB, fotografija, broj osobne iskaznice, broj telefona i e-mail adresa, a koji čine osnovne identifikacije osobne podatke.

- 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);

Člankom 33. stavkom 2. Opće uredbe o zaštiti podataka propisano je da izvršitelj obrade bez nepotrebnog odgađanja izvješćuje voditelja obrade nakon što sazna za povredu osobnih podataka. Za predmetnu povredu nadzorno tijelo je saznalo od strane voditelja obrade putem zaprimljenog Izvješća o povredi osobnih podataka sukladno članku 33. stavku 1. Opće Uredbe o zaštiti podataka od 03. srpnja 2020. U tijeku postupka izvršitelj obrade d.o.o. je priložio informacije i dokaze da je za predmetnu povredu saznao dana 25. lipnja u 13:45 sati putem zaprimljene e-mail poruke od tima IT infrastrukture ___o pojavi potencijalno maliciozne datoteke na poslužitelju ___(poslužitelj smješten na infrastrukturi u ___) te s upitom za provjerom je li navedena datoteka legitimni dio aplikacije, kojoj poruci je bio priložen screenshot s putanjom datoteke na poslužitelju koji su primili od ___d.o.o. je također u svom očitovanju od 11. siječnja 2021. naveo da se svi poslužitelji na kojima se nalazi web aplikacija razvijena od strane društva d.o.o. za___ d.o.o. nalaze na infrastrukturi koju je omogućila i konfigurirala te koju održava društvo___, da društvo d.o.o. ima usko ograničene korisničke račune na tim poslužiteljima te nema mogućnost administracije poslužitelja na razini operativnog sustava, već isključivo prava za administraciju web aplikacije za potrebe funkcionalne nadogradnje.

Također, imajući u vidu navode društva d.o.o. iz istog očitovanja od 11. siječnja 2021., da nemaju niti će imati implementirano vlastito tehničko rješenje za detekciju malicioznog koda ili sadržaja, već je sigurnosna nadogradnja takvog rješenja izvršena od strane ___na razini svih poslužitelja u grupi, te specifičnost predmetne povrede za koju izvršitelj obrade nije mogao saznati prije voditelja obrade, Agencija je utvrdila da d.o.o. nije u konkretnom slučaju bio u mogućnosti ispuniti obvezu iz članka 33. stavka 2. Opće uredbe o zaštiti podataka prema voditelju obrade.

- 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);

Društvu 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);

Nije utvrđeno da je d.o.o. ostvario financijsku dobit kršenjem niti izbjegnuo gubitke, izravno ili neizravno. Međutim, Agencija otegotnom okolnošću nalazi u činjenici da je osnovna

djelatnost društva d.o.o. razvijanje i implementiranje web aplikacija koje uključuju i „privacy by design“, da je navedeno društvo, prema javno dostupnim informacijama društvo koje pruža informatičke usluge i drugim mobilnim operaterima, bankama i državnim institucijama u Republici Hrvatskoj, da isto tako navedeni izvršitelj obrade pruža informatičke usluge i tvrtkama u SAD-u, Velikoj Britaniji, Nizozemskoj, Švedskoj, Rusiji, Sloveniji i drugima, te bi stoga trebao biti relevantni subjekt u davanju mišljenja, smjernica, savjeta i predlagati rješenja voditeljima obrade o implementaciji web aplikacija, koje će istovremeno ispuniti poslovna očekivanja istih, ali i uključiti osmišljavanje i provedbu odgovarajućih tehničkih mjera zaštite obrade osobnih podataka.

Zaključno, iz svega navedenog proizlazi da je izvršitelj obrade d.o.o. propustio provesti odgovarajuće tehničke mjere sigurnosti obrade 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, što je dovelo do neovlaštenog pristupa od strane napadača/vijetnamskih hakera osobnim podacima 28085 ispitanika sadržanih na poslužiteljima voditelja obrade.

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.

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 Zagrebu u roku od 30 dana od dana dostave rješenja.

RAVNATELJ
Zdravko Vukić mag.oec.

Dostaviti:
1. Pismohrana, ovdje
2. Društvo XY