IZVEŠTAJ O OBRADI PODATAKA O LIČNOSTI

-REPUBLIČKI FOND ZA PENZIJSKO I INVALIDSKO OSIGURANJE-

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 penzijsko i invalidsko osiguranje (PIO fond) je pravno lice sa statusom organizacije za obavezno socijalno osiguranje koje je osnovano radi ostvarivanja prava iz penzijskog i invalidskog osiguranja i isplate ovih prava.

Prava, obaveze i odgovornost PIO fonda utvrđene su Zakonom o penzijsko invalidskom osiguranju ("Sl. glasnik RS", br. 34/2003, 64/2004 - odluka USRS, 84/2004 - dr. zakon, 85/2005, 101/2005 - dr. zakon, 63/2006 - odluka USRS, 5/2009, 107/2009, 101/2010, 93/2012, 62/2013, 108/2013, 75/2014 i 142/2014) i Statutom Republičkog fonda za penzijsko i invalidsko osiguranje.

PIO fond obavlja delatnost na čitavoj teritoriji Republike Srbije te ima nadležnost nad svim građanima naše zemlje, kao i stranim državljanima koji imaju penzijsko invalidsko osiguranje u skladu sa Zakonom o penzijsko invalidskom osiguranju. Na dan 30.06.2015. godine u PIO fondu je bilo obavezno osigurano 2.457.897 osiguranika, dok je na isti dan bilo dodatno još 1.736.154 lica koja su korisnici prava.

U skladu sa Pravilnikom o organizaciji Republičkog fonda za penzijsko i invalidsko osiguranje ("Sl. glasnik RS", br. 29/2008) postoji razgranata organizaciona struktura, te se poslovi PIO fonda koji se odnose na obradu podataka o ličnosti obavljaju u:

- **Direkciji** gde se obezbeđuje jedinstvena primena propisa o penzijsko invalidskom osiguranju, obezbeđuje jedinstvena primena informacionih tehnologia u sprovođenju sistema obaveznog penzijskog i invalidskog osiguranja, ustrojava, organizuje i kontroliše matična evidencija o osiguranicima i korisnicima prava u filijalama i vode evidencije propisane zakonom kao i mnogi drugi poslovi u skladu Statutom PIO fonda;

- **Pokrajinskom fondu** koji između ostalog takođe ustrojava, organizuje i kontroliše matične evidencije o osiguranicima i korisnicima prava u filijalama i vodi evidencije propisane zakonom;

- **35 filijala, službama filijala i ispostavama** koje primaju prijave i odjave za osiguranike i unose podatke u matičnu evidenciju o osiguranicima i korisnicima prava, te obavljaju druge poslove u skladu sa Statutom PIO fonda.

Na sajtu PIO fonda, rubrika 'O nama' na stranici 'Međunarodni standardi', sadrži dokument o politikama bezbednosti informacija. U rubrici 'Najčešća pitanja', kategorija 'Opšta pitanja', navodi se odgovor koji se tiče zaštite ličnih podataka, na pitanje o slanju podataka o stažu osiguranika elektronskim putem. Ovakvi podaci se ne šalju, kako se navodi, zbog nemogućnosti odgovarajuće identifikacije lica, a s obzirom na zakonsku obavezu zaštite ličnih podataka korisnika i osiguranika.

Adresa: Dr Aleksandra Kostića 9, 11000 Beograd
E-mail: proffice@pio.rs
Internet sajt: www.pio.rs
Informator o radu: http://www.pio.rs/cir/informator-rf-pio.html

PRAVNI ASPEKTI OBRADE PODATAKA

Zbirke podataka o ličnosti

PIO fond je registrovao 20 zbirki podataka o ličnosti u Centralnom registru zbirki podataka koji vodi Poverenik.

Od toga, 13 zbirki podataka se odnosi na podatke o ličnosti osoba koje su zaposlene u PIO fondu ili obavaljaju poslove u PIO fondu po drugom osnovu, kao što su kadrovska evidencija, evidencija o platama zaposlenih, evidencija rešenja o godišnjim odmorima i druge slične evidncije.

Preostalih 7 zbirki podataka se odnose na podatke o ličnosti osiguranih lica, korisnika prava, dakle građana Srbije i stranih državljana koji imaju obavezno socijalno osiguranje, kao i drugih fizičkih lica koja su se obraćala PIO fondu, a to su:

1. Matična evidencija o osiguranicima, obveznicima plaćanja doprinosa i korisnicima prava iz penzijskog invalidskog osiguranja;
2. Elektronska evidencija o toku postupka i stanju predmeta za osiguranike i korisnike prava iz PIO;
3. Evidencija o predmetima u upravnom postupku;
4. Evidencija o isplati penzija i naknada;
5. Evidencija o predstavkama i pritužbama građana;
6. Evidencija o predstavkama i pritužbama građana upućenih na ime direktora i UO;
7. Evidencija o elektronskim pitanjima građana i odgovori.

Matična evidencija o osiguranicima, obveznicima plaćanja doprinosa i korisnicima prava iz penzijskog invalidskog osiguranja (u daljem tekstu "Matična evidencija") predstavlja najobimniju zbirku podataka koju vodi PIO fond, te je njeno postojanje osnovni preduslov za obavljanje poslova iz nadležnosti PIO fonda, zbog čega su i pravila za vođenje ove evidencije detaljno regulisana Zakonom o penzijskom i invalidskom osiguranju. Ova evidencija je po informacijama iz Centralnog registra Poverenika uspostavljena još 1965 godine.

Stoga smo odabrali Matičnu evidenciju 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 125 Zakona o penzijskom i invalidskom osiguranju gde se navodi da PIO fond vodi Matičnu evidenciju. Dalje članovi 126-149 istog Zakona uređuju obradu podataka, te se precizno navode podaci o ličnosti koji se vode u Matičnoj evidenciji.

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 penzijskom i invalidskom osiguranju i to:

    a. prezime i ime;

    b. jedinstveni matični broj građana i poreski identifikacioni broj;

    c. pol;

    d. dan, mesec i godina rođenja;

    e. zanimanje;

    f. školska sprema;

    g. osnov osiguranja;

    h. datum sticanja i prestanka svojstva osiguranika;

    i. o mirovanju svojstva osiguranika poljoprivrednika, odnosno utvrđenim periodima mirovanja osiguranja;

    j. o stažu osiguranja, zaradama, naknadama zarada, odnosno osnovicama osiguranja, ugovorenim naknadama i drugim naknadama koje služe za određivanje visine prava;

    k. o broju meseci, odnosno dana provedenih na radu i broju meseci, odnosno dana za koje su isplaćene naknade;

    l. o visini uplaćenog doprinosa;

m. da li je osiguranik korisnik penzije;

n. o obvezniku plaćanja doprinosa;

o. o penzijskom stažu - po vrstama;

p. o osiguranicima s telesnim oštećenjem od najmanje 70%, vojnim invalidima od prve do šeste grupe, civilnim invalidima rata od prve do šeste grupe, slepim licima i licima obolelim od distrofije ili srodnih mišićnih i neuromišićnih oboljenja, paraplegije, cerebralne i dečije paralize i multipleks skleroze;

q. osiguranika koji rade na radnim mestima, odnosno poslovima na kojima se staž osiguranja računa sa uvećanim trajanjem, i to podaci o stažu osiguranja, odnosno o vremenu provedenom na tim radnim mestima, odnosno poslovima i stepenu uvećanja staža;

2. **Korisnika prava iz penzijskog i invalidskog osiguranja,** dakle osiguranicima koji stekli pravo na penziju u skladu sa Zakonom i to:

a. prezime i ime;

b. jedinstveni matični broj građana;

c. pol;

d. dan, mesec i godina rođenja;

e. o vrsti penzije;

f. o pravnom osnovu za utvrđivanje penzije;

g. o datumu sticanja prava na penziju i datumu početka isplate, obustave i ponovne isplate penzije, kao i o pravnom osnovu za obustavu, odnosno ponovnu isplatu penzije;

h. o invalidnosti, uzroku invalidnosti i dijagnozi;

i. o iznosu penzije na dan ostvarivanja prava.

PIO fond ima nadležnost nad celom teritorijom Republike Srbije te je na dan 30.06.2015. godine u PIO fondu je bilo obavezno osigurano 2.457.897 osiguranika. Podaci svih lica se nalaze u Matičnoj evidenciji. Pored ovih lica, u Matičnoj evidenciji se nalaze i podaci lica koja su korisnici osiguranja, kojih je na dan 30.06.2015. godine bilo 1.736.154. To znači da se u Matičnoj evidenciji nalaze podaci preko 4,1 miliona lica. Broj lica čiji se podaci nalaze u evidenciji je svakako veći, imajuću u vidu da ona obuhvata i podatke lica koja nisu bila osigurana na dan 30.06.2015. godine, ali jesu u nekom prethodnom periodu.

Veliki broj identičnih podataka o osiguranicima nalazi se i u Matičnoj evidenciji o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osiguranja koju vodi Republički fond za zdravstveno osiguranje kao i u jedinstvenoj bazi podataka osiguranika i osiguranih lica koju vodi Centralni registar obaveznog socijalnog osiguranja imajući u vidu postojanje jedinstvene elektronske prijave na obavezno socijalno osiguranje. Ipak to ne uključuju podatke o plaćenim doprinosima (Centralni registar ima ove podatke samo od 2014. godine), podatke o osiguranicima sa telesnim oštećenjem, podatke o osiguranicima kojima se straž računa sa uvećanim trajanjem kao i podatke o korisnicima prava iz penzijskog osiguranja koji se vode samo u Matičnoj evidenciji PIO fonda.

Načini prikupljanja podataka o ličnosti

Od kada je uspostavljen 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, prijavu 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 PIO fond preuzima i koristi te podatke za potrebe vođenja Matične evidencije, 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

Matična evidencija je registrovana kao zbirka podataka o ličnosti u Centralnom registru koji vodi Poverenik od jula 2011. godine. Pored ove, PIO fond je registrovao još 19 zbirki podataka o ličnosti.

Treba istaći da u skladu sa Zakonom o zaštiti podataka o ličnosti, PIO fond zapravo i nema obavezu registrovanja Matične evidencije imajući u vidu član 48 stav 2 koji između ostalog reguliše da Rukovalac podataka nije dužan da obrazuje i vodi evidenciju obrade podataka koji se obrađuju radi vođenja registara čije je vođenje zakonom propisano. U tom smislu svakako je za pohvalu što je PIO fond registrovao Matičnu evidenciju i tako olakšao građanima i javnosti da se upoznaju sa obradom podataka u PIO fondu.

Sa druge strane, 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 i drugim zahtevom za informacije od javnog značaja, od PIO fonda su traženi interni akti koji regulišu upravljanje i pristup podacima iz Matične evidencije. U skladu sa tim dostavljena su nam sledeća dokumenta:

- **Pravilnik o zaštiti dokumentacije, podataka, informacija i računarske i komunikacione opreme** donet je od strane direktora PIO fonda 1998. godine. Iako se ovim Pravilnikom utvrđuju način i mere obezbeđenja i zaštite dokumentacije, podataka, informacija, računarske i komunikacione opreme u PIO fondu, sasvim je

jasno da je ovaj dokument u potpunosti zastareo, te da su prevaziđene odredbe donete na osnovu odavno nevažećih zakona i u vreme kada u Srbiji nije ni postojala regulativa o zaštiti podataka o ličnosti.

- **Instrukcija za postupanje zaposlenih u primeni propisa iz oblasti zaštite podataka o ličnosti i obezbedivanja slobodnog pristupa informacijama od javnog značaja** koja je izrađena u junu 2010. godine, objavljena na internom portalu i njena primena je obavezna za sve zaposlene u PIO fondu. Cilj ove instrukcije je da ustanovi pravila i procedure za koja zaposlene u PIO fondu u slučajevima kada se građani obraćaju PIO fondu sa zahtevima za obaveštenje, uvid i kopiju podataka o ličnosti koji se nalaze u evidencijama PIO fonda.

- **Na nivou celoga Fonda** pa time i u procesu rada obrade podataka u Matičnoj evidenciji Fond postupa po svim zahtevima zaštite podataka o ličnosti. Fond je integrisano sertifikovan od strane sertifikaciong tela SGS za standard bezbednosti ISO 27001:2013 i za standard kvaliteta ISO 9001:2008. U Fondu se primenjuju sve preporučene kontrole ISO 27001:2013 (133) bez isključenja.

- **Osnovna dokumenta** koja nalažu zaposlenima u Fondu postupanja u zaštiti podataka od neovlašćenog pristupa i obrade u skladu sa zahtevima standarda bezbednosti su:

a) Procedure:

- **Procedura za sistem upravljanja bezbednošću informacija SPR --006**

U PIO fondu je uspostavljeno 8 (osam) nivoa kontrole upravljanja bezbednošću informacija, izvod iz **Procedure:**

Šesti upravljački nivo: ROJ

- *Rukovodioci filijala i sektora u okviru svojih radnih procesa i aktivnosti učestvuju u primeni i proveri uspostavljenog sistema i imaju najveću odgovornost za sisteme.*

Sedmi upravljački nivo: Koordinatori z bezbednost informacija

- *Koordinatore je imenovao predsednik Saveta, sa zadatkom da organizuju i primene sistem bezbednosti informacija na nivou OJ za koju su zaduženi, a u saradnji sa PRB, VOT i OT.*

Osmi upravljački nivo: Zaposleni

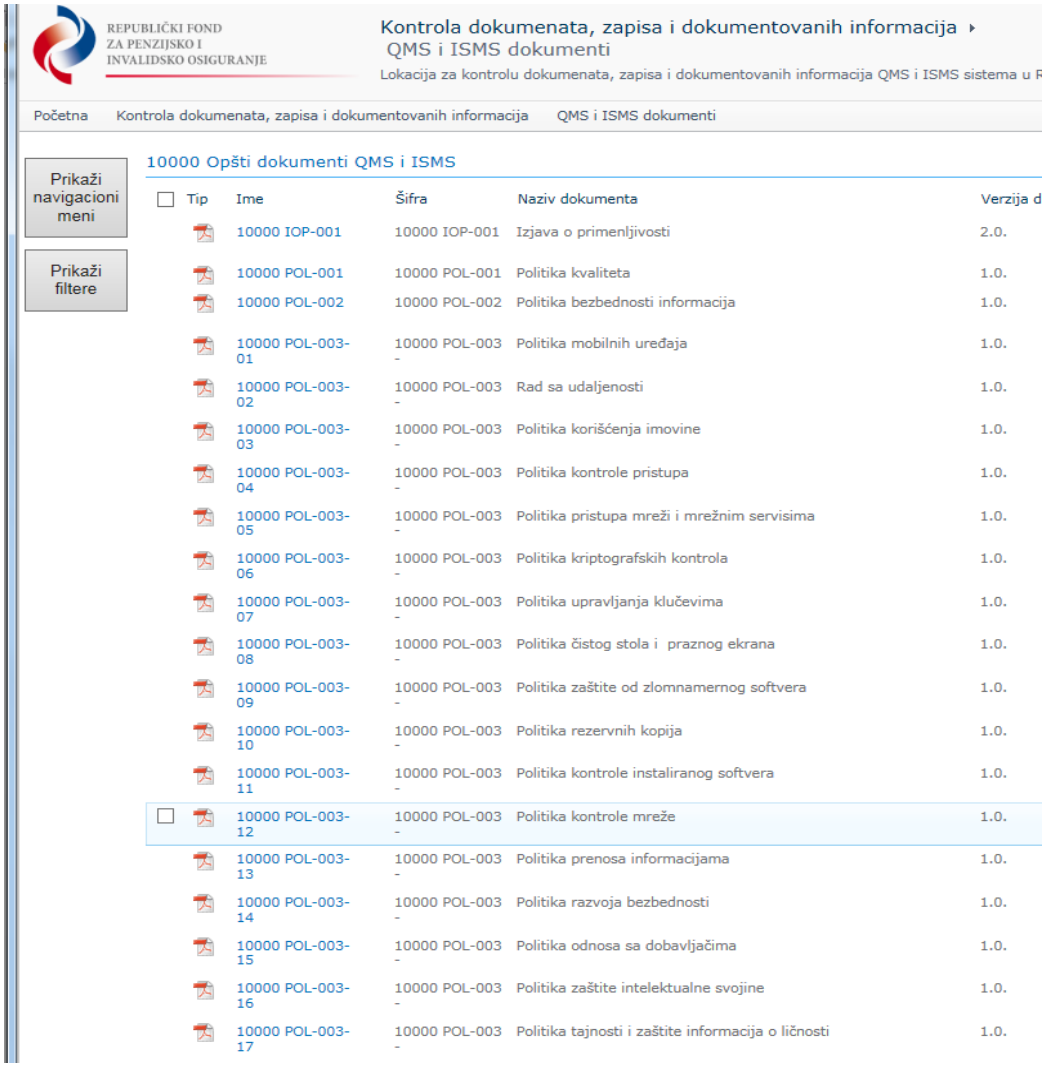
- *Svi zaposleni su uključeni u primenu i održavanje sistema.*

- **Procedura za kontrolu dokumenata, zapisa i dokumentovanih informacija SPR – 004**

- **Procedura komunikacije SPR – 005:**
  Izvod iz procedure:

  - *''Ova procedura utvrđuje pravila interne i eksterne komunikacije uz ispunjenje zahteva sistema upravljanja kvalitetom i sistema bezbednosti informacija, posebno prema zahtevima ISO 27 001:2013 ova procedura opisuje načine razumevanja potreba za bezbednošću informacija u komunikacijama sa zainteresovanim stranama, što u stvari podrazumeva utvrđivanje svih zainteresovanih strana i njihovih zahteva koji su relevantni za bezbednost informacija.''*

b) Politike bezbednosti informacija koje se sprovode u Fondu:



- **Politika tajnosti i zaštite informacija o ličnosti POL-003**
  Izvod iz Politike:

  ''Opredeljenje RFPIO za obezbeđenje tajnosti i zaštitu informacija o ličnosti

  Tajnost i zaštita informacija o ličnosti koje se nalaze u informacionim sistemima RFPIO se mora obezbediti u skladu sa zakonskim zahtevima. Stoga, postoji potreba da se oblast tajnosti i zaštita informacija o ličnosti u informacionim sistemima RFPIO uredi na takav način da se ostvari bezbednost informacija u skladu sa opredeljenjima iznetim u dokumentu Politika bezbednosti informacija POL-002.

  Politika tajnosti i zaštita informacija o ličnosti u RFPIO se sprovodi na takav način da se obezbedi:

  - *Da će se održavati poverljivost informacija;*
  - *Da informacije neće biti otkrivene neovlašćenim osobama, slučajnim ili namernim aktivnostima;*
  - *Da će integritet informacija biti sačuvan kroz zaštitu od neovlašćene izmene;*
  - *Da će biti obezbeđena usaglašenost sa propisima i dokumentima u Fondu preko kojih se politika sprovodi.*

  ***Politika tajnosti i zaštite informacija o ličnosti POL-003-17** se sprovodi preko dokumenata:*

  - *Procedura za sistem upravljanja bezbednošću informacija SPR-006;*
  - *Procedura za operativne poslove It RPR-013;*
  - *Procedura za razvoj softvera i mreže RPR-012;*
  - *Priručnika za administratore RDU-013;*
  - *Priručnika za zaposlene RDU-012.''*

- **Priručnik za zaposlene RDU-012**.
  Izvod iz Priručnika:

- *''Zaštita podataka o ličnosti*

Sve informacije o ličnostima, do kojih se došlo kroz poslovne aktivnosti i događaje proistekle iz njih, vlasništvo su Fonda. Najstrože se zabranjuje njihovo odavanje ili objavljivanje, osim na izričit pisani zahtev nadležnihh instanci, u skladu sa zakonima. Zaštita podataka o ličnosti se sprovodi u skladu sa Politikom tajnosti i zaštitom informacija o ličnosti POL-003-17.

Iz Zakona o zaštiti podataka o ličnosti potrebno je da znate i da se strogo pridržavate pravila o zaštiti podataka prilikom obrade:

1. *Podatak o ličnosti je svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski*

medij i sl), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i sl, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl), ili bez obzira na drugo svojstvo informacije (u daljem tekstu: podatak);

2. *Fizičko lice je čovek na koga se odnosi podatak, čiji je identitet određen ili odrediv na osnovu ličnog imena, jedinstvenog matičnog broja građana, adresnog koda ili drugog obeležja njegovog fizičkog, psihološkog, duhovnog, ekonomskog, kulturnog ili društvenog identiteta (u daljem tekstu: lice);*
3. *Obrada podataka je svaka radnja preduzeta u vezi sa podacima kao što su: prikupljanje, beleženje, prepisivanje, umnožavanje, kopiranje, prenošenje, pretraživanje, razvrstavanje, pohranjivanje, razdvajanje, ukrštanje, objedinjavanje, upodobljavanje, menjanje, obezbeđivanje, korišćenje, stavljanje na uvid, otkrivanje, objavljivanje, širenje, snimanje, organizovanje, čuvanje, prilagođavanje, otkrivanje putem prenosa ili na drugi način činjenje dostupnim, prikrivanje, izmeštanje i na drugi način činjenje nedostupnim, kao i sprovođenje drugih radnji u vezi sa navedenim podacima, bez obzira na to da li se vrši automatski, poluautomatski ili na drugi način (u daljem tekstu: obrada);*
4. *Obrada nije dozvoljena:*

- *Ako fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja;*
- *Ako se vrši u svrhu različitu od one za koju je određena, bez obzira da li se vrši na osnovu pristanka lica ili zakonskog ovlašćenja za obradu bez pristanka;*
- *Ako svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili već ostvarena;*
- *Ako je lice na koje se podaci odnose određeno ili odredivo i nakon što se ostvari svrha obrade;*
- *Ako je način obrade nedozvoljen;*
- *Ako je podatak koji se obrađuje nepotreban ili nepodesan za ostvarivanje svrhe obrade;*
- *Ako su broj ili vrsta podataka koji se obrađuju nesrazmerni svrsi obrade;*
- *Ako je podatak neistinit i nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili je zastareo. ''*

Kao i:

,, Jedna od osnovnih obaveza svakog zaposlenog je obaveza zaštite svake informacije do koje dolazi u posed.

Svaki zaposleni, u Fondu, biće u obavezi da potpiše Izjavu o odgovornosti OBR-0050, koja je sastavni deo dosijea zaposlenog, u kojoj će biti upoznat sa osnovnim pravima i obavezama kao zaposleno lice u Fondu. ''

- Na nivou Fonda se sprovode stalne edukacije zaposlenih za primenu standarda bezbednosti informacija, a sve prema **Proceduri za interne provere SPR-002** i **Priručniku za interne provere RDU-102.**

- U svim filijalama u Fondu nalaze se koordinatori za bezbednost i koordinatori za kvalitet. Njihovo područje delovanja su i službe i ispostave.

Zahtev za ostvarivanje prava

Tokom istraživačkog procesa, član našeg tima je u skladu sa članom 19 ZZPL-a pisanim putem od PIO fonda 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?

Odeljenje za matičnu evidenciju Sektora za ostvarivanje prava iz penzijskog i invalidskog osiguranja PIO fonda odgovorilo je na zahtev za ostvarivanje prava, u prekoračenju zakonom predviđenog maksimalnog roka od 15 dana od dana podnošenja zahteva.

Odgovori su uglavnom preuzeti iz odredbi Zakona o penzijskom i invalidskom osiguranju, dela koji reguliše obradu podataka i vođenje matične evidencije o osiguranicima i korisnicima prava. Pored navođenja podataka o ličnosti koji se unose u matičnu evidenciju, navedeno je da Fond unosi u matičnu evidenciju podatke o osiguranicima, korisnicima prava iz penzijskog i invalidskog osiguranja i obveznicima plaćanja doprinosa za penzijsko i invalidsko osiguranje; da se podaci prikupljaju i unose na osnovu prijava podnesenih na propisanim obrascima; da se podaci koriste prilikom ostvarivanja prava iz penzijskog i invalidskog osiguranja i za statistička istraživanja; da podaci koji se unose u matičnu evidenciju ne služe za dalju distribuciju široj javnosti i da Fond nema zakonska ovlašćenja da te podatke dostavlja trećim licima; kao i da se prijave podataka čuvaju najmanje 30 godina od dana sticanja prava i ne manje od 10 godina od dana prestanka prava.

Precizniji odgovori nedostaju kada su u pitanju vrste obrade podataka koje PIO fond sprovodi, svrhe obrade podataka, kao i ko su korisnici podataka, koji se podaci koriste, po kom pravnom osnovu i u koje svrhe se podaci koriste.

Zaključak

Regulisanje obaveze vođenja Matične evidencije, precizno definisanje podataka o ličnosti koji se vode u Matičnoj evidenciji zakonskom odredbom, u ovom slučaju članom 125 Zakona o penzijskom i invalidskom osiguranju, kao i jasna svrha za orbadu ovih pdoataka 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 125 Zakona o penzijskom i invalidskom 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 obzriom da je od tada došlo do određenih promena u obradi podataka, a naročito osnivanjem Centralnog registra obaveznog socijalnog osiguranja, potrebno je da se ovi podaci ažuriraju.

Interni akti koji regulišu određene aspekte upravaljanja i pristupa podacima iz Matične evidencije predstavljaju pre svega zastarele a u nekim aspektima i nerazumljive akte. Dok je suvišno obrazlagati prevaziđenost Pravilnika iz 1998. godine, skrenuli bismo pažnju na konfuziju koju može izazvati Instrukcija iz 2010. godine. Naime, iako je njen cilj da ustanovi procedure za zaposlene u PIO fondu u slučajevima kada se građani obraćaju sa zahtevima u vezi podataka o ličnosti, na samom početku se navodi definicija podataka iz Zakona o slobodnom pristupu informacijama od javnog značaja a ne definicija podataka iz Zakona o zaštiti podataka o ličnosti, što usmerava zaposlene iz PIO fonda na potpuno drugačiji pravni osnov i vrstu zahteva.

Sa druge strane činjenica je da je u PIO fondu uveden standard ISO 9001 – Sistem upravljanja kvalitetom te da je PIO fond sertifikovan i po zahtevima standarda ISO 27001 Sistem upravljanja bezbednošću informacija. U tom smislu dokumenta koja su izrađena u skladu sa ISO standardima predstavljaju dobra rešenja koja uređuju brojna pitanja vezana za odgovornosti i pravila u vezi sa zaštitom podataka o ličnosti i koja u mnogome smanjuju rizik od evenutalne povrede prava na zaštitu podataka o ličnosti.

ORGANIZACIONI ASPEKTI OBRADE PODATAKA

Lice za zaštitu podataka o ličnosti

U Republičkom fondu za penzijsko i invalidsko osiguranje postoji lice zaduženo za bezbednost informacija, koja bi trebalo da uključuje i zaštitu podataka o ličnosti. Radno mesto direktora IT sektora podrazumeva odgovornost za bezbednost informacija. On je određen u skladu sa zahtevima standarda ISO 27001, gde mora postojati predstavnik rukovodstva za bezbednost informacija..

U PIO fondu, sa druge strane, ne postoji teritorijalna distribucija odgovrnosti za bezbednost informacija, a posebno podataka o ličnosti. Jedno od potencijalno aplikativnih i dobrih rešenja za distribuiranje odgovornosti za bezbednost informacija među zaposlenima PIO fonda, može biti dobra praksa primenjena u Republičkom fondu za zdravstveno osiguranje (RFZO). Naime, oba fonda imaju sličnu strukturu, sa pokrajinskim delovima, filijalama i ispostavama. U okviru PIO fonda postoji 35 filijala širom Srbije, sa velikim brojem ispostava.

U takvoj organizaciji, odgovornost za bezbednost informacija, posebno za zaštitu podataka o ličnosti, trebalo bi da bude distribuirana na više nivoa. Na prvom nivou, odgovornost bi trebalo da postoji u Direkciji PIO fonda u Beogradu. U trenutnoj organizaciji, ta odgovornost je na direktoru sektora informacionih tehnologija. Na drugom nivou bi odgovorna lica trebalo da budu direktori filijala, dok bi određeni nivo odgovornosti trebalo definisati i za rukovodioce u ispostavama PIO fonda.

S obzirom da je PIO fond sertifikovan po zahtevima standarda ISO 27001 sistema upravljanja bezbednošću informacija, odgovornosti 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

Pored navedenih organizacionih i tehničkih odgovornosti imenovanih lica, u opis njihovih nadležnosti je poželjno dodati pitanja koja su vezana i za organizacionu kulturu zaposlenih u PIO fondu, te su uključene i dodatne odgovornosti: :

- 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 u organizaciji na kome se nalaze lokalni koordinatori.

Posebnu pažnju je potrebno obratiti na zaštitu podataka o ličnosti na nivou ispostava, koje se nalaze u manjim mestima, gde je mnogo veća verovatnoća da zaposleni u PIO fondu lično poznaju korisnike, te i interes za neovlašćen pristup podacima o ličnosti može biti veći.

Edukacija

Postojeće stanje: U Republičkom fondu za penzijsko i invalidsko osiguranje je sprovedena obuka zaposlenih za primenu zahteva standarda ISO 27001 - Sistem upravljanja bezbednošću informacija.. Posebna pažnja je prilikom obuka posvećena zaštiti podataka o ličnosti, s obzirom da većina dokumenata kojima upravlja PIO fond sadrži podatke o ličnosti korisnika. Istovremeno, na internom portalu PIO fonda postoje određene instrukcije za postupanje u skladu sa Zakonom o zaštiti podataka o ličnosti. Pored toga, u PIO fondu postoji i Priručnik za zaposlene u pogledu zaštite informacija.

Svi zaposleni PIO fonda, ali i eksterni dobavljači koji svoje poslove obavljaju u prostorijama PIO fonda, potpisali su izjave o odgovornosti (poverljivosti).

Preporuka: Opisane instrukcije se odnose na načine ostvarivanja prava na pristup podacima o ličnosti i zakonskim obavezama PIO fonda u tim slučajevima, pre svega od strane trećih lica, odnosno korisnika. Instrukcije bi svakako trebalo dopuniti primerima dobre, odnosno loše prakse u vezi sa zaštitom podataka o ličnosti. Postoje brojni primeri narušavanja zaštite podataka o ličnosti u drugim institucijama, i takve primere bi trebalo uključiti u instrukcije, kako bi zaposleni stekli širu sliku o tome šta predstavlja kršenje Zakona (namerno ili nenamerno). Na taj način će instrukcije postati mnogo svrsishodnije.

PIO fond upravlja velikom količinom podataka o ličnosti te je od izuzetne važnosti uvesti kontinuiranu edukaciju zaposlenih iz ove oblasti. Takođe, trebalo bi definisati vremenske intervale u kojima se organizuju testiranja znanja zaposlenih iz ove oblasti, kako bi rukovodstvo PIO fonda na svim nivoima imalo konstantna saznanja o stanju sistema u pogledu zaštite podataka o ličnosti.

Pristup zaposlenih Matičnojevidenciji

Postojeće stanje: U PIO fondu je razvijen sistem korisničkih uloga sa različitim pravima pristupa. Pristup je određen kombinacijom korisničkog imena i šifre, koja je vezana za svakog zaposlenog. Prilikom svakog pristupa bazi evidentira se, upisom u odgovarajuće fajlove, i ko je, kada i gde pristupio bazi i koju akciju je radio. Logovi se čuvaju mnogo duže od 30 dana, dok se logovi o matičnoj evidenciji čuvaju godinama. Osnov pristupa se ne beleži, ali je pristup bazi od strane jednog zaposlenog ograničen na predmete za koje je zadužen, i nema mogućnost pretraživanja baze po bilo kom kriterijumu.

Ne postoje zaposleni koji imaju pun pristup svim korisničkim imenima i lozinkama. Nijedan zaposleni ne može pristupiti nijednoj lozinki. Administratori sistema imaju mogućnost da promene i generišu novu lozinku i proslede je zaposlenom. Lozinka generisana na taj način mora biti promenjena u određenom, softerski definisanom periodu. Ne postoje master šifre pomoću kojih se mogu vršiti sve akcije na podacima iz baze. Lozinke moraju da zadovolje 3 od 4 opšteprihvaćena sigurnosna pravila u vezi sa složenošću lozinke.

Pristup podacima iz matične evidencije je omogućen svim zaposlenima koji učestvuju u ostvarivanju prava penzijskog i invalidskog osiguranja. Obim prava pristupa zavisi od vrste posla kojim se bave zaposleni. Deo ovlašćenja definiše ovlašćeno lice u Direkciji PIO fonda, po zahtevu direktora organizacionih jedinica (sektora), a deo direktor organizacione jedinice fonda. Postoje tri nivoa pristupa. Proces se odvija tako što rukovodilac (u slučaju filijale), na osnovu rada na terenu šalje zahtev svom Sektoru u Direkciji PIO fonda, u kome su navedena potrebna ovlašćenja za konkretnog zaposlenog. Nakon odobravanja, u tom slučaju odgovorni Sektor prosleđuje odobreni zahtev Sektoru za informacione tehnologije koji kreira korisnički nalog sa odgovarajućom šifrom.

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.

Preporuka: Pre svega, opravdano je postaviti pitanje efektivnosti definisanja samo tri nivoa pristupa podacima, tačnije pitanje fleksibilnosti koje pruža takav sistem. Pretpostavka je da neće doći do situacije da određeni zaposleni nemaju pristup podacima koji su im potrebni za obavljanje svakodnevnih radnih aktivnosti, ali baš zato što ima samo tri nivoa pristupa postoji mogućnost da će određeni zaposleni imati pristup većoj količini podataka nego što im je potrebna, čime dolazi do povećanja rizika.

Takođe, definisanje ovlašćenja bi trebalo da bude isti proces kao što je određivanje radnog mesta zaposlenog, odnosno samim određivanjem radnog mesta zaposlenog bi trebalo da budu definisana i njegova ovlašćenja. 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.

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 PIO fonda postoji Sektor informacionih tehnologija koji je zadužen za održavanje i implementaciju informacionog sistema. Takođe, u njihove nadležnosti spada i izgradnja jedinstvenog informacionog sistema (JIS) i sa tim povezana migracija podataka matične evidencije u Oracle bazu. Informacioni sistem je u potpunosti razvijen unutar PIO Fonda, od strane zaposlenih IT stručnjaka u Sektoru informacionih tehnologija, što govori o stručnosti zaposlenih. Održavanje informacionog sistema je takođe odgovornost Sektora za informacione tehnologije, za sve filijale na teritoriji centralne Srbije (za filijale u Vojvodini je odgovoran Pokrajinski fond). PIO fond nema izraženih problema sa odlaskom stručnjaka iz ove oblasti, već je fluktuacija u normalnim granicama i odnosi se pre svega na redovnu (starosnu) fluktuaciju.

Sektor za informacione tehnologije ima oko 120 zaposlenih, ali je preko 70 angažovano na poslovima obrade podataka, tako da je oko 50 zaposlenih angažovano na poslovima razvoja i održavanja informacionog sistema.

Postoje spoljne firme koje su angažovane na određenim poslovima održavanja i razvoja informacionog sistema. Svi zaposleni kod ovih firmi moraju biti navedeni u ugovoru o pružanju konsultantskih usluga, i svi moraju pojedinačno potpisati izjave o poverljivosti u okviru ugovora. U okviru PIO fonda za svaki ugovor te vrste postoji odgovorno lice (imenovani zaposleni), koji mora biti prisutan prilikom dolaska pružalaca usluge na lokaciju PIO fonda i njegova je odgovornost da niko ko nije naveden u ugovoru ne sme pristupiti informacionom sistemu PIO fonda. Dalje, kada pristupaju podacima u bezi, eksterna lica to rade preko korisničkih naloga kreiranih posebno za te svrhe i uz prisustvo odgovornog lica iz PIO fonda. Pristup se obavlja na posebnim kompjuterima koji nemaju pristup internetu.

Evidencija u papirnoj formi

Postojeće stanje: U papirnoj formi postoje prijave podataka za matičnu evidenciju, i one se nalaze u filijalama i ispostavama. Kada se unese broj propisan internim aktima PIO fonda, dokumenta se šalju u Direkciju PIO fonda, nadležnom Odeljenju za mikrofilmovanje i skeniranje. Ukoliko neko od zaposlenih želi da pristupi podacima u papirnoj formi, ne evidentira se pristup, niti se beleži razlog pristupa. Međutim, postoje određene objektivne okolnosti koje dovode do smanjenja rizika. Naime, dokumenta u papirnoj formi postoje samo određeno vreme, jer se posle mikrofilmovanja uništavaju. Kasniji pristup mikrofilmovima pretpostavlja pretragu elektronske baze, jer je to jedini način za pronalaženje fizičke pozicije mikrofilma. O pretrazi se čuvaju svi podaci, tako da to predstavlja preventivnu meru zaštite podatka o ličnosti.

Preporuka: Radi daljeg smanjenja rizika, 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 penzijsko i invalidsko osiguranje je uveden standard ISO 9001 – Sistem upravljanja kvalitetom, kao bazni standard serije. Takođe, PIO fond je sertifikovan i po zahtevima standarda ISO 27001 Sistem upravljanja bezbednošću informacija. Prva sertifikacija po ovom standardu je urađena 2014. godine, dok je resertifikacija sprovedena 2015 godine. Na osnovu dostavljene dokumentacije može se zaključiti da su zahtevi standarda ispunjeni u potpunosti.

Zaključak

U Republičkom fondu za penzijsko i invalidsko osiguranje posvećuje se znatna pažnja zaštititi podataka o ličnosti, dok su u toj oblasti uvedena značajna organizaciona i tehnička rešenja. Preporuke date u ovom delu izveštaja mogu dodatno da podignu sposobnost sistema da ispuni sva očekivanja zainteresovanih strana u pogledu zaštite podataka o ličnosti.

Republički fond za penzijsko i invalidsko osiguranje je sertifikovan po zahtevima standarda ISO 27001 Sistem upravljanja bezbednošću informacija, što potvrđuje izuzetno dobro stanje sistema za upravljanje bezbednošću informacija.

TEHNIČKI ASPEKTI OBRADE PODATAKA

Opšte tehničke informacije i struktura sistema

U dosadašnjem poslovanju PIO fonda, svaka filijala je samostalno skladištila podatke za Matičnu evidenciju, dok je odnedavno sve centralizovano u data centrima u Beogradu i Novom Sadu. Filijale imaju svoje servere, dok se u ispostavama nalaze terminali koji se vežu za server u adekvatnoj filijali. Za prikupljanje, obradu i skladištenje podataka o ličnosti, PIO fond koristi ukupno 31 virtuelnu mašinu, 5 uređaja za skladištenje i 38 fizičkih servera. Svi serveri su u vlasništvu PIO fonda i nalaze se u data centrima u Beogradu i Novom Sadu, gde su takođe i centralni serveri na kojima se vrše obrada i skladištenje podataka o matičnoj evidenciji - ukupno 15 servera. Takođe, postoji 24 virtuelnih servera za filijale, odnosno svaka filijala ima svoj server, 5 servera za pregled skenirane arhive, aplikacija i Spidera, 4 servera za razmenu podataka sa drugim institucijama i 4 servera za elektronsku poštu. Na svim serverima se nalaze podaci o Matičnoj evidenciji, osim na serverima za elektronsku poštu.

Pristup internetu

Sajt PIO fonda (www.pio.rs) hostuje EUnet DOO. Ugovor o hostingu je samostalno nabavljen i zaključen kroz otvorenu javnu nabavku, preko ISO standarda 27001:2013. Internet provajder PIO fonda je Telekom Srbija.

Sajt nije direktno povezan sa Matičnom evidencijom, već se Matičnoj evidenciji pristupa kroz DMZ (Demilitarised Zone), što znači da celokupni saobraćaj koji ide u bazu, odnosno upiti koji se šalju Matičnoj evidenciji, prolazi kroz servere koji filtriraju maliciozne upite. Ukoliko korisnik usluga PIO fonda želi da proveri svoje podatke, on pristupa sajtu i unosi određene parametre - JMBG, PIN i verifikacioni kod. Sajt prosleđuje te parametre namenskom delu sistema, gde se nalaze isključivo podaci koji su dostupni korisnicima. To znači da korisnici ne pristupaju Matičnoj evidenciji, već njenj replici.

Opšte informacije	
Naziv ustanove	Republički fond za penzijsko i invalidsko osiguranje
URL	http://www.pio.rs/lat/
Datum vršenja analize	27.04.2015.

WHOIS pretraga	
Ime i Prezime	Zoran Sutara
Adresa	Dr Aleksandra Kostića 9, Beograd
Provider	EUnet D.O.O
URL Provajdera	http://www.eunet.rs/
Registrator	EUnet D.O.O
URL Registratora	http://www.eunet.rs/
Država	Srbija
Nmap	
Broj otvorenih portova	3
Broj filtriranih portova	939
Broj zatvorenih portova	58
OS	Linux 2.6.22-2.6.23
Bezbedan (Nmap)	Da
IP v4	217.26.211.188
IP v6	/
MAC	/

VPN i Cloud usluge

S obzirom na rasprostranjenost PIO fonda na čitavoj teritoriji Republike Srbije, postoji više od 160 organizacionih jedinica (filijala i ispostava), te je korišćenje VPN usluga neizbežno. Sinhronizacija između filijala i ispostava vrši se u realnom vremenu (terminal u ispostavi radi direktno na serveru koji se nalati u filijali). Lica koja ne koriste VPN usluge su eksterna, tehnička lica koja održavaju informacioni sistem kojem nemaju pristup van zgrade PIO fonda. Provajder ovih usluga je Telekom Srbija.
PIO fond ne koristi Cloud usluge i ne postoje planovi da se to promeni.

Serverska podešavanja

Sektor Informacionih tehnologija PIO fonda razvio je celokupni informacioni sistem kao i Matičnu evidenciju o osiguranicima, obveznicima plaćanja doprinosa i korisnicima prava iz penzijskog invalidskog osiguranja. Takođe, oni samostalno održavaju taj informacioni sistem na svim lokacijama centralne Srbije, koji postoji već 30 godina.

Zbog rasprostranjenosti PIO fonda, sinhronizacija podataka između servera u filijalama i centrali vrši se jednom dnevno (na kraju radnog vremena). Vrsta baze Matične evidencije u Beogradu je Cobol, dok je u Novom Sadu baza IBM. Cobol je prilično zastarela tehnologija koja ne inkorporira savremene trendove upravljanja podacima i bezbednosne procedure za zaštitu podataka, ali se ne može reći da je ova tehnologija nepouzdana. Njena pozitivna strana ogleda se u tome što u novije vreme retko ko poznaje dovoljno dobro za uspešan napad. U svakom slučaju, u toku je unapređenje baze na savremeniju Oracle tehnologiju.

Prilikom svakog pristupa bazi evidentira se razlog pristupa i to upisom u fajlove iz kojih se vidi ko je, kada i gde pristupio bazi i koju radnju je izvršio. Realizacija pojedinačnih kadrovskih mera zaštite podataka se odvija dodeljivanjem odgovarajućih šifara i lozinki za rad zaposlenom u čijoj je nadležnosti uvid u podatke uz prethodno pisano odobrenje neposrednog rukovodioca, tako da se u svakom trenutku mogu proveriti lica koja imaju mogućnost pristupa podacima. Tu pojedinačnu šifru i lozinku poznaje samo zaposleni kome se one dodeljuju.

Šifre i lozinke se ukidaju po napuštanju PIO fonda ili prestanku ovlašćenja za pristup podacima. Na svakom aktu se šifra i ime i prezime zaposlenog moraju podudarati. Dodeljivanje šifara i lozinki se vrši u Direkciji PIO fonda, na osnovu pisanog zahteva koji se dostavlja direktno Sektoru za informacione tehnologije. Korisničko ime i lozinka su vezani za konkretnog zaposlenog.

Radna mesta koja imaju pristup svim korisničkim imenima i lozinkama (sistem administratori) direktno i isključivo su vezana za osobe koje vrše dodelu ovlašćenja. Samo zaposleni koji rade na poslovima ostvarivanja prava iz penzijskog i invalidskog osiguranja i poslovima vođenja matične evidencije, imaju mogućnost pristupa podacima osiguranika i korisnika prava iz penzijskog i invalidskog osiguranja.

Kada je reč o kreiranju lozinke, zaposleni moraju poštovati pravila i koristiti kombinacije velikih i malih slova, specijalnih znakova, a lozinka se mora sastojati od više od 8 znakova. Postoji određen vremenski period nakon kojeg zaposleni mora promeniti svoju lozinku.

Na primerku svakog dokumenta PIO fonda koji sadrži podatke o ličnosti, nalazi se i pečat, potpis i šifra zaposlenog koji je imao pristup podacima. Dakle, za svakog zaposlenog se, ukoliko i neovlašćeno daje podatke, može utvrditi da li je izdao pojedinačni dokument.

PIO fond poseduje veliki broj različitih fajlova u kojima se čuvaju informacije o tome ko je koji podatak i kada uneo, promenio ili izbrisao (log fajlovi), a takođe poseduje i informacije ko je i kada pristupao podacima iz Matične evidencije. Fond poseduje više servera, jer je obrada podataka za Matičnu evidenciju distribuirana.

Politika bezbednosti informacija koju PIO fond koristi ima za cilj da uspostavi, sprovodi, održava i poboljšava sistem bezbednosti informacija ispunjavajući zahteve standarda ISO 27001:2013 i svih relevantnih propisa u oblasti bezbednosti informacija.

Namena Politike bezbednosti informacija jeste da obezbedi i zaštiti informacije i imovinu preduzeća od svih pretnji, internih ili eksternih, slučajnih ili namernih, kroz uspostavljanje, primenu, izvršavanje, nadziranje, preispitivanje, održavanje i poboljšanje sistema upravljanja sigurnošću informacija (ISMS). Sprovođenje ove politike i pravila važno je za održavanje integriteta informacionog sistema PIO fonda u pružanju podrške procesima rada, zaposlenima kao i drugim zainteresovanim stranama.

Politika bezbednosti i zaštite obezbeđuje i garantuje:
- da će informacije biti zaštićene od neovlašćenog pristupa;
- da će se održavati poverljivost informacija;
- da informacije neće biti otkrivene neovlašćenim osobama, slučajnim ili namernim aktivnostima;
- da će integritet informacija biti sačuvan kroz zaštitu od neovlašćene izmene;
- da će biti omogućen pristup i izmena informacija ovlašćenim licima kada je to potrebno;
- da će biti obezbeđena usaglašenost sa propisima i zahtevima kontrole;
- da će biti pružena podrška ovoj politici kroz kontinuirane poslovne planove koji će se uređivati, održavati i testirati u stalnom praktičnom radu;
- da će se obuka zaposlenih obavljati kroz sve organizacione delove Fonda i
- da će sve povrede bezbednosti informacija i sigurnog rukovanja informacijama biti razmatrane i istražene.

Svi zaposleni koji učestvuju u postupku ostvarivanja prava iz penzijskog i invalidskog osiguranja imaju pravo pristupa bazi, s tim što obim prava pristupa bazi podataka zavisi od vrste posla kojim se bave i ovlašćenja koja imaju u vezi sa tom vrstom posla, što je propisano odgovarajućim procedurama urađenim po zahtevima standarda ISO 27001.

Preduzete mere zaštite podataka prema Centralnom registru Poverenika za informacije od javnog značaja i zaštite podataka o ličnosti su: *Identifikacija zaposlenih koji pristupaju zbirci podataka, jasno i određeno pravo pristupa (autorizacije) dodeljivanjem šifre zaposlenima koji rade na njihovom izdavanju*.

PIO fond ima propisanu proceduru ukoliko dođe do incidenta od strane zaposlenih. Takođe, u Novom Sadu se nalazi sigurnosna kopija (backup) cele Matične evidencije koja se čuva na posebnim trakama u vatrostalnim sefovima.

Pristup Trećih lica

Pristup podacima registrovanim u matičnoj evidenciji imaju fizička lica i to onim podacima koji se na njih odnose, uz prethodno podnošenje zahteva za dobijanje PIN koda, preko internet aplikacije. Korisnici svojim podacima pristupaju unošenjem JMBG-a, PIN i verifikacionog koda na sajtu PIO fonda - Elektronski servis za građane (https://servisi.pio.rs/gradjani/modules/login/).
Državni organi nemaju direktan pristup evidenciji, već podnose zahtev elektronskim servisom.

Tehnička, eksterna lica koja održavaju informacioni sistem potpisuju izjavu o poverljivosti. Ova lica nemaju pristup sistemu PIO fonda, odnosno ne koriste VPN usluge. Dodeljeni su im posebni korisnički nalozi sa ograničenim pristupima, a izmene na sistemu vrše isključivo uz prisustvo odgovornog lica PIO fonda. Rade na posebnim kompjuterima koji nemaju pristup internetu. U dosadašnjem radu, PIO fond se nije susreo sa kršenjem izjava o poverljivosti u IT sektoru.

Zaključak

PIO fond ima kompleksan sistem za prikupljanje, obradu i skladištenje podataka o ličnosti koji je centralizovan na dva mesta, u Beogradu i Novom Sadu. Celokupna obrada podataka vrši se na centralnim serverima u Beogradu i Novom Sadu. Kao pozitivnu praksu možemo izdvojiti to što PIO fond za razmenu podataka sa drugim institucijama koristi specijalizovane servere isključivo za tu namenu.

Na nivou bezbednosnih politika primenjuju se ISO standardi 27001;2013, dok se sva pretraživanja baze putem interneta filtriraju kroz DMZ što u velikoj meri smanjuje mogućnost za napade na bazu podataka, čime je obezbeđen integritet tih podataka. S obzirom na strukture PIO fonda koji je rasprostranjen na celoj teritoriji Republike Srbije, za komunikaciju između centrala i perifernih jedinica koristi se VPN, a sinhronizacija se vrši jednom dnevno na kraju radnog dana.

Ukoliko se interna pravila koja su u saglasnosti sa ISO standardima doslovno primenjuju u radu PIO fonda i s obzirom na tehničku postavljenost sistema, smatramo da je bezbednost podataka o ličnosti u PIO fondu na visokom nivou.

MEDIJSKA POKRIVENOST

Uvodna napomena

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 značajnog aktera u zaštiti interesa građana.

PIO FOND – Istorijski pregled

Standardne teme kroz koje se mediji bave Republičkim fondom za penzijsko i invalidsko osiguranje, vezane su za probleme povezivanja staža, reforme samog sistema, korupcije i različitih zloupotreba. Sredinom 2000-tih formira se centralna baza od koje se očekuje da kroz javnost podataka omogući i zaposlenima i Fondu PIO da stalno proveravaju uplate poslodavca.

Usluga elektronskog uvida u matičnu evidenciju Fonda PIO postala je operativna 2010. godine a mediji prenose uputstva za korišćenje i opisuju prednosti servisa, kroz izjave nadležnih i saopštenja institucije. Aspekt zaštite podataka ne postavlja se kao posebno pitanje.

Narednih godina, uspostavljanjem instituta Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, te rastom pažnje javnosti prema pravu na privatnost, Fond PIO pominje se kao jedna od institucija na koje se građani najčešće žale kancelariji Poverenika zbog zloupotreba ličnih podataka.

Krajem 2012. mediji otkrivaju da PIO prikuplja podatke o osiguranicima od poslovnih banaka, na osnovu nezakonitog ugovora kojim su se banke obavezale da obaveste Fond ukoliko klijent ne koristi novac sa računa duže od 6 meseci ili ukoliko duže od 12 meseci novac podiže samo ovlašćeno lice. Zbog pritužbi građana i medijskih napisa, Poverenik je tim povodom pokrenuo postupak nadzora nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti u Republičkom fondu za penzijsko i invalidsko osiguranje, nakon čega je postupanje banaka i PIO fonda usklađeno za ZZPL-om.

DOKUMENTACIJA DOBIJENA OD POVERENIKA

Postupci nadzora

U Zapisniku o izvršenom nadzoru br. 164-00-00098/2011-07, od 14.06.2011. navodi se da je Poverenik izvršio nadzor nad PIO fondom zbog predstavke kojom je ukazano da se nezakonito obrađuju podaci o ličnosti osiguranika od strane PIO fonda i firme IT Excelence. Poverenik je izvršio nadzor isključivo u delu koji se odnosi na izvršavanje obaveza koje se tiču obezbeđenja i zaštite podataka o ličnosti. Naime, postojala je sumnja da je kompaniji IT Excelence dato administriranje, odnosno neovlašćen pristup informacionom sistemu PIO fonda, a sve u toku procesa implementacije softvera za jedinstvenu prijavu.

PIO fond je dalje opisao odnos sa IT Excelence i njihov pristup sistemu, i na kraju negirao ove tvrdnje. Objasnili su da je pristup bazama podataka strogo kontrolisan i propisan putem pravilnika i internih akata, tako da osim ovlašćenih osoba Fonda, niko drugi ne može pristupati informacionom sistemu, kako unutar Fonda, tako i eksterno putem interneta. Serverima, aplikacijama i bazama podataka mogu pristupati samo ovlašćeni radnici preko svojih korisničkih naloga, lozinki i posebnih šifara definisanih za svaku aplikaciju i bazu ponaosob. Na pitanje zašto je firmi IT Excellence dato administriranje informacionog sistema PIO Fonda kako je i predviđeno ugovornim obavezama, navedeno je da su ove obaveze "nesrećno napisane" i da IT Excellence nije imao, niti će imati mogućnost administriranja informacionim sistemom, kao i da nije došlo do neovlašćenog pristupa podacima iz baze podataka osiguranika Fonda PIO.

U Upozorenju Poverenika nakon obavljenog nadzora br. 164-00-00034/2011-07, od 17.08.2011., utvrđeno je da je nepoznati zaposleni PIO fonda kopirao lične podatke iz Matične evidencije osiguranika i dostavio ih trećem licu čiji to nisu bili podaci i koje nije imalo pravo da te podatke zahteva, čime je izvršena nedozvoljena obrada podataka, bez pristanka lica čiji se podaci obrađuju, odnosno, bez zakonskog ovlašćenja, gde se pod obradom podrazumeva i kopiranje, prenos i činjenje dostupnim trećem licu. Naime, listing PIO sa ličnim podacima određenog lica dostavljen je njegovoj ćerki kao dokaz u sudskom postupku u fotokopiji i originalu, koji je naknadno vraćen, što je lice kao tužilac, primilo kao prilog uz podnesak tužene u predmetu. Takođe, u Obaveštenju PIO Fonda, 02 broj 181-5014/11, od 05.09.2011., a u vezi sa Upozorenjem Poverenika, navedeno je da je u pitanju moguća svesna zloupotreba obrade podataka od strane određenog pojedinca a ne sistemski propust Fonda. U nastavku Obaveštenja su navedene sistemske organizacione i tehničke mere zaštite podataka o ličnosti.

U Upozorenju Poverenika nakon obavljenog nadzora, br. 164-00-00249/2012-07, od 11.02.2013., utvrđeno je da PIO fond vrši nedozvoljenu obradu podataka, odnosno vrši

obradu bez zakonskog ovlašćenja ili pismene saglasnosti lica, tako što neovlašćenim licima izdaje uverenja iz matične evidencije koja ne glase na ime lica koje je uverenje tražilo, niti ima ovlašćenje za njegovo pribavljanje. Naime, u sudskom postupku se pojavilo uverenje koje sadrži podatke o radnom stažu lica, iako takvo uverenje lice nije tražilo, a uz prijavu je dostavljena i fotokopija uverenja, koju je izdao rukovodilac matične evidencije PIO fonda. U odgovoru PIO fonda, Filijale Novi Sad, navedeno je da je uverenje izdato na osnovu usmenog zahteva, uvidom u lična dokumenta, direktno na šalteru filijale, da dokumentacija na osnovu koje je izdato uverenje nije zadržana, da ne postoji dostavnica kojom se potvrđuje uručenje uverenja i da ovakva praksa proizilazi iz velikog broja zahteva osiguranika za izdavanje uverenja i da bi duže trajanje postupka imalo negativne posledice za osiguranike. Poverenik je dalje konstatovao da podnosilac zahteva nije dao saglasnost za obradu njegovih ličnih podataka, niti je dao ovlašćenje trećem licu za pribavljanje ovih podataka i predložio niz mera i aktivnosti koje treba preduzeti za otklanjanje nepravilnosti u postupku izdavanja uverenja o ličnim podacima osiguranika. U Obaveštenju Fonda u vezi sa Upozorenjem Poverenika, 02 broj 181-1816/13, od 25.03.2013., navedeno je da se Fond slaže sa upozorenjem i planira preduzeti sve potrebne mere kako bi se problem prevazišao.

U upozorenju Poverenika nakon obavljenog nadzora, br. 164-00-00456/2014-07, od 14.01.2015., konstatovano je da PIO fond nije preduzeo sve neophodne tehničke, kadrovske i organizacione mere zaštite podataka o ličnosti. Nalaz koji je za predmet imao procenu radne sposobnosti, a koji sadrži podatke o ličnosti određenog lica (ime i prezime, JMBG, broj lične karte, mesto i adresa) i naročito osetljive podatke (podaci o zdravstvenom stanju), donet u postupku utvrđivanja promena u stanju invalidnosti lica, iznet je iz zbirke podataka PIO fonda i objavljen na internet sajtu informativnog veb portala Soinfo.org. Dalje, Rukovalac, Direkcija Pokrajinskog fonda za penzijsko i invalidsko osiguranje, se izjasnio da se navedeni akt ne dostavlja stranci na koju se odnosi, već se obrađuje i čuva isključivo kod Rukovaoca podataka i da je navedeni nalaz mogao objaviti, odnosno učiniti dostupnim samo zaposleni kod Rukovaoca podataka, koji ima pristup tom dokumentu. Poverenik je zaključio da je Rukovalac podataka bio dužan da obezbedi striktnu primenu od strane zaposlenih Pravilnika o radnoj disciplini i ponašanju zaposlenih i Kodeksa poslovne etike i ponašanja zaposlenih u PIO fondu, kao i primenu samih odredbi člana 47 ZZPL, u vezi organizacionih i tehničkih mera zaštite podataka.

Razni dopisi

U dopisu PIO fonda Povereniku, br. 07-6572/13, od 25.10.2013., Fond je imao obavezu da odgovori na pitanja po kom pravnom osnovu i u koje svrhe vrši obradu podataka u vidu činjenja dostupnim podataka o ličnosti JP Srbija šume, RFZO-u i Upravnom sudu i konstatovao da u aktu Poverenika nije ukazano u čemu se konkretno sastoji neovlašćena obrada podataka, kao ni u čemu se konkretno sastoji nezakonitost obrade. Fond je dalje

naveo da nije neovlašćeno dostavio podatke o ličnosti JP Srbija šume, RFZO-u i Upravnom sudu, ne navodeći konkretne detalje.

U dopisu Poverenika određenom licu, br. 164-00.00700/2013-07, od 13.11.2013., a povodom njegovog podneska sa zahtevom za pokretanje nadzora zbog neovlašćenog činjenja dostupnim njegovih podataka o ličnosti JP Srbija šume, RFZO-u, i Upravnom sudu, oštećeno lice se informiše da je postupak obustavljen jer nema dokaza za njegove tvrdnje. U dopisu se obrazlaže da lice nije dostavilo informacije koje tačno podatke je PIO fond neovlašćeno obrađivao (učinio dostupnim trećim licima) i gde su isti sadržani, kao i kojom tačno radnjom obrade su podaci učinjeni dostupnim trećim licima, što je onemogućilo utvrđivanje činjeničnog stanja. Takođe, uvid u podnetu dokumentaciju i izjave stranaka u postupku nisu ukazivale na to da je došlo do nezakonite obrade podataka, tako da nema mesta preduzimanju radnji i mera iz nadležnosti Poverenika u ovom slučaju.