IZVEŠTAJO OBRADI PODATAKA O LIČNOSTI

-REPUBLIČKI FOND ZA ZDRAVSTVENO OSIGURANJE-

SHARE FONDACIJA
NOVI SAD

USAID
OD AMERIČKOG NARODA

Izrada ovog izveštaja omogućena je uz podršku američkog naroda putem Američke agencije za međunarodni razvoj (USAID). Za sadržaj ovog izveštaja odgovorna je SHARE Fondacija i on ne mora nužno odražavati stavove USAID-a ili Vlade Sjedinjenih Američkih Država.

OPŠTI PODACI

Podaci o osnovnoj delatnosti, sedištu, pravnim aktima, veb sajtu i slično

Republički fond za zdravstveno osiguranje (RFZO) je pravno lice sa statusom organizacije za obavezno zdravstveno osiguranje čija je osnovna delatnost da osiguranim licima obezbedi ostvarivanje prava iz oblasti obaveznog zdravstvenog osiguranja.

Prava, obaveze i odgovornost RFZO-a utvrđene su Zakonom o zdravstvenom osiguranju ("Sl. glasnik RS", br. 107/2005, 109/2005 - ispr., 57/2011, 110/2012 - odluka US, 119/2012, 99/2014, 123/2014 i 126/2014 - odluka US) i Statutom Republičkog fonda za zdravstveno osiguranje ("Sl. glasnik RS", br. 81/2011, 57/2012, 89/2012, 1/2013, 32/2013 i 23/2015).

RFZO obavlja delatnost na čitavoj teritoriji Republike Srbije te ima nadležnost nad svim građanima naše zemlje, kao i stranim državljanima koji imaju zdravstveno osiguranje u skladu sa Zakonom o zdravstvenom osiguranju. U skladu sa tim postoji razgranata organizaciona struktura, te se poslovi RFZO-a obavljaju u:

- **Direkciji** gde se organizuje, vrši kontrola i koordinacija rada filijala i Pokrajinskog fonda, zastupa RFZO, ustrojava i organizuje matična evidencija o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osiguranja, jedinstveno za teritoriju Republike, obavljaju poslovi ustrojavanja, razvoja, korišćenja i održavanja informacionog sistema zdravstvenog osiguranja kao dela integrisanog informacionog sistema Republike kao i mnogi drugi poslovi u skladu sa članom 28 Statuta RFZO-a;

- **Pokrajinskom fondu** koji vrši koordinaciju rada filijala obrazovanih na teritoriji autonomne pokrajine i obavlja druge poslove u skladu sa članom 28 Statuta RFZO-a;

- **31 filijali i njihovim ispostavama** koje sprovode obavezno zdravstveno osiguranje i vode matičnu evidencija osiguranih lica na svom području, te obavljaju druge poslove u skladu sa članom 31 Statuta RFZO-a.

Pravilnik o načinu i postupku zaštite prava osiguranih lica Republičkog fonda za zdravstveno osiguranje, usvojen 2013. godine, u članu 4, stav 3, sadrži napomenu da je zaštitnik prava osiguranih lica obavezan da postupa u skladu sa propisima kojima se uređuje zaštita podataka o ličnosti.

Na sajtu Fonda, u rubrici 'O nama', sekcija 'Upravljanje kvalitetom', nalazi se segment posvećen politici upravljanja bezbednošću informacija u kojem su objašnjeni namena, ciljevi i načini zaštite informacija.

Adresa: Jovana Marinovića br. 2, 11040 Beograd
E-mail: public@rfzo.rs
Internet sajt: www.rfzo.rs
Informator o radu:
http://www.rfzo.rs/download/informator/informator_o_radu_112015.pdf

PRAVNI ASPEKTI OBRADE PODATAKA

Zbirke podataka o ličnosti

RFZO je registrovao 18 zbirki podataka o ličnosti u Centralni registar Poverenika. Od toga, 12 zbirki podataka se odnosi na podatke o ličnosti osoba koje su zaposlene u RFZO-u ili obavaljaju poslove u RFZO-u po drugom osnovu kao što su evidencija o zaradama, evidencija adresa elektronske pošte zaposlenih, evidencija korisnika službenih mobilnih telefona i druge slične evidncije.

Preostalih 6 zbirki podataka se odnose na podatke o ličnosti osiguranih lica i članova njihovih porodica, građana Srbije i stranih državljana koji imaju obavezno zdravstveno osiguranje i to su:

- Matična evidencija o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osiguranja;
- Registracija izabranog lekara;
- Evidencija izdatih recepata;
- Evidencija o licima sa kojima RFZO vodi sudske sporove;
- Evidencija o predmetima u upravnom postupku;
- Digitalna bolnica - iskorišćenost bolničkih postelja.

Od svih nabrojanih, Matična evidencija o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osiguranja (u daljem tekstu "Matična evidencija") predstavlja najobimniju zbirku podataka koju vodi RFZO, i čini osnovni preduslov za obavljanje poslova iz nadležnosti RFZO-a, zbog čega su i pravila za vođenje ove evidencije detaljno regulisana Zakonom o zdravstvenom osiguranju i podzakonskim propisima. Ova evidencija je uspostavljena 2005. godine, nakon što je stupio na snagu važeći Zakon o zdravstvenom osiguranju.

Matičnu evidenciju smo odabrali kao reprezentativnu te se dalja analiza svih aspekata obrade podataka o ličnosti odnosi samo na Matičnu evidenciju.

Pravni osnov

Pravni osnov za vođenje Matične evidencije utvrđen je članom 115 Zakona o zdravstvenom osiguranju gde se navodi da se svojstvo osiguranog lica u obaveznom zdravstvenom osiguranju utvrđuje na osnovu podataka koji se vode u Matičnoj evidenciji koju jedinstveno za teritoriju Republike ustrojava i organizuje RFZO. Dalje, članovi 116-

138 istog Zakona uređuju obradu podataka, precizno navode podatke o ličnosti koji se vode u Matičnoj evidenciji. Članom 138, stav 1, propisano je da se ti podaci koriste samo za potrebe obaveznog zdravstvenog osiguranja, ako zakonom nije drugačije određeno, dok se u stavu 2 navodi da podaci iz Matične evidencije koji se odnose na pojedino osigurano lice, odnosno na korišćenje prava iz obaveznog zdravstvenog osiguranja, jesu lični podaci i predstavljaju službenu tajnu, odnosno ne mogu se iznositi i objavljivati u javnosti.

Podaci o ličnosti

U matičnoj evidenciji se vode i obrađuju podaci o ličnosti:

1. Osiguranika, to jest lica koja su osigurana u skladu sa Zakonom o zdravstvenom osiguranju i to:

- prezime i ime;
- jedinstveni matični broj građana i poreski identifikacioni broj;
- pol;
- dan, mesec i godina rođenja;
- zanimanje;
- školska sprema;
- osnov osiguranja;
- datum sticanja, odnosno prestanka svojstva osiguranika, kao i promene u toku osiguranja;
- staž zdravstvenog osiguranja;
- obveznik plaćanja doprinosa;
- visina uplate doprinosa;
- zarade, naknade zarada i druga primanja i naknade koje služe za utvrđivanje osnovice osiguranja na koju se obračunava i plaća doprinos;
- visina uplaćenog doprinosa;
- adresa prebivališta;
- naziv poslodavca, registarski broj poslodavca, šifra delatnosti i adresa sedišta poslodavca;
- opština na kojoj se nepokretnost nalazi;
- državljanstvo.

2. Članova porodice osiguranika i to:

- prezime i ime;
- jedinstveni matični broj građana;
- pol;
- dan, mesec i godina rođenja;
- srodstvo sa osiguranikom;
- adresa prebivališta;

- zanimanje;
- državljanstvo.

3. O korišćenju prava iz obaveznog zdravstvenog osiguranja i to:

- vrsti prava iz zdravstvenog osiguranja koja se obezbeđuju osiguranom licu;
- pruženim zdravstvenim uslugama;
- novčanim naknadama;
- medicinsko-tehničkim pomagalima i implantatima;
- lekovima izdatim na recept;
- godišnjem iznosu plaćenih participacija;
- izabranom lekaru osiguranog lica;
- ostvarivanju prava pred lekarskim komisijama;
- ostvarivanju prava u vezi sa profesionalnom bolešću ili povredom na radu osiguranika;
- upućivanju na invalidsku komisiju u skladu sa ovim zakonom.

RFZO ima nadležnost nad celom teritorijom Republike Srbije pa se u Matičnoj evidenciji nalaze podaci o ličnosti većine građana Srbije, kao i stranaca koji su po nekom osnovu zdravstveno osigurani. U ovoj evidenciji se ne nalaze samo podaci onih građana koji ni po jednom osnovu nisu osigurani po Zakonu o zdravstvenom osiguranju.

Treba napomenuti da se gotovo identični podaci o osiguranicima nalaze i u Matičnoj evidenciji o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osgiuranja koju vodi Republički fond za penzijsko i invalidsko osiguranje kao i u jedinstvenoj bazi podataka osiguranika, osiguranih lica koju vodi Centralni registar obaveznog socijalnog osiguranja.

Podaci o korišćenju prava iz obaveznog zdravstvenog osiguranja kao podaci o zdravstvenom stanju predstavljaju naročito osetljive podatke u smislu člana 16 Zakona o zaštiti podataka o ličnosti, i ovi podaci se ne nalaze u evidencijama drugih državnih organa, niti se sa njima razmenjuju. Dodatno, članom 9 Uredbe o jedinstvenim metodološkim principima za vođenje matične evidencije uređeno je da ovi podaci predstavljaju službenu tajnu, da se vode odvojeno od drugih podataka, a te podatke može unositi odnosno njima rukovati za to posebno ovlašćeno lice RFZO-a.

Načini prikupljanja podataka o ličnosti

Od kada je uspostavljen i počeo sa radom Centralni registar obaveznog socijalnog osiguranja, podaci o osiguranicima i osiguranim licima koji se vode u Matičnoj evidenciji se prikupljaju preuzimanjem podataka od Centralnog registra a u skladu sa Zakonom o centralnom registru obaveznog socijalnog osiguranja. Naime, tim Zakonom je propisano

da se registracija osiguranika i osiguranih lica vrši podnošenjem jedinstvene prijave isključivo u elektronskom obliku preko portala Centralnog registra. Ove jedinstvene prijave u većini slučajeva podnose poslodavci za svoje zaposlene ili sama fizička lica. U oba slučaja mora postojati kvalifikovani elektronski sertifikat kako bi mogla da se podnese jedinstvena prijava. Izuzetno za fizička lica koja nemaju tehničke mogućnosti za prijavu u elektronskom obliku, nju može podneti neka od organizacija obaveznog socijalnog osiguranja (RFZO, PIO fond). Tada fizička lica na šalteru predaju potrebne dokaze o statusu osiguranika, a ovlašćeni službenik na šalteru za njih popunjava jedinstvenu elektronsku prijavu i podnosi je Centralnom registru.

Podaci koji su navedeni u elektronskoj prijavi se unose u jedinstvenu bazu podataka osiguranika, osiguranih lica koju vodi Centralni registar. Nakon toga RFZO preuzima i koristi te podatke za potrebe vođenja Matične evidencije, a u skladu sa članom 18 Zakona o centralnom registru obaveznog socijalnog osiguranja koji propisuje da organizacije obaveznog socijalnog osiguranja preuzimaju iz Jedinstvene baze podatke neophodne za vođenje Matične evidencije

Forma jedinstvene elektronske prijave je propisana Uredbom o sadržini, obrascu i načinu podnošenja jedinstvene prijave na obavezno socijalno osiguranje, jedinstvenim metodološkim principima i jedinstvenom kodeksu šifara za unos podataka u jedinstvenu bazu centralnog registra obaveznog socijalnog osiguranja („Službeni glasnik RS", br. 54/10, 124/12 и 119/13) i data je na Obrascu M koji je odštampan uz ovu uredbu i čini njen sastavni deo.

Centralni registar Poverenika

Matična evidencija je registrovana kao zbirka podataka o ličnosti u Centralnom registru koji vodi Poverenik od jula 2010. godine. Pored ove, RFZO je registrovao još 17 zbirki podataka o ličnosti.

Nakon registracije Matične evidencije došlo je do promene određenih aspekata obrade podataka o ličnosti, a naročito osnivanjem Centralnog registra obaveznog socijalnog osiguranja, te u tom smislu nisu ažurni podaci iz Centralnog registra koji se odnose na ''način prikupljanja i čuvanja podataka'' i ''spoljne korisnike zbirke''.

Interni akti

Prvim zahtevom za informacije od javnog značaja od RFZO-a su traženi interni akti koji regulišu upravljanje i pristup podacima iz Matične evidencije. U skladu sa tim dostavljena su nam dokumenta Sistema upravljanja kvalitetom (ISO 9001) i Sistema upravljanja

bezbednošću informacija (ISO 27001) koji reguliše određene aspekte upravljanja i pristupa podacima iz Matične evidencije i to:

- **Politika uloga i odgovornosti** (ISO 27001) na opšti način reguliše uloge i odgovornost rukovodilaca i ostalih zaposlenih u RFZO u vezi sigurnošću informacija. Primera radi navešćemo neke uloge i odgovornosti. Opšta odgovornost za sigurnost informacija je na direktoru RFZO-a, dok je primarna odgovornost obazbeđivanja sigurnosti informacija na direktorima organizacionih jedinica RFZO-a (direktori sektora, direktori filijala i direktor pokrajinskog fonda). Sistem administratori su odgovorni za implementaciju sistema za kontrolu pristupa radi očuvanja poverljivosti kao i za bekap procedure. Svi zaposleni su odgovorni za poštovanje svih procedura i pozitivno pravnih propisa kao i za fizički pristup resursima koji su u njihovom vlasništvu. Poslednja verzija ovog dokumenta je iz juna 2013. godine.
- **Politika kontrole logičkog pristupa** (ISO 27001) ima za cilj da ustanovi standard za kreiranje jakih lozinki za pristup informacionim sistemima RFZO-a, kao i zaštitu lozinki i učestalost njihovog menjanja kroz detaljno definisanje tri procesa a) Identifikacije, b) Autentifikacije i c) Autorizacije. Poslednja verzija ovog dokumenta je iz juna 2013. godine.
- **Politika upravljanja korisničkim ulogama** (ISO 27001) ima za cilj da ustanovi pravila za upravljanje korisničkim nalozima i ovlašćenjima zaposlenih u RFZO-u na način kako bi se obezbedilo da samo ovlašćeni korisnici mogu da pristupe informacionim sistemima i da se na taj način spreči neovlašćeni pristup podacima. Poslednja verzija ovog dokumenta je iz juna 2013. godine.
- **Procedura za registraciju i odjavu korisnika** (ISO 27001) ima za cilj da definiše postupak registracije i odjave korisnika informacionih sistema RFZO-a. Poslednja verzija ovog dokumenta je iz juna 2013. godine.
- **Procedura za održavanje, izveštavanje i pružanje podrške korisnicima IS** (ISO 9001) ima za cilj da definiše način i postupak održavanja informacionog sistema RFZO-a. Poslednja verzija ovog dokumenta je iz februara 2013. godine.

Zahtev za ostvarivanje prava

Tokom istraživačkog procesa, član našeg tima je u skladu sa članom 19 ZZPL-a pisanim putem od RFZO-a tražio obaveštenje o obradi svojih podataka o ličnosti i to:

1. Koje podatke o meni obrađujete?
2. Koje vrste obrade podataka sprovodite?
3. Od koga su prikupljeni podaci o meni, odnosno ko je izvor podataka?
4. U koje svrhe se podaci obrađuju?
5. U kojim zbirkama podataka se nalaze podaci o meni?

6. Ko su korisnici podataka o meni? Koji podaci o meni se koriste? Po kom pravnom osnovu i u koje svrhe se podaci o meni koriste?
7. Da li se moji podaci prenose (ustupaju) drugim licima, i koja su to lica? Po kom pravnom osnovu i za koje potrebe se ti podaci prenose?
8. U kom vremenskom periodu se podaci obrađuju, odnosno da li je predviđena obustava obrade mojih podataka u određenom trenutku?

RFZO nije odgovorio na zahtev za ostvarivanje prava u zakonom predviđenom roku od 15 dana od dana podnošenja zahteva. Kada rukovalac nije u mogućnosti da postupi po zahtevu u propisanom roku, podnosilac zahteva se obaveštava o tome i određuje se novi rok za postupanje koji ne može biti duži od 30 dana od isteka prvog propisanog roka. U slučaju odbijanja zahteva, rukovalac je dužan da o tome donese rešenje sa poukom o pravnom sredstvu. Nijednu od propisanih obaveza RFZO nije ispunio.

Zaključak

Regulisanje obaveze vođenja Matične evidencije, te precizno definisanje podataka o ličnosti koji se vode u Matičnoj evidenciji zakonskom odredbom, kao i jasno određena svrha obrade ovih podataka što je sve određeno Zakonom o zdravstvenom osiguranju, predstavlja dobro rešenje, koja je u skladu sa članom 42 stav 2 Ustava Republike Srbije kojim je uređeno da se obrada podataka uređuje zakonom. Ipak čini se da je osnivanjem Centralnog registra obaveznog socijalnog osiguranja došlo do određenih promena u odnosu na grupe podataka o ličnosti koji se vode u Matičnoj evidenciji te bi član 115 Zakona o zdravstvenom osiguranju (koji reguliše grupe podataka o ličnosti) trebalo izmeniti i uskladiti sa novim okolnostima.

Matična evidencija je blagovremeno registrovana kao zbirka podataka o ličnosti u Centralnom registru koji vodi Poverenik ali obzirom da je od tada došlo do određenih promena u obradi podataka, a naročito osnivanjem Centralnog registra obaveznog socijalnog osiguranja, poželjno je da se ovi podaci ažuriraju.

Na zahtev za ostvarivanje prava na obaveštenje o obradi podataka o ličnosti koji smo uputili u svemu u skladu sa Zakonom o zaštiti podataka o ličnosti, RFZO ni na koji način nije odgovorio, niti doneo bilo kakvo rešenje čime se oglušio o svoje zakonom propisane obaveze. Ova činjenica svakako upućuje na zaključak da u RFZO ne postoje jasne procedure i odgovornost za odgovore na zahteve građana u skladu sa Zakonom o zaštiti podataka o ličnosti.

Interni akti, odnosno dokumenti Sistema upravljanja kvalitetom (ISO 9001) i Sistema upravljanja bezbednošću informacija koji regulišu određene aspekte upravaljanja i pristupa podacima iz Matične evidencije a koji su navedeni predstavljaju dobra rešenja u mnogim aspektima, jer na precizan način uspostavljaju procedure i pravila za unos, izvos, prenos, bekap podataka o ličnosti.

ORGANIZACIONI ASPEKTI OBRADE PODATAKA

Lice za zaštitu podataka o ličnosti

Postojeće stanje: U Republičkom fondu za zdravstveno osiguranje postoje lica zadužena za bezbednost informacija, što bi trebalo da uključuje i zaštitu podataka o ličnosti. Lica su određena rešenjima direktora Fonda i pored poslova i odgovornosti za bezbednost informacija obavljaju i druge poslove.

Kao primer dobre prakse u Republičkom fondu za zdravstveno osiguranje može se navesti distribucija odgovornosti za bezbednost informacija kroz organizaciju. Odgovornost za bezbednost informacija je distribuirana u skladu sa svim specifičnostima organizacione strukture Republičkog fonda za zdravstveno osiguranje. Naime, odgovornost za bezbednost informacija je na:

- Direktorima sektora u Direkciji;
- Direktorima filijala;
- Direktoru pokrajinskog fonda.

Na ovaj način raspoređena odgovornost stvara osnovu za razvijanje odgovarajućeg nivoa bezbednosti informacija, među kojima su najznačajniji podaci o ličnosti korisnika. Analizom organizacione strukture RFZO može se jasno videti da je odgovornost za bezbednost informacija definisana na dva nivoa. U Direkciji RFZO, direktori sektora su na hijerarhijskom nivou koji obezbeđuje punu primenu njihovih zahteva u vezi sa zaštitom podataka, a sa druge strane su dovoljno uključeni u procese rada da bi uvideli sve probleme u ovoj oblasti. Takođe, direktori filijala su među ključnim učesnicima u procesu zaštite podataka o ličnosti, pre svega zbog geografske dislociranosti filijala, u kojima bi iz tog razloga moglo biti teže primeniti zahteve vezane za zaštitu podataka o ličnosti. Sa druge strane, u Autonomnoj pokrajini takođe postoje dva nivoa, s tim što je prvi nivo odgovornosti na direktoru Pokrajinskog fonda, dok je drugi nivo ponovo na direktorima filijala u Autonomnoj pokrajini.

Zvanično, odgovornosti na ovaj način imenovanih lica uključuju:

- Obezbeđivanje razvoja adekvatnih kontrola u skladu sa osetljivošću resursa kome se pristupa;
- Obezbeđivanje da samo autorizovani korisnici imaju imaju pravo pristupa resursima koji su u njihovoj nadležnosti i poštovanje usvojenih procedura;
- Obezbeđivanje da svi korisnici nakon promene radnog mesta ili prekida radnog odnosa prođu zvaničnu proceduru promene prava pristupa.

Preporuka: Pored navedenih organizacionih i tehničkih odgovornosti imenovanih lica, u opis njihovih nadležnosti bilo bi poželjno dodati pitanja koja su vezana i za organizacionu kulturu zaposlenih u Fondu, kao što su:

- sprovođenje određene politike o zaštiti podataka o ličnosti među zaposlenima;
- promovisanje zaštite podataka o ličnosti među zaposlenima radi shvatanje njihove uloge u zaštiti podataka
- organizovanje edukacije iz oblasti zaštite podataka o ličnosti za zaposlene;
- izveštavanje rukovodstva o nivou zaštite podataka i predlaganje mera za podizanje nivoa zaštite i dr.

Deo ovih nadležnosti je trenutno dodeljen lokalnim koordinatorima, ali se tu postavlja pitanje hijerarhijskog nivoa na kome se nalaze lokalni koordinatori.

I pored pozitivno istaknute distribucije odgovornosti za bezbednost informacija u RFZO, dodatno bi trebalo razmotriti uvođenje određene odgovornosti i na poslednjem organizacionom nivou, na nivou ispostava. Trenutno, svaka od filijala RFZO ima jednu ili više ispostava u manjim mestima. Opravdano je postaviti pitanje svesti zaposlenih o važnosti zaštite podataka o ličnosti u ispostavama RFZO, pre svega zbog dislociranosti i nedovoljnog kontakta sa direktorima filijala kao poslednjim nivoom na kojem je jasno definisana odgovornost za bezbednost informacija. Jasno je da ti zaposleni, posmatrajući tehnički aspekt, svakako rade u okviru koji je definisan na nivou celog RFZO i koji pruža odgovarajući nivo zaštite podataka o linosti, ali problem može predstavljati svest zaposlenih. Pitanje može biti posebno osetljivo na nivou ispostava u manjim mestima, gde je veća verovatnoća da zaposleni u RFZO lično poznaju korisnike, te i interes za neovlašćen pristup podacima o ličnosti može biti veći.

Edukacija

Postojeće stanje: U Republičkom fondu za zdravstveno osiguranje sprovedena je sistematska obuka zaposlenih za primenu zahteva standarda ISO 27001 - Sistem upravljanja bezbednošću informacija. Takođe, na internom portalu se nalaze određene instrukcije za postupanje u vezi sa bezbednošću informacija. Istraživačkom timu nije poznato u kojoj meri je akcenat prilikom obuka za uvođenje standarda ISO 27001 stavljen na zaštitu podataka o ličnosti, kao najosetljivijim podacima kojima upravlja RFZO, jer je standard generički i njegovi zahtevi se odnose na svu dokumentaciju u organizaciji.

Preporuka: Republički fond za zdravstveno osiguranje upravlja velikom količinom podataka o ličnosti te je od izuzetne važnosti uvesti kontinuiranu edukaciju zaposlenih iz ove oblasti. Takođe, trebalo bi definisati vremenske intervale za testiranja znanja

zaposlenih iz ove oblasti, kako bi rukovodstvo RFZO na svim nivoima imalo saznanja o stanju sistema u pogledu zaštite podataka o ličnosti.

Pristup zaposlenih Matičnoj evidenciji

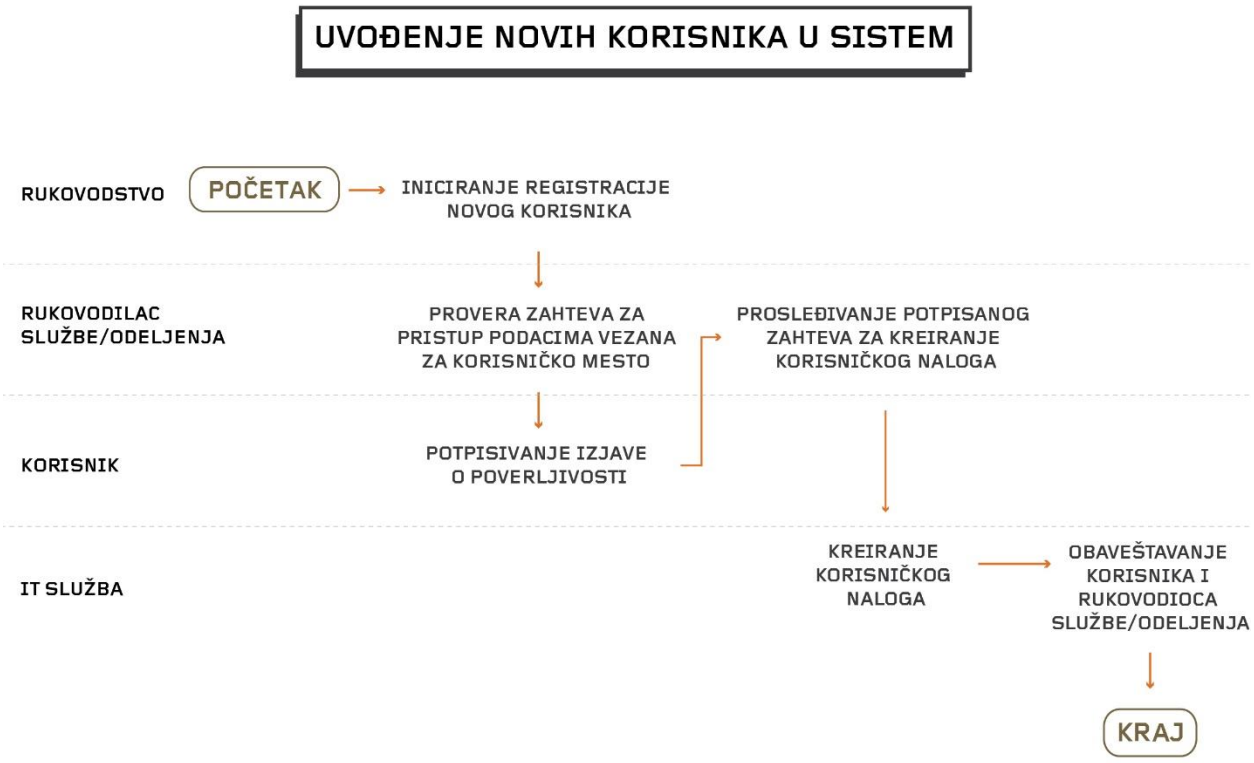
Postojeće stanje: U Republičkom fondu za zdravstveno osiguranje je razvijen sistem korisničkih uloga sa različtim pravima pristupa. Pristup je određen kombinacijom korisničkog imena i šifre, koja je vezana za svakog zaposlenog. Svaki pristup bazi se beleži (ko je pristupio, kada, šta je radio), ali se ne evidentira razlog pristupa bazi.

S obzirom da je Matična evidencija (MEOP baza/sistem) distriburiana po filijalama pristup je ograničen na podatke samo iz jedne filijale, pa zaposleni iz jedne filijale ne mogu da pristupe podacima u drugoj filijali.

U svakoj od filijala postoji jedno ili više lica koje su zaduženo za izdavanje korisničkih imena i šifara za pristup MEOP sistemu, samo zaposlenima u toj filijali i za pristup podacima konkretne filijale. Takođe, administrator može da vidi samo korisničko ime zaposlenog. Kada kreira lozinku za zaposlenog, od zaposlenog se traži da je odmah promeni, koja tako ostaje nepoznata i za administratore.

Pristup podacima iz Matične evidencije je omogućen svim zaposlenima čije radne aktivnosti to zahtevaju. Obim prava pristupa zavisi od vrste posla kojim se bave zaposleni. Među korisnicima koji imaju pristup Matičnoj evidenciji, javljaju se, u okviru Direkcije: Pomoćnik direktora za razvoj i održavanje informacionog sistema, Načelnik Odeljenja za matičnu evidenciju i Pomoćnik načelnika Odeljenja za matičnu evidenciju. Istovremeno, pristup matičnoj evidenciji je omogućen i zaposlenima na 13 radnih mesta u filijalama i ispostavama. Zaposleni imaju različita prava pristupa. Jasno je da je princip bio da se pristup omogući samo licima čiji neposredni rad to zahteva, ali data podela odgovornosti ukazuje da pristup nije dovoljno disperzovan na najvišem hijerarhijskom nivou, te se javlja pitanje šta se dešava kada neko od rukovodilaca u Direkciji ima opravdanu potrebu da pristupi bazi, ili neko od zaposlenih u samom Odeljenju za matičnu evidenciju.

Razvijena je jasna procedura za uvođenje novih korisnika u sistem, po zahtevima standarda ISO 27001. U sistemu u kojem su definisane korisničke role, ključan je proces dodeljivanja korisničkih uloga, odnosno kreiranja novih korisnika i njemu je potrebno posvetiti posebnu pažnju. Proces uvođenja novog korisnika prikazan je šematski:



Preporuka: Na osnovu dostupne dokumentacije, i odgovora zaposlenih na postavljena pitanja, došlo se do modela procesa uvođenja novih korisnika u sistem. Opravdano je postaviti određena pitanja u vezi sa optmizacijom ovog procesa. Rukovodilac službe/sektora proverava zahteve za pristup podacima prema potrebama posla, nakon određenog iniciranja od strane Rukovodstva i tek onda izdaje nalog IT službi za kreiranje korisničkog naloga. Ovaj proces se odvija na lokalnom nivou.

Međutim, ukoliko je uveden sistem korisničkih rola, on bi trebalo da prepoznaje tipske role, koje su vezane isključivo za radna mesta zaposlenih. U tom slučaju, nakon angažovanja novog zaposlenog, ili promene radnog mesta postojećeg, zaposleni iz Sektora za ljudske resurse bi trebalo da obaveste IT službu o promeni i zaposleni bi po automatizmu (u skladu sa radnim mestom) trebalo da dobije određena prava pristupa. U tom slučaju, opisani proces bi se sprovodio samo prilikom promene sistematizacije, ukidanja, promene ili uvođenja novih radnih mesta. Takođe, na taj način se eliminiše rizik da zaposleni na istim radnim mestima imaju različite nivoe pristupa.

U Republičkom fondu za zdravstveno osiguranje postoji Matrica privilegija sa 26 različitih nivoa pristupa – korisničkih uloga. U Matrici privilegija su navedeni svi korisnici sa jasno definisanim privilegijama, kao i svi sistemi/aplikacije. Matrica privilegija prisutna u RFZO svakako predstavlja primer dobre prakse, s tim što bi trebalo da sadrži nazive radnih mesta umesto imena korisnika, kako bi se standardizovao pristup bazi širom organizacije.

Dalje, u informacionom sistemu bi trebalo da postoji funkcija automatskog prekida sesije ukoliko protekne određeni vremenski interval bez aktivnosti korisnika (npr. zbog izlaska iz kancelarije, *session timeout*). Vremenski interval bi trebalo da bude određen tako da ne predstavlja preveliku smetnju zaposlenima u obavljanju radnih aktivnosti (Predlog – 30 minuta).

Sektor za održavanje informacionog sistema

Postojeće stanje: Na nivou Direkcije Republičkog fonda za zdravstveno osiguranje postoji Sektor za razvoj i informacione tehnologije, u okviru kojeg postoje sledeće organizacione jedinice, vezane za održavanje informacionog sisema: Odsek za održavanje informacionog sistema, Odeljenje za održavanje informacionog sistema, Grupa za održavanje računarske mreže i sistemsko održavanje, Odeljenje za održavanje računarske mreže i sistemsko održavanje.

Trenutno se 26 zaposlenih u Direkciji bavi poslovima održavanja informacionog sistema, ali i u filijalama postoje zaposleni koji se bave održavanjem informacionog sistema. Razlikuju se prava pristupa sistemu između zaposlenih koji se bave održavanjem informacionog sistema u Direkciji, i zaposlenih koji obavljaju te poslove u filijalama.

Deo poslova održavanja informacionog sistema obavlja i Elektrotehnički fakultet Univerziteta u Beogradu (ETF), i ima pristup određenim podacima. Republički fond za zdravstevno osiguranje ima potpisan ugovor sa ETF-om, gde je jedna od odredbi poverljivost svih podataka. Elektrotehnički fakultet je jedini koji održava MEOP bazu (sistem). Međutim, druga pravna lica se bave održavanjem drugih softverskih podsistema u okviru Republičog fonda za zdravstveno i penziono osiguranje. Lica angažovana na ETF-u imaju ad hoc pristup bazi podataka, u smislu da bi pristup podacima trebalo da imaju samo iz prostorija RFZO.

Evidencija u papirnoj formi

Postojeće stanje: Iako je u poslednje vreme značajno smanjen obim papirnih dokumenata u Republičkom fondu za zdravstveno osiguranje, u svakoj od filijala postoje arhive dokumenata, koje su zaključane. S obzirom da su sva dokumenta u paprinoj formi unesena u sistem, i postoje i u elektronskoj formi, u najvećem broju slučajeva dokumentima u papirnoj formi nakon nastanka više niko i ne pristupa. Ne postoje dosijea korisnika, već samo prijave. Međutim, ukoliko neko od zaposlenih želi da pristupi podacima u papirnoj formi, ne evidentira se pristup, niti se beleži razlog pristupa.

Preporuka: Uvesti jasnu proceduru za čuvanje podataka u papirnoj formi, u kojoj će biti definisano: gde se čuvaju podaci, ko ima pravo pristupa, ko je odgovoran za čuvanje i za evidentiranje pristupa, i druga pitanja od najveće važnosti.

ISO standardi

Postojeće stanje: U Republičkom fondu za zdravstveno osiguranje je uveden standard ISO 9001 – Sistem menadžmenta kvalitetom, kao bazni standard serije. Takođe, kao izuzetno bitno za potrebe istraživanja potrebno je istaći da je RFZO sertifikovan i po zahtevima standarda ISO 27001 Sistem menadžmenta bezbednošću informacija. Na osnovu dostavljene dokumentacije može se zaključiti da su zahtevi standarda ispunjeni u velikoj meri.

Zaključak

Republički fond za zdravstveno osiguranje predstavlja primer dobre prakse u upravljanju bezbednošću informacija i zaštitom podataka o ličnosti među ustanovama u Republici Srbiji. Informacioni sistem je osposobljen da omogući odgovarajući nivo zaštite podataka o ličnosti, a istovremeno da pruži dovoljno fleksibilnosti za obavljanje osnovne delatnosti RFZO. Preporuke date u ovom delu izveštaja su organizacione prirode i date su u cilju daljeg unapređenja sistema u oblasti zaštite podataka o ličnosti.

TEHNIČKI ASPEKTI OBRADE PODATAKA

Opšte tehničke informacije i struktura sistema

RFZO u svojoj celoj mreži ima ukupno 237 servera, vlasnik je celokupne IT opreme, uključujući i sve servere. Svaka ispostava ima svoju MEOP bazu podataka (Matičnu Evidenciju na lokalnom nivou), a tako distribuirana baza podataka se sa centralnom bazom u Direkciji fonda sinhronizuje na svakih 10 do 15 minuta od trenutka nastanka promene. To znači da postoji centralno mesto u mreži (Direkcija) gde u svakom trenutku stižu podaci o osiguranicima, ali ne u realnom vremenu. Ceo informacioni sistem RFZO povezan je privatnom komunikacionom mrežom (VPN). U toku su aktivnosti na reviziji informacionog sistema MEOP; tako da je planirano da se do kraja 2016. godine uspostavi jedinstveni, centralizovani MEOP informacioni sistem, odnosno da postoji samo jedna centralna MEOP baza podataka u Direkciji.

Postoje po jedan veb i server za elektronsku poštu, te 235 servera za baze podataka (MS SQL i Oracle) koji su distribuirani u Direkciji u Beogradu i u svim ispostavama i filijalama u Srbiji. Matična evidencija se nalazi na serverima u ispostavama, replikacija svih baza na nivou filijale nalazi se na serverima u filijalama, a centralna kompletna matična evidencija na serverima u Direkciji. Matična evidencija koju aplikacije koriste za unos i obradu podataka je SQL baza (struktuisan prikaz podataka).

Napomena: Prilikom implementacije razvojnog plana, trebalo bi razmotriti bezbednosne politike centralne instance MEOP-a u smislu enkripcije, hešovanja i regulisanja fizičkog pristupa server sali. Takođe, važno je uspostaviti enkriptovane kanale komunikacije između direkcije i ispostava i filijala u Srbiji.

Pristup internetu

Sajt i matična evidencija RFZO-a nisu na istom serveru, već postoji poseban (namenski) server koji RFZO koristi samo za hostovanje sajta (http://www.rfzo.rs), što bi značilo da RFZO samostalno hostuje sajt, odnosno usluge hostinga se zakupljuju sa strane. Internet Servis Provajder je Telekom Srbija.

Opšte informacije	
Naziv ustanove	Republički fond za zdravstveno osiguranje
URL	http://www.rfzo.rs/
Datum vršenja analize	27.04.2015.

WHOIS pretraga	
Ime i Prezime	Olivera Videnović
Adresa	Jovana Marinovića 2, Beograd
Provider	TELEKOM SRBIJA A.D.
URL Provajdera	http://www.telekom.rs/
Registrator	TELEKOM SRBIJA A.D.
URL Registratora	http://www.telekom.rs/
Država	Srbija
Nmap	
Broj otvorenih portova	2
Broj filtriranih portova	998
Broj zatvorenih portova	0
OS	Linux 2.6.18
Bezbedan (Nmap)	Da
IP v4	212.200.153.146
IP v6	/
MAC	/

VPN i Cloud usluge

Ceo informacioni sistem RFZO povezan je putem VPN-a, a provajder tih usluga je Telekom Srbija, kod kojeg imaju zakupljene IP adrese čiji opseg iz razloga bezbednosti nismo dobili. Cloud usluge se za sada ne koriste, te ne postoji plan da će se u doglednom periodu početi koristiti.

Serverska podešavanja

Svaka ispostava RFZO-a ima svoju MEOP bazu podataka (Matičnu Evidenciju na lokalnom nivou), a tako distribuirana baza podataka se sa centralnom bazom u Direkciji fonda sinhronizuje na svakih 10 do 15 minuta od trenutka nastanka promene.

Na aplikativnom nivou, u okviru MEOP aplikacije, čuvaju se transakcijski logovi, odnosno aktivno se beleže sve akcije korisnika u aplikaciji. Pristup bazi (MEOP) uslovljen je unosom korisničkog imena i lozinke. Ime i lozinka eksplicitno određuju prava pristupa bazi podataka za svakog zaposlenog na određenom radnom mestu. U log fajlu se evidentira i sa kog računara je izvršen pristup, pri čemu administratori vode evidenciju prava pristupa korisnika po sistemima/aplikacijama u tzv. matrici privilegija.

Interni akti RFZO-a koji regulišu mere zaštite su već navedeni: *Politika uloga i odgovornosti, Politika kontrole logičkog pristupa, Politika upravljanja korisničkim ulogama, Procedura za registraciju i odjavu korisnika, Procedura za održavanje, izveštavanje i pružanje podrške korisnicima IS*.

Izdvajamo delove navedenih akata koji se odnese na tehničku bezbednost sistema:

Politika uloga i odgovornosti*/ Sistem administrator*
Sistem administratori su lica zaposlena u RFZO, koja upravljaju IS poverenim od strane RFZO. Svaka vrsta informacija i sistem može imati jedan ili više namenskih sistem administratora. Oni su odgovorni za zaštitu informacija, uključujući implementaciju sistema za kontrolu pristupa za očuvanje poverljivosti i sprovođenje back up procedure kako bi obezbedili očuvanje informacija od gubitka. Samostalni stručni saradnik sistem administrator u Direkciji RFZO, odnosno Načelnik odeljenja za održavanje IS i računarske mreže u filijalama RFZO i Pokrajinskom fondu odgovoran je za instalaciju, konfiguraciju, upravljanje i održavanje informacionih resursa u skladu sa usvojenim Politikama i drugim dokumentima u okviru ISO 27001:2005.

Politika uloga i odgovornosti*/ IT zaposleni*
IT zaposleni su odgovorni za instalaciju, konfiguraciju, upravljanje, održavanje informacionih resursa organizacije u skladu sa usvojenim Politikama i drugim dokumentima u okviru ISO 27001:2005. Takođe, odgovorni su za pomaganje (edukaciju) korisnika i predstavljaju osobe koje su zadužene za prijavljivanje incidenata vezano za sigurnost korisničkih naloga.

Politika upravljanja korisničkim nalozima*/ Autorizacija za upravljanje korisničkim nalozima i privilegijama*
Upravljanje nalozima i privilegijama za računare i softver je ograničeno na ovlašćeno i stručno osoblje. Ovlašćenje se može dobiti od rukovodstva ili od osobe koja je zadužena za određenu opremu ili softver.

Povezivanje ličnih računara ili opreme na računarsku mrežu organizacije je dozvoljeno samo kada postoji odobrenje od rukovodstva i/ili administratora mreže. Uslov za povezivanje ovakvih uređaja je da IT služba ima mogućnost pregledanja konfiguracije pre nego što uređaj bude povezan. Kada je povezivanje odobreno, sistem administrator

odgovoran je da obezbedi samom konfiguracijom da korišćenje uređaja bude u skladu sa politikama sigurnosti organizacije.

Politika upravljanja korisničkim nalozima*/ Upravljanje korisničkim nalozima i privilegijama*
Lica koja su odgovorna za kreiranje korisničkih naloga moraju da obezbede da nalozi budu kreirani samo za one osobe koje su kvalifikovane da imaju nalog i čiji je identitet potvrđen. Privilegovani nalozi su oni nalozi kojima su dodeljene specijalne privilegije za IS i oni se obično dodeljuju sistem administratorima.

Politika upravljanja korisničkim nalozima*/ Upravljanje lozinkama*
Kada je odobren pristup sistemu ili aplikaciji, korisnik će biti obavešten o njihovoj privremenoj lozinci na bezbedan način. Ova privremena lozinka mora biti promenjena nakon prvog logovanja korisnika, kada sistem automatski traži od korisnika da promeni lozinku.

Politika kontrole logističkog pristupa*/ Zahtevi politike*
Sve lozinke na nivou sistema (root, admin i sl.) moraju biti promenjene najmanje jednom u 12 meseci. Sve lozinke za korisničke naloge na domenima moraju biti promenjene najmanje jednom u mesec dana.

Politika kontrole logističkog pristupa*/ Korišćenje lozinki za autentifikaciju*
Prilikom izbora i korišćenja lozinki moraju se poštovati sledeća uputstva:

- sve šifre moraju biti lične i poverljive
- korisnici moraju biti sigurni da njihova šifra nije poznata drugima
- različito korisničko ime i lozinka moraju se izdati zamenicima ili asistentima
- korisnici ne smeju držati svoju lozinku na papiru ili u nezaštićenoj elektronskoj formi
- lozinka se mora promeniti kada postoji indikacija da se može zloupotebiti
- lozinke ne bi trebalo da budu sastavljene tako da je neko drugi može lako pogoditi (ne treba da sadrže ime osobe, e-mail, naziv sektora, korisničko ime i sl.).
- korisnici treba da budu u mogućnosti da sami biraju lozinku
- lozinka se ne prikazuje prilikom unosa
- automatska blokada korisničkog imena nakon maksimalnih 10 pogrešnih unosa
- beleženje svakog pogrešnog unosa
- korisnici mogu promeniti lozinku bilo kada
- lozinke se daju korisnicima na bezbedan način, u zatvorenoj koverti.

Ukoliko je tehnički moguće, relevantni događaji vezani za bezbednost sistema su evidentirani u log fajlovima koji kasnije mogu biti korišćeni kao dokazi ukoliko se ukaže

potreba za tim. Elektronske dnevnike (log fajlove) koji sadrže informacije klasifikovane kao poverljive, kontrolišu sistem administratori.

Pristup korisnika MEOP sistemu je kontrolisan i preispitan od strane odgovornih lica u cilju smanjenja sigurnosnih rizika:

- korisnička prava moraju biti prilagođena na takav način koji obezbeđuje da korisnicima bude odobren samo neophodan i autorizovan nivo pristupa;
- prilagođavanje treba izvoditi kada dođe do promena u zahtevima poslovanja, promene radnog mesta korisnika, prekida radnog odnosa i slično;
- članovi svih privilegovanih grupa i njihovih uloga treba da se preispitaju periodično, a najmanje jednom godišnje;
- periodično, opšte preispitavanje korisničkih naloga treba da obezbedi ukidanje pristupa na naloge koji nisu više potrebni ili su suvišni;
- nalozi kojima je odobren privremeni pristup, treba da budu isključeni ili obrisani kada pristupsa tog naloga više nije potreban.

Pristup trećih lica

Pravo pristupa Matičnoj evidenciji imaju zaposleni sa ETF-a po Ugovoru o odžavanju i unapređenju MEOP sistema. Zbog poverljivosti podataka, ETF je u obavezi da primenjuje ISO standarde koji regulišu ovu oblast i tačka ugovora eksplicitno naglašava da ETF ove podatke neće koristiti u druge svrhe i da ih neće odavati trećim licima, osim ukoliko je to neophodno za izvršenje predmeta ugovora, uz saglasnost RFZO-a. Lica koja održavaju sistem, isključivo prilikom dolaska u RFZO mogu pristupiti Matičnoj evidenciji i MEOP sistemu, odnsono nemaju pristup iz svojih prostorija preko VPN-a.

Ugovoreni partneri i ugovoreni konsultanti moraju potpisati izjavu o poverljivosti informacija, pre pristupanja poverljivim informacijama. Zaposleni koji se bave informacionim tehnologijama su odgovorni za implementiranje izjave o poverljivosti.

Prilikom istraživanja i slanja zahteva za pristup informacijama od javnog značaja, jedno od postavljenih pitanja odnosilo se na pravo pristupa bazi podataka državnih i nadzornih organa, Ministarstva, policije, bezbednosnih agencija i sudova. Na ovo pitanje nismo dobili odgovor, niti smo pronašli odgovor u dokumentima i Politikama koje smo primili u sklopu odgovora ili koji su javno objavljeni.

Zaključak

S obzirom na to da se radi o disperziranom i kompleksnom sistemu, upravljanje podacima o ličnosti jeste izazov određene vrste. U svakom slučaju, može se reći da RFZO ima jasno

definisana pravila po kojima se rukovode svi relevantni segmenti organizacije, a koja se tiču upravljanja informacionim sistemom na adekvatan način.

Kao odgovor na zahteve za pristup informacijama od javnog značaja, dobili smo interne akte koje je ova organizacija izradila, donela i koje primenjuje. Dokumenti ovog tipa nažalost nisu svakodnevica kod svih rukovaoca, stoga se može reći da je po pitanju dokumentacije bezbednog menadžmenta informacionog sistema, ovo jedan od primera dobre prakse u okviru ovog istraživanja.

Naravno, kao i u svakom sistemu postoje segmenti koji bi mogli da se reše na bolji ili bezbedniji način. Kao primer bismo izdvojili autentifikaciju prilikom pristupa MEOP bazi, zasnovanu na unosu korisničkog imena i šifre, dok i dalje ne postoji drugi stepen zaštite kao što bi recimo bio digitalni sertifikat. S obzirom na to da je autorizacija usko vezana sa autentifikacijom (pristupna prava su vezana za određenog korisnika, t.j. svaki korisnik nema istu "dubinu" pristupa), te da je integritet podataka u MEOP bazi od izuzetnog značaja, smatramo da je potrebno poboljšati način pristupa bazi.

MEDIJSKA POKRIVENOST

Uvodne napomene

Pregled novinskih izveštaja o pojedinačnim institucijama obuhvaćenih analizom, odnosi se na period od početka 2000-tih do 2015. godine, na osnovu pretraživih digitalnih arhiva celovitog teksta članaka štampanih dnevnih i nedeljnih izdanja, posebno iz perspektive zaštite ličnih podataka.

Domaća regulativa ove oblasti relativno je nova – zakon iz 1998. nudio je nedovoljna i prevaziđena rešenja, da bi nestankom saveznih instanci praktično postao nesprovodiv. Novijeg datuma je i pažnja globalne javnosti za aspekte privatnosti u digitalnom okruženju. Stoga je očekivano da interes štampe za zaštitu podataka o ličnosti u organima državne uprave, tokom proteklih petnaestak godina, bude oskudan i gotovo po pravilu vođen incidentima, odnosno događajima koji svedoče o kršenju prava građana što je, konačno, i suštinska uloga medija u savremenim demokratijama.

Sa druge strane, aktivno učešće institucija državne uprave u javnom dijalogu posvećenom zaštiti privatnosti i ličnih podataka koje prikupljaju i obrađuju, moglo bi se pokazati kao ključni doprinos daljem uređenju ove oblasti ali i sopstvenoj promociji kao vodećeg aktera u zaštiti interesa građana.

RFZO – ISTORIJSKI PREGLED

S obzirom na to da je Zakon o zaštiti podataka o ličnosti usvojen 2008. godine, u prethodnom periodu u medijima praktično nema izveštaja o ovom pravu. RFZO (do izmena zakona 2011. pod nazivom Republički zavod za zdravstveno osiguranje) često je u fokusu javne pažnje, ali u kontekstu ogromnih dugova Fonda, korupcije, zloupotreba, problema osiguranja pojedinih ranjivih grupa, subvencija i slično.

Zbirke podataka se ne pominju, ali da postoji potreba pažljive obrade i zaštite ličnih podataka može se naslutiti iz povremenih incidenata vezanih za krađu identiteta radi neovlašćenog ostvarivanja prava na zdravstveno osiguranje.

Takođe, iz medijskih izveštaja jasno je da se procedure za ostvarivanje prava komplikuju dok između pojedinih ustanova ne postoji ni osnovna razmena podataka o osiguranicima.

Sredinom 2000-tih, zbog učestalih optužbi za netransparentnost i zloupotrebe, Fond odlučuje da javno objavljuje liste čekanja za različite operacije. Kako se navodi, identitet pacijenata je bio delimično zaštićen.

Provera podataka o uplaćenim doprinosima za zdravstveno osiguranje zaposlenih takođe često figurira u napisima o RFZO, vezanim za podatke o ličnosti a u prilog javnosti podataka i objavljivanja pretraživih baza.

Početkom naredne decenije, na sajtu RFZO aktiviran je još jedan servis preko kojeg se može proveriti da li osiguranici imaju izabranog lekara. U javnosti se ni ovom prilikom zaštita podataka ne postavlja čak ni kao tehničko pitanje.

Višegodišnji planovi za uvođenje elektronske knjižice u medijima se prate u svetlu efikasnijeg ostvarivanja prava na osiguranje, transparentnosti i kontrole, dok se aspekti zaštite privatnosti potpuno izostavljaju.

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti sproveo je nadzor nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti u tadašnjem RZZO, i početkom 2011. upozorio na niz kršenja zakonskih odredbi prilikom prikupljanja i obrade podataka osiguranika. Četiri godine kasnije, RFZO je izvestio Poverenika o preduzetim merama u skladu sa upozorenjem. Retki mediji objavili su tim povodom kratke vesti u vidu saopštenja.

DOKUMENTACIJA KOJA JE DOBIJENA OD POVERENIKA

Postupci nadzora

U Upozorenju Poverenika br. 164-01-00015/2010-07 od 31.03.2011. nakon obavljenog postupka nadzora nad RFZO, ustanovljene su nepravilnosti u sprovođenju i izvršavanju Zakona o zaštiti podataka o ličnosti, pogotovo kada su u pitanju prikupljanje i obrada naročito osetljivih podataka o ličnosti i primena tehničkih i organizacionih mera zaštite podataka. Tako je, između ostalog, pronađeno da se obrada naročito osetljivih podataka iz Kadrovske evidencije koji se tiču sindikalnog članstva, nacionalnosti, veroispovesti zaposlenih ne vrši u skladu sa Zakonom, dok raspoložive tehničke i organizacione mere zaštite podataka, koji se tiču povreda na radu i profesionalnih bolesti, ili lica sa kojima RFZO vodi sudske sporove, nisu preduzete u skladu sa članom 47 ZZPL.

Razni dopisi

Dopisom br. 011-00-00628/2015-05 od 15.05.2015 Poverenik se izjasnio povodom zahteva za mišljenje RFZO-a po pitanju da li je potreban pristanak odnosnog lica kako bi se Ministarstvu za rad, zapošljavanje, boračka i socijalna pitanja dostavlili podaci o ostvarenom pravu na medicinsko-tehničko pomagalo, a u svrhu priznavanja navedenog prava pred nadležnim organom uprave. Poverenik je dao odgovor načelne prirode ističući da RFZO može dostaviti sporni podatak Ministarstvu na njihov zahtev ukolilo postoji zakonsko ovlašćenja, a u nedostatku istog, samo na osnovu punovažnog pristanka lica. Poverenik je takođe istakao da podaci o zdravstvenom stanju, u ovom slučaju, invaliditetu lica, spadaju u kategoriju naročito osetljivih podatka i da su način i uslovi pristanka za njihovu obradu propisani posebnim članom ZZPL.

Dopisom br. 011-00-00628/2015-05 od 15.05.2015 Poverenik se izjasnio povodom zahteva za mišljenje RFZO-a u vezi sa zahtevom Gradske uprave Čačka za dostavljanje podataka iz Matične evidencije i to podataka o imenu, prezimenu, adresi, JMBG i nazivu i adresi poslodavca kod koga su zaposleni i prijaveljeni na zdravstveno osiguranje, a u svrhu utvrđivanja zaposlenih građana. Poverenik je istakao da nije jasno po kom pravnom osnovu je Gradska uprava tražila navedene podatke i da rukovalac mora proveriti da li postoji pristanak lica na koje se podaci odnose, ili zakonsko ovlašćenje koje se izričito odnosi na takvu vrstu podataka. Poverenik je takođe istakao da zakoni kojima se na uopšten način uređuje saradnja i razmena podataka između organa državne uprave, organa lokalne samouprave i drugih državnih organa se ne mogu smatrati pravnim osnovom koji navedenu obradu čini dozvoljenom.

U dopisu Poverenika RFZO-u, br. 011-00-00576/2013-05, od 09.09.2013., a povodom zahteva za mišljenje RFZO-a po pitanju traženja uvida i kopije zdravstvenog kartona osiguranog lica, a po zahtevu javnog tužilaštva u Nišu, Poverenik je zaključio da policija ima pravo uvida i pristupa dokumentaciji, jer kao organ vlasti može da obrađuje podatke bez pristanka lica, ako je obrada neophodna radi obavljanja poslova iz svoje nadležnosti određenih zakonom, u cilju sprečavanja, otkrivanja, istrage i gonjenja krivičnih dela, a u drugim slučajevima na osnovu pismenog pristanka lica, s tim da je na policiji i tužilaštvu odgovornost za zakonitost dalje obrade po njihovom pribavljanju.