REPUBLIKA HRVATSKA
OPĆINSKI PREKRŠAJNI SUD U ZAGREBU
Zagreb, Avenija Dubrovnik 8

Poslovni broj: 24. Pp-15921/2022

U IME REPUBLIKE HRVATSKE

PRESUDA

Općinski prekršajni sud u Zagrebu, po sutkinji Tonki Grgičević uz sudjelovanje Jadranke Povoljnjak, kao zapisničarke, u prekršajnom predmetu protiv okrivljene pravne osobe A1 Hrvatska d.o.o., predstavljen po prema punomoći, zastupan po branitelju odvjetniku zbog prekršaja iz čl. 119.st.1.točka 58. Zakona o elektroničkim komunikacijama (Narodne novine br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), povodom optužnog prijedloga Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM), nakon glavne i javne rasprave održane u nazočnosti okrivljenika, dana 27. ožujka 2023. godine javno je objavio i

presudio

I. Okrivljenik: A1 Hrvatska d.o.o. – pravna osoba, Zagreb, Vrtni put 1, OIB 29524210204, operatora javnih komunikacijskih mreža i operatora javno dostupnih elektroničkih komunikacijskih usluga

kriv je

što u Zagrebu, na adresi sjedišta okrivljene pravne osobe, dana 8. veljače 2022. godine, u 15:14 sati, kada je poslao elektroničku poruku društvu D d.o.o. sa zahtjevom za izradom forenzičkog izvješća, i sa sigurnošću raspolagao informacijom o sigurnosnom incidentu, nije bez odgode, čim su podaci o sigurnosnom incidentu bili dostupni, a najkasnije do 16:14 sati navedenog dana, upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način, te putem PiXi platforme, izvijestio HAKOM o sigurnosnom incidentu koji je prema navodima A1 Hrvatska d.o.o. (dalje: A 1) uzrokovan neovlaštenim pristupom sustavu A 1 uz prijetnju objavljivanja neovlašteno stečenih osobnih podataka preko 100.000 broja korisnika A1 (dalje: incident), sukladno obvezi propisanoj člankom 99. stavak 7. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), člankom 6. stavak 3. i člankom 7. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21; dalje: Pravilnik) kojim je propisana obveza operatora da u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, putem predloška propisanog u Dodatku 3. izvijesti Agenciju o nastalom incidentu, te putem PiXi platforme, na način propisan člankom 7. Pravilnika, a što je A 1 učinio tek 9. veljače 2022. godine, i to temeljem naknadne upute HAKOM-a,

a što je sve utvrđeno od strane inspektora elektroničkih komunikacija HAKOM-a u provedenom inspekcijskom nadzoru na način d a j e isti izvršio uvid u dostavljena očitovanja i dokumentaciju od strane A1, što je sve konstatirano i okončano Rješenjem HAKOM-a, KLASA: UP/I-344-07/22-01/15, URBROJ: 376-05-22-10 od 20. lipnja 2022., u okviru kojeg je utvrđeno da je A1 najkasnije dana 8. veljače 2022. u 15:14h, bio svjestan i imao saznanja o nastupu incidenta budući d a j e u tom trenutku prijavu incidenta poslao društvu D d.o.o., ali je propustio o tome izvijestiti Agenciju na način i u rokovima propisanim člankom 99. stavak 7. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), u vezi s člankom 6. stavak 3. Pravilnika i člankom 7. Pravilnika,

- čime je počinio prekršaj opisan i kažnjiv u članku 119. stavka 1. točke 58. Zakona o elektroničkim komunikacijama ("Narodne novine" br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17).

pa mu se na osnovi istog članka istog propisa izriče

novčana kazna u iznosu od 45.000,00[1] (slovima: četrdesetpettisuća) eura/339.052,50 (slovima: tristotridesetdevettisućapedesetdvijekunepedesetlipa) kuna

II. Temeljem odredbe članka 33.stavka 11. Prekršajnog zakona okrivljenik je obvezan platiti novčanu kaznu u roku od 30 dana po pravomoćnosti ove presude, a ukoliko u roku koji mu je određen za plaćanje novčane kazne uplati dvije trećine izrečene novčane kazne, smatrat će se da je novčana kazna u cjelini plaćena.

III. Temeljem odredbe članka 139.stavka 3., u vezi članka 138.stavka 3.točke 3. Prekršajnog zakona okrivljenik je obvezan naknaditi troškove prekršajnog postupka u paušalnom iznosu od 150,00[1] (slovima: stopedeset) eura/1.130,18 (slovima: tisućustotridesetkunaosamnaestlipa) kuna, u korist Državnog proračuna prema priloženoj uplatnici, u roku od 30 dana po pravomoćnosti ove presude, jer će se u protivnom postupiti po odredbama članka 152.stavka 4. i 11. Prekršajnog zakona.

Obrazloženje

1. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) podnijela je dana 20. listopada 2022. godine optužni prijedlog broj: Klasa: 344-08/22-06/05, Urbroj: 376-08-22-4, te dopunu optužnog prijedloga Klasa: 344-08/22-06/05, Urbroj: 376-08-22-06 od 28.studenog 2022. godine protiv okrivljenika, zbog djela prekršaja činjenično i pravno opisanog u izreci ove presude.

2. Okrivljenik je u svojoj pisanoj obrani od 23.01.2023., te dopuni pisane obrane od 21.03.2023. poricao izvršenje djela prekršaja te je naveo da se ne smatra krivim za prekršaj koji mu se stavlja na teret, iz razloga što stvarno činjenično stanje ne odgovara onom sadržanom u činjeničnom opisu optužnog prijedloga, kao i zbog pogrešne primjene materijalnog prava. Istakao je da HAKOM u optužnom prijedlogu, u bitnom, navodi da je A1 Hrvatska prekasno izvijestio HAKOM o neovlaštenom (hakerskom) pristupu sustavu A1 Hrvatska, prilikom kojeg incidenta je neovlašteno

[1]Fiksni tečaj konverzije 7,53450

preuzet dio osobnih podataka 100.311 korisnika A1 Hrvatska. HAKOM smatra da taj incident, zbog povreda "autentičnosti" i "povjerljivosti", predstavlja "značajni sigurnosni incident" iz Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN 112/2021, dalje: Pravilnik), te ga je stoga A1 Hrvatska HAKOM-u morao prijaviti u roku od sat vremena od trenutka kada su ispunjeni kriteriji iz Dodatka 2 Pravilnika (prema kojim kriterijima incident i stječe karakter "značajnog"), a sa čime je navodno zakasnio. Pored toga, HAKOM smatra da je A1 Hrvatska u istom roku incident morao prijaviti i putem PiXi platforme (a s obzirom da je incident imao i računalnu komponentu), što je također navodno zakasnio napraviti. Ova dva kašnjenja po HAKOM-u predstavljaju biće prekršaja iz članka 119. stavka 1. točke 58. ZEK-a, a u vezi s odredbama čl. 6.3., 6.4. i 7. Pravilnika.

2.1. Nadalje, okrivljenik je naveo da se optužni prijedlog temelji na pogrešno utvrđenom činjeničnom stanju, obzirom da je, po njihovom mišljenju, HAKOM pogrešno utvrdio da su ispunjeni činjenični kriteriji iz Dodatka 2 Pravilnika, odnosno pogrešno je utvrdio da su postojale okolnosti koje bi sporni incident pretvorile u "značajni sigurnosni incident" za telekomunikacijske mreže i usluge. Suprotno tome, ti kriteriji nikada nisu bili ispunjeni, pa incident nije bio "značajan" u smislu Pravilnika, te nije niti nastala obveza obavještavanja HAKOM-a u roku iz čl. 6. st. 3. Pravilnika. Istakli su da podredno, čak i da se incident na koncu pokazao "značajnim", HAKOM je pogrešno utvrdio da je A1 Hrvatska već u trenutku kada je zatražio forenzičko izvješće o incidentu od strane društva D d.o.o. (dana 8.2.2022. u 15:14) mogao raspolagati informacijom o ispunjenju kriterija iz Dodatka 2 Pravilnika. U nastavku svoje obrane naveli su da se optužni prijedlog temelji i na pogrešnoj primjeni materijalnog prava, s obzirom da u Optužnom prijedlogu HAKOM tereti A1 Hrvatska za dostavljanje obavijesti putem PiXi platforme izvan roka od sat vremena, iako za dostavljanje te obavijesti nije propisan rok od sat vremena, tako da propuštanje dostave te obavijesti u tom roku uopće ne predstavlja prekršaj, te da HAKOM povrede "autentičnosti" i "povjerljivosti" ne tumači u skladu s odredbama Pravilnika, zbog kojeg pogrešnog tumačenja izvodi i pogrešan zaključak o postojanju prekršaja. U odnosu na ***n***edostavljanje obavijesti HAKOM-u putem dostave obrasca iz Dodatka 3 Pravilnika u roku od sat vremena, istakli su da Pravilnik odredbom čl. 6. st. 3. propisuje obvezu obavještavanja HAKOM-a u roku od sat vremena ukoliko incident stekne svojstvo "značajnog sigurnosnog incidenta". Taj rok počinje teći od trenutka ispunjenja kriterija propisanih Dodatkom 2 Pravilnika. Obvezu obavještavanja operator ispunjava dostavom HAKOM-u obrasca iz Dodatka 3 Pravilnika. Prema odredbi čl. 6. st. 1. Pravilnika, operator je obvezan provjeriti ispunjava li incident Kvantitativne kriterije iz Dodatka 2, a ukoliko oni nisu ispunjeni, operator je dužan provjeriti ispunjava li incident Kvalitativne kriterije iz Dodatka 2. HAKOM smatra da je sporni incident ispunio kvantitativni kriterij kako je to definirano Pravilnikom. Konkretno, HAKOM smatra da je incident utjecao na povjerljivost i autentičnost neke od telekomunikacijskih usluga, s time daje obuhvaćeno preko 1% krajnjih korisnika koji koriste tu konkretnu uslugu.

2.2. Međutim, u optužnom prijedlogu uopće nije navedeno koja je to točno usluga bila pogođena incidentom (nepokretna ili pokretna telefonija, nepokretni ili pokretni internet, odašiljanje radijskih ili TV programa ili slično), a također uopće nije navedeno kako je to točno incident utjecao na povjerljivost ili autentičnost neke od usluga. Niti jedno niti drugo (niti koja je konkretno usluga bila pogođena incidentom, niti kako je to točno incident utjecao na povjerljivost ili autentičnost te usluge) nije navedeno niti u

Rješenju inspektora HAKOM-a od 20.6.2022. I u tom Rješenju HAKOM tek paušalno navodi kako "iz čl. 6. st. 1. Pravilnika jasno proizlazi da su ispunjeni Kvantitativni kriteriji za izvješćivanje iz Dodatka 2 Pravilnika... budući da se u konkretnom slučaju radilo o sigurnosnom incidentu koji utječe na autentičnost i povjerljivost te je incidentom obuhvaćeno više od 1% korisnika od ukupnog broja korisnika koji koriste te usluge u Hrvatskoj".

2.3. Okrivljenik je mišljenja da HAKOM vjerojatno smatra da je do povrede "autentičnosti" i "povjerljivosti" došlo zato sto je prilikom incidenta došlo to povrede povjerljivosti osobnih podataka korisnika. Nesporno jest da je prilikom incidenta došlo do povrede osobnih podataka, no pravne posljedice povreda osobnih podataka su predmet zasebnih upravnih i prekršajnih postupaka. Međutim, kada je riječ o odredbama ZEK-u i odredbama Pravilnika, te "značajnim sigurnosnim incidentima" u smislu tih propisa, povrede "autentičnosti" i "povjerljivosti" se ne odnose na zaštitu osobnih podataka, već na zaštitu rada telekomunikacijske mreže i usluge, što jasno potvrđuju i odredbe čl.99.st.7. ZEK-a, te odredba čl.6.st.1., u svezi čl.2.st.1.točka 11., 14. i 19. Pravilnika kojima je definirano "utjecaj na autentičnost", "utjecaj na povjerljivost", te "sigurnosni incident", kao i dodatak 2. Pravilnika,

2.4. Obzirom na definicije navedene u Pravilniku, HAKOM je u optužnom prijedlogu trebao precizno navesti koja je usluga zahvaćena (pokretna ili nepokretna, govorna ili prijenos podataka i slično), te kako su i kod kojeg broja korisnika, i to prema definicijama Pravilnika, povrijeđeni autentičnost ili povjerljivost konkretne usluge. Uopće ne opisujući te okolnosti, (već tek paušalno utvrđujući da postoje povrede autentičnosti i povjerljivosti, vjerojatno temeljem paušalne opservacije o povredama povjerljivosti osobnih podataka) HAKOM je propustio opisati okolnosti nužne za postojanje bića prekršajnog djela.

2.5. Nadalje, istakao je da niti kod jedne usluge A1 Hrvatska prilikom spornog incidenta nije došlo do utjecaja na autentičnost ili povjerljivost usluge. Do utjecaja na povjerljivost komunikacije, komunikacijskih podataka ili metapodataka nije došlo niti u jednom slučaju, s obzirom da sama komunikacija između korisnika uopće nije bila zahvaćena neovlaštenim upadom. Također nije zabilježen niti jedan slučaj kompromitiranja korisničkog identiteta. Kako je to već ranije opisano, hakerskim napadom na sustav A1 Hrvatska preuzet je od strane napadača dio osobnih podataka korisnika, no u slučaju niti jednog korisnika nisu poduzete bilo kakve daljnje radnje od strane napadača koje bi imale za posljedicu kompromitaciju identiteta osobe na koju se ti podaci odnose.

2.6. Okrivljenik je također naveo da u trenutku dostavljanja obavijesti rok za dostavu obrasca iz Dodatka 3 Pravilnika nije ni počeo teći. Naime, dana 8.2.2022. godine, odnosno u trenutku zahtjeva forenzičkog izvješća o incidentu, A1 Hrvatska nije znao niti je mogao znati o kojem točno opsegu sigurnosnog incidenta se radi, no svakako je bilo jasno da se ne radi o značajnom utjecaju na rad mreža i usluga jer su i mreža i usluge besprijekorno funkcionirale. Dakle, potpuno je pogrešna činjenična tvrdnja HAKOM-a da je A1 Hrvatska već 8.2.2022. u 15:44 znao da se radi o značajnom sigurnosnom incidentu u smislu Pravilnika. Činjenica da je u tom trenutku zatraženo forenzičko izvješće dokazuje upravo suprotno - daje Al Hrvatska u tom trenutku tražio pouzdane informacije o vrsti i dosegu povrede. HAKOM u tom pogledu za navodno znanje A1 Hrvatska o ispunjenju kriterija iz Dodatka 2 nije dostavio niti jedan valjani dokaz.

2.7. U odnosu na nedostavljanje obavijesti putem PiXi platforme u roku od sat vremena, okrivljenik je pojasnio da pored obveze dostavljanja obrasca iz Dodatka 3, ukoliko značajni incident nije samo sigurnosni, već dodatno i računalno-sigurnosni (sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata), incident je potrebno dodatno prijaviti i putem PiXi platforme. HAKOM u opisu bića prekršajnog djela spominje i navodno neispunjenje te obveze u roku od sat vremena. Međutim, za obavještavanje putem PiXi platforme (odredba čl. 6. st. 4. i odredba čl. 7. Pravilnika) nije propisan nikakav rok (kao što je propisan za dostavu Obrasca 3 u odredbi čl. 6. st. 3. Pravilnika), a HAKOM niti ne spori da A1 Hrvatska obavijest putem te platforme jest dostavio. S obzirom da odredbama čl. 6.4. i 7. Pravilnika (na koje se HAKOM poziva povodom ove navodne povrede,) ne postoji obveza dostave obavijesti putem PiXi platforme u roku od sat vremena, probijanje tog roka ne predstavlja protupravnu radnju, a posljedično niti prekršaj.

2.8. Okrivljenik je detaljno obrazložio svoje postupanja prilikom incidenta, navodeći da Pravilnik propisuje o kojim se sigurnosnim incidentima HAKOM mora biti obaviješten. O ostalim incidentima svaki operator tek može obavještavati HAKOM (prema odredbama čl. 6. st. 8. Pravilnika), no te fakultativne obavijesti nisu podložne nikakvim rokovima. Neprovjerenu informaciju o potencijalnoj povredi osobnih podataka i povezanom sigurnosnom incidentu A1 Hrvatska je prvotno zaprimio 7.2.2022. godine u 23:21 putem elektroničke pošte poslane od strane nepoznatog pošiljatelja na 5 adresa elektroničke pošte unutar društva A1 Hrvatska, od kojih jedna nije u uporabi jer se radi o bivšem zaposleniku kao primatelju. S obzirom na vrijeme slanja i okolnost daje predmetna poruka poslana na generičke adrese elektroničke pošte službe za korisnike A1 Hrvatska, na koje svakodnevno pristižu velike količine dolaznih poruka, provjera istinitosti navoda iz predmetne poruke izvršena je dana 8.2.2022. godine. Odmah po provjeri navoda, a radi utvrđivanja prirode povrede i opsega sigurnosnog incidenta, utvrđivanja potencijalnih posljedica i rizika na ispitanike, utvrđivanja kategorija kompromitiranih osobnih podataka ispitanika te procjene broja ispitanika o čijim se osobnim podacima radi, pokrenute su sveobuhvatne i žurne aktivnosti. Prethodno navedena kritična i uvjerljivo najvažnija faza postupka upravljanja sigurnosnim incidentom i povredom osobnih podataka obuhvaćala je i istovremeno definiranje hitnih sigurnosnih mjera sprječavanja nastanka štete za korisnike, minimiziranja ili sprječavanja nastanka štetnih posljedica i sprječavanja eventualnog ponavljanja sigurnosnog incidenta, temeljem kojih je A1 Hrvatska prikupio sve relevantne informacije koje su se objektivno u tom kratkom razdoblju mogle prikupiti i provjeriti radi jasnog informiranja nadležnih tijela. Obzirom da su sve okolnosti ukazivale da je riječ o kaznenom djelu, A1 Hrvatska je bez odlaganja, dana 9.2.2022. podnio kaznenu prijavu Policijskoj upravi zagrebačkoj, Policijskoj postaji Maksimir, Petrova ulica 152,10000 Zagreb, zbog osnovane sumnje da je NN počinitelj počinio kazneno djelo neovlaštenog pristupa iz članka 266. stavka 1., oštećenja računalnih podataka iz članka 268. stavka 1., iznude iz članka 243. u vezi članka 34. Kaznenog zakona. Paralelno s ovim aktivnostima, i iako u tom trenutku nije imao nikakvih indicija da su ispunjeni kriteriji iz Dodatka 2 Pravilnika (što je na kraju i potvrđeno forenzičkom analizom), A1 Hrvatska je, uzimajući o obzir načelo transparentnosti i praksu uske suradnje s HAKOM-om, o incidentu obavijestio i HAKOM. Poslije kontinuiranog telefonskog obavještavanja, uslijedio je i niz obavijesti i ažuriranja informacija putem elektroničke pošte. Tijekom te intenzivne komunikacije, a na izričit zahtjev djelatnika HAKOM-a, A1 Hrvatska je HAKOM-u obavijest dostavio i putem obrasca iz Dodatka

3. Valja naglasiti da je bila riječ o situaciji bez presedana, s mnoštvom postupaka koje je trebalo poduzimati paralelno i u jako kratkom vremenu (od utvrđivanja načina i opsega neovlaštenog upada, preko suradnje s policijom oko otkrivanja počinitelja i s AZOP-om u pogledu zaštite osobnih podataka, do suradnja s HAKOM-om u pogledu zaštite telekomunikacijskih usluga i mreža). U tom mnoštvu aktivnosti nije bilo vremena za detaljne pravne i činjenične analize, pa je A1 Hrvatska HAKOM-u na njegov zahtjev zaista i dostavio obrazac iz Dodatka 3 Pravilnika (iako za to nije postojala zakonska obveza). Dakle, to dostavljanje obavijesti iz Obrasca 3 ne predstavlja nikakvo "priznanje" da se zaista radilo o značajnom sigurnosnom incidentu. Nadalje, okrivljenik je naveo da sam ZEK radi razliku između povrede osobnih podataka i povrede sigurnosti i cjelovitosti mreža i usluga. Istakao je da Zakon o elektroničkim komunikacijama koji je bio na snazi u vrijeme spornog incidenta (NN 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17, dalje: Stari ZEK) je pitanje sigurnosti i cjelovitosti mreža i usluga uređivao člankom 99. Odvojeno od pitanja zaštite sigurnosti i cjelovitosti mreža, Stari ZEK je pitanje zaštite osobnih podataka je uređivao u zasebnom članku 99.a. Dakle, stari ZEK ne samo da jasno razdvaja pitanja sigurnosti i zaštite mreža od pitanja zaštite osobnih podataka, već odvojeno uređuje rokove i načine obavijesti za te dvije vrste incidenata. Rokovi i načini obavijesti vezanih zaštitu sigurnosti i cjelovitosti mreža i usluga se moraju propisati Pravilnikom, što je i učinjeno, dok se rokovi i načini obavijesti zaštite osobnih podataka tek mogu propisati, no nisu propisani Pravilnikom. Istakao je da je sadržaj dostavljenog obrasca 3 koji je okrivljenik dostavio HAKOM-u irelevantan za utvrđivanje postojanja prekršaja, obzirom da je sadržaj obrasca koji je "u žurbi i na nagovor HAKOM-a dostavljen HAKOM-u ne održava stvarno stanje stvari", te da je Sud dužan utvrditi da li je zaista ili ne došlo do povrede autentičnosti i povjerljivosti u smislu Pravilnika, a što je ključna činjenica.

3. Na okolnosti postupanja A1 Hrvatska nakon samog incidenta i posebno na okolnosti komunikacije s HAKOM-om ispitan je predstavnik okrivljenika koji je naveo da osobni podaci i komunikacijski podaci nisu istoznačnice. Komunikacijski podaci su regulirani čl. 99. Zakona o elektroničnim komunikacijama, dok su drugi regulirani čl.99.a. Zadnjom izmjenom Zakona povreda osobnih podataka se više uopće ne prijavljuje HAKOM-u, pri čemu je Pravilnik koji je sporan odnosno koji to regulira je isti, jer se on i dalje primjenjuje na ono i na što se uvijek primjenjivao, a to je čl.99., a ne čl.99a. Zakona. A1 je u noćnim satima 07. veljače primio predmetni mail koji je došao na generičku adresu službe za korisnike, na koju svakodnevnu pristiže veliki broj mailova. Odmah slijedeće jutro, 08.veljače, mail je zamijećen, analiziran i eskaliran unutar kompanije. Oformljen je krizni tim, koji je shvatio da se iza toga potencijalno nešto krije i odmah kontaktirao svog vanjskog eksperta za pitanja sigurnosti informatičkih sustava D d.o.o. da im pomogne u analizi i rasčišćavanju činjenica što je posrijedi. Primarni fokus je bio zaštita korisnika, da li je nastala šteta, ako nije kako osigurati da ni ne može nastati, da napad ne bi ponovio ponovnu stvar. Istakao je da paralelno s tim direktor Regulatornih poslova ima otvorenu telefonsku liniju s HAKOM-om s kojim dnevno surađuje po cijelom nizu pitanja. Tijekom tih telefonskim razgovora s HAKOM-om s mnogim kolegama, uključujući i ravnatelja i članove vijeća HAKOM-a kolegica dobiva savjet da se to prijavi i na neki strukturirani način, pa zašto ne, koristiti i obrazac koji postoji. Kolegica je pitala njega za obvezu prijave HAKOM-u na što je on odgovorio da nema tu nikakve obveze prijave HAKOM-u već samo AZOP-u, na što mu je ona odgovorila da obzirom na odnos kakav ima s HAKOM-om ne želi ovakve stvari prešućivati, iako ne postoji obveza prijave. Obzirom

na transparentan odnos koji imaju općenito s HAKOM-om, te naročito uzimajući u obzir okolnost da su oni prvi izašli u javnost s ovom informacijom, kolegica se odlučila da će im tu informaciju dati na bilo koji način, pa kako i traže. Kako su iz HAKOM-a rekli da iskoriste obrazac i pošalju ga na mail "osobni podaci HAKOM-a i incident", te je kolegica poslala na te adrese i na dodatne adrese, dakle, sve je to slano u duhu transparentnog izvještaja relevantnih kolega u HAKOM-u. Napomenuo da ih je AZOP kaznio za povredu osobnih podataka, a što oni smatraju da je i bila jedina povreda.

4. Tužitelj je, osvrćući se na pisane obrane okrivljenika, kao i na iskaz ispitanog predstavnika okrivljenika , naveo da okrivljenik u svojoj pisanoj obrani poriče prekršaj i ne smatra se krivim za isti, iz razloga što prema njegovim navodima, stvarno činjenično stanje ne odgovara onome sadržanom u činjeničnom opisu iz optužnog prijedloga, kao i zbog pogrešne primjene materijalnog prava. U odnosu na istaknute argumente okrivljenika i to nedostavljanje obavijesti HAKOM-u putem obrasca iz Dodatka 3 Pravilnika u roku sat vremena naveli su da okrivljenik navodi kako je člankom 6. stavkom 3. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21; dalje: Pravilnik) propisana obveza obavještavanja HAKOM-a o značajnim sigurnosnim incidentima u rokovima koji počinju teći u trenutku ispunjavanja kriterija propisanih u Dodatku 2 Pravilnika, te da takvi kriteriji u konkretnom slučaju nisu bili ispunjeni. Nadalje okrivljenik navodi kako HAKOM smatra da je incident utjecao na povjerljivost i autentičnost neke od elektroničkih komunikacijskih usluga, ali da pritom nije naveo o kojim se to uslugama radilo.

4.1. Međutim, ovlašteni tužitelj smatra da navedena činjenica nije ni sporna u predmetnom postupku budući da su te činjenice jasno vidljive iz obrasca obavijesti koje je okrivljenik naknadno i nakon proteka propisanih rokova, ispunio i dostavio ovlaštenom tužitelju putem Dodatka 3 Pravilnika. Isto tako, okrivljenik ističe da u optužnom prijedlogu nije navedeno o kojem se-incidentu točno radi." što je također potpuno netočno budući da je u optužnom prijedlogu precizno navedeno o kojem se incidentu radilo i kada je isti nastupio, kada je okrivljenik isti otkrio, a kada o incidentu izvijestio HAKOM. Također, ovakva tvrdnja okrivljenika je potpuno promašena budući da je okrivljenik u konačnici dostavio svoju obavijest potpuno svjestan o kojem se incidentu radi, samo izvan propisanih rokova.

4.2. U odnosu na tvrdnje okrivljenika kako se utjecaj na autentičnost i povjerljivost koja je definirana Pravilnikom ne odnose na zaštitu osobnih podataka, već na zaštitu rada telekomunikacijske mreže i usluge, ovlašteni tužitelj prije svega ističe kako su ovakve tvrdnje potpuno promašene. Povjerljivost i autentičnost svih podataka, uključujući i osobnih podataka, preduvjet je osiguravanja sigurnosti mreža i usluga.

4.3. Naime, odredba članka 99. stavka 1. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14, 72/17; dalje: ZEK.) koji se primjenjuje na predmetni prekršaj jasno navodi da operatori moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere radi zaštite sigurnosti elektroničke komunikacijske mreže i usluga. Stavkom 4. istog članka definirano je da mjere moraju osobito osigurati da osobnim podacima mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe. Dakle, ZEK-om je definirano da sve sigurnosne mjere koje se poduzimaju, između ostalog, moraju posebno voditi računa o zaštiti osobnih podataka korisnika usluga.

4.4. Upravo je iz navedenog razloga Dodatkom 2 Pravilnika utvrđeno kako kriterij za izvješćivanje o sigurnosnom incidentu u slučaju utjecaja na povjerljivost i/ili autentičnost nije dostupnost ili prekid usluge, već isključivo broj korisnika obuhvaćenih incidentom. U tom "smislu su argumenti " okrivljenika potpuno neosnovani.

4.5. Okrivljenik u svojoj pisanoj obrani nadalje pojašnjava relevantne pojmove iz Pravilnika, osporavajući da se u konkretnom slučaju radilo o incidentu koji je imao utjecaja na autentičnost, budući da, prema mišljenju okrivljenika, nije došlo do kompromitacije korisničkog identiteta. Prema shvaćanju okrivljenika, kompromitiranje korisničkog identiteta predstavlja isključivo neovlašteno korištenje, odnosno zlouporabu identiteta krajnjeg korisnika. Ovlašteni tužitelj ističe da kompromitiranje podrazumijeva daleko širi pojam, koji obuhvaća bilo koji oblik neovlaštenog uvida, obrade i korištenja podataka o korisnicima. U konkretnom slučaju nesporno je došlo do neovlaštenog pristupa podacima o korisnicima (ime i prezime, OIB, MSISDN, tarifni model koji korisnik koristi) od strane nepoznate osobe, koja je izuzela preko 100.000 korisničkih podataka, objavila ih na javnoj Internet adresi i zaprijetila da će ih prodati na tzv. dark webu.

4.6. Također, prema ucjenjivačkoj elektroničkoj pošti koju je okrivljenik zaprimio od strane nepoznatog počinitelja proizlazi da je baza izuzetih podataka učitana na tri različita web sjedišta, no okrivljenik je u svom očitovanju od 8. ožujka 2022. godine naveo referencu samo na jedno web sjedište te je konstatirao da je osigurao da u navedenom razdoblju ni od jedne strane nije došlo do preuzimanja ili druge vrste obrade osobnih podataka potencijalno izloženih korisnika. Naknadno, inspektor je tijekom inspekcijskog pregleda zatražio očitovanje od okrivljenika o tome je li zatražio dokaze za prethodnu tvrdnju, odnosno pristupne logove web poslužitelja od pružatelja usluge web hostinga. Okrivljenik je na takav upit odgovorio da je njegova pretpostavka da nije došlo do preuzimanja tih datoteka te da nije zatražio pristupne logove od pružatelja usluge web hostinga.

5. Očitujući se na navode predstavnika okrivljenika na glavnoj raspravi, predstavnica tužitelja je navela da se ovaj prekršajni postupak ne odnosi na eventualni propust u prijavi povrede osobnih podataka, niti na članak 99.a Zakona već se odnosi na povredu prijave sigurnosnog incidenta u roku. Primjeri koje navodi okrivljenik odnose se na prometne podatke znači vrijeme pozivanja, pozivatelj, pozivana strana, a u ovom slučaju se radi o kompromitaciji podataka koji uključuju ime prezime, OIB i MSISDN što je zapravo broj telefona i tarifni model. Pravilnik, kada govori o utjecaju na povjerljivost govori o kompromitiranju povjerljivosti komunikacije, komunikacijskih podataka ili meta podataka. Komunikacijski podaci nisu isključivo osobni podaci niti su isključivo prometni podaci, nego je to širi pojam kao što je pojam meta podatka koji obuhvaća sve podatke koji su nužni za pružanje usluge, a što u svakom slučaju podrazumijeva osobne podatke, MSISDN i tarifni model. zato smatramo da je u konkretnom slučaju došlo do utjecaja na povjerljivost, jer su svi spomenuti podaci bili javno objavljeni i dostupni za potencijalne zlouporabe koje A1 nije utvrdio niti dokazao da do istih nije došlo, niti da li će doći. Sama činjenica da su oni bili dostupni javno i da se prijetilo njihovom zlouporabom dovoljna je za ispunjenje uvjeta iz Pravilnika. Isto tako utjecaj na autentičnost je definirana kao kompromitiranje korisničkog identiteta, što isto tako ne podrazumijeva isključivo OIB, ime i prezime, nego sve ove podatke koji su bili kompromitirani, odnosno kojima je neovlašteno pristupila i javno objavila nepoznata osoba. U odnosu na rok za prijavu iz očitovanja jasno je da su već 08.02.2022. godine izvršene analize pristupnih logova, iz čega je okrivljeniku moralo biti jasno da je do incidenta došlo i da su navodi iz poruke

nepoznatog napadača od 07.02.2022. godine točni. Odjel za korporativnu sigurnost A1 je dobio informaciju o sigurnosnom incidentu u 14.33 sati dana 08.02.2022.godine, a u 15.14 sati je angažiran D koji je trebao obaviti daljnju forenziku. Iz toga slijedi da je već 08.02.2022. godine najkasnije u 15.14 sati okrivljeniku bila poznata činjenica da je do incidenta došlo, te da su navodi nepoznatog počinitelja točni. Ispravila je navode predstavnika okrivljenika da je u usmenoj komunikaciji s HAKOM-om dobivena informacija da bi bilo dobro prijavu obaviti ili izvršiti i u "nekom strukturiranom obliku" već je izričita uputa bila, kada su dobivene informacije, da se sigurnosni incident prijavljuje na način propisan Pravilnikom.

6. U dokaznom postupku sudac je ispitao svjedokinju, inspektoricu te je pročitao i izvršio uvid u mail od 09.veljače 2022. godine, u predložak za izvješćivanje o sigurnosnom incidentu dodatak 3, u mail od 09. veljače 2022. godine u 14,23 sati, u izviješće o povredi osobnih podataka, u mail korespondenciju, u isprint hakerske poruke, u rješenje HAKOM-a klasa: UP/I-344-07/22-01/15, urbroj 376-05-22-10 od 20.lipnja 2022. godine, s očitovanjem D d.o.o., u obavijest, u izvod iz sudskog registra, te u izvod iz prekršajne evidencije, dok sudac nije proveo dokaz vještačenja po vještaku telekomunkacijske struke na okolnost da prilikom konkretnog incidenta nisu ispunjene pretpostavke predviđene Dodatkom 2 Pravilnika, jer je ocijenio da je taj dokaz nepotreban i suvišan, obzirom da se istim ne bi utvrdila nikakva nova bitna činjenica, jer je činjenica na koju se predlaže vještačenje nesporna, a vještačenjem bi došlo samo do nepotrebnog odugovlačenja postupka.

7. Svjedokinja, inspektorica, navela je da je 07.02.2022. godine A1 dobio mail u kojem je navedeno da su dostupni osobni podaci korisnika od A1, te da se planira te podatke staviti na dark web, gdje bi oni bili dostupni za ilegalno korištenje. Dana 08.02.2022. godine u 15,14 sati je A1 prijavio taj incident D u, kompaniji koja se bavi forenzikom, te je također A1 u svom izvještaju naveo da je provjerio navode iz tog maila, što znači da je tada već bio svjestan da je nastupio incident odnosno da ono što piše u mailu stoji. Istakla je da su HAKOM telefonskim putem kontaktirati 09.02.2022. godine, u jutarnjim satima i to više osoba u menadžmentu, pokušavajući dobiti informaciju na koji način se prijavljuje incident, a što ukazuje da ne poznaju Pravilnik, odnosno da ne znaju što treba učiniti prilikom ovako velikih incidenata. Nakon toga su dobili potrebne informacije, te su tog dana u 12,07 sati prijavili na propisani način na propisanom obrascu i na propisanu adresu e pošte. Nadalje je istakla da prije nego što je A1 kontaktirao HAKOM mediji su već izašli s tom informacijom, te je HAKOM zaprimio veliku količinu poziva od uplašenih korisnika, ne znajući o čemu se točno radi. Iz tog razloga u Pravilniku stoje propisani rokovi u kojima se treba prijaviti incident, kako bi HAKOM kao institucija na koju se korisnici oslanjaju mogao pravovremeno imati dostupne informacije, te pružiti odgovor krajnjim korisnicima.

7.1. Na poseban upit koji uvjeti moraju biti ispunjeni i kada operater mora u roku od sat vremena prijaviti incident HAKOM-u svjedokinja je navela da se ovdje radilo o utjecaju na povjerljivost i autentičnost, te su za to propisani kriteriji neovisno o trajanju ako je obuhvaćeno više od 1% krajnjih korisnika određene usluge, a što je u ovom slučaju bilo ispunjeno. Što se tiče povjerljivosti, sukladno ISO STANDARDU 27000:2018 povjerljivost je opisana ili definirana kao svojstvo da informacija nije dostupna ili otkrivena neovlaštenim osobama, entitetima, procesima ili pojedincima. Ovdje je jasno da su osobni podaci bili otkriveni neovlaštenim osobama, kao i korisnički

podaci zaposlenika. Ovaj optužni prijedlog je išao na činjenicu da A1 nije prijavio u propisanim rokovima i na propisan način ovaj incident u kojem je bila narušena povjerljivost i autentičnost.

7.2. Na pitanje branitelja da li kao inspektor zna kako Pravilnik definira povredu povjerljivosti svjedokinja je navela da je to kompromitacija povjerljivosti komunikacije, komunikacijskih podataka ili meta podataka. Ta definicija opisuje u konkretnom slučaju da je došlo do kompromitacije podataka što korisničkih, a što povjerljivosti podataka zaposlenika. Konkretan incident bi definirala odnosno podvela pod povredu komunikacijskih podataka i meta podataka i to iz razloga što osobni podaci kao što su broj telefona, OIB spadaju pod te kategorije, te je ukoliko se ti podaci nalaze kod neovlaštenih osoba, narušena povjerljivost. Autentičnost je kompromitacija korisničkog identiteta, ti podaci su bili dostupni na tri različite adrese, A1 je provjerio samu jednu i naveo je da je uklonio podatke, te da nitko nije oštećen odnosno da nitko nije preuzeo te podatke. Istakla je da ih je u samom inspekcijskom postupku upitala kako to znaju, odnosno da li su zatražili logove web poslužitelja od pružatelja usluga web hostinga da mogu sa sigurnošću tvrditi, oni su odgovorili da nisu zatražili logove, te da je to samo njihova pretpostavka, a iz čega proizlazi da je moguće da su podaci kompromitirani odnosno da će biti u budućnosti kompromitirani.

7.3. U konkretnom postupku bilo je bitno utvrditi o kakvom se sigurnosnom incidentu radi, odnosno da li su ispunjeni uvjeti iz čl.6. Pravilnika, te posljedično da li je okrivljenik u propisanom roku, ukoliko su ispunjeni uvjeti, postupio po tom članku, te obavijestio HAKOM o sigurnosnom incidentu.

8. Sudac nije prihvatio obranu okrivljenika koji u bitnom navodi da se u konkretnom slučaju ne radi o incidentu koji je utjecao na povjerljivost i autentičnost neke od elektroničnih komunikacijskih usluga, obzirom da je ista neuvjerljiva i u suprotnosti s dokazima koje se nalaze u spisu, posebno s predloškom Dodatka 3 koji je okrivljenik sam ispunio. Naime, ta činjenica nije niti sporna u predmetnom postupku, jer je ista vidljiva i iz sadržaja naprijed navedenog predloška za izvješćivanje o sigurnosnom incidentu, dodatak 3, koji je okrivljenik nakon proteka roka propisanog Pravilnikom, dostavio tužitelju.

9. Naime, tvrdnja okrivljenika da taj predložak ne može biti relevantan dokaz je u najmanju ruku neozbiljna, jer čak i kada bi se prihvatio navod okrivljenika da je isti dostavio predložak nakon što ga je na to uputio HAKOM, sam sadržaj ispunjenog predloška ne bi smio biti doveden u pitanje, jer bi u tom slučaju okrivljenik priznao da se radi o "neistinitim" podacima koje je dostavio Agenciji, što obzirom na dosadašnje ponašanje okrivljenika, njegovu veličinu, te postupanje nije prihvatljivo, a dovelo bi u sumnju i sve ostale navode i ponašanje okrivljenika, te je stoga sudac podatke iz predloška uzeo kao vjerodostojne.

10. Navodi o postupanju, koje je okrivljenik naveo u svojoj obrani, samo ukazuju na neupućenost okrivljenika o postupanju koje je potrebno slijediti u slučaju nastanka ovakvog incidenta, kao i obveze koje proizlaze iz propisa koje obvezuju operatore elektroničkih komunikacija. lako je razumljivo da se radilo o izvanrednoj situaciji, od operatora elektroničkih komunikacijskih usluga koji pruža usluge velikom broju korisnika i koji raspolaže iznimno osjetljivim podacima u svojim mrežama, očekuje se da ima razrađene procedure postupanja i podjelu uloga i odgovornosti, a ne da se o svojim obvezama, koje su utvrđene propisima, konzultira telefonski s djelatnicima ovlaštenog tužitelja.

11. Sudac nije prihvatio navod obrane okrivljenika da u optužnom prijedlogu nije navedeno o kojem se incidentu točno radi, budući da je u optužnom prijedlogu precizno navedeno o kojem se incidentu radilo i kada je isti nastupio, kada je okrivljenik isti otkrio, a kada o incidentu izvijestio HAKOM. Također, ovakva tvrdnja okrivljenika je potpuno promašena budući da je okrivljenik u konačnici dostavio svoju obavijest potpuno svjestan o kojem se incidentu radi, samo izvan propisanih rokova, a što je već naprijed navedeno.

12. Također, nije prihvaćen navod okrivljenika u odnosu na njegove tvrdnje kako se utjecaj na autentičnost i povjerljivost koja je definirana Pravilnikom ne odnose na zaštitu osobnih podataka, već na zaštitu rada telekomunikacijske mreže i usluge, jer su ovakve tvrdnje potpuno promašene, obzirom da su povjerljivost i autentičnost svih podataka, uključujući i osobnih podataka, preduvjet je osiguravanja sigurnosti mreža i usluga, a što je potvrdila i ispitana svjedokinja inspektorica

13. Naime, odredba članka 99. stavka 1. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14, 72/17; dalje: ZEK.) koji se primjenjuje na predmetni prekršaj jasno navodi da operatori moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere radi zaštite sigurnosti elektroničke komunikacijske mreže i usluga. Stavkom 4. istog članka definirano je da mjere moraju osobito osigurati da osobnim podacima mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe. Dakle, ZEK-om je definirano da sve sigurnosne mjere koje se poduzimaju, između ostalog, moraju posebno voditi računa o zaštiti osobnih podataka korisnika usluga. U konkretnom slučaju nije došlo do povrede odredbi temeljem čl.99.a budući je okrivljenik obavijestio HAKOM o nastaloj povredi, te sukladno uputi HAKOM-a o nastalom incidentu obavijestio i krajnje korisnike, već je, kako je naprijed navedeno, došlo do povrede odredbe čl.99. ZEK-a.

14. Upravo je iz navedenog razloga Dodatkom 2 Pravilnika utvrđeno kako kriterij za izvješćivanje o sigurnosnom incidentu u slučaju utjecaja na povjerljivost i/ili autentičnost nije dostupnost ili prekid usluge, već isključivo broj korisnika obuhvaćenih incidentom, te su u tom smislu argumenti okrivljenika potpuno neosnovani, obzirom da iz predloška za izvješćivanje o sigurnosnom incidentu, kao i ostale dokumentacije, proizlazi da je incidentom obuhvaćeno više od 100.000 korisnika.

15. Dakle, u konkretnom slučaju radilo se o sigurnosnom incidentu koji utječe na autentičnost i povjerljivost, te je incidentom obuhvaćeno više od 1% korisnika od ukupnog broja korisnika koji koriste te usluge u Hrvatskoj, te su stoga zadovoljeni kvantitativni kriteriji za izvješćivanje, te je okrivljenik imao obvezu izvijestiti HAKOM u propisanom roku.

16. Pravilnik, kada govori o utjecaju na povjerljivost govori o kompromitiranju povjerljivosti komunikacije, komunikacijskih podataka ili meta podataka. Komunikacijski podaci nisu isključivo osobni podaci niti su isključivo prometni podaci, nego je to širi pojam kao što je pojam meta podatka koji obuhvaća sve podatke koji su nužni za pružanje usluge, a što u svakom slučaju podrazumijeva osobne podatke, MSISDN i tarifni model, te je stoga u konkretnom slučaju došlo do utjecaja na povjerljivost, jer su svi spomenuti podaci bili javno objavljeni i dostupni za potencijalne zlouporabe koje A1 nije utvrdio niti dokazao da do istih nije došlo, niti da li će doći. Isto tako utjecaj na autentičnost je definirana kao kompromitiranje korisničkog identiteta, što isto tako ne podrazumijeva isključivo OIB, ime i prezime, nego sve ove podatke koji su bili kompromitirani, odnosno kojima je neovlašteno pristupila i javno objavila nepoznata osoba. U odnosu na rok za prijavu iz očitovanja jasno je da su već 08.02.2022. godine izvršene analize pristupnih logova, iz čega je moralo biti jasno da

je do incidenta došlo i da su navodi iz poruke nepoznatog napadača od 07.02.2022. godine točni. Odjel za korporativnu sigurnost A1 je dobio informaciju o sigurnosnom incidentu u 14.33 sati dana 08.02.2022. godine, a u 15.14 sati je angažiran D koji je trebao obaviti daljnju forenziku. Iz toga slijedi da je već 08.02.2022. godine najkasnije u 15.14 sati okrivljeniku bila poznata činjenica da je do incidenta došlo, te da su navodi nepoznatog počinitelja točni.

17. Sudac je u cijelosti poklonio vjeru iskazu ispitane svjedokinje inspektorice , koja je iskazivala stručno, okolnosno i uvjerljivo, te je njezin iskaz u cijelosti u suglasnosti s dokumentacijom u spisu i to posebno sa sadržajem obrasca iz dodatka 3 Pravilnika koji je okrivljenik dostavio tužitelju nakon proteka roka i to dana 09.02.2022. godine, kao i s rješenjem HAKOM-a Klasa: UP/I-344-07/22-01/15, urbroj: 376-05-22-10 od 20. lipnja 2022. godine.

18. Iz sadržaja navedenog predloška za izvješćivanja o sigurnosnom incidentu, koji je ispunio sam okrivljenik, navedeno je da se radi o tipu incidenta B-drugi utjecaj na usluge (npr. povjerljivost, cjelovitost, autentičnost), te D-prijetnja ili ranjivost (npr. otkrivanje slabosti u kriptiranju), kod podatka "obuhvaćene usluge" označena je nepokretna telefonija, te prijetnja objavljivanja neovlašteno stečenih podataka broj korisnika 100.000 min. Kao izvorni uzrok navedeno je zlonamjerne radnje i greška treće strane. Pod tehničkim uzrocima označeno je krađa identiteta, te drugo-neovlašteni pristup, dok je kod tehničke imovine obuhvaćene incidentom označeno App, a kod čimbenika značajnosti označen je "broj obuhvaćenih korisnika", te kod skale utjecaja označen je "veliki utjecaj".

19. Nadalje, kod čimbenika ozbiljnosti prijetnje (za tip "D") koji je naprijed označen, naznačena je "srednja ozbiljnost prijetnje". Pod rješavanje sigurnosnog incidenta i opis poduzetih mjera navedeno je: u najkraćem mogućem roku postavljen je zahtjev za uklanjanjem podataka s linkova navedenih u spornoj email poruci tj. onemogućivanjem preuzimanje istih, napravljena je analiza pristupnih logova, resetiranje svih relevantnih pristupnih podataka (zaporki), te ograničavanje geo lokacijskog pristupa na partnerski portal, dok su mjere poduzete nakon otklanjanja sigurnosnog incidenta TBD.

20. Dakle, iz sadržaja ovog predloška nedvojbeno je da je sam okrivljenik priznao da se radi o sigurnosnom incidentu opisanom u izreci presude, u kojem slučaju Pravilnik propisuje obvezu dostave obavijesti Agenciji bez odgode, čim su podaci dostupni, i to putem predloška propisanog u Dodatku 3 Pravilnika, u roku od najviše jedan sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2, u roku od najviše jedan sat nakon otklanjanja sigurnosnog incidenta, odnosno u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku, elektroničnim putem, na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način.

21. Činjenica što je po navodima okrivljenika predložak dostavio naknadno, van roka, i to isključivo na sugestiju djelatnika ovlaštenog tužitelja, iako nije ni smatrao ili bio svjestan svojih obveza, ne isključuje odgovornost okrivljenika, niti umanjuje vjerodostojnost sadržaja ovog predloška, već samo potvrđuje zaključak o nepoznavanju obveza okrivljenika u konkretnom slučaju.

22. U postupku je utvrđeno da je A1 obavijest o predmetnom incidentu dobio 07.02.2022. godine u 23,21 sati na nekoliko službenih A1 službenih adresa elektroničke pošte, te je dana 08.02.202. godine u 15,14 sati prijavio incident D d.o.o. u svrhu izrade forenzičkog izvješća, a iz čega proizlazi da je A1 bio potpuno svjestan i imao saznanja o nastalom sigurnosnom incidentu najkasnije u trenutku prijave incidenta društvu D d.o.o.

23. HAKOM je službenu prijavu incidenta od A1 zaprimio tek 09.02.2022. godine kada je incident već bio objavljen u medijima, te nakon što je A1 bio upozoren da prijava incidenta nije izvršena na način propisan čl.6. Pravilnika.

24. U odnosu na očitovanje okrivljenika o okolnostima pravovremene prijave incidenta pogrešno je i neosnovano shvaćanje A1 da nije imao obvezu izvijestiti HAKOM o navedenom incidentu, budući da sam incident nije zadovoljio ni kvalitativne ni kvantitativne kriterije za izvješćivanje iz dodatka 2 Pravilnika, jer nije utjecao na rad A1 mreže ili pružanje usluga.

25. Naime, čl.6.st.1. Pravilnika propisuje obvezu pružateljima obavještavanja Agencije o sigurnosnom incidentu koji je značajnije utjecao na rad mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2 Pravilnika, pri čemu pružatelji provjeravaju ispunjavanje kvantitativnih kriterija, te ukoliko isti nisu zadovoljeni, provjeravaju ispunjenost kvalitativnih kriterija iz navedenog Dodatka.

26. U slučaju svakog sigurnosnog incidenta, pružatelji uvijek moraju provjeriti je li došlo do značajnog računalno-sigurnosnog incidenta iz navedenog Dodatka. U tom smislu je potpuno neosnovana tvrdnja okrivljenika da se u konkretnom slučaju nije radilo o sigurnosnom incidentu, budući da iz čl.6.st.1. Pravilnika, kao i iz ispunjenog predloška proizlazi da su ispunjeni kvantitativni kriteriji za izvješćivanje iz Dodatka Pravilnika, te je A1 također morao provjeriti da li je došlo do računalno-sigurnosnog incidenta.

27. Također, budući da je sukladno Taksonomiji došlo do značajnog računalno-sigurnosnog incidenta, odnosno kompromitacije korisničkog računa i iznude, A1 je trebao prijaviti incident i putem PiXi platforme, na način propisan članom 7. Pravilnika, a što je isti učinio tek 09.02.2022. godine i to temeljem naknadne upute HAKOM-a.

28. Stoga je nedvojbeno da okrivljenik nije postupio sukladno obvezi propisanoj čl.99.st.7. Zakona o elektroničkim komunikacijama, te čl.6.st.3. i čl.7. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosni i cjelovitosti mreža i usluga kojima je propisana obveza operatora da u roku od najviše jedan sat nakon ispunjenja kriterija za izvješćivanje putem predloška propisanog u Dodatku 3 izvijesti Agenciju o nastalom incidentu, te putem PiXi platforme na način kako je to propisano u čl.7. Pravilnika, već da je okrivljenik to učinio tek 09. veljače 2022. godine.

29. Nakon ovako provedenog postupka, analizirajući obranu okrivljenika i sve provedene dokaze kako pojedinačno tako i u njihovoj uzajamnoj povezanosti, sud nalazi nedvojbeno utvrđenim da je okrivljenik počinio prekršaj koji mu se stavlja na teret.

30. Naime, nesporno je utvrđeno da je okrivljenik kritične zgode u Zagrebu, na adresi sjedišta okrivljene pravne osobe dana 8. veljače 2022. godine u 15:14 sati, kada je poslao elektroničku poruku društvo D d.o.o. sa zahtjevom za izradu forenzičkog izvješća i sa sigurnošću raspolagao informacijom o sigurnosnom incidentu, dakle, bio je svjestan i imao je saznanja o nastupu incidenta, nije bez odgode, čim su podaci o sigurnosnom incidentu bili dostupni, a najkasnije do 16:14

sati navedenog dana, upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način, te putem PiXi platforme, izvijestio HAKOM o sigurnosnom incidentu koji je prema navodima A1 Hrvatska d.o.o. (dalje: A1) uzrokovan neovlaštenim pristupom sustavu A1 uz prijetnju objavljivanja neovlašteno stečenih osobnih podataka preko 100.000 broja korisnika A1 (dalje: incident), sukladno obvezi propisanoj člankom 99. stavak 7. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), člankom 6. stavak 3. i člankom 7. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21; dalje: Pravilnik) kojim je propisana obveza operatora da u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, putem predložaka propisanog u Dodatku 3. izvijesti Agenciju o nastalom incidentu, te putem PiXi platforme, na način propisan člankom 7. Pravilnika, a što je A1 učinio tek 9. veljače 2022. godine, i to temeljem naknadne upute HAKOM-a.

31. Stoga je u djelu okrivljenika sudac našao obilježja prekršaja iz citirane odredbe navedenog propisa, pa ga je proglasio krivim te mu izrekao novčanu kaznu za koju smatra da je primjerena težini počinjenog prekršaja i stupnju njegove odgovornosti.

32. Prilikom odmjeravanja kazne okrivljeniku uzete su u obzir okolnosti koje utječu na vrstu i visinu kazne, olakotne okolnosti da okrivljenik do sada nije kažnjavan za istovrsne prekršaje, da se radi o izvanrednoj situaciji, činjenicu da je okrivljenik naknadno ispunio svoju obvezu, te na propisan način izvijestio tužitelja o sigurnosnom incidentu, te ponašanje okrivljenika nakon izvršenja prekršaja, dok otegotne nisu utvrđene, radi čega je sudac okrivljeniku izrekao novčanu kaznu kao u izreci presude.

33. Sudac je prilikom odmjeravanja kazne također uzeo u obzir da se radi o operatoru elektroničkih komunikacijskih usluga koji pruža usluge velikom broju korisnika i koji raspolaže iznimno osjetljivim podacima u svojim mreža, te se za istog očekuje da ima razrađenu proceduru postupanja i podjelu uloga i odgovornosti.

34. Temeljem u izreci citiranih propisa, kako je okrivljenik proglašen krivim, to je obvezan naknaditi troškove prekršajnog postupka u paušalnom iznosu, koji je odmjeren s obzirom na složenost i duljinu trajanja postupka.

U Zagrebu, 27. ožujka 2023. godine

Zapisničarka
Jadranka Povoljnjak, v.r.

Sutkinja
Tonka Grgičević, v.r.

UPUTA OPRAVNOM LIJEKU:

Protiv ove presude dopuštena je žalba u roku od 8 (osam) dana od primitka presude. Žalba se podnosi Općinskom prekršajnom sudu u Zagrebu, Avenija Dubrovnik 8, u dva istovjetna primjerka o žalbi odlučuje nadležni sud.

Za točnost otpravka – ovlašteni službenik
Jadranka Povoljnjak