



Komentari T-HT Grupe¹ u okviru javne rasprave o prijedlogu odluke HAKOM-a o uvođenju Sustava pokazatelja – SPOK kao elektroničkog načina prikupljanja podataka o tržištu elektroničkih komunikacija, listopad 2009.

Zahvaljujemo na mogućnosti da kroz javnu raspravu izložimo svoje komentare na prijedlog uvođenja Sustava pokazatelja – SPOK kao elektroničkog načina prikupljanja podataka o tržištu elektroničkih komunikacija u Republici Hrvatskoj (dalje u tekstu: Sustav SPOK) i da time skrenemo pažnju na pojedina pitanja koja se u okviru uspostave Sustava SPOK nameću važnima.

Na početku je važno istaknuti kako članice T-HT Grupe podržavaju nastojanja Hrvatske agencije za poštu i elektroničke komunikacije (HAKOM) usmjerena ka poboljšanju učinkovitosti u radu HAKOM-a, u smislu informatizacije postupka prikupljanja i obrade podataka o poslovanju operatora i stanju na tržištu elektroničkih komunikacija. Ovo osobito iz razloga što se sredstva za financiranje rada HAKOM-a prvenstveno osiguravaju iz sredstava operatora, bilo u vidu naknada za uporabu ograničenih resursa (brojeva, adresa, frekvencija), bilo u vidu posebne naknade za obavljanje drugih poslova HAKOM-a, te su stoga inicijative koje vode ka modernizaciji rada HAKOM-a putem informatizacije procesa i usluga, a kojima se potiče produktivnost i bolja učinkovitost, a time posredno utječe i na smanjenje troškova u poslovanju HAKOM-a, u interesu svih sudionika na tržištu.

Stoga, načelno gledajući, prijedlog uvođenja Sustava SPOK držimo pozitivnim pomakom na hrvatskom tržištu, te potičemo i podržavamo modernizaciju rada HAKOM-a.

Međutim, s obzirom da se u jednom dijelu predloženog modela Sustava SPOK operatorima nameću određene dodatne obveze, te vodeći računa o tome da će operatori putem Sustava SPOK upućivati HAKOM-u i povjerljive podatke, čija se zaštita mora osigurati, ispod dajemo detaljniji osvrt na upravo navedena, najvažnija pitanja u ovom projektu.

1) Dodatne obveze na strani operatora

Nesporno je da je HAKOM, sukladno članku 15. Zakona o elektroničkim komunikacijama (dalje u tekstu: ZEK), ovlašten prikupljati od operatora sve potrebne podatke i obavijesti, uključujući financijske podatke i klasificirane podatke te podatke koji su određeni poslovnom tajnom, za potrebe obavljanja poslova koji sukladno članku 12. ZEK-a ulaze u nadležnost HAKOM-a. S druge strane, operatori su obvezni postupiti po zahtjevu HAKOM-a za prikupljanje podataka, ukoliko je taj zahtjev razmjeran poslovima koje HAKOM obavlja te ukoliko isti sadrži pravni temelj, predmet i svrhu zahtjeva, razinu podrobnosti zatraženih podataka i primjeren rok za provedbu zahtjeva (članak 15. stavak 2. ZEK-a).

Prema našem shvaćanju dokumenta koji je predmet javne rasprave, Sustav SPOK bi, kao elektronički sustav prikupljanja podataka, zamijenio dosadašnji proces prikupljanja podataka o tržištu elektroničkih komunikacija u RH koji je uključivao pisanu korespondenciju između HAKOM-a i operatora i dostavu putem pošte, što je načelno prihvatljivo.

¹ HT-Hrvatske telekomunikacije d.d., T-Mobile Hrvatska d.o.o., Iskon Internet d.d.



Međutim, prema opisu Sustava SPOK, takav sustav zahtijeva i izradu tzv. „lokalnih sustava u domeni operatora elektroničkih komunikacija“, što bi drugim riječima značilo izradu posebnih sučelja na strani operatora, koji bi bili u stalnoj vezi sa središnjim informatičkim sustavom HAKOM-a.

Skrećemo pažnju da se ovime operatorima nameće obveza dodatnih ulaganja u svrhu izrade odgovarajućeg sučelja za dostavu podataka, a za što ne nalazimo temelj u važećim propisima.

Naime, kao što smo prethodno naveli, HAKOM je ovlašten prikupljati a operatori su dužni dostaviti podatke u pisanom obliku međutim, članak 15. ZEK-a ne daje HAKOM-u pravo nametati operatorima bilo kakve druge dodatne obveze (što uključuje i obvezu izrade i uspostave zasebnog elektronskog sučelja) osim dužnosti dostave podataka u pisanom obliku, a koju obvezu operatori već sada uredno izvršavaju putem pisanih priopćenja koja se dostavljaju poštom.

Stoga, makar podržavamo modernizaciju postupanja HAKOM-a u dijelu prikupljanja podataka o stanju tržišta, držimo da isto ne bi smjelo ići na štetu operatora, u smislu nametanja operatorima bilo kakvih dodatnih troškova radi udovoljavanja bilo kakvim dodatnim obvezama za koje ne postoji uporište u važećim propisima.

S obzirom da u dokumentima koji su predmet ove javne rasprave nisu detaljnije opisani zahtjevi koje bi lokalni sustavi morali zadovoljavati, odnosno nije jasno da li će operatori samostalno osiguravati razvoj lokalnog sustava ili će od strane HAKOM-a biti ponuđeno gotovo rješenje, u nastavku iznosimo samo načelne komentare za koje smatramo da je nužno da ih HAKOM uzme u obzir prije donošenja konačne odluke o uvođenju Sustava SPOK.

Ovdje skrećemo pozornost da operatori već izdvajaju znatne iznose za rad HAKOM-a, i to u znatno povećanim iznosima u odnosu na iznose koji su se plaćali po propisima koji su bili na snazi prije donošenja novog Pravilnika o plaćanju naknada za obavljanje poslova HAKOM-a (NN 154/08, dalje u tekstu Pravilnik). Naime, prema ovom Pravilniku naknada za rad HAKOM-a koja se plaća u postotku od godišnjeg bruto prihoda operatora povećala se sa 0,2% na 0,32%, dok su se naknade za frekvencije/numeraciju koje plaćaju operatori pokretnih elektroničkih komunikacijskih mreža također znatno povećale.

Uz sve navedeno, skrećemo pažnju da je HAKOM u okviru nedavno provedenih postupaka analize veleprodajnih tržišta nametnuo članicama T-HT Grupe veliki broj dodatnih obveza na veleprodajnoj i maloprodajnoj razini, koje obveze zahtijevaju angažman znatnih financijskih sredstava kako bi se istima udovoljilo u propisanim rokovima.

Stoga, sudionici hrvatskog tržišta elektroničkih komunikacija, a osobito operatori kojima su nametnute obveze uslijed statusa znatnije tržišne snage, već su po osnovi regulacije tržišta elektroničkih komunikacija znatno opterećeni naknadama kao i troškovima udovoljavanja regulatornim obvezama, te se postavlja pitanje kako osigurati učinkovito pružanje usluga, a naročito kako poboljšati učinkovitosti na strani operatora, ako će se dodatne obveze, a time i dodatni troškovi usklađivanja s regulatornim zahtjevima, konstantno povećavati.

Dapače, dodatne obveze i pripadajući troškovi potiču upravo suprotno, tj. generiraju dodatne sustave na strani operatora, izdatke za njihovo održavanje, zahtijevaju angažman (i obučavanje) ljudskih resursa koji će raditi na tim sustavima, što sve zajedno povećava trošak i dovodi u pitanje učinkovitost i cilj uvođenja Sustava SPOK.



Prema našim preliminarnim procjenama troška, uvođenje i održavanje lokalnog SPOK sustava na strani T-HT-a nosi jednokratni trošak od cca. 120.000 kn za implementaciju sučelja, dok bi troškovi održavanja iznosili cca. 30.000 kn godišnje. Međutim, s obzirom da nismo imali mogućnost uvida u WDSL specifikaciju web servisa za Sustav SPOK, moguće je da će ovi troškovi biti i viši, ovisno o rješenjima predviđenim u WDSL specifikaciji.

Drugim riječima, trošak operatora nije sveden samo na početno ulaganje u uspostavu lokalnog sustava, nego će posljedično nastati i stalni operativni troškovi, za koje je upitno mogu li uvođenjem predloženog sustava biti niži od sadašnjih troškova operatora pri izradi i dostavi izvješća HAKOM-u u pisanom obliku putem pošte.

Slijedom gore navedenog, naš prijedlog je uspostaviti središnji informatički sustav SPOK na strani HAKOM-a ali bez obveze uspostave lokalnih sustava u domeni operatora elektroničkih komunikacija, s obzirom da bi nametanjem takve obveze operatorima, prema našem mišljenju, HAKOM postupao bez pravne osnove, već na način da se operatorima omogući da pristupaju Sustavu SPOK putem sigurnosno zaštićenog web sučelja HAKOM-a. Stoga pozivamo HAKOM da razmotri naš prijedlog te ga definira i kao takvog uputi na ponovnu javnu raspravu.

2) Zaštita povjerljivih podataka

Zaštita povjerljivih podataka o poslovanju operatora koji će se dostavljati HAKOM-u putem Sustava SPOK, ističe se kao jedno od važnih pitanja koje prepoznaje i HAKOM u prijedlogu odluke. Dapače, zaštita sigurnosti razmjene, obrade i pohrane podataka operatora ističe se u prijedlogu odluke HAKOM-a kao jedan od razloga uvođenja Sustava SPOK, jer će spomenuti sustav, prema mišljenju HAKOM-a, povećati razinu sigurnosti podataka time što će se izbjeći zaprimanje i evidentiranje izvještaja u pisarnicama, razmjena podataka elektroničkom poštom, pohranjivanje podataka po računalima i poslužiteljima, pohranjivanje na medije i slično.

U vezi s pitanjem zaštite povjerljivosti podataka, skrećemo pozornost na dva važna aspekta:

- a. poštivanje dodatnih obveza po pitanju objave poslovnih podataka, vodeći računa o uvrštenju dionica T-HT-a na burze vrijednosnih papira, i
- b. tehnički aspekt zaštite povjerljivosti podataka, sukladno normi ISO 27001

Vežano uz pitanje pod točkom a. gore, izražavamo zadovoljstvo za ukazano razumijevanje HAKOM-a te već uspostavljene mehanizme zaštite povjerljivih podataka T-HT-a, uključujući i podatke povezanih društava T-HT-a, u dosadašnjim postupcima dostave podataka, i to osobito u pogledu onih podataka o poslovanju društva koji se smatraju povlaštenim informacijama u smislu Zakona o tržištu vrijednosnih papira.

S obzirom da će potreba zaštite povlaštenih informacija postojati i u okviru predloženog Sustava SPOK, podsjećamo na naša očitovanja po ovom pitanju od 22. listopada i 21. prosinca 2007. godine, te tamo opisane dodatne obveze po pitanju objave poslovnih podataka kompanije, što osobito uključuje zabranu objave povlaštenih informacija na bilo koji način (uključujući i web stranice HAKOM-a) prije njihove objave na burzama dionica.



Međutim, s obzirom da se o okviru predloženog Sustava SPOK predviđaju nove „sigurnosne razine korisnika“ na strani HAKOM-a, kojima će biti dopušten uvid u podatke koji će se tamo generirati, potrebno je provjeriti da li će uslijed uvođenja Sustava SPOK biti potrebno ažurirati popis osoba koje se na strani HAKOM-a smatraju osobama koje raspoložu povlaštenim informacijama o T-HT-u (tzv. upućenici), a koje su uvrštene u *Stalni popis upućenika HT-Hrvatskih telekomunikacija d.d.*

Također, a s obzirom na gore spomenute nove „sigurnosne razine korisnika“ središnjeg sustava HAKOM-a (voditelj, stručnjak i gost), smatramo potrebnim detaljnije definirati prava i obveze za svaku sigurnosnu razinu korisnika, s obzirom da trenutne definicije nisu jasne.

Naime, prema prijedlogu odluke, razina korisnika voditelj „ima najvišu razinu sigurnosti koja omogućava ograničenje pristupa u nekom razdoblju vezano za sve izvještaje određenog operatora“, međutim, iz ove formulacije nije jasno:

- kome voditelj ograničava pristup (da li ostalim „sigurnosnim razinama korisnika“ ili se ograničavanje pristupa odnosi na objavu podataka na službenim stranicama HAKOM-a)? Prema našem mišljenju ovlasti voditelja odnosile bi se na obje situacije.
- tko određuje razdoblje trajanja ograničenja pristupa?
- da li se ograničavanje pristupa odnosi na sve izvještaje operatora ili je moguće odrediti uži skup podataka na koje će se ograničenje odnositi?

U svrhu uklanjanja dvojbi, ističemo kako je prema našem mišljenju operator dužan ukazati HAKOM-u na potrebe ograničenja pristupa pojedinim podacima.

Predlažemo dodatno razmotriti gore navedena pitanja i detaljno ih definirati u pravilima korištenja/upravljanja Sustavom SPOK, pri čemu smatramo nužnim dodatno konzultirati operatore.

Vezano uz pitanje pod točkom b. gore, a uzimajući u obzir zahtjeve norme ISO27001 koja je na međunarodnoj razini prihvaćena kao sigurnosni standard, navodimo sljedeće.

Norma ISO27001 daje smjernice za implementaciju, izvršavanje, nadzor, provjeru, održavanje i poboljšavanje sustava upravljanja informacijskom sigurnošću. Poštivanje navedene norme jamči poštivanje dostupnosti, cjelovitosti i povjerljivosti podataka i informacijskih sustava te osiguravanje poslovnih, pravnih i ugovorenih sigurnosnih obveza. Ova norma omogućava i certifikaciju po navedenom standardu, koja tada potvrđuje da certificirana kompanija provodi upravljanje sustavom informatičke sigurnosti u skladu s trenutno najboljom međunarodnom praksom po ovom pitanju.

S obzirom da je T-HT trenutno u procesu certifikacije po spomenutoj normi, dužni smo slijediti njene preporuke u pogledu postupanja s podacima i informacijskim sustavima.

Stoga, a uzimajući u obzir da će se u okviru Sustava SPOK između operatora i HAKOM-a razmjenjivati podaci kategorije „*povjerljivo*“ i/ili „*stogo povjerljivo*“, takvi podaci moraju biti šifrirani tijekom bilo kojeg prijenosa, bilo da se radi o prijenosu između operatora i sustava HAKOM-a, bilo da se radi o internom prijenosu unutar lokalne mreže HAKOM-a.

Također, takvi podaci trebaju biti šifrirani i u bazi podataka Sustava SPOK, kao i svim ostalim bazama podataka u koje će se isti uvrstiti/u kojima će se navedeni podaci prikupljati.



Datoteka u kojoj će se bilježiti radnje na Sustavu SPOK mora biti zaštićena od neautoriziranog pristupa, promjena i brisanja. Naime, u prijedlogu odluke trenutno se navodi jedino da se sve radnje na Sustavu SPOK „bilježe ...u sigurnosnoj posebno zaštićenoj datoteci“, ali bez izričitog navođenja da i pristup takvoj datoteci mora biti zaštićen i strogo nadziran.

Također, smatramo kako je u dokumentu potrebno dodatno razraditi način osiguranja sigurnosti podataka u odnosu na administratore koji će na strani HAKOM-a održavati aplikaciju, otklanjati greške i obavljati nadogradnju sustava, a koji pritom ne bi smjeli imati uvid u sadržaj aplikacije (tj. u podatke).

Dalje, u prijedlogu odluke nije definiran rok čuvanja „*povjerljivih*“ i „*strogo povjerljivih*“ podataka te način njihovog uništavanja nakon isteka roka za njihovu uporabu. Brisanje podataka nakon prestanka potrebe za istima treba biti izvedeno na siguran način koji onemogućuje obnavljanje tako izbrisanih podataka. Vodeći se normom ISO27001, molimo HAKOM da u okviru dokumenta koji će regulirati pravila korištenja Sustava SPOK opiše način na koji planira provesti spomenuto trajno brisanje nepotrebnih podataka.

Zaključno, a uzimajući u obzir pravila čuvanja „*povjerljivih*“ i „*strogo povjerljivih*“ podataka prema normi ISO27001, držimo da bi operatori trebali imati pravo na uvid u sigurnosne mjere koje su u primjeni na strani HAKOM-a i to na onim informacijskim resursima kojima se ostvaruje pristup, čuvanje i prijenos „*povjerljivih*“ i „*strogo povjerljivih*“ podataka operatora.

3) Tehnički aspekti Sustava SPOK

Makar smatramo da u važećim propisima ne postoji pravno valjano uporište za nametanje operatorima dodatne obveze u vidu izrade „*lokalnih sustava na strani operatora*“, a kako smo to detaljnije obrazložili pod točkom 1) ovih komentara, ispod se opreza radi detaljnije očitujemo i po pitanju predviđenog roka za uspostavu spomenutih sustava, kao i tehničkog rješenja, ne umanjujući time cilj i važnost našeg očitovanje pod točkom 1) gore.

Rok uspostave lokalnih sustava

Prema točki III dispozitiva prijedloga odluke HAKOM-a, operatori elektroničkih komunikacija bili bi dužni implementirati „*lokalne sustave u domeni operatora*“ najkasnije u roku 3 mjeseca od dana donošenja odluke o uvođenju Sustava SPOK.

Skrećemo pozornost da je za implementaciju lokalnih sustava na strani T-HT-a neophodna tehnička specifikacija, tj. WSDL specifikacija web servisa na strani HAKOM-a te da je ista trebala biti priložena prijedlogu odluke, te prezentirana javnosti u okviru javne rasprave. Tek po analizi tehničke specifikacije biti će moguće utvrditi mogućnost implementacije Sustava SPOK u roku od 3 mjeseca.

Stoga, a kako u ovom trenutku nismo u mogućnosti očitovati se o tome da li je rok od 3 mjeseca dovoljan za implementaciju „*lokalnog sustava u domeni operatora*“, te makar stojimo kod našeg prijedloga u smislu uspostave „web sučelja“ za dostavu podataka HAKOM-u, podredno i opreza radi napominjemo kako bi definiranje rokova za uspostavu „*lokalnih sustava u domeni operatora*“ trebalo podlijegati dogovoru između HAKOM-a i operatora.



Komentari tehničke prirode

U dokumentu koji će definirati pravila korištenja Sustava SPOK, osim opisanih sigurnosnih zahtjeva potrebno je dodati i sljedeće:

- sesija korisnika treba biti ograničena na definirani vremenski interval (maksimalno 30 min), a ne na proizvoljno kratki period;
- svakom korisniku treba kreirati jedinstveno korisničko ime, sa korisničkom lozinkom minimalne dužine 8 znakova, kombinacija velikih i malih slova i brojeva;
- trajanje korisničke lozinke mora biti ograničeno na maksimalno 90 dana.

Osim postojećeg priloga prijedloga odluke HAKOM-a, odluci o uvođenju Sustava SPOK potrebno je priložiti i sljedeće dokumente, a koji trebaju, kao što smo već napomenuli, biti predmet prethodne javne rasprave:

- Tehničku specifikaciju web servisa na strani HAKOM-a
- Proceduru za eskalaciju incidenata Sustava SPOK
- Proceduru za upravljanje korisničkim računima Sustava SPOK

Makar stojimo kod našeg prijedloga u smislu uspostave „web sučelja“ za dostavu podataka HAKOM-u, podredno i opreza radi, a s obzirom da operatori već imaju implementirana druga sučelja prema HAKOM-u za potrebe ispunjenja drugih obveza, predlažemo da HAKOM razmotri mogućnosti uspostave standardnog rješenja za komunikaciju prema HAKOM-u (bilo da se radi o agencijskoj bazi za potrebe prenosivosti broja, bilo o prikupljanju podataka).

Zaključno, predlažemo da se po pitanju uspostave Sustava SPOK održi sastanak na kojemu bi se detaljnije razmotrili gore navedeni komentari te razriješile dvojbe (ukoliko će ih biti) te u tom smislu ističemo da smo otvoreni za daljnju suradnju u ovom projektu.