REPUBLIKA HRVATSKA
HRVATSKA REGULATORNA AGENCIJA
ZA MREŽNE DJELATNOSTI

KLASA: UP/I-344-07/23-01/33
URBROJ: 376-05-2-25-10
Zagreb, 9. rujna 2025.

Na temelju članka 16. stavka 1. točke 25. i članaka 161. i 162. Zakona o elektroničkim komunikacijama (NN br. 76/22 i 14/24), te članka 96. Zakona o općem upravnom postupku (NN br. 47/09 i 110/21), u ponovljenom postupku inspekcijskog nadzora pokrenutom po službenoj dužnosti protiv operatora Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, OIB: 70133616033, radi kršenja odredbe članka 43. Zakona o elektroničkim komunikacijama (NN br. 76/22 i 14/24), inspektor elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti donosi

**RJEŠENJE**

I. Utvrđuje se da je trgovačko društvo Telemach Hrvatska d.o.o., Josipa Marohnića 1, Zagreb, postupalo protivno odredbi članka 43. stavku 1. i stavku 2. Zakona o elektroničkim komunikacijama (NN br. 76/22 i 14/24) u razdoblju od 1. studenog 2021. do 6. srpnja 2023., na način da je primjenjivalo mjere nadzora SMS prometa između krajnjih korisnika i blokiralo određene vrste SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge te koje mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.

II. Zabranjuje se društvu iz točke I. ovog rješenja primjena mjera nadzora SMS prometa i blokade SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge i koje nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.

III. U slučaju nepostupanja po ovom rješenju, odgovornoj osobi izvršenika, izreći će se novčana kazna u iznosu od 7.000,00 eura (slovima: sedam tisuća eura). U slučaju daljnjeg neispunjavanja obveze, izreći će se druga, veća novčana kazna.

**Obrazloženje**

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) zaprimila je 3. travnja 2025. presudu Visokog upravnog suda Republike Hrvatske (dalje: VUS) od 18. veljače 2025., poslovni broj: Us II-30/2025-2 (dalje: Presuda) kojom je poništeno Rješenje HAKOM-a KLASA: UP/I-344-07/23-01/33, URBROJ: 376-05-2-23-07 od 6. srpnja 2023. (dalje: Rješenje) i predmet vraćen na ponovni postupak.

Presudom se VUS nije posebno osvrnuo na opravdanost i zakonitost primjene mjera od strane Telemacha, već je uputio HAKOM da u ponovljenom postupku izvede dokaze na okolnost je li

primjena takve mjere nadzora prometa dopuštena u smislu Zakona o kibernetičkoj sigurnosti (NN 14/2024; dalje ZKS).

Naime, u prvotnom postupku inspektor je samostalnom provjerom u razdoblju od 24. veljače 2023. do 2. ožujka 2023. slanjem SMS poruka s broja […] na brojeve […] koji se nalaze u Telemach mreži, čiji je sadržaj identičan ili sličan sadržaju poruka koje aplikacije redovito šalju korisnicima prilikom verifikacije korisničkih računa (npr. Facebook, Google, Instagram i sl.) utvrdio kako se predmetne poruke ne isporučuju primateljima, dok su istovremeno istim primateljima isporučene poruke sadržaja „Test" i/ili „Proba". Primjeri sadržaja poruka koje nisu isporučene su sljedeći: *„Account: xxxxxx is your Samsung account verification code", „Use xxxxx for two-factor authentication on Facebook"* te *„xxxxx is your Google verification code"*. Poruke istih sadržaja upućene u mreže drugih operatora zaprimljene su bez ograničenja.

Temeljem tadašnjeg zahtjeva inspektora Telemach je 13. ožujka 2023. dostavio očitovanje u kojem je, u bitnome, istaknuo kako primjenjuje mjere zaštite svojih korisnika i svoje mreže, a koje se odnose na sprječavanje različitih vrsta poznatih zlouporaba, uključujući onih putem SMS poruka te u tu svrhu Telemach koristi SMS vatrozid (*eng. firewall*) čija je svrha automatizirani nadzor SMS prometa, uključujući usmjeravanje (*eng. routing*) prometa. […]. Telemach je u tadašnjem očitovanju napomenuo kako se ne radi o mjerama nadzora i provjere sadržaja, već o automatiziranim postavkama usporedbe […], a sve u svrhu detekcije potencijalnih zlouporaba, odnosno zaštite sigurnosti i cjelovitosti komunikacijske mreže i njezinih korisnika, sprječavanja nedopuštenog usmjeravanja prometa i neželjene elektroničke komunikacije (*eng. spam*). Također, navodi kako […] te dodatno ističe da nitko nema pristup sadržaju SMS poruka uključujući administratora vatrozida i da se blokirani SMS-ovi dalje ne pohranjuju, ne obrađuju i da nije moguće otključavanje kodiranih meta podataka.

U odnosu na konkretne poruke, Telemach se ranije očitovao da su od partnera koji šalju različite tipove verifikacijskih poruka (banke, Facebook, Google, Tik Tok i sl.) dobili sadržaj koji je implementiran u SMS vatrozid te sustav, kod usporedbe uzorka teksta, isti uspoređuje sa sadržajem dobivenim isključivo od autoriziranog pošiljatelja.

U prilogu navedenog očitovanja Telemach je dostavio svojevrsnu izjavu dobavljača sustava […] te je ukratko opisano kako se radi o kodiranom sadržaju SMS poruka koji se ne otkriva korisnicima sustava (ni bilo kojoj trećoj osobi).

Nakon zaprimljenog očitovanja, inspektor je 14. ožujka 2023. zatražio dodatno očitovanje u odnosu na razloge uvođenja ovakvog nadzora odnosno pojašnjenje iz kojeg razloga su upravo konkretne poruke predstavljale rizik odnosno opasnost za sigurnost mreža i usluga.

U dodatnom očitovanju od 17. ožujka 2023. Telemach je dostavio pojašnjenje nastavno na upit inspektora vezano za rizik koje su predmetne poruke predstavljale odnosno pojašnjenje opasnosti za sigurnost mreže i usluga Telemacha. Istaknuo je kako su predmetne poruke upućene s MSISDN-a krajnjeg korisnika, a koji pri tome nije autorizirani partnerski kanal, odnosno nije očekivana komunikacija krajnjeg korisnika te naveo kako je krajnji cilj slanja takvih poruka drugim krajnjim korisnicima dobivanje povjerenja u legitimitet pošiljatelja pa ju sustav automatizmom identificira i blokira kao *smishing* poruku (skraćenica za "*SMS phishing*"). Drugim riječima, Telemach smatra da blokiranjem navedenih poruka sprječava krađu identiteta krajnjih korisnika te dodatno ističe kako u kontekstu *smishing-a* isti može biti potpomognut zlonamjernim softverom ili internetskim stranicama za prijevare. Nadalje, navodi da trenutno blokiranje predmetnih poruka obeshrabruje prevarante u

slanju velike količine SMS poruka (*SMS spamming*), čime se postiglo očuvanje sigurnosti cjelokupne elektroničke komunikacijske mreže i usluga.

Telemach je u svom očitovanju nastavno na pitanje inspektora vezano za dostavu primjera poruka koje su evidentno utjecale na sigurnost Telemach elektroničke komunikacijske mreže i usluge naveo kako nema primjera poruka jer ne pohranjuje sadržaj poruka i prevenciju obavlja SMS vatrozid. Konačno, Telemach u svom očitovanju u ranijem postupku navodi da je implementirao SMS vatrozid […] te je istakao pozitivne strane korištenja predmetnog sustava u cilju sprječavanja krađe osjetljivih podataka, a koje krajnji korisnici imaju na svojim telefonima, u aplikacijama i sl. Kao osnovu navedenog postupanja Telemach je naveo Opću uredbu o zaštiti podataka (GDPR), Direktivu 2022/2555 o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije (NIS 2 Direktiva) i relevantne ENISA dokumente.

S obzirom da je u ponovljenom očitovanju bilo nejasno što prema navodima Telemacha predstavlja „autorizirani partnerski kanal“ inspektor je zatražio dodatno očitovanje vezano za predmetno te je Telemach 24. ožujka 2023. dostavio pojašnjenje kako se […].
Na prijedlog Telemacha, a u svrhu dodatnog pojašnjenja načina postupanja i primjene SMS nadzora, dana 27. travnja 2023. održana je usmena rasprava na kojem su predstavnici Telemacha dodatno pojasnili funkcioniranje SMS vatrozida u dijelu koji se odnosi na blokiranje dolaznih SMS poruka […]. Predstavnik Telemacha je napomenuo kako sustav po njihovu mišljenju zadovoljava sve EU standarde te da je usklađen sa svim pravnim propisima. Isto tako, napomenuto je kako Telemach primjenjuje blokiranje SMS poruka na način […]. Predstavnica Telemacha je završno ponovila kako se prilikom nadzora ne ulazi u sadržaj SMS poruka te da Telemach mora poduzeti sve kako bi zaštitio svoje krajnje korisnike.

Na usmenoj raspravi predstavnica Telemacha predala je u spis Izjavu […] (dalje: Izjava), direktora programa organizacije Mobile Ecosystem Forum Ltd, (dalje: MEF) čiji je Telemach član, kao i prezentaciju pod nazivom *„The Mobile Ecosystem Forum (MEF) & System Messaging Anti-Fraud“*.

Prezentacija MEF-a koja je dostavljena u spis ukratko izlaže o organizaciji, ciljevima i načinu rada udruženja te opisuje tzv. SMS Sender ID Registry programe i njegove rezultate u Ujedinjenom Kraljevstvu, kao i *Business SMS Fraud Framework* koji definira rizike SMS prijevare. Prezentacija opisuje na koji način *Business SMS Ecosytem* funkcionira odnosno način osiguravanja autorizirane rute izravno od pošiljatelja prema primatelju poruke te pojašnjava vrste SMS prijevara i posljedice odnosno učinke pojedinih vrsta prijevara, kojih je ukupno prepoznato četrnaest. Također, prezentacijom je ukratko opisan sadržaj Kodeksa ponašanja čiji su potpisnici članovi MEF-a.

U ponovljenom postupku inspektor je zaključkom zatražio očitovanje od Telemacha vezano uz presudu VUS-a od 18. veljače 2025. te dostavu eventualnih novih dokaza vezanih za navode iz ranijeg postupka.

Telemach je dostavio svoje očitovanje 12. svibnja 2025. te uz navode zakonskih propisa koji su po njemu relevantni za navedeni inspekcijski nadzor ponovno je obrazložio razloge primjene vatrozida odnosno kako njegova primjena nije protivna članku 43. stavku 1. Zakona o elektroničkim komunikacijama (NN br. 76/22 i 14/24; dalje: ZEK) već je zakonita i potrebna budući je potrebna za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga kao i za otkrivanje i otklanjanje sigurnosnog rizika ili napada na elektroničke komunikacijske mreže i usluge.

Dodatno, Telemach se u svom očitovanju osvrnuo na ZKS kojim su propisane dužnosti operatora u primjeni mjera potrebnih za postizanje i očuvanje visoke razine kibernetičke sigurnosti. Telemach tako ističe kako je cilj tih mjera odnosno kako je dužnost operatora zaštiti mrežne i informacijske sustave i fizičko okruženje tih sustava od incidenata uzimajući u obzir sve opasnosti kojima su ti sustavi izloženi. Ističe kako odredbe članka 24., 26. stavka 1., 2. i 3. te članka 27. ZKS-a propisuju obveze operatora za implementaciju predmetnih mjera koje služe za sprječavanje ili smanjivanje na najmanju moguću mjeru učinka incidenta na mrežne i informacijske sustave. Naveo je u očitovanju kako ZKS u članku 4. stavku 1. točki 11., 45. i 46. propisuje pojmove sigurnosti, incidenta i rizika, a koji nisu definirani ZEK-om i kako isti potvrđuju opravdanost i nužnost implementacije sustava vatrozida koji mora blokirati SMS poruke koje dolaze od neakreditiranog pošiljatelja i koje sadrže obilježja poslovne transakcije. Prema navodima Telemacha, radi se o odgovarajućoj i razmjernoj mjeri upravljanja kibernetičkim sigurnosnim rizicima.

Konačno, Telemach dostavlja u očitovanju statističke podatke vezano za prijevare korisnika elektroničkih komunikacija i to vezano za krađu identiteta, prijevare pri internetskoj kupnji te u slučaju phishing napada iz kojih je vidljiv porast prijevara u proteklom razdoblju te navodi da je u određenim zemljama EU (Finska, Poljska i Belgija) dozvoljena primjena mjera kojima je cilj identificiranje, prevencija i sprečavanje prijevara.

Isto tako, Telemach u svom očitovanju predlaže dokaz vještačenjem po ovlaštenom sudskom vještaku za informacijsku sigurnost i zaštitu informacija na okolnost je li vatrozid Telemacha u smislu odredbi ZKS-a dopuštena mjera nadzora SMS poruka, koja je nužna za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.

U predmetnom postupku inspektor je uzeo u obzir sve dokaze i očitovanja prikupljena u prethodnom i ponovljenom postupku te razmotrio navode Telemacha u odnosu na opravdanost primjene mjera sukladno odredbama ZKS-a. U odnosu na predloženo vještačenje na okolnost je li vatrozid Telemacha u smislu odredbi ZKS-a dopuštena mjera nadzora SMS poruka, inspektor je zaključio kako ovako predloženo vještačenje ne bi bilo opravdano. Naime, sadržaj predloženog vještačenja upravo se odnosi na predmet ovog postupka. Ocjena opravdanosti primjene mjera je u nadležnosti HAKOM-a, konkretno inspektora u ovom postupku te se ne može prepustiti vještaku ili nekoj trećoj osobi. Kako činjenice u ovom postupku nisu sporne te ne postoje činjenice za čije utvrđivanje ili ocjenu bi inspektoru bilo potrebno stručno znanje vještaka, inspektor nije temeljem prijedloga Telemacha odredio vještačenje u ovom postupku.

Nakon zaprimanja očitovanja na zaključak, inspektor je u ponovljenom postupku zaključio kako je Telemach u razdoblju od 1. studenog 2021. do donošenja rješenja inspektora 6. travnja 2024. postupao protivno odredbi članka 43. stavka 1. i 2. ZEK-a prilikom primjene opisanih mjera nadzora i kontrole SMS poruka budući je odredbom članka 43. stavka 1. ZEK-a propisano kako je u svrhu osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama zabranjeno slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 52. ZEK-a te u slučajevima utvrđenim posebnim zakonima.

Stavkom 2. istog članka propisana je iznimka od spomenute zabrane kojom je utvrđeno da se zabrana ne primjenjuje na tehničku pohranu podataka koji su nužni za prijenos komunikacije, u slučajevima kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža

i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, ne zadirući pri tome u načela zaštite tajnosti podataka.

Iz dokaza prikupljenih u predmetnom postupku, kako iz novog tako i iz prethodnih očitovanja Telemacha, proizlazi kako je Telemach implementirao mjere nadzora sadržaja SMS poruka, bez valjanog opravdanja ili argumentacije iz koje bi proizlazilo da je isto nužno potrebno te dodatno ničim ne opravdava da blokirane SMS poruke predstavljaju sigurnosni rizik ili bilo kakvu vrstu opasnosti za elektroničke komunikacijske mreže ili usluge, a što predstavlja preduvjet sukladno spomenutoj zakonskoj odredbi. Naime, sama činjenica […], ne znači istodobno da prijenos ili zaprimanje takvih poruka može potencijalno ugroziti sigurnost mreža ili usluga. Telemach u svojim očitovanjima ni na koji način nije obrazložio konkretni rizik ili opasnost za sigurnost mreža ili usluga, nije obrazložio da bi blokiranje takvih poruka bilo nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, već navedeno opravdava zaštitom krajnjih korisnika od eventualnih zlouporaba. Telemach se također poziva na obveze koje proizlaze iz GDPR-a, NIS2 Direktive i ENISA-ne dokumente, ne pojašnjavajući zbog kojih je to konkretno obveza vatrozid implementiran.

Nadalje, prezentacija koja je dostavljena u spis, nije ukazala na opravdanost i zakonitost postupanja Telemacha budući da se isključivo radi o opisu načina na koji se u današnje vrijeme vrše prijevare putem SMS poruka. Isto tako, spomenuta prezentacija nisu dostavljene od stranke u postupku, već se radi o trećim osobama odnosno udruženju koje nije stranka u postupku.

Iz svega navedenog slijedi da postupanje Telemacha podrazumijeva nadzor SMS prometa koji se, između ostalih parametara, vrši i […]. U postupku je nesporno utvrđeno kako implementirani sustav Telemacha vrši nadzor cjelokupnog SMS prometa odnosno provodi nadzor sadržaja SMS poruka, a primjena automatiziranog nadzora bez ljudskog posredovanja, mjera kriptiranja ili ograničavanja uvida u zapise ne mijenja prethodni zaključak.

Naime, kriptiranje podataka ne utječe na činjenicu da sustav koji je pod nadzorom Telemacha vrši kontrolu sadržaja (točnije uzorka teksta) koji se razmjenjuje između krajnjih korisnika, koja je odredbom članka 43. stavak 2. ZEK-a dopuštena samo u iznimnim slučajevima (kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge*)*.
Ova iznimka utvrđena je za konkretne, iznimne slučajeve koji bi morali opravdati primjenu takvih mjera. U konkretnom slučaju ne postoji valjano opravdanje da bi predmetne poruke na bilo koji način utjecale na sigurnost elektroničkih komunikacija i/ili usluga odnosno da bi bio ispunjen bilo koji od uvjeta iz članka 43. stavka 2. ZEK-a koji opravdava iznimku od propisanu stavkom 1. istog članka.

Isto tako, treba imati na umu da su sporne SMS poruke bez bilo kakvih ograničenja su bile dostavljene i u mrežu Hrvatskog Telekoma d.d. i u mrežu A1 Hrvatska d.o.o. Navedeni operatori imaju daleko veći broj korisnika od Telemacha te bi stoga neprimjena spornih mjera u njihovim mrežama, prema procjenama sigurnosnih rizika Telemacha, trebala uzrokovati enormne štete i za krajnje korisnike i za te operatore, što očito u praksi ipak nije slučaj.

Vezano uz uputu VUS-a da se u ponovljenom postupku provjeri opravdanost ovih mjera u odnosu na ZKS, inspektor je u odnosu na navedeno zatražio očitovanje Telemacha. Telemach se u svom očitovanju od 12. svibnja 2025. pozvao na obveze ZKS-a te naveo važnost sprječavanja ili

smanjivanja učinka incidenta na mrežne i informacijske sustave pritom smatrajući da je implementacija SMS vatrozida jedna od u mjera koja je nužna kako bi zaštitili svoje poslovanje i pružanje usluga. Nadalje, primjenu SMS vatrozida smatraju odgovarajućom i razmjernom mjerom sukladno ZKS-u.

Vezano za primjenu ZKS-a inspektor ističe kako ZKS u svojim odredbama ne uređuje primjenu specifičnih mjera sigurnosti. Odredbe članka 26. ZKS-a koje je Telemach citirao u svom očitovanju definiraju obvezu primjene odgovarajućih i razmjernih mjera upravljanja kibernetičkim sigurnosnim rizicima, kojima je cilj zaštita mrežnih i informacijskih sustava od incidenata, uzimajući pritom u obzir sve opasnosti kojima su ti sustavi izloženi. Kao što je i prethodno utvrđeno, Telemach ničime nije dokazao da se u slučaju slanja konkretnih poruka radi o bilo kakvom riziku za sigurnost mrežnih i informacijskih sustava, već isključivo ukazuje na preveniranje potencijalnih opasnosti za krajnje korisnike.

Nadalje, člankom 30. stavkom 4. ZKS-a propisano je da se mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe uređuju uredbom iz članka 24. ZKS-a odnosno Uredbom o kibernetičkoj sigurnosti (NN 135/24). Prilog II poglavlje 6. predmetne uredbe odnosi se na osiguravanje kibernetičke sigurnosti mreže od strane subjekata te točka 6.4. koja se odnosi na predmetnu situaciju navodi sljedeće: *„implementirati mehanizme praćenja odlaznog i dolaznog mrežnog prometa u svrhu smanjenja rizika od kibernetičkog napada te definirati metode filtriranja nepoželjnog mrežnog prometa u smislu prepoznavanja potencijalnih indikatora kompromitacije. Ovo uključuje postavljanje odgovarajućih alata za praćenje i analizu mrežnog prometa koji omogućuju identifikaciju i automatsko blokiranje potencijalno opasnih aktivnosti. Također, subjekt mora definirati i primijeniti metode filtriranja nepoželjnog mrežnog prometa, poput upotrebe sustava za otkrivanje i sprječavanje napada (IDS/IPS) i drugih sigurnosnih rješenja. Svi implementirani mehanizmi i metode filtriranja moraju biti redovito revidirani i ažurirani kako bi se održala visoka razina sigurnosti mreže. Ova mjera ne utječe na zabranu nadzora elektroničkih komunikacija reguliranu zakonom koji uređuje elektroničke komunikacije“*. Slijedom navedenog, obveze propisane ZKS-om su primjenjive samo ukoliko iste nisu u suprotnosti s obvezama odnosno zabranama nadzora prometa koje proizlaze iz ZEK-a, a što nije slučaj u predmetnom inspekcijskom nadzoru.

Stoga je inspektor sagledavajući sve utvrđene relevantne činjenice točkom II. rješenja naložio zabranu primjene mjera nadzora elektroničkih komunikacija predmetnih SMS poruka, kada nisu ispunjeni uvjeti iz članka 43. stavka 2. ZEK-a, a na način kako je to vršio Telemach.

Nadalje, inspektor je temeljem članka 142. Zakona o općem upravnom postupku (NN br. 47/09, 110/21) za slučaj nepostupanja po ovom rješenju odgovornoj osobi izvršenika zaprijetio izricanjem novčane kazne u iznosu od 7.000,00 eura (slovima: sedam tisuća eura), a za slučaj daljnjeg neispunjavanja obveze, izricanjem druge, veće novčane kazne.

Na temelju svega navedenog odlučeno je kao u izreci.

Ovo rješenje će se na odgovarajući način objaviti na internetskoj stranici HAKOM-a.

**UPUTA O PRAVNOM LIJEKU:**
Protiv ovog rješenja žalba nije dopuštena. Protiv ovog rješenja može se, u roku od 30 dana od dana njezina primitka, pokrenuti upravni spor pred Visokim upravnim sudom.

***INSPEKTOR ELEKTRONIČKIH KOMUNIKACIJA***

***Andro Marčev dipl. ing. prom.***

Dostaviti:

1. Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, UP – osobna dostava
2. U spis