VODIČ ZA ORGANE VLASTI

ZAŠTITA PODATAKA O LIČNOSTI

USAID
OD AMERIČKOG NARODA

SHARE FOUNDATION

"VODIČ ZA ORGANE VLASTI – ZAŠTITA PODATAKA O LIČNOSTI"
SHARE FONDACIJA
MART 2016.
UREDNICI: ĐORĐE KRIVOKAPIĆ, DANILO KRIVOKAPIĆ
AUTORI: DANILO KRIVOKAPIĆ, ĐORĐE KRIVOKAPIĆ, IVAN TODOROVIĆ, STEFAN KOMAZEC, ANDREJ PETROVSKI, KATARINA ERCEGOVIĆ
OBRADA TEKSTA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ: 600

IZRADA OVE PUBLIKACIJE OMOGUĆENA JE UZ PODRŠKU AMERIČKOG NARODA PUTEM AMERIČKE AGENCIJE ZA MEĐUNARODNI RAZVOJ (USAID). ZA SADRŽAJ OVE PUBLIKACIJE ODGOVORNI SU AUTORI I ONA NE MORA NUŽNO ODRAŽAVATI STAVOVE USAID-A ILI VLADE SJEDINJENIH AMERIČKIH DRŽAVA.

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
004.738.5:351.083.8(497.11)(036)
ZAŠTITA podataka o ličnosti : vodič za organe vlasti / [autori Danilo Krivokapić ... et al.]. - Novi Sad : Share fondacija, 2016 (Novi Sad : NS press). - 67 str. ; 24 cm
Tiraž 600.
ISBN 978-86-89487-07-7
1. Кривокапић, Данило [аутор]
а) Интернет - Заштита података - Србија - Водичи
COBISS.SR-ID 304490247

SADRŽAJ

INDEKS POJMOVA I SKRAĆENICA

PREDGOVOR

PREDGOVOR

Uspostavljanje savremenih standarda zaštite privatnosti, odnosno zaštite podataka o ličnosti je bez izuzetka jedan od glavnih zadataka sa kojima se suočavaju tranzicione zemlje. Nije nimalo lak ni brzo ostvariv, budući da podrazumeva kopernikanski obrt u sistemu vrednosti, nužnost da se privatnost građana koja se godinama u okviru kolektivističkog sistema vrednosti nalazila na samom dnu lestvice vrednosti podigne visoko, praktično na vrh.

I Srbija je, naravno, suočena sa tim zadatkom. Od pre šest godina imamo Zakon o zaštiti podataka o ličnosti koji, iako nedovoljno usklađen sa standardima zaštite podataka afirmisanim u EU, ipak bar na načelnom nivou proklamuje te standarde. Nažalost, u proteklom periodu nismo ostvarili rezultate koje smo mogli i morali ostvariti.

Opravdanja za to nema, ali postoji objašnjenje. Za svaku tranzicionu zemlju, radi ozbiljnog i odgovornog pristupa tako složenom i teškom zadatku kakav je prihvatanje evropskih standarda zaštite podataka o ličnosti, neophodan akt je Strategija zaštite podataka o ličnosti. Vlada Srbije nije Strategiju donela kao što bi to bilo logično, pre ili istovremeno sa donošenjem Zakona o zaštiti podataka o ličnosti, 2008, već je usvojila tek (na inicijativu Poverenika, u tekstu koji je on pripremio, iako je to bila obaveza Vlade) dve godine kasnije, u leto 2010. Nužna pretpostavka za realizaciju Strategije je, naravno, Akcioni plan za njeno sprovođenje, koji je trebalo da bude usvojen u roku od tri meseca. Nije usvojen, a njegovo donošenje "dosledno" je odlagano uprkos tome što potrebu za njim na doslovno dramatičan način, svakodnevno "argumentuje" naša stvarnost, teškim povredama privatnosti građana iz kojih nedopustivo često stoje upravo oni koji bi trebalo da je štite, državni organi.

Zbog toga docnimo na tri bitna plana. Na normativnom, jer su nam propisi daleko od usklađenosti ne samo sa standardima EU, nego i sa našim Ustavom. Na faktičkom, jer se aktivnosti državnih organa na zaštiti podataka o ličnosti u nedopustivo visokom procentu svode samo na aktivnosti Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti. I, što je možda najvažnije, docnimo na planu edukacije, kako građana tako i onih koji se njihovim podacima o ličnosti bave. To je pogotovo važno za subjekte iz javnog sektora, gde su i koncentracija podataka o ličnosti i odgovornost veći.

Edukacija je doslovno neophodna, jer je, naročito u javnom sektoru, potrebno ne samo podizati nivo svesti o značaju zaštite podataka, već i graditi sposobnost i znanje za primenu tehničkih i organizacionih mera zaštite podataka.

Upravo u tom kontekstu, Vodič za organe vlasti "Zaštita podataka o ličnosti", finalni rezultat jednog atraktivnog i vrednog projekta koji je sprovela SHARE Fondacija uz podršku USAID-ovog Projekta za reformu pravosuđa i odgovornu vlast, predstavlja vrlo vredan i koristan doprinos. Verujem da će moje mišljenje podeliti svi oni koji će ga koristiti u želji da svoj rad unaprede većim stepenom odgovornosti prema podacima o ličnosti koje obrađuju, odnosno kvalitetnijom i efikasnijom zaštitom tih podataka.

RODOLJUB ŠABIĆ,

Poverenik za informacije od javnog značaja
i zaštitu podataka o ličnosti

UVOD

UVOD

Decembra 2014. godine javnost je saznala za najmasovniju povredu privatnosti i prava na zaštitu podataka o ličnosti građana Srbije. Naime, tih dana je SHARE Fondacija utvrdila da je na sajtu Agencije za privatizaciju dostupan dokument koji sadrži lične podatke o 5.190.396 građana Srbije - njihovo ime i prezime, srednje ime i jedinstveni matični broj (JMBG). U postupku nadzora koji je potom sprovela služba Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, ustanovljeno je da je sporni dokument 10 meseci bio javno dostupan na sajtu Agencije za privatizaciju sa kog je, po rečima nadležnih iz Agencije, preuzet "više" puta. Posledice ovog slučaja teško da se sada mogu u potpunosti sagledati i čini se da još uvek nedostaje puno razumevanje ozbiljnosti incidenta. Javnost se nije bavila ovim slučajem dalje od ponekog senzacionalističkog naslova, dok je utvrđivanje odgovornosti potpuno izostalo. Više od godinu dana kasnije i dalje se ne zna da li je reč o slučajnosti, sistemskom propustu ili zloj nameri. Posebno zabrinjava činjenica da različiti akteri koji rukuju podacima građana i dalje koriste JMBG kao vrstu identifkatora, što znači da je samo na osnovu ličnog imena i teško kompromitovanog matičnog broja moguće pristupiti podacima o ličnosti u pojedinim registrima organa vlasti, ili čak obavljati pojedine poslove u banci telefonskim putem.

Slučaj Agencije za privatizaciju otkrio je razmere rizika kom su izloženi naši podaci, ali je ukazao i na nedostatak pouzdanih saznanja o praktičnim i tehničkim uslovima u kojima se podaci građana prikupljaju, obrađuju i čuvaju. SHARE Fondacija je stoga rešila da istraži koji se podaci prikupljaju u javnom sektoru, ko i na koji način ima pristup podacima građana, te koje se mere zaštite u ovim procedurama primenjuju. Značaj istraživanja je, srećom, prepoznat u USAID-ovom Projektu za reformu pravosuđa i odgovornu vlast, pa je tako projekat SHARE Fondacije pod nazivom "Podaci o ličnosti u javnom sektoru – Mapiranje infrastrutkure obrade podataka u Srbiji" dobio neophodnu podršku.

Rad je započet u aprilu 2015. godine, obimnim istraživanjem o vrstama obrade i načinima zaštite podataka o ličnosti u javnom sektoru, čiji su procesi zatim analizirani sa pravnog, organizacionog i tehničkog aspekta, predstavljenim u ovom Vodiču. Istraživanje je obuhvatilo šest državnih institucija: Republički fond za zdravstveno osiguranje, Republički fond za penzijsko i invalidsko osiguranje, Centralni registar obaveznog socijalnog osiguranja, Poreska uprava, Agencija za privredne registre i Gradski centrar za socijalni rad Beograd. Metodološki je istraživanje zasnovano na javno dostupnim podacima, ali i podacima dobijenim putem zahteva za pristup informacijama od javnog značaja. Institucije su bile spremne na saradnju, te je sa predstavnicima održan niz sastanaka zahvaljujući kojima su istraživači bolje upoznavali i razumevali procese rukovanja podacima građana u javnom sektoru.

Tokom rada, istraživači SHARE Fondacije su imali neprocenjivu podršku službe Poverenika za pristup informacijama od javnog značaja i zaštitu podataka o ličnosti. Značajno iskustvo koje zaposleni u službi Poverenika imaju u ovoj oblasti bilo je dragoceno za rad istraživača, a posebno njihova dostupnost i spremnost za aktivnu razmenu znanja.

Kao krajnji rezultat istraživanja, Vodič obuhvata najbolje prakse i procedure zaštite podataka koje se primenjuju u analiziranim institucijama, ali i višegodišnje iskustvo službe Poverenika iz ove oblasti te znanje i inovativnost SHARE Fondacije koja se posebno bavi pitanjima privatnosti u digitalnom okruženju.

Vodič je namenjen pre svega organima vlasti, ali s obzirom na to da je zaštita podataka o ličnosti oblast uređena zakonom koji se tiče svih aktera, analize i preporuke iz istraživanja SHARE Fondacije biće od koristi i rukovaocima podataka iz privatnog sektora. Konačno, najvažnija svrha istraživanja predstavljenog u ovom Vodiču, jeste doprinos boljem razumevanju podataka o ličnosti, značaja njihove zaštite, kao i dužnosti rukovaoca i obrađivača podataka, te tehničkih i organizacionih mera koje su im na raspolaganju ili koje su u obavezi da primene kako bi zaštitili podatke o ličnosti građana Srbije.

U prvom delu Vodič razmatra osnovne pojmove ove, relativno nove oblasti. Zakon o zaštiti podataka o ličnosti pisan je u skladu sa celokupnim narativom domaćeg pravnog sistema, strukovnim jezikom neophodnim za efikasnu primenu, a koji ponekad može biti neprohodan manje upućenom čitaocu. Razjašnjenja pojedinih odredbi i termina kao što su 'rukovalac', 'obrada podataka', pa i sam 'podatak o ličnosti', data su kroz primere,

stvarne ili hipotetičke. Bolje razumevanje smisla osnovnih pojmova i principa Zakona o zaštiti podataka o ličnosti, nužan je uslov za prepoznavanje prava na privatnost i zaštitu podataka o ličnosti kao otelotvorenja suštinske potrebe svakog građanina, a ne spoljašnjeg mehanizma nametnutog prolaznom pravnom normom.

U odeljku posvećenom organizacionim merama za zaštitu podataka izložene su analize i preporuke namenjene upravi i kadrovskoj službi organa vlasti, kao niz korisnih smernica za organizaciju zaposlenih u skladu sa načelom smanjenja rizika od povrede prava na zaštitu podataka o ličnosti. Posebno su obrađena pitanja poput odgovornosti za zaštitu podataka, lica koja se bave tim poslovima, edukacije zaposlenih, neophodnih internih akata i druga.

Tehničke mere za zaštitu podataka namenjene su prvenstveno tehničkim ekspertima u organima vlasti, a u tom delu su izložena iskustva i preporuke za adekvatnu strukturu informacionog sistema, te problemi pristupa, čuvanja i zaštite podataka u digitalnom okruženju.

Poslednji, četvrti deo Vodiča tretira praksu lica ovlašćenih da postupaju po zahtevima za ostvarivanje prava iz Zakona o zaštiti podataka o ličnosti. Tu su obrađene procedure i načini na koji organ vlasti treba da postupa po ovim zahtevima građana, uz poseban osvrt na nedoumice ili nejasnosti koje su uočene prilikom razlikovanja zahteva vezanih za zaštitu podataka od zahteva za pristup informacijama od javnog značaja.

SHARE Fondacija, mart 2016.

OSNOVNI POJMOVI

PODACI O LIČNOSTI

ŠTA SU PODACI O LIČNOSTI?

Podatak o ličnosti predstavlja svaku informaciju koja se odnosi na fizičko lice koje se u nekom trenutku može identifikovati. Dakle, da bi se konstatovao podatak o ličnosti neophodno je utvrditi četiri odvojena elementa: 1) informaciju, 2) koja se odnosi, 3) na identifikovano ili podložno identifikaciji, 4) fizičko lice.

Prilikom procene svojstva podatka o ličnosti, nije od značaja da li fizičko lice na koje se odnosi informacija poseduje poslovnu sposobnost, već je dovoljno samo to da se informacija odnosi na ljudsku jedinku, u skladu sa savremenom teorijom jednake opšte pravne sposobnosti čoveka. Podaci preminulih lica takođe uživaju zaštitu po Zakonu o zaštiti podataka o ličnosti (ZZPL), pa je tako članom 35 propisano čuvanje i korišćenje podataka u slučaju smrti, dok zakonski naslednici mogu da podnose zahteve za ostvarivanje prava u ime preminulih lica.

Da bi informacija predstavljala podatak o ličnosti nije od značaja njen kvalitet, odnosno da li ona predstavlja činjenicu, laž ili mišljenje.[1] Podatak o ličnosti stoga može predstavljati svaku vrstu sadržaja, informaciju koja ima značenje i smisao, poput nečijeg rukopisa, crteža deteta, uzorka krvi ili metapodatka koji se odnosi na vreme pristupa određenom sadržaju. Takođe, forma informacije nije od značaja, te podatak o ličnosti može biti u običnoj pisanoj ili digitalnoj formi, bazi podataka, foto, video ili zvučnom zapisu, odnosno u bilo kojoj drugoj vrsti zapisa i skladišta koji informaciju čuva tako da joj se može ponovo pristupiti. Dodatno, treba smatrati i da enkriptovani podaci, koji su nerazumljivi za sve osim ovlašćenog primaoca, predstavljaju podatke o ličnosti.

Kako bi predstavljala podatak o ličnosti, informacija mora biti u relaciji sa fizičkim licem. U tom smislu, informacija i fizičko lice mogu biti dva entiteta između kojih postoji direktna veza, a mogu biti i u vezi posredno kroz više objekata. Kvalitet uspostavljene veze mora biti zasnovan bar na jednom od tri sledeća elementa:

- **Sadržaj** - informacija opisuje lice (zelene oči - čita redovno Peščanik - lenj)
- **Svrha** - informacija omogućava procenu lica, odnosno određeni tretman (listing telefona određene pozicije u firmi, u kontekstu efikasnosti lica koje radi na toj poziciji)
- **Efekat** - informacija može imati uticaj na lice ili njegov interes, pravo, slobodu (korišćenje lokacije mobilnog uređaja kako bi se obezbedila optimalna usluga licu koje koristi mobilni uređaj)

Okolnost da se jedna informacija nalazi u relaciji sa nizom lica nije od značaja prilikom procene da li određena informacija predstavlja podatak o ličnosti. Takođe, jedan zapis koji poseduje više informacija može predstavljati podatak o ličnosti u odnosu na više lica, za svakog u različitim segmentima, ili jedan segment predstavlja podatak o ličnosti više lica.

PRIMER:

Sudska odluka kojom se rešava brakorazvodna parnica predstavlja dokument koji u svojim različitim segmentima sadrži podatke o ličnosti velikog broja osoba. Tako se na početku presude nalaze lični podaci sudije (lično ime, sud u kome radi), advokata (lično ime) a zatim i podaci osoba između kojih se vodi parnica, a koji se redovno nalaze u presudama (lično ime, datum rođenja, adresa prebivališta). Ali, tu se mogu naći i brojni drugi podaci koji su navedeni u izreci i

01 Ipak, prema mišljenju Poverenika iz predmeta 07-00-002452/2014-06 od 03.12.2014. godine subjektivni stav i mišljenje jednog lica ne predstavlja podatak o ličnosti u odnosu na lice na koga se subjektivni stav ili mišljenje odnosi. S druge strane, izjava svedoka u sudskom postupku, kao izraz njegovog subjektivnog doživljaja stvarnosti, jeste podatak o ličnosti svedoka.

obrazloženju presude, kao što su visina prihoda, podaci o zdravstvenom stanju, ličnim navikama (često dolazi kući u alkoholisanom stanju) i tako dalje. Ako se presudom mora rešiti i pitanje vršenja roditeljskog prava, u presudi će se naći i podaci o maloletnoj deci lica koja se razvode.

Podatak o ličnosti konačno mora imati element koji identifikuje, odnosno može identifikovati lice na koje se informacija odnosi. Dakle, "informacija" mora sadržati ili biti u vezi sa identifikatorom koji predstavlja sredstvo identifikacije i informaciju sa bliskim i privilegovanim odnosom sa licem. Identifikatori su u praksi informacije poput ličnog imena i JMBG-a, koje mogu direktno utvrditi osobenost i individualnost određenog lica razlikovanjem od svih ostalih. U savremenom digitalnom okruženju, u okviru koga se ljudi konstantno kreću kroz informacione prostore, ne odvajajući se od elektronskih uređaja, raste broj potencijalnih sredstava identifikacije (broj mobilnog telefona, email adresa, IMEI - jedinstveni broj mobilnog uređaja, IP adresa, biometrijski podaci, ritam otkucaja srca itd).

Do identifikacije takođe može doći i indirektnim putem, kombinovanjem informacija koje nisu sredstva identifikacije (pol, godine, mesto boravišta, profesija itd), ali koje usled svog karaktera i međusobne veze zajedno omogućavaju identifikovanje lica određenoj zajednici.

PRIMER:

Novine objave vest da postoje osnovi sumnje da je mito primila ženska osoba koja ima 27 godina, zaposlena je u odeljenju za finansije Opštinske uprave Stara Pazova, te u svom vlasništvu poseduje 3 stana i 2 lokala. Iako nijedan od ovih podataka pojedinačno ne može identifikovati konkretno fizičko lice, kada se dovedu u međusobnu vezu, posebno u kontekstu manje sredine, identitet osobe se može utvrditi bez većih poteškoća.

Prilikom utvrđivanja podatka o ličnosti možemo se susresti sa brojnim nejasnoćama, te bi se svakoj situaciji trebalo posebno posvetiti. Iste informacije, u zavisnosti od konteksta, mogu biti tretirane na različite načine. Informacija o lekovima koje su doktori prepisali, a koja ne sadrži vezu sa pacijentima, čini se da nije podatak o ličnosti jer ne postoji način da se identifikuje pacijent. Međutim, relacija između lekova i doktora može biti od interesa za farmaceutsku industriju i njihova marketing odeljenja, te bi u tom kontekstu ova informacija predstavljala podatak o ličnosti doktora.

ZZPL propisuje isključivo zaštitu prava fizičkih lica. Informacije koje se odnose na pravna lica, kao što su privredna društva, udruženja ili državni organi, po pravilu ne predstavljaju podatke o ličnosti. Ipak, postoje određene granične kategorije gde pre svega treba voditi računa o svrsi obrade i mogućnosti za povredu prava ličnosti.

PRIMER:

Preduzetnik je poslovno sposobno fizičko lice koje obavlja delatnost u cilju ostvarivanja prihoda i koje je, kao takvo, registrovano u registru privrednih subjekata. U ovom registru se vode podaci koji se odnose na preduzetničku radnju i to su poslovni podaci koji ne predstavljaju podatke o ličnosti (poreski identifikacioni broj, matični broj preduzetničke radnje, šifra delatnosti i slično). Podatak o sedištu preduzetničke radnje prvenstveno je poslovni podatak koji se ne odnosi na fizičko lice, čak i kada je preduzetnik svoju radnju registrovao na kućnoj adresi, što nije redak slučaj. Ukoliko se taj podatak koristi u svrhe poslovanja (dostavljanje faktura, poslovna komunikacija), on i dalje neće steći status podatka o ličnosti. Međutim, ukoliko se zna da se preduzetnička radnja nalazi na kućnoj adresi, a taj podatak se koristi u svrhe uznemiravanja drugih ukućana koji žive na toj adresi, onda bi podatak o sedištu radnje mogao da dobije status i zaštitu koju imaju podaci o ličnosti.

Jasno je da se bilo koji podatak koji se odnosi na fizičko lice može svrstati pod pojam podatka o ličnosti, međutim, samo neki od njih uživaju pravnu zaštitu. ZZPL predviđa dva mehanizma za ostvarivanje odgovarajuće zaštite podataka u skladu sa potrebama društva u odnosu na zaštitu privatnosti građana. Tako su sa jedne strane propisane situacije u kojima se ZZPL ne primenjuje, dok su sa druge strane definisani naročito osetljivi podaci.

PODACI NA KOJE SE NE PRIMENJUJU ODREDBE ZAKONA O ZAŠTITI PODATAKA O LIČNOSTI

Postoje situacije u kojima podaci o ličnosti neće uživati zaštitu propisanu Zakonom, kada je kontekst i svrha obrade ne opravdavaju. Konkretno, ZZPL u članu 5 navodi da se odredbe ovog Zakona o uslovima za obradu, kao i o pravima i obavezama u vezi sa obradom, ne primenjuju na obradu:

- **podataka** koji su **dostupni svakome** i objavljeni su u javnim glasilima i publikacijama, ili pristupačni u arhivama, muzejima i drugim sličnim organizacijama;
- **podataka** koji se obrađuju za **porodične i druge lične potrebe** i nisu dostupni trećim licima;
- **podataka** koji se o članovima **političkih stranaka, udruženja, sindikata**, kao i drugih oblika udruživanja obrađuju od strane tih organizacija, pod uslovom da član dâ pismenu izjavu da određene odredbe ovog zakona ne važe za obradu podataka o njemu za određeno vreme, ali ne duže od vremena trajanja njegovog članstva;
- **podataka koje je lice**, sposobno da se samo stara o svojim interesima, **objavilo o sebi**.

Da ne bude zabune, svi ovi podaci i dalje zadržavaju status podataka o ličnosti, ali je jasno da ne postoji potreba da se na njih primenjuje strogi režim zaštite. Nije potrebno da se građani koji obrađuju podatke o ličnosti u vidu albuma porodičnih fotografija, telefonskih imenika svojih poznanika i slično, tretiraju kao rukovaoci, uz sve obaveze koje taj status sa sobom nosi, niti je potrebno da se dalje štiti tajnost podataka koji su javno objavljeni u publikacijama, ili ih je lice na koje se odnose samo objavilo.

Naravno, ukoliko očigledno pretežu interesi lica da se zaštita podataka ipak ostvari, i u netipičnim situacijama bi moglo da dođe do primene ZZPL-a. Pretežni interes osobe na koju se podaci odnose predstavlja temelj pravnog standarda koji treba tumačiti u svakom konkretnom slučaju i u skladu sa načelima Zakona, koji izviru iz ustavnog prava građana na privatnost.

PRIMER:

Tabloid nezakonito, bez pravnog osnova i bez ičije saglasnosti, objavi slike iz bolnice, dijagnozu bolesti, spisak lekova i preporučenu terapiju estradne umetnice. Iako su ovi podaci objavljeni u javnom glasilu i na taj način postali dostupni javnosti, za šta će naravno postojati pravna odgovornost tabloida i lica koje je te podatke učinilo dostupnim, to ne znači da je dalja obrada tih podataka slobodna i da ne treba da uživaju dalju zaštitu. U tom smislu bi se i dalje objavljivanje takvih informacija, kao i komentarisanje stručnjaka za oblast medicine o konkretnoj bolesti, smatralo nedozvoljenom obradom podataka.

NAROČITO OSETLJIVI PODACI

Određeni podaci o ličnosti su "ličniji" od drugih, a njihovom obradom se dublje zadire u privatnost građana kao osnovno ljudsko pravo, te je stoga ovim podacima potrebno dati drugačiji status kako bi mere njihove zaštite bile strože u odnosu na ostale podatke o ličnosti. Jasno je da broj patika koje nosimo ne može biti podatak koji uživa istu zaštitu kao i naše versko uverenje.

ZZPL je u skladu sa tim definisao naročito osetljive podatke koje bismo mogli da podelimo u dve grupe:

- **Podaci** koji se mogu obrađivati **samo na osnovu pristanka lica**, propisanog članom 17 ZZPL-a, i to samo onda kada zakonom nije zabranjena obrada ni uz pristanak. To su podaci koji se odnose na:

- nacionalnu pripadnost
- rasu
- jezik
- veroispovest
- seksualni život
- pol

Ovde se može postaviti pitanje svrsishodnosti označavanja pola kao naročito osetljivog podatka, imajući u vidu da se ovaj podatak može uvek saznati iz drugih podataka koji nemaju ovaj status, kao što je JMBG, a u najvećem broju slučajeva i lično ime. Sa druge strane naročito osetljiv bi bio podatak o promeni pola.

- **Podaci** koji se mogu obrađivati bez pristanka lica, **samo ako je to zakonom propisano.** To su podaci koji se odnose na:
  - pripadnost političkoj stranci
  - sindikalno članstvo
  - zdravstveno stanje
  - primanje socijalne pomoći
  - žrtvu nasilja
  - osudu sa krivično delo

Ovde je bitno napomenuti da ZZPL ne navodi striktno da se podaci koji se odnose na žrtvu nasilja i osudu za krivično delo mogu obrađivati bez pristanka lica, ali to je previd zakonodavca, imajući u vidu da su određeni organi vlasti zakonom ovlašćeni da obrađuju naročito osetljive podatke. Tako je organ starateljstva (Centar za socijalni rad) dužan da vodi evidenciju i dokumentaciju o licima prema kojima je izvršeno nasilje u porodici.

U slučajevima kada organi vlasti obrađuju naročito osetljive podatke, trebalo bi da posebno označe ovu obradu i da primene posebne mere zaštite. Posebne mere zaštite naročito osetljivih podataka trebalo je da budu uređene Uredbom Vlade, u skladu sa ZZPL-om, ali ni više od 7 godina nakon stupanja na snagu ZZPL-a ova Uredba nije doneta. To ipak ne znači da ne postoji obaveza organa vlasti da naročito osetljive podatke zaštite posebnim merama, već to znači da u nedostatku konkretnih tehnika i principa koje bi bile propisane Uredbom, organi vlasti treba sami da ovakve mere propišu i primene.

OBRADA PODATAKA

ŠTA JE OBRADA PODATAKA?

Svaka radnja preduzeta u vezi sa podacima o ličnosti smatra se obradom podataka. ZZPL navodi najčešće radnje od kojih ćemo navesti samo neke:

- prikupljanje i beleženje;
- obezbeđivanje i držanje;
- stavljanje na uvid, objavljivanje ili na drugi način činjenje dostupnim;
- pretraživanje, proveravanje, razvrstavanje, objedinjavanje, ukrštanje;
- prepisivanje, umnožavanje, kopiranje;
- izmeštanje i na drugi način činjenje nedostupnim;
- iznošenje iz zemlje.

Ipak, ni poduža lista radnji koje se smatraju obradom, a koja se navodi u ZZPL-u, nije konačna, već se obradom smatra i svaka druga radnja u vezi sa podacima o ličnosti. Suštinski, teško je zamisliti situaciju u kojoj bi se organ vlasti našao u dodiru sa podacima o ličnosti a da se to ne smatra obradom podataka, s obzirom da se i samo držanje ili uvid u podatke smatra radnjama obrade.

PRIMERI OBRADE PODATAKA O LIČNOSTI OD STRANE ORGANA VLASTI:

Organ vlasti samo čuva zbirke podataka na svojim serverima bez ikakvog uvida u njih.

Organ vlasti služi samo kao primalac dokumentacije i nakon vrlo kratkog vremena je prosleđuje dalje.

Organ vlasti samo vrši uvid u podatke bez mogućnosti da ih menja.

Organi vlasti mogu imati razne uloge prilikom obrade podataka pa je mnogo bitnije odrediti kakvu ulogu ima organ vlasti kada obrađuje podatke. U tom smislu, on može biti:

- **rukovalac** podataka
- **obrađivač** podataka
- **korisnik** podataka

RUKOVALAC PODATAKA

Organ vlasti će imati status rukovaoca podataka kada **određuje svrhu i način obrade** podataka o ličnosti, ili su svrha i način obrade podatka ustanovljeni zakonom radi obavljanja poslova iz njegove nadležnosti. U ovom kontekstu, svrha bi se odnosila na razlog i potrebu zbog kojih se podaci obrađuju, dok se način obrade odnosi na pitanja kao što su "koji podaci će se obrađivati?", "koliko dugo će se podaci obrađivati?", "ko će imati pristup podacima?" i ostalo.

Dakle, svojstvo rukovaoca organ vlasti može steći na osnovu zakona ili to može proizaći iz aktivnosti organa vlasti o kojima samostalno donosi odluku.

PRIMER 1:

Zakonom o zdravstvenoj dokumentaciji i evidencijama je utvrđeno da zdravstvene ustanove vode zdravstvene kartone. Takođe su određeni podaci koji se vode u zdravstvenim kartonima (medicinski podaci, dijagnoze i ostalo), te da se kartoni čuvaju 10 godina nakon smrti lica, kao i da pristup podacima iz kartona imaju samo medicinski radnici u svrhu očuvanja i unapređenja zdravlja pacijenata.

PRIMER 2:

Javno preduzeće iz razloga bezbednosti i zaštite svoje imovine uvodi sistem video nadzora u svoje prostorije. Uz to, utvrdi koje prostorije će se snimati, da će se video snimci čuvati mesec dana i da niko sem radnika obezbeđenja i zakonom ovlašćenih lica neće imati pristup video snimcima.

OBRAĐIVAČ PODATAKA

Obrađivač je, kao i rukovalac, lice koje obrađuje podatke. Ipak, to nije lice koje samo određuje svrhu i načine obrade podataka, niti je to ustanovljeno zakonom za njegove potrebe, već je to lice kome rukovalac podataka na osnovu zakona ili ugovora poverava određene poslove u vezi sa obradom. To znači da je obrađivač odvojeni pravni entitet od rukovaca, te da obrađivač u kontekstu obrade podataka postupa u skladu sa nalozima koje mu je dao rukovalac.

U skladu sa tim, organ vlasti se može naći u ulozi obrađivača, ali takođe i u ulozi rukovaoca koji poverava određene poslove u vezi sa obradom drugom licu kao obrađivaču.

PRIMER 1:

Javno preduzeće "Beograd vode" iz razloga nedostatka poslovnog prostora zaključi ugovor sa gradskom upravom Grada Beograda radi čuvanja dokumentacije u arhivi Grada Beograda. U odnosu na dokumentaciju koja sadrži određene podatke o ličnosti "Beograd vode" će biti rukovalac, a gradska uprava Grada Beograda će biti obrađivač, s obzirom da je ugovorom predviđeno da će za "Beograd vode" čuvati dokumentaciju u svojoj arhivi.

PRIMER 2:

Javno preduzeće koje iz razloga bezbednosti i zaštite svoje imovine uvede sistem video nadzora u svoje prostorije, angažuje privatnu firmu na čijim serverima će se čuvati kopije snimaka u periodu od mesec dana. U ovom slučaju javno preduzeće je rukovalac, a obrađivač je privatna firma koja vrši obradu podataka (čuvanje video snimaka) po nalogu javnog preduzeća.

Bez obzira koji status ima organ vlasti, **u odnosu rukovaoca i obrađivača moraju se poštovati sledeći principi:**

- Rukovalac može poveriti određene poslove u vezi sa obradom samo **obrađivaču koji ima odgovarajuće tehničke i organizacione kapacitete** za obradu podataka;
- **Rukovalac je odgovoran** za izbor obrađivača;
- Prava i obaveze rukovaoca i obrađivača treba da se urede **ugovorom u pisanom obliku**, koji treba da sadrži sledeće odredbe:
  - obavezu obrađivača da obrađuje podatke samo u okviru dobijenog ovlašćenja;
  - podaci se ne smeju koristiti u svrhe koje nisu ugovorene;
  - obavezu obrađivača da obezbedi organizacione i tehničke mere zaštite podataka;
  - zaposleni kod obrađivača imaju obaveze čuvanja poverljivosti podataka;
  - obaveze koje obrađivač ima po okončanju ugovorene obrade podataka.

KORISNIK PODATAKA

Korisnik podataka je lice koje je zakonom ili po pristanku lica ovlašćeno da koristi podatke. U tom smislu, korisnik podataka takođe obrađuje podatke ali nema status rukovaoca, jer ne određuje svrhu i načine obrade, niti ima status obrađivača jer ne vrši obradu podataka po nalogu rukovaoca.

PRIMER:

Zakonom o prekršajima je predviđeno vođenje Registra novčanih kazni, te je propisano da se podaci o licima koja nisu platila novčane kazne, a čiji se podaci vode u ovom registru, mogu izdati sudovima, nadležnom tužilaštvu, policiji i organima inspekcije, pa u tom smislu svi ovi organi predstavljaju korisnike podataka.

ODGOVORNOST I OBAVEZE RUKOVAOCA, OBRAĐIVAČA I KORISNIKA PODATAKA

Od statusa organa vlasti u konkretnom slučaju, zavisiće i njegove odgovornosti i obaveze.

Rukovalac je primarno odgovoran za obradu podataka o ličnosti i ima sve obaveze propisane ZZPL-om:

- Obavezu da vrši obradu podataka u skladu sa zakonom i načelima obrade podataka;
- Obavezu da primenjuje organizacione i tehničke mere za zaštitu podataka;
- Odgovornost za izbor obrađivača;
- Obavezu da obavesti lica o obradi pre samog početka obrade(član 15 ZZPL-a);
- Obavezu da postupa po zahtevima za ostvarivanje prava (članovi 19-43 ZZPL-a);
- Obaveze u vezi vođenja evidencija i Centralnog registra Poverenika (članovi 48-52 ZZPL-a).

Obrađivač ima:

- Obavezu da vrši obradu podataka u skladu sa Zakonom i načelima obrade podataka;
- Obavezu da primenjuje organizacione i tehničke mere za zaštitu podataka;
- Obavezu da postupa u svemu u skladu sa nalogom koji mu je dao rukovalac.

Korisnik podataka ima:

- Obavezu da vrši obradu podataka u skladu sa Zakonom i načelima obrade podataka.

U principu, za svaku obradu podataka je od presudnog značaja odrediti ko je rukovalac. ''To znači da je prva i najvažnija uloga postojanja koncepta rukovaoca da se utvrdi ko je prvenstveno odgovoran za poštovanje pravila o zaštiti podataka o ličnosti, i da se utvrdi prema kome građani mogu ostvarivati svoja prava. Drugim rečima, da se dodeli odgovornost.''[2] Ovo je veoma važno, jer rukovalac ima obavezu ali i mogućnosti da presudno utiče na zakonitu obradu podataka o ličnosti. Pored toga što i sam mora poštovati sve obaveze propisane ZZPL-om, on je odgovoran za izbor obrađivača i za zakonito ustupanje podataka korisniku podataka.

KADA JE OBRADA PODATAKA O LIČNOSTI DOZVOLJENA

Da bi obrada podataka o ličnosti bila dozvoljena, tokom čitavog trajanja obrade mora biti ispunjen makar jedan od dva uslova:

- Podaci se obrađuju na **osnovu zakonskog ovlašćenja;**
- Podaci se obrađuju **na osnovu pristanka lica** čiji se podaci o ličnosti obrađuju.

Dakle, organ vlasti u svakom trenutku mora voditi računa da li je jedan od ova dva uslova ispunjen, jer u protivnom grubo krši ZZPL ali potencijalno i druge zakone Republike Srbije, što za sobom može povući prekršajnu, krivičnu, građansko-pravnu i disciplinsku odgovornost. Izuzetak od ovog pravila je propisan jedino u članu 13 ZZPL-a, ali taj izuzetak se vrlo restriktivno tumači, o čemu će biti više reči u odeljku o obradi bez pristanka.

Dodatno, bez obzira na ispunjenost jednog od dva uslova (zakonsko ovlašćenje/pristanak), da bi obrada podataka o ličnosti bila dozvoljena, organ vlasti se sve vreme mora pridržavati i načela obrade koja ćemo detaljno obrazložiti.

ZAKONSKO OVLAŠĆENJE KAO OSNOV ZA OBRADU PODATAKA

Organi vlasti će se veoma često naći u situaciji da ovlašćenje za obradu podataka crpe iz zakona, imajući u vidu da su upravo zakonima utvrđene nadležnosti i obaveze organa vlasti u svrhe za čije ostvarenje je neophodno obrađivati podatke o ličnosti.

Veoma je bitno pojasniti šta znači zakonsko ovlašćenje, odnosno šta je potrebno da bude regulisano zakonom, kako bi organ vlasti mogao zakonito da obrađuje podatke koji su mu neophodni za obavljanje svojih nadležnosti i delatnosti. U tom smislu zakon treba da reguliše:

- **Koji organ vlasti** je ovlašćen da obrađuje podatke o ličnosti - organ vlasti može biti konkretno određen, npr. Nacionalna služba za zapošljavanje ili barem odrediv, npr. državni organ nadležan za tržište rada;
- **Svrha zbog koje se podaci obrađuju** - svrha može biti direktno određena;

02 Radna grupa za zaštitu podataka, Mišljenje o konceptu rukovaoca i obrađivača, 2010, strana 4. Dostupno na: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169 _ en.pdf

tako Zakon o zdravstvenom osiguranju reguliše da se podaci iz matične evidencije koriste samo za potrebe obaveznog zdravstvenog osiguranja, dok sa druge strane Zakon o penzijskom i invalidskom osiguranju ne propisuje direktno za šta se podaci iz matične evidencije koriste, ali iz čitavog Zakona jasno proizlazi da se ti podaci mogu koristiti isključivo u svrhu ostvarivanja prava iz penzijskog i invalidskog osiguranja;

- **Vrsta i skup podataka** koji se obrađuju - ovo bi značilo da bi u zakonu trebalo da se konkretno navedu podaci koji će se obrađivati (npr. JMBG, adresa prebivališta, podaci o zaradi itd), kao i u odnosu na koja lica će se ovi podaci obrađivati (svi građani Republike Srbije, obavezno zdravstveno osigurana lica, građani koji imaju prebivalište na teritoriji Valjeva, itd)
- Ko ima ovlašćenje za **pristup podacima** - ovo bi značilo da se odredi koji organi vlasti i u koju svrhe mogu pristupati podacima koji se obrađuju, odnosno ko su korisnici podataka..

Kako je ZZPL stupio na snagu tek 1. januara 2009. godine, i dalje postoje brojni zakoni koji utvrđuju nadležnosti organa vlasti za koje je neophodno prikupljanje i obrada podataka, ali ti isti zakoni ni na koji način ne regulišu ovlašćenje za obradu podataka u navedenom smislu, ili to ne rade u dovoljnoj meri. U tom slučaju se organi vlasti mogu naći u nezavidnoj poziciji da zbog svoje delatnosti obrađuju podatke o ličnosti, a da nemaju adekvatno zakonsko ovlašćenje za to. U tim slučajevima bi trebalo da na svaki način zagovaraju izmene postojećih ili donošenje novih zakona, kako bi svoje postupanje u potpunosti uskladili sa ZZPL-om i Ustavom Republike Srbije.

Bitno je naglasti da samo zakon može ustanoviti ovlašćenje za obradu podataka o ličnosti, a to nikako ne može biti podzakonski ili drugi pravni akt niže snage, kojim se mogu urediti načini pribavljanja i drugi tehnički detalji prikupljanja podataka.

UPOZORENJE POVERENIKA

broj 164-00-00300/2012-07 od 03.10.2014. godine: "Kako je prema članu 42. Ustava Republike Srbije, prikupljanje, čuvanje, obradu i korišćenje podataka o ličnosti moguće urediti isključivo zakonom, a članom 8.tačka 2. ZZPL je propisano da obrada podataka o ličnosti nije dozvoljena ako fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja, tako i skup podataka o ličnosti koje se obrađuje i svrha obrade moraju biti definisani samim zakonom. Podzakonskim propisima moguće je urediti način pribavljanja (od koga se podaci prikupljaju), kao i druge tehničke detalje prikupljanja zakonski definisanih podataka od trećih lica, ali se ne može određivati rukovalac podataka koji je ovlašćen da prikuplja podatke, kao ni svrha, odnosno skup podataka koji se mogu obrađivati".

PRISTANAK KAO OSNOV ZA OBRADU PODATAKA

Organi vlasti će po pravilu pristanak tražiti u slučajevima kad obrađuju podatke o ličnosti za potrebe koje nisu u svrhu izvršavanja poslova iz nadležnosti i ovlašćenja organa vlasti.

Pristanak mora imati sledeće karakteristike kako bi obrada na osnovu pristanka bila zakonita:

- Pristanak mora dati **lice na koje se podaci odnose.** No, i u ovom slučaju se primenjuju osnovni instituti građanskog prava, tako da je punovažan i pristanak koji je dat preko punomoćnika (punomoćje mora biti overeno, osim ukoliko je zakonom drugačije propisano), kao i pristanak koji daje zakonski zastupnik ili staralac. Moguće je dati i pristanak za obradu podataka o licu koje je umrlo (član 10, stav 6 ZZPL-a);
- Pre nego što da pristanak, **lice mora da bude obavešteno o svim aspektima obrade podataka** (svrsi obrade, načinu korišćenja, pravu da pristanak opozove i drugim aspektima koji su propisani

članom 15, stav 1 ZZPL-a). Ipak, treba napomenuti da u određenim opravdanim situacijama ovakvo obaveštenje nije potrebno (član 15, stav 2 ZZPL-a);

- Pristanak se mora dati u **pisanoj formi.** Pisana forma u skladu sa članom 3 stav 1 tačka 3 ZZPL-a svakako obuhvata i davanje saglasnosti u elektronskoj formi, i to pod uslovima iz zakona kojim se uređuje elektronski potpis. Razvoj informacionih tehnologija je zapravo doveo do toga da se danas najveći broj obrada podataka dešava upravo na internetu, te je davanje davanje pristanka u elektronskoj formi postao čest vid davanja saglasnosti, koji omogućava dinamičan razvoj usluga na daljinu, pa i razvoj elektronske uprave. Ipak, treba napomenuti da je danas dominantan vid davanja pristanka na Internetu putem tzv konkludentnih, odnosno zaključnih radnji kao eksplicitno datog izraza volje (npr. klikom na "pristajem", "dalje","I agree", itd). Nažalost, ZZPL nije predvideo mogućnost davanja pristanka konkludentnom radnjom, što će svakako biti neophodno kako bi se pravni okvir uskladio sa realnošću digitalnog doba.

OBRADA BEZ PRISTANKA

Članom 13 ZZPL-a propisano je kada organi vlasti mogu obrađivati podatke o ličnosti bez pristanka lica. Formulacija ovog člana može izazvati nedoumice, pa bi se van konteksta moglo zaključiti da organi vlasti mogu obrađivati podatke bez pristanka jedino na osnovu člana 13 ZZPL-a. To naravno nije tačno; podsetimo, obrada podataka o ličnosti je dozvoljena kad postoji zakonsko ovlašćenje ili pristanak lica čiji se podaci obrađuju, što važi za privatni i za javni sektor. U tom smislu, član 13 ZZPL-a treba tumačiti kao izuzetak od postavljenog pravila i organi vlasti ga mogu primeniti samo u vanrednim i hitnim situacijama, a nikako ne može služiti kao osnov za redovnu obradu podataka koja proističe iz nadležnosti organa vlasti.

Da bi po ovom osnovu organ vlasti mogao da obrađuje podatke, neophodno je da kumulativno budu ispunjeni sledeći uslovi:

- obrada se vrši radi obavljanja poslova iz **nadležnosti organa vlasti određenih zakonom,** a nikako radi obavljanja poslova koji su utvrđeni nižim pravnim aktom ili su slobodna delatnost organa vlasti;
- **obrada je neophodna** za obavljanje ovih poslova, odnosno ne postoji mogućnost da se ti poslovi obavljaju bez predmetne obrade;
- obrada se vrši samo u cilju **ostvarivanja jednog od navedenih interesa:**
  - nacionalna ili javna bezbednost;
  - odbrana zemlje;
  - otkrivanje, istraga i gonjenje za krivična dela;
  - ekonomski, odnosno finansijski interesi države;
  - zaštita zdravlja i morala;
  - zaštita prava i sloboda;
  - drugi javni interesi;

Primena ovog člana bi trebalo da bude izuzetak koji se primenjuje samo u situacijama kada je potrebno zaštititi najvažnije interese društva, te se on nikako ne može koristiti kao pravni osnov za najveći deo obrade podataka o ličnosti u javnom sektoru. Pobrojani interesi se već štite brojnim zakonima Republike Srbije, koji daju zakonsko ovlašćenje za obradu podataka u smislu koji smo već naveli. Takođe, svi naizgled široko postavljeni interesi, poput zaštite morala i drugih javnih interesa, moraju se tumačiti izuzetno restriktivno i njihovoj zaštiti u smislu ovog člana ZZPL-a treba pribegavati samo u slučajevima kada je potrebno zaštititi najvažnije interese društva.

Dodatno, ukoliko primenju član 13 ZZPL to ne isključuje obavezu organa vlasti da primenjuje sva postavljena načela obrade podataka o ličnosti, ali i da poštuje odredbe drugih zakona, tako da ovaj član ne daje neograničeno ovlašćenje za obradu podataka.

PRIMER:

Više javno tužilaštvo u Beogradu, u cilju sprovođenja istrage, od operatora mobilne telefonije zahteva podatke o ličnosti P.A. i to listing poziva i geo-lokaciju njegovog mobilnog telefona (zadržani podaci). Na prvi pogled moglo bi se reći da postoje svi uslovi za primenu člana 13, imaući u vidu

da bi se obrada (prikupljanje) podataka vršila radi obavljanja poslova iz nadležnosti tužilaštva određenih zakonom (Zakon o krivičnom postupku i Zakon o javnom tužilaštvu), da je prikupljanje podataka u ovom slučaju neophodno za istragu i da ne postoji drugi način da se istraga sprovede, te da se obrada vrši u cilju otkrivanja, istrage i gonjenja za krivična dela. Ipak, iako su u opisanom slučaju ispunjeni svi neophodni uslovi, Više javno tužilaštvo u Beogradu ne bi bilo ovlašćeno da navedene podatke prikuplja bez odluke suda, imajući u vidu član 41, stav 2 Ustava Republike Srbije, u kome je propisano da se od tajnosti sredstava komuniciranja može odstupiti samo na osnovu odluke suda, ili član 128, stav 2 Zakona o elektronskim komunikacijama, koji nalaže da pristup zadržanim podacima (npr. listing i geo-lokacija) nije dopušten bez odluke suda.

NAČELA OBRADE PODATAKA

Nakon što je utvrdio da postoji neki od opisanih uslova za dozvoljenost obrade, organ vlasti sve vreme tokom obrade mora voditi računa da se poštuju načela obrade, te da usklađuje obradu podataka o ličnosti sa načelima. To znači da zakonsko ovlašćenje, pristanak lica, a u specifičnim situacijama i dozvoljenost obrade bez pristanka, predstavljaju samo prvi filter o kome organi vlasti moraju voditi računa kada je u pitanju dozvoljenost obrade. Drugi filter predstavljaju dodatna pravila o tome kada će obrada podataka o ličnosti biti dozvoljena i koja postoje kako bi organe vlasti dalje usmeravala, jer zakonsko ovlašćenje i pristanak lica čiji se podaci obrađuju ne omogućavaju neograničenu obradu podataka.

NAČELO ZAKONITOSTI I PRAVIČNOSTI

Ovo načelo nije eksplicitno navedeno u ZZPL-u, ali proizlazi iz odredbi Ustava Republike Srbije, Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu podataka, koju je Srbija ratifikovala, kao i pojedinačnh odredbi ZZPL-a. "Zakonitost" kao element ovog načela ima relativno jasno značenje sadržano u ZZPL-u, a iz kojeg proizlazi da obrada podataka uvek mora biti zasnovana na jednom od dva osnova (ovlašćenje/pristanak) te da se uvek moraju poštovati sve odredbe ZZPL-a, ali i drugih zakona. Suštinski, ovo načelo uspostavlja pravila po kojima se moraju prikupiti podaci kako bi uopšte bilo dozvoljeno da uđu u proces obrade. Sa druge strane, pravičnost kao element ovog načela nešto je širi pojam koji podrazumeva da se prilikom obrade uvek mora voditi računa o interesima i razumnim očekivanjima lica čiji se podaci obrađuju. Konkretno, to bi značilo da se podaci o ličnosti ne smeju obrađivati na štetu lica, da se ne sme iskorišćavati monopolski položaj rukovaoca podataka, te da se podaci uvek moraju obrađivati na transparentan način.

NAČELO OGRANIČENOSTI SVRHE

Osnovno načelo zaštite podataka o ličnosti, prepoznato od strane međunarodnih instrumenata, ali i ZZPL-a u članu 8, stav 1, tačke 2 i 3, predstavlja načelo ograničenosti svrhe. Ovim se uspostavlja pravilo da svrha obrade podataka mora biti dozvoljena, konkretna i unapred utvrđena, te da nije dozvoljena obrada podataka koja nije u skladu sa prvobitno navedenom svrhom obrade.[3] U praksi, ovo načelo uspostavlja osnovna pravila po kojima organi vlasti mogu da koriste podatke koje su zakonito prikupili.

Povrede ovog načela su danas vrlo česte, a sekundarna upotreba podataka i druge radnje povrede najčešće nisu ni uočene usled nedostataka transparentnosti. U praksi, organi vlasti nikada ne bi smeli da koriste podatke u svrhu koja je različita od one određene zakonom, ili svrhe koju je organ vlasti utvrdio pre početka obrade.

03 Working Party 29 guidance on purpose limitation principle, dostupno na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203 _ en.pdf

PRIMER:

Gradska uprava raspiše konkurs o dodeljivanju socijalnih stanova i, u svrhu sprovođenja konkursa i izbora porodica koje ispunjavaju uslove za dodelu stanova, prikuplja finansijske podatke lica koja su se prijavila (podatke o primanjima, zaduženjima, vlasništvu nad imovinom i ostalo). Svako korišćenje ovih podataka van navedene svrhe, kao što je na primer svrha utvrđivanja poreskih obaveza, ili dostavljanje ovih podataka bankama kako bi pripremile ponude kredita za lica koja su se prijavila na konkurs, predstavlja kršenje načela ograničenosti svrhe.

NAČELO SRAZMERNOSTI

Načelo srazmernosti je propisano tačkama 6 i 7 stava 1, člana 8 ZZPL-a, kojima je utvrđeno da "obrada nije dozvoljena ako je podatak koji se obrađuje nepotreban ili nepodesan za ostvarivanje svrhe obrade ili ako su broj i vrsta podataka koji se obrađuju nesrazmerni svrsi obrade".

Ako načelo ograničene svrhe uspostavlja osnovna pravila po kojima rukovaci mogu da koriste podatke koje su zakonito prikupili, načelo srazmernosti daje detaljne instrukcije da se obrađuju samo oni podaci koji su relevantni i neophodni za donošenje neke odluke (ostvarenje svrhe), a ne svi koji su eventualno na raspolaganju i koji se mogu smatrati prekobrojnim. To praktično znači da obrada podataka o ličnosti nije dozvoljena ukoliko se svrha obrade može ostvariti i bez upotrebe ovih podataka, odnosno organ vlasti bi trebalo da obrađuje minimum podataka koji su potrebni da bi se svrha obrade ostvarila.

PRIMER:

Organ vlasti ima pisanu proceduru kojom je uređeno da će radnici obezbeđenja na pisarnici zadržavati lične karte građana prilikom ulaska u službene prostorije. S obzirom da je svrha ovakvog zadržavanja bezbednost i zaštita imovine, jasno je da se ona može ostvariti i uvidom u ličnu kartu, kao i prepisivanjem određenih podataka lica (ime, prezime, broj i vrsta lične isprave, vreme i razlog ulaska i izlaska...). Zadržavanje lične karte je nepotrebno i nesrazmerno svrsi obrade, te bi se tim činom učinila povreda ZZPL-a, što za sobom povlači prekršajnu odgovornost. O ovom problemu se više puta izjašnjavao i Poverenik koji je, između ostalog, tim povodom uputio upozorenje MUP-u, nakon čega je postupajući po tom upozorenju ministar unutrašnjih poslova svim policijskim upravama u Srbiji dostavio akt kojim je naloženo "da odmah prestanu sa zadržavanjem lične karte i druge javne isprave sa fotografijom lica kojima se izdaje dnevna propusnica za ulazak u objekte MUP-a i drugih objekata na teritoriji Republike Srbije gde su policijski službenici angažovani na poslovima obezbeđenja."

NAČELO TRANSPARENTNOSTI OBRADE

Načelo transparentnosti obrade predstavlja princip kojim se licima čiji se podaci obrađuju, pruža pravo da zahtevaju od rukovaoca da budu potpuno obavešteni o radnjama obrade i podacima o ličnosti koji se za tu svrhu koriste. To znači da u praksi građani najpre moraju biti obavešteni o obradi i ovlašćeni da pristupe svim podacima koji su o njima prikupljeni, uključujući informacije o načinu njihovog prikupljanja. Tako lica imaju pravo na obaveštenje o obradi, pravo na uvid i pravo na kopiju podataka koji se o njima prikupljaju:

ZAŠTITA PRAVA LICA ČIJI SE PODACI OBRAĐUJU

Pravo na obaveštenje o obradi	Pravo na uvid	Pravo na kopiju

O načinima ostvarivanja ovog načela više detalja u delu koji se odnosi na zahteve građana u vezi sa obradom podataka o ličnosti.

NAČELO TAČNOSTI (KVALITETA INFORMACIJA)

Načelo kvaliteta informacija zahteva da se podaci o ličnosti obrađuju na način kojim se obezbeđuje njihova istinitost, potpunost i ažurnost, uključujući relevantnost i dozvoljenost u kontekstu svrhe obrade. U praksi ovo načelo nameće rukovaocu obavezu da ima aktivan odnos prema podacima koje obrađuje, dok lice čiji se podaci prikupljaju ovlašćuje da utiče na proces obrade. Do povrede ovog načela dolazi ako su obrađivani podaci netačni ili dovode u zabludu (npr. nepotpuni podaci) u kontekstu svrhe obrade.

Ažuriranje podataka podrazumeva usklađivanje podataka sa njihovim aktuelnim stanjem. Svrha za koju se podaci koriste će svakako biti od značaja prilikom odlučivanja o potrebi ažuriranja. Stoga u pogledu podataka na osnovu čije automatske obrade se češće donose odluke (na dnevnom i nedeljnom nivou), postoji maltene neprestana obaveza za ažuriranjem, dok u pogledu podataka koji se obrađuju i koriste jednom u dužem periodu to može biti ređe. Takođe, i priroda obrade i način upotrebe rezultata analize u velikoj meri utiču na odgovornost rukovaoca za loš kvalitet podataka.

Treba voditi računa da se ovo načelo ne primenjuje neograničeno, odnosno da postoje situacije kada upravo zbog svrhe obrade treba sačuvati podatak koji nije tačan.

PRIMER:

Ne sme se ispravljati dokumentacija o lečenju brisanjem prvobitno postavljene pogrešne dijagnoze. Uspostavljene pravne i etičke obaveze istinitog dokumentovanja svakog koraka u lečenju, nalažu da se svi koraci preduzeti u postupku zdravstvene zaštite moraju detaljno arhivirati kako bi, prilikom daljeg donošenja odluka, bile uzete u obzir sve relevantne informacije. Brisanjem prvobitno postavljene pogrešne dijagnoze ugrožava se integritet podataka o lečenju, što može uticati na uspešnost daljih procesa. Stoga, posebno problematični mogu biti podaci kojima nedostaje element koji u određenom kontekstu može usloviti potpuno drugačije rezultate obrade.

Načelo kvaliteta informacija u sinergiji sa načelom transparentnosti obrade kreira princip participacije i kontrole. Naime, usled okolnosti da protokom vremena i promenom drugih uslova prirodno dolazi do opadanja kvaliteta informacija, neophodno je da lice može nezavisno da vrši proveru kvaliteta i zahteva ispravku, dopunu, ažuriranje, brisanje, kao i prekid i privremenu obustavu obrade. S tim u vezi su ustanovljeni posebni pravni zahtevi u korist lica na koje se ovi podaci odnose.

NAČELO OGRANIČENOG ZADRŽAVANJA

U vezi sa načelom ograničavanja svrhe je i načelo ograničenog zadržavanja, koje definiše rok u kojem podaci o ličnosti mogu zakonito da se obrađuju. Nakon ostvarivanja svrhe obrade, rukovaoci su dužni da revidiraju svoje baze podataka o ličnosti i da obrišu ili trajno anonimizuju podatke.

PRIMER:

Nakon završenog konkursa za dodelu studentskih stipendija, organ vlasti koji je organizovao konkurs bi trebalo da obriše ili anonimizuje lične podatke svih studenata koji nisu ostvarili uslov za dobijanje stipendije, s obzirom da više ne postoji razlog niti svrha da se ti podaci čuvaju.

ZABRANA DISKRIMINACIJE

Budući da zaštita podataka o ličnosti predstavlja univerzalno ljudsko pravo, ona se obezbeđuje svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, seksualnost, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva.

RAZMENA PODATAKA O LIČNOSTI

Imajući u vidu nadležnosti i prirodu posla kojim se bave, organi vlasti će često imati potrebu da razmenjuju podatke sa drugim organima vlasti, ali i sa drugim pravnim i fizičkim licima. Bez obzira na potrebe, treba imati u vidu da je razmena podataka jedan od vidova obrade, te da se i u ovom slučaju moraju primenjivati sva pravila o dozvoljenosti obrade. Konkretno, to znači da se podaci mogu razmenjivati samo ako postoji zakonski osnov ili pristanak lica na koje se podaci odnose, te da se i u ovom slučaju moraju primenjivati sva načela obrade. Načelno govoreći, iako postoji takva mogućnost, nije primereno da pravni osnov za razmenu bude pristanak građana, već bi pitanje razmene podataka između organa vlasti uvek trebalo urediti zakonom jer se na taj način obezbeđuje pravna sigrukovaoce podataka,

PRIMER ZAKONSKOG OVLAŠĆENJA KAO OSNOVE ZA RAZMENU PODATAKA:

U članu 18, stav 2 Zakona o centralnom registru obaveznog socijalnog osiguranja regulisano je da "organizacije obaveznog socijalnog osiguranja preuzimaju iz Jedinstvene baze podatke neophodne za vođenje matične evidencije, odnosno druge evidencije propisane zakonom koji uređuje penzijsko i invalidsko osiguranje, zdravstveno osiguranje i osiguranje za slučaj nezaposlenosti". Član 19 istog zakona kaže da se "podaci iz Jedinstvene baze koriste radi obavljanja poslova iz delatnosti organizacija povezanih u sistem Centralnog registra". Time je zakonskim odredbama regulisano:

- **sa kim** se mogu razmenjivati podaci (organizacije obaveznog socijalnog osiguranja),
- **koji podaci** se mogu razmenjivati (podaci neophodni za vođenje matične evidencije) i
- **u koju svrhu** se podaci razmenjuju (radi obavljanja delatnosti ovih organizacija)

Dakle, i u slučaju razmene podataka moraju se ispuniti svi uslovi koji su neophodni da bi obrada na osnovu zakonskog ovlašćenja bila dozvoljena, odnosno mora se utvrditi koji se podaci mogu razmenjivati, sa kim i u koju svrhu.

MIŠLJENJE POVERENIKA broj 011-00-00377/2014-02 od 12.05.2014. godine, povodom zahteva gradske uprave grada Čačka kojim je od RFZO-a traženo da dostavi podatke iz Matične evidencije, a u svrhu utvrđivanja zaposlenih građana: "Zakoni kojima se na uopšten način uređuje saradnja i razmena podataka između organa državne uprave, organa lokalne samouprave i drugih organa vlasti se ne mogu smatrati pravnim osnovom koji navedenu obradu (dostavljanje, odnosno razmena podataka - prim. aut) čine dozvoljenom."

ZBIRKE PODATAKA

ŠTA JE ZBIRKA PODATAKA?

ZZPL **zbirku podataka** definiše kao "skup podataka koji se automatizovano ili neautomatizovano vode i dostupni su po ličnom, predmetnom ili drugom osnovu, nezavisno od načina na koji su pohranjeni i mesta gde se čuvaju".

To praktično znači da zbirku podataka čini svaki skup podataka koji u sebi sadrži najmanje jedan podatak o ličnosti bez obzira na formu - to mogu biti baze, evidencije, registri, upisnici, spiskovi, ali i razni ugovori, zapisnici, zdravstveni kartoni, video snimci i drugo.

KOJE ZBIRKE PODATAKA VODE ORGANI VLASTI?

Organi vlasti redovno vode tri vrste zbirki podataka:

- **Zbirke podataka** koje u sebi sadrže podatke o licima koja su zaposlena u organu vlasti ili obavljaju poslove u organu vlasti po drugom osnovu, kao što su:
  - Kadrovska evidencija;
  - Evidencija o platama;
  - Evidencija o naknadama za prevoz;
  - Evidencija o prisutnosti na radu;
  - Evidencija korisnika službenih mobilnih telefona;
  - Video nadzor serverske sobe.
- **Zbirke podataka** koje sadrže i podatke lica koja nisu zaposlena u organu vlasti, a koje nastaju u radu organa vlasti, dok obaveza njihovog vođenja nije propisana zakonom, kao što su:
  - Video nadzor ulaznih prostorija organa vlasti;
  - Evidencija o predstavkama i pritužbama građana;
  - Evidencija o licima sa kojima organ vlasti vodi sudske sporove;
  - Zbirka sigurnosnih kopija službene elektronske pošte organa vlasti.
- **Zbirke podataka** čije je vođenje propisano zakonom, kao što su:
  - Matična evidencija o osiguranicima, obveznicima plaćanja doprinosa i korisnicima prava iz penzijskog i invalidskog osiguranja, koju vodi PIO fond u skladu sa članom 125 Zakona o penzijskom i invalidskom osiguranju;
  - Jedinstvena baza podataka osiguranika i osiguranih lica, koju vodi Centralni registar obaveznog socijalnog osiguranja, u skladu sa članom 29a Zakona o Centralnom registru obaveznog socijalnog osiguranja.

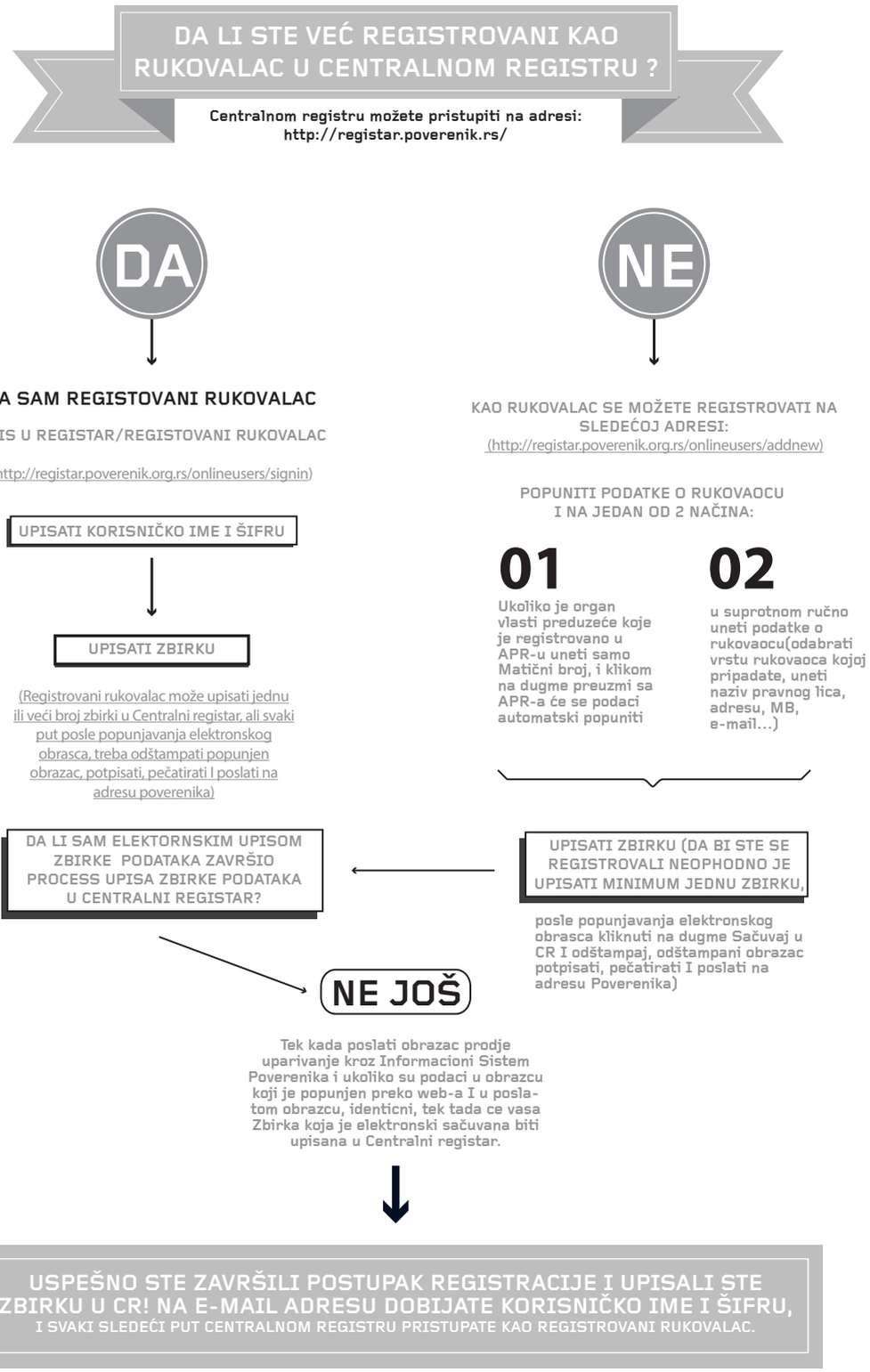
KOJE SU OBAVEZE ORGANA VLASTI KOJI VODI ZBIRKU PODATAKA?

Organ vlasti je dužan da obrazuje i vodi Evidenciju o obradi, koja sadrži podatke o nazivu zbirke podataka, vrsti podataka, radnjama i svrsi obrade, roku čuvanja podataka, preduzetim merama zaštite i druge podatke, što je propisano članom 48 ZZPL-a.

Organ vlasti je dužan da **prijavi evidenciju o zbirci podataka** Povereniku koji vodi Centralni registar zbirki podataka. Tehnički, ovu prijavu organ vlasti obavlja tako što se registruje na sajtu Poverenika, popuni elektronski obrazac, a zatim i pisanim putem dostavi Povereniku potpisane i pečatirane obrasce.

Postupak registracije i prijave zbirki podataka prikazan je na grafikonuu desni strani.

Organ vlasti je dužan da pre uspostavljanja zbirke podataka koju namerava da vodi radi obrade podataka čiji je pravni osnov pristanak lica, dostavi Povereniku **obaveštenje o nameri uspostavljanja zbirke,** i to najkasnije 15 dana pre uspostavljanja zbirke podataka.



KADA ORGAN VLASTI NEMA NAVEDENE OBAVEZE?

Iz razloga svrsishodnosti, organ vlasti nije dužan da obrazuje i vodi Evidenciju o obradi, niti da Povereniku prijavi zbirku podataka u sledećim situacijama:

- Podaci koji se nalaze u evidenciji obrađuju se isključivo **u porodične i druge lične svrhe** (što se po pravilu neće desiti u organu vlasti);
- Vođenje zbirke podataka je **propisano zakonom;**
- Zbirku podataka čine samo **javno objavljeni podaci;**
- Zbirku čine podaci koji se odnose na lice čiji **identitet nije određen**, a rukovalac, odnosno korisnik, nije ovlašćen da odredi identitet.

PRIMER:

PIO fond nije dužan da vodi Evidenciju o obradi koja se odnosi na Matičnu evidenciju osiguranika, niti je dužan da istu prijavi Povereniku, imajući u vidu da je vođenje Matične evidencije propisano članom 125 Zakona o penzijskom i invalidskom osiguranju.

Dodatno, organ vlasti nije dužan da obavesti Poverenika o nameri uspostavljanja zbirke kada je zakonom određena svrha obrade, vrsta podataka koji se obrađuju, vrste korisnika kojima će podaci biti dostupni, kao i vreme za koje će podaci biti arhivirani.

PRIMER: Nacrtom Zakona o evidencijama u oblasti unutrašnjih poslova, ustanovljena je obaveza vođenja Evidencije o izvršiocima krivičnih dela, utvrđeno je precizno koji podaci o izvršiocima krivičnih dela će se nalaziti u toj evidenciji. Propisano je da će se ti podaci koristiti u svrhu registracije izvršilaca krivičnih dela i prekršaja, da će se ti podaci čuvati trajno, a detaljno je utvrđeno i kako se ti podaci mogu ustupati drugim organima. U tom slučaju, MUP nije dužan da pre uspostavljanja zbirke podataka obavesti Poverenika o nameri uspostavljanja zbirke podataka.

ZAŠTO JE BITNO PRIJAVITI ZBIRKU PODATAKA POVERENIKU?

Pored toga što je prijava zbirke zakonska obaveza propisana ZZPL-om čije neispunjenje povlači prekršajnu odgovornost, treba reći da je zapravo u interesu organa vlasti da prijavljuje zbirke podataka Povereniku, pa čak i u slučajevima kada nema takvu obavezu. Razlozi za to su sledeći:

- Na taj način organ vlasti postupa **u skladu sa načelom transparentnosti** i zapravo obaveštava građane o zbirkama podataka koje vodi. Tako se smanjuje broj zahteva po pravu na obaveštenje, uvid i kopiju, te organ vlasti ima manje troškove po ovom osnovu;
- Državni organ se **može osloboditi obaveze postupanja po zahtevima** u vezi sa pravom na obaveštenje o obradi, ukoliko se podaci traženi takvim zahtevom već nalaze u Centralnom registru;
- Samim procesom prijave zbirke podataka, organ vlasti će se **bolje upoznati sa zakonskom regulativom** koja se odnosi na zaštitu podataka o ličnosti, kao i sa svojim obavezama u tomj oblasti;
- U slučaju da organ vlasti ima nameru da obrazuje novu evidenciju podataka o ličnosti, a ne postoji svest da ona nije u skladu sa zakonom, Poverenik će mu nakon obaveštenja o nameri uspostavljanja zbirke skrenuti pažnju na nezakonitost vođenja takve zbirke. Na taj način organ vlasti može da **izbegne eventualne troškove** koje bi imao ukoliko bi se nezakonitost utvrdila po uspostavljanju takve zbirke podataka.

ORGANIZACIONE MERE ZA ZAŠTITU PODATAKA O LIČNOSTI I UPRAVLJANJE PODACIMA O LIČNOSTI

ZAŠTO JE BITNO UPRAVLJATI PODACIMA O LIČNOSTI?

Upravljanje podacima jedna je od najmlađih naučnih disciplina, uslovljena razvojem informacionih tehnologija i potrebom da se formalizuju odgovarajuće prakse u organizacionom ciklusu prikupljanja, obrade i čuvanja podataka.

Praktično, ova disciplina obuhvata sve osnovne koncepte upravljanja – analizu potreba, planiranje, strukturiranje, kontrolu, evaluaciju – s obzirom na potrebe različitih organizacija i vrstu podataka kojima upravljaju.

Iako bi se sistematizacija znanja mogla činiti suvišnom u oblasti za koju su dovoljne veštine stečene iskustvom, suštinski značaj ovakvog pristupa ogleda se u definisanju ovlašćenja i odgovornosti. S obzirom na količinu podataka o ličnosti koje prikupljaju i obrađuju organi vlasti, kao i na značaj tih podataka za svakodnevni život građana i ostvarenje različitih garantovanih prava pa, konačno, i za funkcionisanje države, loše upravljanje podacima utiče na vitalne javne interese.

Osnovna funkcija nekih od najvećih rukovalaca podacima među organima vlasti praktično se svodi na upravljanje podacima. Dobra organizacija posla sprečiće gomilanje zahteva i zastoj prilikom prikupljanja podataka, ostvarivanja prava na uvid i ispravku i slično. Sem toga, definisanjem ovlašćenja i odgovornosti omogućava se stalna kontrola procesa, kako bi se predupredilo kompromitovanje baza i kršenje zakona.

VRSTE ODGOVORNOSTI

Neadekvatno rukovanje podacima o ličnosti unutar organa vlasti može imati dalekosežne posledice i u skladu sa tim aktivirati različite vrste odgovornosti:

- **Prekršajna odgovornost** – ZZPL u članu 57 propisuje niz prekršaja u slučaju nepoštovanja odredbi ovog Zakona. U slučajevima kada se utvrdi prekršajna odgovornost, novčanom kaznom se može kazniti:
  - **organ vlasti kao pravno lice**, i to novčanom kaznom od 50.000 do 1.000.000 dinara;
  - **fizičko lice**, odnosno odgovorno lice u organu vlasti, novčanom kaznom od 20.000 do 500.000 dinara.
- **Građansko-pravna odgovornost** – Ukoliko usled neadekvatnog rukovanja podacima o ličnosti u okviru organa vlasti, lice na koje se podaci odnose pretrpi materijalnu štetu (npr. gubitak prihoda) ili nematerijalnu štetu (duševni bol usled povrede časti i ugleda), to lice može po opštim pravilima građanskog prava pokrenuti parnični postupak za naknadu štete. U ovom slučaju štetu će biti dužan da nadoknadi:
  - **organ vlasti kao pravno lice**, ukoliko je štetu prouzrokovao njegov zaposleni u radu ili u vezi sa radom;
  - **zaposleni u organu vlast**i, ukoliko je štetu prouzrokovao namerno.
- **Krivična odgovornost** - Nezakonita obrada podataka o ličnosti može za sobom povući i krivičnu odgovornost lica koja su zaposlena u organima vlasti. Krivičnu odgovornost će uvek snositi fizičko lice, a nikada organ vlasti kao pravno lice, imajući u vidu član 3 Zakona o odgovornosti pravnih lica za krivična dela. Ovom prilikom ćemo skrenuti pažnju samo na najvažnije članove Krivičnog zakonika (KZ) koji su od značaja kada je zaštita podataka o ličnosti u pitanju:
  - Član 146 KZ-a predviđa **krivično delo neovlašćenog prikupljanja ličnih podataka** za koje se lice koje podatke o ličnosti koji se prikupljaju, obrađuju i koriste na osnovu zakona neovlašćeno pribavi, saopšti drugom ili upotrebi u svrhu za koju nisu namenjeni, može ka-

zniti novčanom kaznom ili zatvorom do jedne godine. Dodatno, u istom članu je previđen i kvalifikovani oblik ovog krivičnog dela ukoliko ga je učinilo službeno lice u vršenju službe, te se takvo lice može kazniti zatvorom do 3 godine.

- Član 298 KZ-a predviđa da ko neovlašćeno **izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program**, kazniće se novčanom kaznom ili zatvorom do jedne godine. Dodatno, ukoliko je usled toga nastupila šteta koja prelazi određeni novčani iznos, učinilac se može kazniti i zatvorom do pet godina.
- Član 301 KZ-a predviđa da **ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak** i time utiče na rezultat elektronske obrade i prenosa podataka, u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine. Dodatno, ukoliko je usled toga nastupila šteta koja prelazi određeni novčani iznos, učinilac se može kazniti i zatvorom do deset godina.

- **Disciplinska odgovornost** - Zaposleni koji je na neadekvatan i nezakonit način koristio podatke uvek treba i disciplinski da odgovara u zakonom i internim aktima predviđenom disciplinskom postupku u određenom organu vlasti. Posledice po zaposlenog zavise od vrste povrede i između ostalog mogu biti:
  - **novčana kazna;**
  - određivanje neposredno **nižeg platnog razreda;**
  - **zabrana napredovanja;**
  - premeštaj na **radno mesto u neposredno niže zvanje;**
  - **prestanak radnog odnosa.**

Međutim, iako su sve navedene vrste odgovornosti jasno regulisane brojnim zakonima, iskustvo iz prethodnih godina, odnosno mnogobrojni slučajevi kršenja zakona i neadekvatnog rukovanja podacima o ličnosti, ukazuju da je neophodno upravljati podacima o ličnosti unutar organizacije, odnosno postaviti sistemska rešenja koja smanjuju verovatnoću da će doći do kršenja Zakona i odgovornosti.

Organi vlasti, odnosno organizacije koje vrše javna ovlašćenja se razlikuju po delatnostima, veličini, zakonima koji uređuju njihov rad, teritorijalnoj rasprostranjenosti, tehničkoj opremljenosti i drugo, ali bez obzira na razlike, **sve organizacije koje vrše javna ovlašćenja moraju sistemski da upravljaju podacima o ličnosti, odnosno da odgovore na sledeća pitanja.**

KOJIM INTERNIM AKTIMA UREDITI UPRAVLJANJE PODACIMA O LIČNOSTI U OKVIRU ORGANA VLASTI?

Organi vlasti bi trebalo da urede oblast zaštite podataka o ličnosti sopstvenim internim aktima, kako bi formalizovali postupke i pravila, i na nivou sistema postigli željeni nivo zaštite podataka o ličnosti, ali i stvorili osnovu da taj nivo kontinuirano podižu. Kao osnovni interni akti koji utiču na zaštitu podataka o ličnosti, javljaju se:

OPŠTI AKT O ZAŠTITI PODATAKA O LIČNOSTI

Regulisanje oblasti zaštite podataka o ličnosti kroz interne akte je dobra praksa u mnogim razvijenim zemljama. Neophodnost postojanja internog akta koji reguliše oblast zaštite podataka o ličnosti je prepoznata i u novom Modelu zakona o zaštiti podataka o ličnosti koji je izradio Poverenik, koji u članu 63 predviđa da svi rukovaoci podataka koji obrađuju osetljive podatke o ličnosti za više od 500 lica, moraju da imaju ovaj opšti akt kojim uređuju oblast zaštite podataka o ličnosti.

Opštim aktom bi trebalo urediti pitanja koja se odnose na postupak obrade podataka, zaštitu bezbednosti podataka o ličnosti, obaveštavanje lica o načinu ostvarivanja prava u vezi sa obradom podataka i neophodnim merama zaštite podataka, pristup podacima o ličnosti i odgovornost za njihovu nezakonitu obradu i korišćenje, kao i vođenje registra evidencija o obradi za svaku zbirku podataka.

SAVET

Opšti akt nije obavezan po postojećem Zakonu o zaštiti podataka ličnosti, ali Nacrt novog zakona o zaštiti podataka o ličnosti koji je izradilo Ministarstvo pravde, kao i Model zakona o zaštiti podataka o ličnosti koji je izradio Poverenik, prepoznaju tu vrstu obaveze, te se organima vlasti preporučuje proaktivni pristup i što ranije uvođenje opšteg akta o zaštiti podataka o ličnosti.

PRAVILNIK O UNUTRAŠNJOJ ORGANIZACIJI I SISTEMATIZACIJI RADNIH MESTA

Uvođenje baznog standarda iz ISO serije, standarda SRPS ISO 9001:2015 zahteva obavezno uvođenje šest dokumentovanih procedura. Dokumentovane procedure podrazumevaju propisan način odvijanja nekog procesa, a ISO 9001 zahteva dokumentovanost sledećih procesa:

- Upravljanje dokumentacijom;
- Upravljanje zapisima;
- Interne provere;
- Upravljanje neusaglašenostima;
- Korektivne mere;
- Preventivne mere.

Međutim, organizacija može svoje poslovanje, odnosno procese, urediti sa koliko god procedura smatra da je optimalno. Stoga se organima vlasti predlaže uvođenje dodatnih procedura za:

- **Upravljanje dokumentacijom u papirnoj formi** koja sadrži podatke o ličnosti korisnika;

SAVET

Ova procedura treba da se razlikuje od obavezne procedure za upravljanje dokumentacijom, koja ima za cilj pre svega da se u izdavanje, izmenu i povlačenje dokumenata u organima vlasti uvede princip sledljivosti. Procedurom treba definisati ko i na koji način ima pravo pristupa ovoj vrsti papirne dokumentacije, te koje akcije obrade može vršiti nad dokumentacijom.

- Praćenje izvršenja ugovora na održavanju i razvoju informacionih sistema organa vlasti;

SAVET

Procedurom definisati određivanje odgovornog lica za ugovor, njegove zadatke u pogledu ograničavanja i kontrole pristupa spoljnih korisnika sistemu, što je detaljno opisano u delu Vodiča koji se odnosi na organizaciju održavanja informacionog sistema organa vlasti.

IZJAVE O POVERLJIVOSTI

Izjave o poverljivosti informacija moraju biti polazna osnova za zaštitu podataka o ličnosti u organu vlasti, jer se njima definiše lična odgovornost fizičkog lica za čuvanje informacija, između ostalog i podataka o ličnosti. Izjave bi trebalo da potpišu svi zaposleni ali, što je još važnije, i sva fizička lica koja na neki način (kroz ugovore između pravnih lica) ostvaruju pristup podacima o ličnosti korisnika.

LICE ZA ZAŠTITU PODATAKA O LIČNOSTI

DA LI U OKVIRU ORGANA VLASTI TREBA DA POSTOJI LICE ZADUŽENO ZA ZAŠTITU PODATAKA O LIČNOSTI?

U svakom organu vlasti koji obavlja poslove koji uključuju prikupljanje i obradu podataka o ličnosti, od suštinske je važnosti da postoji i odgovornost u okviru organizacije za zaštitu podataka o ličnosti, zbog čega je potrebno da postoji najmanje jedno lice koje je formalno zaduženo za zaštitu podataka o ličnosti. Odgovornosti ovog lica mogu biti precizirane na dva načina:

- **Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mesta,** čime bi zapravo odgovornost u okviru organizacije za zaštitu podataka o ličnosti koji se prikupljaju i obrađuju, bila prvenstveno vezana za radno mesto, ili više radnih mesta, i gde bi odgovornosti lica zaduženog za zaštitu podataka o ličnosti bile definisane kroz opis posla radnog mesta na kojem se ono nalazi u organizacionoj strukturi;
- **Posebnom odlukom rukovodioca organa vlasti,** kojom bi konkretan zaposleni, ili više njih, bio zadužen za zaštitu podataka o ličnosti koji se prikupljaju i obrađuju.

KOJE POSLOVE TREBA DA OBAVLJA OSOBA ZADUŽENA ZA ZAŠTITU PODATAKA O LIČNOSTI?

Aktivnosti koje lice zaduženo za zaštitu podataka o ličnosti treba da obavlja su sledeće:

- **učestvuje u pripremi opšteg akta** o zaštiti podataka o ličnosti, predlaže njegove izmene i dopune i odgovorno je za njegovu primenu;
- **vrši kontrolu, predlaže i preduzima mere** i daje savete o zaštiti podataka o ličnosti;
- **vrši nadzor** u domenu upravljanja podacima o ličnosti;
- **predlaže pokretanje disciplinskog postupka** u slučaju kršenja uredbi koje se odnose na upravljanje podacima o ličnosti;
- predlaže i preduzima **mere za posebno obeležavanje, zaštitu i sprečavanje neovlašćenog pristupa podacima o ličnosti**, a naročito osetljivim podacima;
- predlaže i preduzima mere za **istinito i potpuno obaveštavanje lica o obradi njihovih podataka o ličnosti;**

- preduzima sve druge mere za zaštitu podataka o ličnosti u skladu sa zakonom, naročito vodeći računa o zakonitosti, svrsishodnosti i srazmernosti obrade podataka o ličnosti;
- obezbeđuje **ostvarivanje svih prava koja lica imaju u vezi sa obradom podataka o ličnosti** saglasno zakonu (pravo na obaveštenje, uvid, kopiju, kao i prava povodom izvršenog uvida);
- **obaveštava lica** da su njihovi podaci bili predmet prodora u bezbednost podataka;
- **stara se o vođenju registra evidencija** o obradi za svaku zbirku podataka rukovaoca i o objavljivanju na internet stranici rukovaoca;
- **obezbeđuje sprovođenje određene politike** o zaštiti podataka o ličnosti među zaposlenima;
- **promoviše zaštitu podataka o ličnosti** među zaposlenima radi razumevanja njihove uloge u zaštiti podataka; organizuje edukativne aktivnosti iz oblasti zaštite podataka o ličnosti za zaposlene;
- **prati regulativu** iz oblasti zaštite podataka o ličnosti;
- **izveštava rukovodstvo** o nivou zaštite podataka i predlaže mere za podizanje nivoa zaštite;
- obavlja **druge poslove** koji se odnose na zaštitu podataka o ličnosti, u skladu sa zakonom.

DA LI U ORGANIMA VLASTI TREBA DA POSTOJI POSEBNO RADNO MESTO SAMO ZA POSLOVE UPRAVLJANJA PODACIMA O LIČNOSTI?

Imajući u vidu da je upravljanje podacima o ličnosti i održavanje velikih baza podataka jedna od osnovnih funkcija pojedinih organa vlasti, obim ovih poslova na prvi pogled može biti indikator za formiranje radnog mesta isključivo za obavljanje navedenih aktivnosti. Međutim, zaposleni na takvom radnom mestu bi morali da poseduju različita, krajnje heterogena znanja, pre svega iz oblasti kao što su IT i pravo, kao i odgovarajuće radno iskustvo. Zbog toga smatramo da bi organima vlasti bilo izuzetno teško da pronađu odgovarajuće kadrove opisanog profila. Takođe, za uspešno upravljanje podacima o ličnosti poželjno bi bilo da takvo radno mesto bude na visokom nivou hijerarhije, ako ne i najvišem (prva linija menadžmenta), da bi upravljanje podacima o ličnosti dobilo na značaju. Kako ovakvo rešenje nije primenjivo u organima vlasti, preporuka je da se poslovi iz domena upravljanja podacima dodele određenim zaposlenima, kao dodatne aktivnosti koje obavljaju pored redovnog posla.

Zbog toga je potrebno razdvojiti upravljačke i operativne poslove iz domena upravljanja podacima o ličnosti. Strateški poslovi podrazumevaju definisanje internih pravila u vezi sa upravljanjem podacima o ličnosti, kao i obezbeđivanje njihovog sprovođenja. Operativni poslovi uključuju implementaciju definisanih pravila u svakodnevnom poslovanju. Krajnje neefikasno bi bilo objediniti sve ove poslove u okviru jednog radnog mesta. Strateške odluke bi trebalo da se donose na najvišem hijerarhijskom nivou, dok bi operativni poslovi trebalo da budu samo neke od aktivnosti na izvršnim radnim mestima, u zavisnosti od vrste posla koju je potrebno obaviti.

PRIMER:

Kada se odrede nivoi pristupa zaposlenih podacima o ličnosti, potrebno je to primeniti u informacionom sistemu; kada se definiše postupak vođenja arhive, neophodno je čuvati dokumentaciju i evidentirati pristup dokumentima u papirnoj formi na propisan način; potrebno je pripremati odgovore fizičkim licima u slučaju primljenih zahteva za pristup prikupljenim podacima o ličnosti, itd.

Iz navedenih razloga bi organizaciono rešenje ovog problema trebalo tražiti u dodeli odgovornosti određenom zaposlenom, odnosno zaposlenima, kroz Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mesta ili posebnom odlukom rukovodi-

oca organa vlasti. Dakle, ili kroz opis posla konkretnog radnog mesta ili kroz odgovarajuća rešenja. Pored tako definisane odgovornosti, odnosno aktivnosti iz domena zaštite podataka o ličnosti koje bi trebalo da sprovodi, taj zaposleni bi trebalo da obavlja i druge poslove u skladu sa opisom posla njegovog radnog mesta.

KO IZ ORGANA VLASTI TREBA DA BUDE ZADUŽEN ZA ZAŠTITU PODATAKA O LIČNOSTI?

S obzirom na opisane odgovornosti, jasno je da bi lice zaduženo za zaštitu podataka u ovom smislu trebalo da bude lice koje se nalazi na pozicijama višeg hijerarhijskog nivoa. Analiza primera dobre prakse u Srbiji i inostranstvu je pokazala da bi to lice trebalo da bude deo najviše linije menadžmenta.

Međutim, u mnogim organima vlasti koji prikupljaju i obrađuju podatke o ličnosti, prisutan je divizioni model organizacione strukture, usled teritorijalne razuđenosti organizacionih jedinica. U takvim organizacionim sistemima rešenje bi trebalo tražiti u uvođenju odgovornosti na dva nivoa. Na prvom nivou bi trebalo imenovati lice zaduženo za strateška pitanja iz oblasti zaštite podataka o ličnosti u okviru čitavog organa vlasti, i to bi trebalo da bude neko iz najviše linije menadžmenta. Na drugom nivou bi u svakoj od izmeštenih organizacionih jedinica trebalo da postoji lice zaduženo za zaštitu podataka o ličnosti, odgovorno za operativno sprovođenje strateških odluka iz oblasti zaštite podataka o ličnosti, u okviru svoje organizacione celine.

EDUKACIJA ZAPOSLENIH

NA KOJI NAČIN BI ZAPOSLENE TREBALO UPOZNATI SA PRAVILIMA KOJA SE ODNOSE NA UPRAVLJANJE PODACIMA O LIČNOSTI?

Svi organi vlasti koji upravljaju podacima o ličnosti posebnu pažnju bi trebalo da posvete konstantnoj edukaciji svojih zaposlenih u toj oblasti. Pre svega, organ vlasti treba da ima razvijen barem jedan interni akt koji bliže uređuje oblast zaštite podataka o ličnosti, koji će u potpunosti biti u skladu sa Zakonom o zaštiti podataka o ličnosti, ali će istovremeno sadržati bliže odrednice o primeni zakona u delatnosti kojom se organ vlasti bavi.

Vrste i načine za sprovođenje edukacije je najpogodnije klasifikovati u odnosu na radni staž zaposlenog u organu vlasti, te možemo razlikovati vremenske faze:

Prilikom započinjanja radnog odnosa:

- novozaposleni treba da se upozna sa internim aktom organa vlasti o zaštiti podataka o ličnosti, te da potpiše izjavu o tome, čime formalno preuzima odgovornost za postupanje sa podacima o ličnosti u skladu sa internim aktima, odnosno Zakonom o zaštiti podataka o ličnosti;
- novozaposleni treba da potpiše izjavu o poverljivosti informacija do kojih dolazi u toku obavljanja redovnih i vanrednih radnih aktivnosti.

U toku radnog odnosa:

- interni akt o zaštiti podataka o ličnosti mora biti stalno dostupan svim zaposlenima na internom portalu organa vlasti;
- u definisanim vremenskim intervalima treba organizovati obuke za zaposlene koji upravljaju podacima o ličnosti. Suština ovih obuka bi trebalo da bude ne samo u približavanju odredbi zakona zaposlenima, već u navođenju najčešćih primera kršenja zakona i loše prakse u organima vlasti.

SAVET

U definisanim vremenskim intervalima bi takođe trebalo organizovati testiranje zaposlenih iz oblasti zaštite podataka o ličnosti. Testiranje bi, pored čisto teorijskih pitanja, trebalo da bude bazirano na studiji slučaja iz delokruga rada organa vlasti, gde bi se od zaposlenih očekivalo da odgovore na pitanje šta bi uradili, odnosno kako bi postupili u konkretnoj situaciji.

PRISTUP PODACIMA O LIČNOSTI

KO SVE IMA PRAVO DA PRISTUPA PRIKUPLJENIM PODACIMA O LIČNOSTI?

Organi vlasti koji prikupljaju podatke o ličnosti imaju potrebu ili obavezu da obezbede pristup tim podacima različitim interesnim grupama. Te grupe mogu biti:

- **zaposleni** u organu vlasti koja prikuplja podatke o ličnosti;
- **pravna lica/drugi organi vlasti** koja imaju pravni osnov da pristupe prikupljenim podacima o ličnosti i obrađuju ih;
- **fizička lica** o kojima se prikupljaju podaci;
- **javnost.**

U organima vlasti koji prikupljaju i obrađuju podatke o ličnosti, obavljanje osnovne delatnosti povezano je sa rukovanjem ovim podacima. Zbog toga je neophodno da zaposlenima u tim organima vlasti bude omogućen pristup različitim podacima o ličnosti. Međutim, pristup podacima od strane zaposlenih treba da bude usaglašen sa procesnom strukturom organizacionog sistema. Naime, zaposlenima je potrebno obezbediti pristup samo onim podacima o ličnosti koji su im potrebni za realizaciju aktivnosti za koje su nadležni, a ne kompletnoj zbirci podataka o ličnosti. Dakle, potrebno je prilagoditi prava pristupa podacima o ličnosti opisima poslova iz važećeg pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mesta organa vlasti. Takođe, ukoliko je u organu vlasti implementiran sistem upravljanja kvalitetom, potrebno je usaglasiti prava pristupa zaposlenih sa njihovim ulogama u procedurama.

Podaci o ličnosti koje određeni organ vlasti prikuplja često treba da budu dostupni drugim organima vlasti koji ih koriste za obavljanje osnovne delatnosti, ukoliko imaju pravni osnov. U takvim slučajevima neophodno je obezbediti pristup prikupljenim podacima o ličnosti za potrebe drugih pravnih lica, pod ograničenim i kontrolisanim uslovima, u skladu sa zakonom. Podatke o ličnosti koje obrađuje rukovalac ustupa, odnosno čini dostupnim primaocu, na osnovu pisanog zahteva primaoca. Pisani zahtev mora da sadrži naziv, odnosno ime primaoca, svrhu i pravni osnov za potraživanje podataka, kao i navođenje podataka koji se potražuju. Samo u posebnim situacijama podaci o ličnosti mogu biti

ustupljeni na osnovu usmenog zahteva, u skladu sa zakonom. Pritom, rukovalac vodi posebnu evidenciju o primljenim zahtevima, koja sadrži sve informacije i podatke iz pisanog zahteva, a u slučaju usmenog zahteva sačinjava službenu belešku sa svim elementima za pisani zahtev.

Prema ZZPL, svi rukovaoci podacima o ličnosti su dužni da fizičkim licima o kojima neposredno prikupljaju podatke omoguće pristup podacima i ispravku podataka koji se na njega odnose. Pored toga, rukovaoci su dužni da fizičkim licima omoguće uvid u svaki zahtev za pristup njihovim podacima, ukoliko dolazi do razmene podataka sa drugim pravnim licima. Takođe, rukovaoci podacima o ličnosti su u obavezi da o svrsi obrade obaveste sva fizička lica o kojima prikupljaju podatke.

Konačno, određene kategorije podataka o ličnosti su po zakonu dostupne na uvid javnosti, i u takvim slučajevima organ vlasti koji ih prikuplja mora omogućiti pravo pristupa tim podacima svakom ko ga zatraži. Osim ukoliko je drugačije definisano zakonom, rukovaoci su u obavezi da evidentiraju svaki pristup podacima o ličnosti i da omoguće uvid u svaki pristup i svrhu obrade fizičkom licu čijim podacima je pristupljeno,.

KOJI NIVO PRISTUPA PODACIMA O LIČNOSTI TREBA DOZVOLITI RAZLIČITIM INTERESNIM GRUPAMA?

Neophodno je osigurati da pristup prikupljenim podacima o ličnosti bude omogućen samo onima koji imaju pravni osnov za njihovu obradu, uz odgovarajuću evidenciju svakog pristupa i eventualnog ažuriranja. Zbog toga je u svakom organu vlasti koja prikuplja i obrađuje podatke o ličnosti neophodno implementirati sistem korisničkih rola, kojim će biti definisani odgovarajući nivoi prava pristupa prikupljenim podacima o ličnosti. Sistem rola mora precizno da definiše najpre kojim podacima korisnik kome je dodeljena određena rola uopšte može da pristupi, a zatim i na koji sve način može da ih obrađuje.

ZAPOSLENI U ORGANU VLASTI

- Neophodno je usaglasiti korisničke role koje su namenjene zaposlenima sa njihovim ulogama u poslovnim procesima, odnosno sa opisima njihovih poslova;
- potrebno je zaposlenima omogućiti pristup isključivo onim podacima o ličnosti koji su im potrebni za realizaciju aktivnosti koje obavljaju;
- ažuriranje podataka o ličnosti, odnosno izmenu i brisanje podataka, treba omogućiti samo onim zaposlenima kojima to spada u opis posla;
- sistemom rola mora biti definisano koji korisnici mogu unositi nove podatke o ličnosti u elektronsku zbirku podataka, u skladu sa ulogama u poslovnim procesima;
- izvoz i štampanje podataka o ličnosti takođe moraju biti kontrolisani i omogućeni samo onim zaposlenima čiji opis posla to zahteva;

Dakle, korisničke role namenjene zaposlenima treba da imaju dve dimenzije:

1. prva se odnosi na radno mesto i usaglašavanje prava pristupa i obrade podataka o ličnosti sa opisom posla radnog mesta i sistemom menadžmenta kvalitetom, ukoliko je implementiran u organu vlasti;

2. druga se odnosi na konkretnog zaposlenog, kako bi se omogućio dodatni nivo zaštite i eventualno onemogućili zaposleni da pristupe podacima o ličnosti koji se ne odnose na predmete koji su im dodeljeni, ukoliko postoji potreba za tim.

PRIMER:

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 (akcija) se beleži (ko je pristupio, kada, šta je radio...).

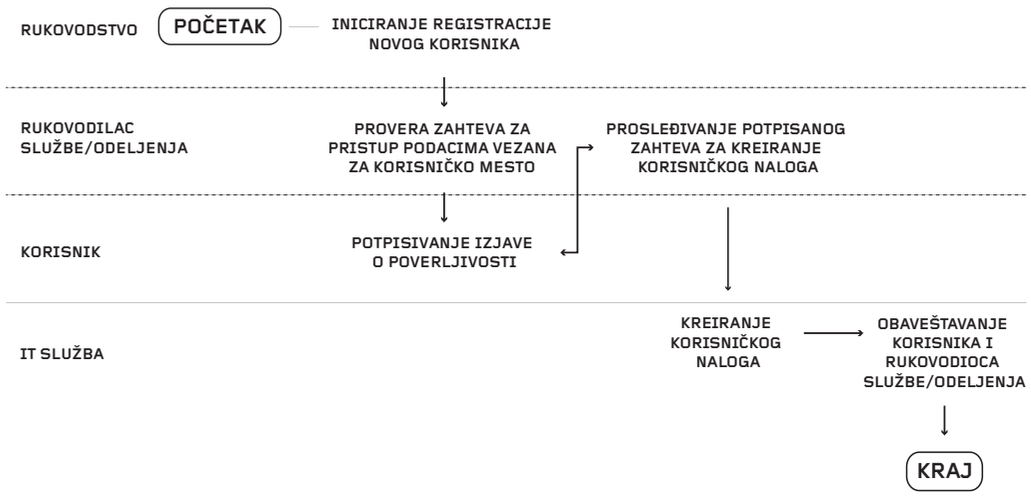
S obzirom da je baza podataka "Matična evidencija o osiguranim licima i korišćenju prava iz obaveznog zdravstvenog osiguranja" (MEOP) distribuirana po filijalama, pristup je ograničen na podatke samo iz jedne filijale, u smislu da zaposleni u jednoj filijali ne mogu da pristupe podacima iz druge filijale. 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, nakon čega administrator više ne može da vidi novu lozinku.

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 zaposleni na 4 radna mesta u okviru Direkcije. Istovremeno, pristup matičnoj evidenciji je omogućen i zaposlenima na 13 radnih mesta u filijalama i ispostavama. Zaposleni imaju različita prava 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 je preporuka da ona sadrži nazive radnih mesta umesto imena korisnika, kako bi se standardizovao pristup bazi širom organizacije.

U skladu sa navedenim, 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. Ključne aktivnosti u procesu uvođenja novog korisnika su prikazane na sledećoj slici:

UVOĐENJE NOVIH KORISNIKA U SISTEM



SAVET

Ukoliko organ vlasti ima implementiran standard SRPS:ISO 9001:2015, i u okviru njega razvijene procedure i radna uputstva za obavljanje osnovne delatnosti, odnosno osnovnih procesa, to može predstavljati osnovu za optimizaciju sistema korisničkih rola u informacionom sistemu i podizanje nivoa zaštite podataka o ličnosti. Naime, izuzetno je bitno uskladiti korisničke role u informacionom sistemu sa pozicijama radnih mesta u radnim procesima, što bi trebalo da bude adekvatno predstavljeno upravo u procedurama.

DRUGI ORGANI VLASTI KOJI KORISTE PRIKUPLJENE PODATKE O LIČNOSTI ZA OBAVLJANJE OSNOVNE DELATNOSTI I OSTALA PRAVNA LICA

- Ukoliko neko pravno lice ima pravni osnov za pristup podacima o ličnosti koje prikuplja i obrađuje neki od organa vlasti, taj organ vlasti treba da omogući pristup samo onim podacima o ličnosti na koje se odnosi taj pravni osnov, kroz odgovarajuću korisničku rolu;
- ovako definisana korisnička rola ne sme posedovati mogućnost izmene ili brisanja podataka o ličnosti, već isključivo pregleda i preuzimanja takvih podataka u propisanom formatu;
- u slučaju da postoji potreba, rukovaoci mogu pravnim licima koja imaju pravni osnov za pristup podacima koje oni obrađuju obezbediti više korisničkih naloga, ali svi oni moraju biti sa odgovarajućom korisničkom rolom, usklađenom sa pravnim osnovom po kom se vrši pristup podacima o ličnosti.

PRIMER:

Elektronska baza podataka ''Evidencija podataka osiguranika, osiguranih lica i evidencija obveznika doprinosa'', koja je u nadležnosti Centralnog registra obaveznog socijalnog osiguranja (CROSO), svakodnevno se sinhronizuje sa bazama podataka koje su u nadležnosti drugih organa vlasti, RFZO, PIO fonda, Nacionalne službe za zapošljavanje, APR i Poreske uprave. Ažuriranje se obavlja automatski, putem sigurnih kanala telekomunikacije, uz sve neophodne mere zaštite. Na ovaj način navedeni organi vlasti vrše razmenu podataka koje prikupljaju, uključujući i podatke o ličnosti.

Takođe, druga pravna lica mogu preko elektronskog sertifikata pristupiti elektronskoj bazi podataka ''Evidencija podataka osiguranika, osiguranih lica i evidencija obveznika doprinosa'', koja je u nadležnosti CROSO, i sprovoditi različite akcije u sistemu, poput prijave i odjave zaposlenih. Obveznik doprinosa, odnosno njegov zakonski zastupnik ili ovlašćeno lice, može uneti nove i izmeniti postojeće podatke koji se odnose na korisnički nalog, pregledati podatke za svoje zaposlene, samo za period osiguranja kod njega, i na portalu CROSO vršiti predaju prijave, odjave, odnosno promene na obavezno socijalno osiguranje.

FIZIČKA LICA

- Organ vlasti koja prikuplja i obrađuje podatke o ličnosti i koji ih čuva u elektronskoj bazi, treba da kroz odgovarajuću korisničku rolu omogući fizičkom licu pregled svih podataka o njemu koji su prikupljeni;
- korisnička rola za fizička lica bi trebalo da poseduje i mogućnost pregleda svih pristupa podacima koji su o njemu prikupljeni, kako bi fizičko lice imalo uvid u to ko je sve, kada, po kom osnovu i u koje svrhe pristupao njegovim podacima;
- korisnička rola za fizička lica treba da sadrži i mogućnost iniciranja izmene podataka o ličnosti koji se odnose na njega i prilaganja potrebne dokumentacije, koja se izvršava automatski ukoliko nije potrebna verifikacija izmena, ili nakon verifikacije od strane ovlašćenog lica iz organa vlasti, u zavisnosti od procedure.

PRIMER:

Fizička lica mogu pristupiti bazi podataka ''Evidencija podataka osiguranika, osiguranih lica i evidencija obveznika doprinosa'', koja je u nadležnosti CROSO, i videti isključivo svoje podatke, ali prethodno moraju da zatraže pravo pristupa bazi i da dobiju odgovarajući mehanizam pristupa od CROSO. Fizička lica trenutno mogu pristupiti ovoj bazi podataka na tri načina:

- preko kvalifikovanog elektronskog sertifikata,
- pomoću lične karte,
- unošenjem korisničkog imena i lozinke.

JAVNOST

- Ukoliko je zakonom predviđeno da je prilikom pristupa podacima o ličnosti koji su od javnog značaja, neophodno izvršiti identifikaciju pristupnika, organi vlasti koji prikupljaju takve podatke i čuvaju ih u elektronskoj bazi treba da kroz odgovarajuću korisničku rolu omoguće svim fizičkim licima pristup takvim podacima;
- ovako definisana korisnička rola ne sme posedovati mogućnost ažuriranja podataka, već isključivo pregleda, dok mogućnost preuzimanja ili štampanja treba da bude usaglašena sa zakonom;
- ako za podatke o ličnosti koji su od javnog značaja zakonom nije predviđena identifikacija pristupnika, organi vlasti koji ih prikupljaju i obrađuju treba da omoguće javno dostupnu pretragu i pregled takvih podataka bez autentifikacije korisnika.

PRIMER:

Na zvaničnom sajtu APR se može vršiti pregled i pretraga kompletnog Registra privrednih subjekata, bez ograničenja, što podrazumeva i pregled prikupljenih podataka o ličnosti. Naravno, kompletan sistem je projektovan u skladu sa zakonskom regulativom, kojom je definisano da su podaci iz Registra privrednih subjekata javno dostupni.

NA KOJI NAČIN INTERESNIM GRUPAMA TREBA OMOGUĆITI PRISTUP PODACIMA O LIČNOSTI?

PODACI O LIČNOSTI KOJI SE ČUVAJU U ELEKTRONSKIM BAZAMA PODATAKA

Ukoliko se podaci o ličnosti čuvaju u elektronskoj formi, ne sme postojati nijedan korisnik koji im može pristupiti bez autentifikacije i evidentiranja pristupa.

U idealnom slučaju, pristup elektronskoj bazi podataka koja sadrži podatke o ličnosti svakom od zainteresovanih lica treba da bude omogućen upotrebom kvalifikovanog elektronskog sertifikata, koji izdaje ili verifikuje organ vlasti koji vodi bazu podataka. Međutim, u najvećem broju slučajeva postojeća infrastruktura ne dozvoljava primenu ovog rešenja. U tim slučajevima je korisnicima potrebno omogućiti pristup bazi podataka unosom korisničkog imena i lozinke. Lozinka mora biti sistemski generisana i poznata samo korisniku. Korisnik treba da ima mogućnost promene lozinke.

SAVET

Od krucijalne je važnosti da fizičkim licima pristup elektronskoj zbirci podataka koja sadrži podatke o ličnosti ne bude omogućen isključivo unosom JMBG, s obzirom da je to kompromitovan podatak. Ukoliko se za pristup ne koristi kvalifikovani elektronski sertifikat, JMBG može da bude korisničko ime, ali je neophodno da postoji i lozinka poznata samo tom fizičkom licu koju je potrebno uneti kako bi se ostvario pristup.

Neophodno je osigurati da se lozinka od sistema do korisnika kreće isključivo bezbednim telekomunikacionim kanalima. Ukoliko su u pitanju zaposleni, to može biti interna telekomunikaciona mreža koja zadovoljava sve bezbednosne standarde.

SAVET

Slanje lozinke za pristup elektronskoj bazi podataka koja sadrži podatke o ličnosti na mejl adresu nije bezbedno i može dovesti do kompromitovanja pristupnih parametara.

Ako se lozinka šalje spoljnim korisnicima, koji mogu biti predstavnici pravnih lica sa pravnim osnovom za pristup prikupljenim podacima o ličnosti, fizička lica o kojima se prikupljaju podaci o ličnosti, ili bilo koje fizičko lice u slučaju javno dostupnih podataka, neophodno je uspostaviti siguran kanal za slanje lozinki ili uvesti lično preuzimanje pristupnih parametara, koji se automatski generišu i nisu poznati zaposlenima u organu koji prikuplja i obrađuje podatke (poput izdavanja PIN koda u bankama).

SAVET

U organima vlasti koji čuvaju podatke o ličnosti u elektronskoj formi ne sme postojati nijedan zaposleni koji ima pristup svim korisničkim imenima i lozinkama u sistemu. Administratori baze podataka, odnosno zaposleni na radnim mestima kojima su dodeljena administratorska prava, mogu videti sva korisnička imena, kreirati nove korisnike, menjati korisničke role korisnicima, blokirati pravo pristupa određenim korisnicima ili inicirati dodelu nove lozinke korisnicima ukoliko se pojavi potreba, ali ne smeju imati mogućnost pristupa lozinkama. Isključivo zaposleni koji imaju korisničke naloge su odgovorni za čuvanje svoje lozinke za pristup.

Samo u slučajevima kada je zakonom definisano da su podaci o ličnosti koji se prikupljaju i obrađuju javno dostupni za pregled, i da nije potrebno evidentirati ko je izvršio pregled tih podataka, rukovaoci mogu ponuditi javnu pretragu i pregled podataka o ličnosti koji se čuvaju u elektronskoj zbirci podataka, u skladu sa zakonom. U takvim situacijama ne sme biti omogućen direktan pristup zbirci podataka, već moraju biti korišćena aplikativna rešenja i web servisi koji pristupaju zbirci podataka preko sigurnih kanala. Takođe, neophodno je osigurati bezbednost podataka i onemogućiti njihovu izmenu prilikom ovakvog pristupa. Pored toga, rukovaoci su dužni da osiguraju da način javne pretrage i eventualni izvoz ili preuzimanje podataka o ličnosti bude u potpunosti u skladu sa zakonom.

ANONIMIZACIJA PODATAKA O LIČNOSTI U ORGANIMA VLASTI

Pod anonimizacijom podataka podrazumeva se zamena ili izostavljanje podataka o ličnosti i drugih podataka, na način da treća strana koja pregleda ili obrađuje dokument ne bi mogla da identifikuje lice na koje se ti podaci odnose. Kada je to potrebno predlaže se anonimizacija sledećih podataka kao najčešćih identifikatora:

- ime i prezime fizičkog lica;
- datum i mesto rođenja;
- adresa (prebivalište i boravište fizičkog lica);
- JMBG – jedinstveni matični broj građana;
- broj lične karte, pasoša, vozačke dozvole, registarske oznake vozila ili drugih ličnih isprava koje bi mogle da dovedu do otkrivanja identiteta fizičkog lica
- broj telefona, web ili adresa elektronske pošte fizičkog lica, odnosno drugi podatak o ličnosti i drugi podaci na osnovu kojih lice može biti određeno ili odredivo.

Pored toga što je anonimizacija potrebna prilikom javnog ustupanja dokumenata koja sadrže podatke o ličnosti (o čemu će biti vise reči u poslednjem delu Vodiča), ona može biti i dobar mehanizam u poslovnim procesima unutar organa vlasti. Iako nije moguće uvesti potpunu anonimizaciju u rad

organa vlasti, postoje koraci koji se mogu preduzeti kako bi se nivo anonimizacije podigao i samim tim značajno smanjio rizik od kršenja ZZPL od strane zaposlenih u organima vlasti. Anonimizacija bi mogla da bude sprovedena tako što se prilikom prvog unosa podataka o ličnosti konkretne osobe u informacioni sistem organa vlasti, odnosno prilikom kreiranja određene vrste dosijea, kreira i interna šifra za taj dosije. Svaka dalja obrada u sistemu se vrši preko šifre kreirane na taj način, dok se svi ostali, u tim slučajevima nepotrebni podaci o ličnosti ne pojavljuju. Na kraju procesa, prilikom izdavanja određenih uverenja ili rešenja, jasno je da zaposleni mora videti podatke o ličnosti. Cilj anonimizacije u organima vlasti je da podatke o ličnosti mogu da vide samo oni zaposleni kojima je to neophodno za obavljanje radnih aktivnosti, a to su u najvećem broju slučajeva zaposleni koji su u kontaktu sa korisnicima i nalaze se na oba kraja procesa obrade podataka.

PRIMER:

Odgovarajući primer procesa gde se može uvesti anonimizacija na ovakav način, može se naći u praksi Gradskog centra za socijalni rad Beograd. Na početku procesa, zaposleni na radnom mestu prijemnog radnika (koji je stručno lice) pregleda dokumentaciju, unosi neophodne podatke u informacioni sistem i na osnovu prirode slučaja određuje dalji tok procesa, odnosno kretanje predmeta među odgovarajućim stručnim licima Gradskog centra. Međutim, u tom delu procesa prijemni radnik slučaj predaje administrativnom radniku koji unosi dokument nazvan ,,Zahtev'' u informacioni sistem Gradskog centra i povezuje sve papirne dokumente u košuljicu, odnosno formira dosije. Administrativni radnik vidi sve podatke o korisniku usluga Gradskog centra, iako ne učestvuje ni u jednom stručnom delu procesa. Slučaj dalje, kroz dostavnu knjigu, dolazi do rukovodioca službe koji određuje voditelja slučaja. S obzirom da je administrativni radnik lice koje obavlja operativne pomoćne poslove i ne učestvuje u stručnim procesima Centra, ne postoji ni potreba za pristupom podacima o ličnosti bilo kog od korisnika usluga Centra. Predložena anonimizacija bi se uvela tako što prijemni radnik formira šifru slučaja, a administrativni radnik unosi Zahtev u informacioni sistem pod šifrom, bez uvida o osnovne podatke o korisniku usluge (ime i prezime, JMBG, drugi podaci nepotrebni za njegov deo procesa, a na osnovu kojih je moguće izvršiti identifikaciju korisnika). Rukovodilac službe ima pristup bazi u kojoj se nalaze podaci o ličnosti korisnika povezani sa šiframa slučaja (ukoliko je potrebno), i može nastaviti obavljanje svog dela procesa.

Sve procese iz osnovne delatnosti organa vlasti u kojima se vrši obrada podataka o ličnosti bi trebalo preispitati iz ove perspektive i pronaći mogućnosti za uvođenje anonimizacije.

Ukoliko je nemoguće ili nepraktično potpuno skrivanje podataka o ličnosti u informacionom sistemu organa vlasti, zamena podataka se javlja kao jedno od potencijalnih rešenja:

- Anonimizacija imena i prezimena se može vršiti zamenom sa dva ista velika slova;
- Anonimizacija brojčanih i svih drugih podataka osim imena i prezimena (kućne i adrese elektronske pošte, JMBG…) vrši se zamenom sa tri tačke, pri čemu se zadržava oznaka vrste tog podataka, ukoliko je ista navedena.

PODACI O LIČNOSTI KOJI SE ČUVAJU U PAPIRNOJ FORMI

Organi vlasti čuvaju veliki broj podataka o ličnosti u papirnoj formi, te je značajno dati preporuke za zaštitu i na taj način prikupljenih podataka o ličnosti. Pre svega, dokumentacija koja sadrži podatke o ličnosti mora da bude uskladištena na odgovarajući način, u prostorijama, ormarima ili drugim objektima koji se mogu zaključati. Ključ treba da bude odgovornost jednog od zaposlenih na lokaciji. U idealnom slučaju, to će biti lice ranije određeno za zaštitu podataka o ličnosti. S obzirom da veliki broj institucija ima filijale i ispostave, i da se u njima čuva i skladišti najveći broj papirnih dokumenata, bitno je da odgovornost za zaštitu podataka o ličnosti bude definisana na tom nivou.

Organ vlasti treba da ima jasno definisanu proceduru za upravljanje dokumentima u

papirnoj formi koji sadrže podatke o ličnosti, koja se može razlikovati od procedure za upravljanje ostalim dokumentima koji ne sadrže takve podatke. Ukoliko je u organu vlasti implementiran sistem menadžmenta kvalitetom, pored procedure za upravljanje dokumentima koja je jedna od šest procedura koje nameće standard ISO 9001, posebna procedura za upravljanje dokumentima u papirnoj formi koji sadrže podatke o ličnosti takođe treba da bude deo tog sistema. Naime, bez obzira koja od zainteresovanih strana za podatke o ličnosti je u pitanju (zaposleni, drugo pravno lice, samo fizičko lice, javnost), ovom procedurom je potrebno rešiti najmanje tri pitanja:

- Ko ima pravo pristupa podacima?
- Na koji način može da pristupi podacima?
- Koje vrste obrade može da sprovodi nad dokumentima?

S druge strane, određene mere je potrebno uvesti kako bi se poboljšala zaštita podataka o ličnosti koji se nalaze u dokumentima u papirnoj formi. Pre svega, nakon završetka radnog vremena, na stolovima zaposlenih ne bi trebalo da ostaju dokumenti koji sadrže podatke o ličnosti, već bi trebalo da budu u fiokama koje se zaključavaju. Takođe, kancelarije bi obavezno trebalo zaključavati nakon radnog vremena.

Pored toga, dokumentima koja sadrže podatke o ličnosti, a koja se čuvaju u papirnoj formi, treba upravljati u skladu sa regulativom koja se odnosi na kategorije registratorskog materijala i rokove čuvanja.

NA KOJI NAČIN TREBA ZABELEŽITI SVAKI PRISTUP I OBRADU PODATAKA O LIČNOSTI?

U svakom od opisanih slučajeva pristupa podacima o ličnosti, od suštinske je važnosti evidentirati svaki pristup, kao i svaku obradu podataka koja bude sprovedena. Neophodno je da organi vlasti koji prikupljaju podatke o ličnosti u svakom trenutku i za svaki prikupljeni podatak nedvosmisleno mogu da utvrde koji korisnik je pristupio podatku, u koje vreme, odakle i koju vrstu obrade podataka je eventualno sproveo.U slučaju ažuriranja podataka, neophodno je evidentirati sve izmene koje su obavljene, kao i prethodno stanje podatka.

U slučaju čuvanja podataka o ličnosti u elektronskim bazama podataka, potrebno je obezbediti čuvanje logova koji sadrže informacije o pristupu elektronskoj bazi podataka o ličnosti.Svaki pristupni log bi trebalo da sadrži informacije o:

- korisniku koji je pristupio bazi podataka;
- datumu i vremenu pristupa;
- IP adresi sa koje je pristupljeno bazi podataka;
- podatku o ličnosti kom je pristupljeno;
- vrsti obrade podatka (pregled/unos/izmena/brisanje/izvoz/štampa);

Logove je potrebno čuvati najmanje godinu dana, a ukoliko postoji mogućnost i duže. Pored toga, informacioni sistem je neophodno projektovati tako da se za svaki podatak o ličnosti, od trenutka nastanka, odnosno unosa, pa sve do trenutka brisanja, pamte sve izmene. Dakle, prilikom svake obrade podatka o ličnosti je potrebno čuvati informacije o:

- korisniku koji je obradio podatak;
- vrsti obrade (unos/izmena/brisanje);
- datumu i vremenu obrade;
- vrednosti podatka.

U slučaju čuvanja podataka o ličnosti u papirnoj formi, kao jedna od ključnih preporuka može se navesti obavezno beleženje svakog pristupa dokumentima u papirnoj formi koji sadrže podatke o ličnosti, uz beleženje osnova pristupa gde god je moguće.

SAVET

Osnov pristupa nije neophodno beležiti samo u situacijama gde zaposleni u organu vlasti koriste dokumente u papirnoj formi za obavljanje svakodnevnih radnih aktivnosti, kada bi beleženje pristupa i osnova pristupa bilo praktično nemoguće sprovesti, odnosno bilo bi izuzetno neefikasno.

DA LI POSTOJI STANDARDNI NAČIN ZA ZAŠTITU PODATAKA O LIČNOSTI?

U svim navedenim slučajevima je neophodno istovremeno obezbediti i adekvatnu zaštitu podataka o ličnosti, u skladu sa zakonom. Mehanizam omogućavanja pristupa podacima o ličnosti i njihove zaštite značajno se razlikuje od načina čuvanja podataka, odnosno zavisi od toga da li se podaci čuvaju u elektronskoj bazi ili u papirnoj formi.

U pogledu uvođenja procedura sistema menadžmenta, jedan od ciljeva organa vlasti koji su veliki rukovaoci podataka, jeste uvođenje standarda ISO 27001:2013 - Sistem menadžmenta zaštite i bezbednosti informacija (ISMS). Standard je namenjen prvenstveno organizacijama koje rukuju osetljivim i poverljivim podacima, i najveće efekte ostvaruje u organizacijama koje u tu svrhu koriste velike informacione sisteme. Međutim, njegovi zahtevi i efekti nisu ograničeni samo na elektronske podatke, već obuhvataju:

- pisane informacije;
- štampane informacije;
- informacije u elektronskim formatima;
- informacije poslane poštom;
- informacije poslane elektronskom poštom;
- foto, audio, video informacije - audiovizuelne informacije;
- informacije saopštene u razgovoru - verbalne informacije.

Standard je generički, primenjiv u svim vrstama organizacija, njegovi zahtevi se odnose na sve vrste informacija, a cilj je poboljašanje sistemske zaštite u oblasti informacione bezbednosti i uvođenje odgovornosti svih zaposlenih u organizaciji za bezbednost informacija. Konkretni ciljevi su:

- Uspostavljanje pravilnih podešavanja naloga;
- kontrola na pristupom informacijama;
- kontrola nad mrežnim uslugama;
- kontrola obavljanja usluga od trećih strana;
- ostvarivanje zaštite podataka o ličnosti;
- zaštita medijuma sa podacima u tranzitu.

U svrhu ostvarivanja ovih ciljeva, pored svega ostalog, standardom je predviđeno uvođenje više od 100 kontrolnih tačaka, koje se odnose na bezbednost informacija.

SAVET

Organi vlasti koji prikupljaju i obrađuju podatke o lličnosti, a pritom ih čuvaju u elektronskim bazama podataka, trebalo bi da teže uvođenju standarda ISO 27001, Sistem upravljanja bezbednošću informacija. S obzirom na delatnosti koje obavljaju takvi organi vlasti, za njihovo poslovanje on najčešće predstavlja najbitniji standard ISO serije. Standardom bi trebalo formalno regulisati pristup i upravljanje podacima o ličnosti koji se prikupljaju i obrađuju.

KAKO ORGANIZOVATI ODRŽAVANJE INFORMACIONOG SISTEMA I ELEKTRONSKE BAZE KOJA SADRŽI PODATKE O LIČNOSTI?

U idealnom slučaju, razvoj i održavanje informacionih sistema u organima vlasti koji upravljaju velikom količinom podataka o ličnosti trebalo bi da bude u potpunosti pod okriljem zaposlenih, koji su organizovani u posebnoj organizacionoj jedinici za informacione sisteme i tehnologije, sa direktorom koji je član najvišeg rukovodstva organa vlasti.

Organizaciona jedinica za informacione tehnologije bi trebalo da ima zaposlene inženjere, sa minimum VII stepenom stručne spreme, koji pokrivaju dve osnovne oblasti:

- administracija baze podataka;
- administracija mreže i telekomunikacija.

Takođe, izuzetno je bitno istaći da je poželjno da, gde god je moguće, u slučajevima organa vlasti koji imaju filijale i ispostave, u filijalama postoji barem jedan zaposleni koji će se baviti održavanjem mreže, ali i administriranjem pristupa bazi podataka, makar u delokrugu dodeljivanja korisničkih imena i lozinki, odnosno promena lozinki.

Preporuka organima vlasti u vezi sa organizacijom organizacione jedinice za informacione tehnologije ide u pravcu promene sistematizacije. Naime, uslovi na tržištu rada su takvi da zaposleni sa navedenim kvalifikacijama veoma lako mogu pronaći posao u privatnim firmama, gde će u najvećem broju slučajeva biti bolje plaćeni nego u organima vlasti. Stoga organi vlasti moraju naći načine da smanje rizik od odliva kadrova iz ove oblasti, bilo da je to povećavanjem koeficijenta za obračun zarada na radnim mestima u ovoj organizacionoj jedinici, odnosno povećanjem plata, bilo dodatnim pogodnostima kao što su (ne)plaćena odsustva, slobodni dani, obuke i slično. Cilj je da se očuva sposobnost organa vlasti da sami administriraju bazu podataka i upravljaju bezbednošću mrežne komunikacije, kako ne bi postali potpuno zavisni od drugih.

Međutim, s obzirom da su izuzetno retki slučajevi gde su organi vlasti sposobni samostalno da razviju, a samim tim kasnije i da potpuno samostalno održavaju informacione sisteme, eksterne firme često moraju biti angažovane na poslovima razvoja i održavanja informacionog sistema. Zbog toga organi vlasti koji prikupljaju i obrađuju podatke o ličnosti moraju razviti procedure za zaštitu podataka o ličnosti i u slučajevima kada druge firme pristupaju sistemu, radi razvoja ili održavanja.

Preporuke za sadržaj procedure za razvoj i održavanje informacionog sistema organa vlasti od strane trećih lica:

- Pre svega, ugovor o razvoju i/ili održavanju informacionog sistema između organa vlasti, rukovaoca podacima o ličnosti, i firmi koje pružaju usluge iz oblasti informacionih sistema (pružalac usluge) mora sadržati klauzulu o poverljivosti;
- sva lica zaposlena kod pružaoca usluge, koja će učestvovati u pružanju usluga, moraju biti jasno navedena u ugovoru o pružanju usluge ili u nekom od pratećih protokola ovog ugovora;
- sva lica zaposlena kod pružaoca usluge, koja su navedena u ugovoru o pružanju usluge, moraju pojedinačno potpisati izjave o poverljivosti;
- gde god je moguće i tehnički izvodljivo, potrebno je onemogućiti pristup informacionom sistemu organa vlasti pružaocu usluge, osim iz prostorija organa vlasti;
- među zaposlenima kod organa vlasti (rukovaoca podacima) mora biti određena osoba zadužena za praćenje realizacije ugovora o pružanju usluge, pri čemu se zaposleni određuje rešenjem za svaki ugovor i ta odgovornost nije vezana za radno mesto, već je pitanje odluke direktora;
- obaveza zaposlenog koji je odgovoran za praćenje realizacije ugovora jeste da bude prisutan svaki put kada zaposleni kod pružaoca usluge dolaze na lokacije organa vlasti, kako bi obezbedio da samo lica navedena u ugovoru pristupe informacionom sistemu organa vlasti;
- za svaki rad na informacionom sistemu organa vlasti, zaposlenima kod pružaoca usluge se kreiraju novi korisnički nalozi, samo za tu svrhu;
- rad na razvoju i održavanju informacionog sistema, kada je to izvodljivo, treba da se sprovodi na računarima koji nemaju pristup Internetu.

TEHNIČKE MERE ZA ZAŠTITU PODATAKA

INFORMACIONA PRIVATNOST

Shodno vrsti podataka koje obrađuju i razmenjuju, organi vlasti su dužni da primene odgovarajuće tehničke mere zaštite osetljivih podataka. Počev od internog do poslovanja sa drugim organima vlasti i građanima, za standardizaciju bezbednosti podataka neophodne su utvrđene procedure. Analizom strukture informacionog sistema uz pomoć tehničkih administratora, moguće je usvojiti odgovarajuće strategije zaštite za svaki organ vlasti ponaosob.

INFORMACIONA PRIVATNOST

Dužnost rukovalaca podataka da preduzmu odgovarajuće mere zaštite i smanje rizik povrede prava na zaštitu podataka o ličnosti, proizlazi iz ustavnih garancija privatnosti građana kao i zakonskih odredbi.

Informaciona privatnost - **pravo građana da samostalno određuju kada, kako i u kojoj meri će se informacije o njima saopštavati drugim licima** - podrazumeva pravo uvida u podatke koji se odnose na određenu osobu, kao i pravo da bude upoznata s načinima na koje se ti podaci obrađuju, gde se čuvaju i ko sve može da im pristupi. Iz ovoga sledi obaveza rukovalaca podataka da u svakom trenutku imaju potpunu kontrolu nad čitavim ciklusom prikupljanja, obrade i čuvanja podataka.

Povrede ovih obaveza mogu nastati u vidu prekomernog prikupljanja ličnih podataka, otkrivanja podataka bez dozvole, ali i usled nestručnog rukovanja podacima.

NARUŠAVANJE ZAŠTITE PODATAKA O LIČNOSTI

Svaka povreda informacione privatnosti mogla bi se smatrati narušavanjem zaštite podataka o ličnosti. Preduzimanje tehničkih mera za zaštitu podataka podrazumeva rešavanje predvidivih rizika po informacionu privatnost. Najčešće, rizici se javljaju u slučajevima kada su podaci o ličnosti:

- neprecizni;
- nepotpuni ili zastareli;
- prekomerni ili irelevantni;
- čuvani predugo;
- dostupni licima koja nisu zakonom ili na drugi način ovlašćena da im pristupaju;
- obrađivani na načine koji nisu prihvatljivi ili očekivani od strane osobe na koju se odnose ili na načine koji nisu propisani pravnim aktom;
- neadekvatno čuvani.

U ovom delu vodiča fokusiraćemo se na podatke o ličnosti u digitalnom okruženju, odnosno u okviru informacionih sistema koji obrađuju podatke o ličnosti. Tehničke mere zaštite su kompleksne i neophodan je sveobuhvatan pristup, jer je svaki informacioni sistem bezbedan onoliko koliko je bezbedna njegova najslabija tačka.

STRUKTURA SISTEMA

Svaki organ vlasti kao rukovalac podacima o ličnosti pruža različite usluge, odnosno obavlja poslove iz različitih domena, što znači da će svaki organ vlasti imati različite potrebe i da će informacioni sistem (IS) biti prilagođen poslovnom procesu. Struktura sistema jednog organa vlasti ogleda se u celokupnoj tehničkoj i organizacionoj šemi sistema, odnosno u hardveru i softveru, obradi podataka, administraciji pristupa podacima, kao i u vrsti baze podataka gde se ti podaci skladište. Da bi sistem bio zaštićen i siguran, sve segmente sistema bi trebalo uskladiti sa internim politikama poslovanja.

VLASNIŠTVO

Punu kontrolu nad podacima ima svako ko kontroliše, odnosno poseduje uređaje na kojima se ti podaci nalaze. Na prvom mestu je vlasništvo nad serverom svakog organa vlasti, jer ukoliko su serveri na kojima se nalaze baze podataka, ili aplikacije kojima se obrađuju podaci o ličnosti, u vlasništvu trećih lica (privatnih kompanija koje pružaju usluge skladištenja ili hostovanja), organ vlasti ne može pouzdano znati ko sve može da pristupi podacima. Kontrola nad podacima, kao i nad pristupom podacima predstavlja prvi nivo zaštite podataka o ličnosti.

Od jednakog značaja za zaštitu podataka jeste vlasništvo nad softverom, budući da kompjuterski program čini jezgro IS. Vlasništvo nad softverom podrazumeva licenciran program pod zakonski propisanim pravima vlasnika autorskih prava, što su u ovom slučaju organi vlasti. Vlasništvo nad programskim kodom omogućava nezavisne revizije. Ove revizije su veoma korisne za otkrivanje grešaka u programskom kodu, prepoznavanje slabih tačaka i detekciju sporednih ulaza u sistem, namenski kreiranih za napad (backdoors).

Najbolje rešenje za sigurnost softvera jeste interni razvoj informacionog sistema pojedinog organa vlasti za sopstvene potrebe. Ukoliko je zbog nedostatka resursa to nemoguće, alternativa je prepuštanje posla privatnom sektoru (outsourcing). Pažnju bi trebalo obratiti na to da organ vlasti ne sme doći u situaciju da zavisi isključivo od firme ili pojedinca koji je razvio softver (tzv. vendor lock), već mora imati svoja tehnička lica koja poznaju softver i koja su obučena za njegovo održavanje.

> Sektor informacionih tehnologija PIO fonda je razvio celokupni IS, aplikacije i baze podataka koji se koriste za obradu, odnosno skladištenje podataka. Ovaj sektor održava isti IS već 30 godina.

PRIVATNOST UGRAĐENA U SOFTVER

Softver je vezivno tkivo IS, jer se njime praktično obavljaju svi oblici rukovanja podacima, počev od unosa, preko obrade do skladištenja. To znači da je softver prva i poslednja borbena linija u zaštiti podataka, jer bez obzira na to koliko je sistem zaštićen od spoljašnjih napada, softverska greška (bug) može lako da kompromituje podatke.

Privatnost ugrađena u softver (Privacy by design) je pristup izrade kompjuterskog programa IS koji razvija privatnost podataka uporedo sa razvojem samog sistema, odnosno isključuje potrebu za naknadnim podešavanjem kako bi se integrisala privatnost. Stoga, gde god je moguće treba započeti od nule i razviti sistem koji u svojoj osnovi sadrži mere zaštite privatnosti.

Sveobuhvatni pristup omogućava detaljnu analizu svih aspekata upravljanja podacima, kroz ceo "životni ciklus", od unosa do arhiviranja, odnosno brisanja. Na ovaj način razvojni tim, zadužen za izgradnju IS, ima u vidu kvalitet i kvantitet podataka kojima će se rukovati, te se potencijalni problemi i nedostaci mogu identifikovati u ranoj fazi razvoja sistema što znači da će njihovo uklanjanje biti brže, efikasnije i jeftinije.

Budući da se dizajn sistema bazira na sveobuhvatnoj analizi poslovnog procesa iz ugla privatnosti, sami organi vlasti mogu aktivno učestvovati u prepoznavanju potencijalnih nedostataka i time unaprediti razumevanje značaja zaštite podataka odnosno privatnosti. Na taj način se dodatno umanjuje rizik kršenja regulative o zaštiti podataka o ličnosti.

Konačno, razmatranje pitanja privatnosti u kontekstu razvoja IS, na nivou organizacionih jedinica i na nivou čitavog organa vlasti, utiče na rad pojedinaca i integriše zaštitu podataka o ličnosti u njihove svakodnevne operacije.

VEB SAJTOVI I MOBILNE APLIKACIJE

Najefikasniji kanal komunikacije sa građanima, pravnim licima i ostalim institucijama je svakako veb sajt ili veb prezentacija organa vlasti. Namena sajta može biti široka, počev od osnovnih informacija o organu, preko objavljivanja informatora o radu i godišnjih izveštaja, do naprednih pretraga koje su omogućene korišćenjem određenih bezbednosnih parametara (lozinka, PIN, sertifikat). Kako bi funkcionalnost sajta bila maksimalno prilagođena posetiocu, veb sajtovi najčešće inkorporiraju tehnologije (kolačiće) koje prikupljaju podatke o posetiocima sajta. To su podaci koji se odnose na njegovu lokaciju, hardver i softver koji koristi, preferiran jezik i pismo, i slično; ovi podaci generišu sliku o posetiocu. Organi vlasti bi trebalo da obaveste posetioce svojih sajtova o prikupljanju podataka na ovaj način i da za to traže pristanak, odnosno da ostave mogućnost posetiocu da ne pristane na prikupljanje njegovih podataka.

U svrhu pružanja javnih usluga, organi vlasti mogu razviti i mobilne aplikacije, što umnogome olakšava komunikaciju sa građanima i ubrzava rešavanje zahteva. Međutim, mobilno okruženje ima posebne karakteristike koje zahtevaju dodatne mere zaštite privatnosti. To se odnosi na podatke o ličnosti koje mobilne aplikacije prikupljaju tokom rada, kao što su serijski broj uređaja, serijski broj SIM kartice, broj mobilnog telefona, lokacija uređaja u datom trenutku. Stoga je veoma važno voditi računa i poštovati ZZPL prilikom izrade i korišćenja aplikacije.

SAVET

Principi Privacy by Design pristupa:

- Prevencija umesto "lečenja"

Ovaj pristup karakteriše prevencija, odnosno identifikacija i rešavanje nedostataka pre nego što dođe do incidenta.

- Privatnost kao zadata vrednost

Zadate vrednosti (default) su najlakše za korišćenje jer su unapred postavljene, odnosno korisnici ne moraju da podešavaju program kako bi omogućili privatnost.

- Privatnost ugrađena u dizajn

Privatnost je ugrađena u sve segmente sistema, koji se iz osnova postavlja tako da mu zaštita ličnih podataka bude jedna od glavnih fokalnih tačaka.

- Puna funkcionalnost

Podjednako se uvažavaju privatnost i bezbednost, odnosno ova dva principa se ne suprotstavljaju.

- Pun "životni ciklus"

Princip zaštite privatnosti u osnovi je svakog segmenta procesa, od prikupljanja do bezbednog arhiviranja, odnosno uništavanja podataka na kraju ciklusa.

- Vidljivost i transparentnost

Komponente i operacije sistema ostaju otvorene korisnicima.

- Podređenost korisnicima

Sistem podređen interesima korisnika omogućava zaštitu privatnosti, odgovarajuća obaveštenja, kao i korisniku razumljive opcije.

LOKACIJA

Puna kontrola nad podacima nemoguća je ukoliko se podaci nalaze van Republike Srbije, ili kada se u nekim slučajevima uopšte ne zna njihova lokacija.

Član 53, ZZPL:

Podaci se mogu iznositi iz Republike Srbije u državu članicu Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka Saveta Evrope.

Podaci se mogu iznositi iz Republike Srbije u državu koja nije članica konvencije iz stava 1.ovog člana, odnosno međunarodnu organizaciju, ako je u toj državi, odnosno međunarodnoj organizaciji, propisom, odnosno ugovorom o prenosu podataka, obezbeđen stepen zaštite podataka u skladu sa konvencijom.

Prilikom iznošenja podataka iz stava 2.ovog člana, Poverenik utvrđuje da li su ispunjeni uslovi i sprovedene mere zaštite podataka prilikom njihovog iznošenja iz Republike Srbije i daje dozvolu za iznošenje.

CENTRALIZOVANOST PODATAKA

Poslovni proces u velikoj meri definiše arhitekturu informacionog sistema. Centralizovani IS je sistem u kom se svi podaci nalaze u jednoj, centralnoj tački, dok disperzirani sistem, s druge strane, ima više jezgara, odnosno podaci su lokalizovani u skladu sa svrhom obrade. U vreme kada su stabilnost i brzina internet veze bili slabi, organi vlasti koji imaju disperziranu strukturu (podružnice, filijale) praktično su bili uslovljeni da imaju odgovarajuće disperzirani IS. Sa savremenim standardima brzine interneta, bezbednosti i kvaliteta veze, ova prepreka više ne postoji, pa i organi koji imaju disperziranu strukturu mogu da centralizuju svoje informacione sisteme.

CENTRALIZACIJA SISTEMA

Lakše upravljanje podacima na višem nivou

Jednostavnije sprovođenje mera zaštite podataka

Izazovi za stabilnost mreže, nedostatak garancije za pun radni kapacitet, rizici rada na daljinu u realnom vremenu

Preporučuje se uz uslov poštovanja strikne procedure izrade sigurnosnih kopija (backup) i zaštite

DISPERZIJA SISTEMA

Lakše upravljanje podacima na lokalnom nivou

Efikasniji rad

Veća mogućnost za curenje podataka

Preporučuje se kada je organizacija postavljena tako da sistem mora biti disperziran

Prednosti centralizovanog sistema ogledaju se u lakšem upravljanju podacima, s obzirom da su locirani na jednom mestu. Takođe, korisnik nije u obavezi da pristupi svom nalogu isključivo sa jednog računara, već je pristup omogućen sa bilo kog računara u okviru informacionog sistema organa vlasti. Sprovođenje mera zaštite podataka centralizovanog sistema jednostavnije je u odnosu na decentralizovani sistem. Preporučuje se centralizacija sistema, odnosno čuvanje svih podataka u jednom, centralizovanom i visoko obezbeđenom data centru.

Centralizacijom sistema smanjuje se mogućnost uticaja ljudskog faktora. Automatizovanost centralizovanog sistema podrazumeva striktna pravila o pristupu. Preciznije, sistem se postavlja tako da korisnici sistema mogu da izvršavaju samo zadatke koje im nadređeni dodeljuju i samim tim imaju pristup samo onom delu sistema koji je njima potreban. Najozbiljniji rizici u upravljanju podacima o ličnosti jesu krađa i curenje podataka. U disperziranim sistemima nivo bezbednosti varira od jedinice do jedinice, te se uniformna restriktivnost pristupa u tehničkom i fizičkom smislu ne može uvesti, jer je u pitanju zajednica autonomnih sistema koji se međusobno razlikuju.

Disperzija podataka se preporučuje ukoliko je nemoguće oformiti centralizovani data centar, zbog rasprostranjenosti i kompleksnosti informacionog sistema organa vlasti. Zbog optimizacije rada i bezbednosti podataka, ne preporučuje se dvostruko čuvanje podataka u okviru sistema. To bi otežalo kontrolu nad pristupom podacima, kao i samu sinhronizaciju među bazama podataka.

U okviru istraživanja SHARE Fondacije tokom 2015. godine, ustanovljeno je da veliki rukovaoci podacima (APR, Centar za socijalni rad Beograd, RFZO, PIO fond, CROSO i Poreska uprava) već imaju formirane centralne data centre ili planiraju da u bliskoj budućnosti to ostvare. Ovi organi vlasti su prepoznali centralizaciju podataka kao efikasniji i bezbedniji način skladištenja podataka.

SERVER SALA

- FIZIČKA BEZBEDNOST

Svi serveri treba da budu smešteni u posebnoj server sali, u kojoj se poštuju određene sigurnosne mere. Pristup sali mora biti ograničen na službenike iz IT sektora koji su zaduženi za održavanje sistema, servera, mreže i telekomunikacija. Takođe, sala se mora zaključavati sigurnosnom bravom. Na serverima treba da bude jasno označena njihova namena, odnosno funkcija i broj pod kojim su zavedeni u registru servera.

SAVET

Registar servera je interni akt organa vlasti u kome su katalogizovani svi serveri i detaljno definisane informacije o njima - njihova namena, datum od kada je svaki server pojedinačno u upotrebi, operativni sistem koji koriste, komponente, tehničke specifikacije i slično.

Serveri treba da budu zaštićeni od svih vrsta udara i fizičkih oštećenja, od preterano visokih ili niskih temperatura, kao i od suviše visoke ili niske vlažnosti vazduha. Serveri se uobičajeno nalaze na regalima iznad patosa, kako bi se izbegla oštećenja u slučaju poplave. U sali treba da postoji klima uređaj koji pročišćava vazduh od prašine. Takođe, veoma je važno koristiti uređaje za neprekidno napajenje električnom energijom (Uninterruptible Power Supplies - UPS). Svu potrebnu opremu za bezbednost fizičkog okruženja treba redovno održavati.

- LOGIČKA BEZBEDNOST

Pristup operativnom sistemu servera treba omogućiti samo licima koja održavaju sistem. Osim ovlašćenih lica, pristup sistemu treba obezbediti licima kojima je pristup potreban zbog pojedinačnog slučaja (npr. na zahtev organa vlasti). Korisnički pristup sistemu treba da bude na najnižem nivou, odnosno da poseduje minimalne privilegije, i to isključivo delu sistema koji je korisniku potreban za rad. Takođe, sistem administator treba da konfiguriše sistem tako da se nakon određenog vremena neaktivna sesija prekine. Ovo podešavanje treba da bude na nivou celog sistema, odnosno da važi za svakog korisnika. Softver treba ažurirati blagovremeno.Svaki server treba da sadrži određene mere zaštite sistema kao što su anti-virus i zaštitni zid (firewall).

- SOFTVER

Serverski softveri moraju biti autorizovani i instalirani od strane tehničke podrške određenog organa vlasti, ili ovlašćenog trećeg lica. Sve softverske instalacije, ažuriranja i izmene moraju biti zabeležene u registru servera. Softvere i sadržaje po-

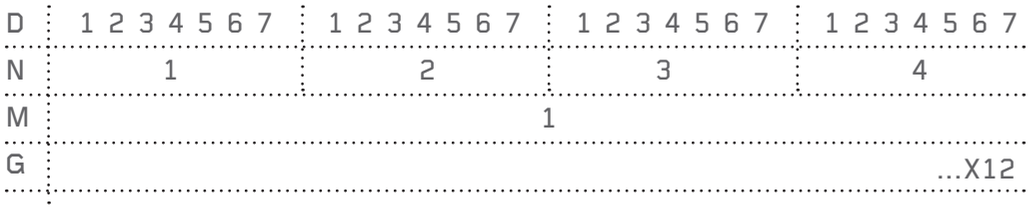
dataka na serverima treba redovno revidirati, a kritične podatke treba odstraniti. Reviziju softvera treba da obavljaju isključivo lica zadužena za održavanje sistema servera. Neovlašćeni softver i podaci moraju biti uklonjeni.

- REZERVNA KOPIJA

Stvaranje rezervne kopije (backup) ne utiče na stepen bezbednosti samog sistema, ali je od ključnog značaja kada se posle bezbednosne krize javi potreba da se izgubljeni podaci povrate. Ponekad je na osnovu rezervne kopije moguće utvrditi uzrok pada sistema, rekonstrukcijom sigurnosnih propusta ili grešaka u sistemu, i slično.

Preporučeno je i eksterno i interno čuvanje kopija. Eksterni backup se odnosi na čuvanje kopija podataka na posebnim diskovima u posebnim sefovima koji su zaštićeni od mogućih nezgoda (npr. vatrostalni sefovi otporni na toplotu). Interni backup podrazumeva čuvanje kopija baze podataka u okviru sistema, odnosno na različitim serverima ili na serveru koji je namenjen za rezervne kopije.

Servere treba kopirati noću, diferencijalna kopiranja (backup promena) treba obavljati svake noći, dok celokupni backup treba obavljati jednom u sedam dana. Dnevne izrade kopije treba čuvati nedelju dana, dok bi sedmični trebalo čuvati jedan mesec. Mesečne bezbednosne kopije treba čuvati jednu godinu, dok bi godišnje trebalo čuvati zauvek. Podrazumeva se da te rezervne kopije treba zaštiti od svih vrsta fizičkih povreda. Treba imati u vidu da se izbrisani podaci ponekad ne mogu povratiti.



Oznaka	Opis	Period čuvanja
D	Dnevni backup	7 dana
N	Nedeljni backup	1 mesec
M	Mesečni backup	1 godina
G	Godišnji backup	Neograničeno

- HARDVER GARANCIJA I ZAMENA U SLUČAJU KVARA

Prilikom odabira servera, treba voditi računa od koga se nabavlja. Minimalna preporučena dužina garancije svakog servera treba da bude 3 godine, s mogućnošću produženja na još dve godine, odnosno sve ukupno 5 godina od trenutka kupovine. Nakon isteka garancije, fizički serveri treba da budu zamenjeni. Svi serveri moraju biti u garanciji. U suprotnom, treba napraviti ugovor o vangarantnom održavanju sa prodavcem opreme ili trećim licem. Važno je da tehnička podrška bude obezbeđena danonoćno.

- ODSTRANJIVANJE

Kada dođe vreme uklanjanja postojećih servera iz službe, njihove hard diskove treba ukloniti i razmagnetisati pre odlaganja. Memoriju treba odstraniti iz kućišta. Konvencionalno brisanje podataka sa računara nije efikasno rešenje za trajno brisanje, jer postoje načini da se izbrisani podaci povrate uz pomoć posebnog softvera. Rešenje za ovaj problem su programi koji kompleksnim algoritmima za razlaganje podataka prave od dokumenata digitalnu "kašu" koja se više nikako ne može vratiti u prvobitni oblik.

Dobra praksa upućuje da se prilikom bacanja stare opreme - nakon što je poseban softver izvršio dubinsko čišćenje diskova - oprema rasklopi kako bi se uništili ulazi i polomili pinovi na priključcima.

BAZA

Baza podataka je kolekcija podataka organizovanih za brzo pretraživanje i pristup, koja zajedno sa sistemom za administraciju, organizovanje i memorisanje tih podataka, čini sistem baze podataka. Korisnici pristupaju bazi podataka prvenstveno preko upita. Korišćenjem ključnih reči i svrstavanjem komandi korisnici mogu brzo da pronađu, preurede, grupišu i odaberu oblast u mnogim zapisima koje treba vratiti, ili pomoću kojih treba sastaviti izveštaje o posebnom skupu podataka.

INTERNET

HOSTING

Hosting provajder na svojim serverima pohranjuje sve podatke koji čine jednu platformu i vodi računa o tome da on bude dostupan na mreži. Domen je registrovana jedinstvena URL adresa koja upućuje na sajt.

Prilikom odabira hostinga, treba obratiti pažnju na sledeće:

- **kvalitet i bezbednost server sale** provajdera gde se sajt "fizički" nalazi;
- **dostupnost tehničke podrške** koja ne zavisi samo od prijave i onlajn komunikcije;
- **mogućnost provere** likvidnosti i reputacija hosting provajdera;
- **odsustvo rizika** od primene regulative vezane za iznošenje podataka iz oblasti zaštite podataka o ličnosti;

Tehnička podrška jedan je od najbitnijih segmenata usluge hostinga. U slučaju da nešto pođe po zlu, ova služba je tačka za kontakt koja mora biti potpuno kooperativna kako bi se problem što pre rešio. Poželjno je odabrati kompaniju čija je služba tehničke podrške operativna danonoćno, svakog dana u nedelji.

Delovi platfome koji služe za pretragu i druge operacije vezane za podatke o ličnosti, trebalo bi da budu hostovani u okviru organizacije, a ne kod hosting provajdera.

Takođe, kroz veb platformu korisnici ne treba da pristupaju centralnoj bazi, odnosno matičnoj evidenciji, već treba postaviti klon baze u tzv.demilitarizovanoj zoni i filtrirati sve upite koji dolaze u bazu kroz zaštitni zid (firewall).

SAVET

Zaštitni zid (firewall) je hardver ili softver koji u sklopu računarske mreže sprečava nepropisni ili neželjeni prenos podataka preko mreže, u skladu sa utvrđenim politikama privatnosti. Odgovarajućom konfiguracijom mrežnih barijera, zaštitni zid zatvara nepotrebne portove koje nijedna aplikacija na serveru ne koristi.

Demilitarizovana zona (DMZ) predstavlja fizičku ili logičku mrežu koja sadrži i objavljuje usluge jednog organa vlasti ka većoj i nepouzdanoj mreži, najčešće na Internetu. Celokupni saobraćaj, odnosno svi upiti koji se šalju bazi podataka prolaze kroz servere koji filtriraju maliciozne upite.

Klon baze podataka (database clone) je potpuna i odvojena kopija sistema baze podataka koja sadrži poslovne podatke, softver i bilo koje druge aplikacije koje čine njenu okolinu.

Kloniranje baze se razlikuje od replikacije po tome što je klonirano okruženje potpuno funkcionalno samo po sebi. Takođe, to okruženje može biti modifikovano usled promene konfiguracije ili podataka. Replikacija baze podrazumeva kreiranje i održavanje višestrukih kopija iste baze, pri čemu bi trebalo voditi računa o sihnronizaciji baza.

HIBRIDNI HOSTING

Dobar hosting takođe podrazumeva decentralizaciju. Ne preporučuje se da se server za hostovanje sajta istovremeno koristi kao mejl server ili data centar. Veb server mora da bude dostupan sa javnog interneta, dok bi dostupnost data centra sa javnog interneta bio ozbiljan bezbednosni problem. Ukoliko postoji potreba da se podacima koji se nalaze u data centru pristupa na daljinu, za to je najbolje koristiti VPN usluge.

VPN

Bezbedan način za rad na daljinu je povezivanje putem virtuelne privatne mreže (VPN - Virtual Private Network-). Reč je o usluzi stvaranja izdvojenog tunela između dva računara na javnoj mreži, koji se posebno šifruje radi zaštite. Od više vrsta virtualnih privatnih mreža najsigurnije je koristiti tzv. protokol bezbednog prenosa podataka (TSL - Transport Layer Security). Pored ovog protokola, preporučuje se i enkripcija saobraćaja.

U okviru jednog organa vlasti, VPN se može koristiti za prenos podataka između perifernih sistema, kao što su filijale, ispostave i slično, ka centralnom data centru organa. Kada je reč o komunikaciji sa partnerima i institucijama sa kojima se vrši razmena podataka (državni i nadzorni organi ili treća lica/firme koji održavaju sistem), korišćenje VPN tehnologije je neizbežno.

SAVET

Preporučeno je da treća lica koja pristupaju sistemu putem VPN-a pristupe isključivo zatvorenom delu sistema gde se nalaze podaci koji su tom licu potrebni za obavljanje posla.

CLOUD

Cloud servisi koriste RAID (Redundant Array of Independent Disks) tehnologiju, zasnovanu na modelu uporednog korišćenja više uređaja za skladištenje podataka, pri čemu se svaki podatak nalazi na najmanje dve lokacije koje su fizički i geografski odvojene jedna od druge.

Organi vlasti moraju imati punu kontrolu nad podacima, kako bi u svakom trenutku znali gde se podaci nalaze. Ovo je praktično nemoguće kada se koristi Cloud, stoga se ne preporučuje upotreba Cloud tehnologija za skladištenje podataka o ličnosti. Način skladištenja podataka koji više odgovara ovoj nameni jeste formiranje sopstvenog data centra u kome će se čuvati svi podaci od značaja za organ vlasti.

Veliki rukovaoci podacima, organi vlasti kao što su APR, Poreska uprava, CROSO, Centar za socijalni rad Beograd, RFZO i PIO fond, ne koriste Cloud computing usluge.

PRISTUP SISTEMU

Svaki organ vlasti čiji poslovi zahtevaju prikupljanje i obradu podataka o ličnosti mora imati kontrolu nad pristupom podacima. Internim aktima i politikama neophodno je odrediti i definisati kako sistemu pristupaju zaposleni, a kako tehnička lica koja održavaju informacioni sistem, državni organi kojima je pristup podacima neophodan zbog poslovanja, korisnici usluga i treća lica.

PROVERA AUTENTIČNOSTI

Ponekad se usled prilično zahtevnog uspostavljanja složenog sistema dešava da se previdi pitanje lozinke, elementarnog nivoa zaštite. Kao najčešće korišćen metod odobravanja pristupa, lozinke treba da budu što kompleksnije. Za početak, treba savladati naviku da se za kriterijum dobre šifre uzima to koliko se ona lako pamti.

Osnovno pravilo pri kreiranju lozinke jeste izbegavanje podataka iz privatnog života kao što su datum rođenja, ime kućnog ljubimca, omiljeno mesto i slično, kao i bilo kakve reči prirodnog jezika. Klasične metode probijanja lozinke danas podrazumevaju automatizovane pretrage po spiskovima reči (dictionary attack) koje mogu obuhvatiti na milione pojmova iz različitih jezika.

Kod informacionih sistema predviđenih za veliki broj korisnika, administratori uobičajeno automatski generišu inicijalne lozinke. Neretko, lozinke se korisnicima šalju elektronskom poštom, što nije bezbedan kanal komunikacije.

SAVET

Da bi se eliminisao rizik od presretanja poruke koja sadrži lozinke, ne treba ih slati mejlom. Prilikom razvoja IS, sistem treba postaviti tako da administrator kreira naloge samo sa korisničkim imenima, a da se korisnicima prepusti mogućnost da sami postave lozinku prilikom prve prijave u sistem.

Sve lozinke se čuvaju u bazama ili datotekama koje se nalaze na serverima. Takve baze se moraju enkriptovati, tako da ni sam sistem administrator ne može da ih pročita.

Iz praktičnih razloga administratoru treba ostaviti mogućnost da resetuje lozinke, što je uobičajena praksa u organima vlasti obuhvaćenim istraživanjem SHARE Fondacije: CROSO, PIO fond, Gradski centar za socijalni rad Beograd, Poreska uprava, RFZO i APR.

Šifra od 12 brojeva ima 1.000.000.000.000 kombinacija, preciznije 1012. Šifra od 12 znakova koja sadrži cifre, velika i mala slova i specijalne karaktere, ima 475.920.310.000.000.000.000.000 kombinacija, imajući u vidu da je ukupan broj svih alfanumeričkih i specijalnih karaktera 94.

Šifra od 12 brojeva ili manje, može se razbiti za manje od sat vremena. Sa tehnologijom u slobodnoj prodaji, potrebno je oko pet miliona godina da bi se probila šifra iste dužine koja, osim brojeva, sadrži velika i mala slova i specijalne karaktere.

OVLAŠĆENJA

Autorizacija ili dodela ovlašćenja u okviru IS podrazumeva formiranje sistema privilegija i rola u skladu sa delatnostima svakog korisnika i prema sistematizaciji radnih mesta organa vlasti. Administratori sistema (IT služba) u saradnji sa zaposlenima koji su zaduženi za ljudske resurse i predstavnicima svih organizacionih jedinica treba da mapiraju IS, odnosno da odrede kojim delovima IS koji zaposleni treba da pristupaju u skladu sa potrebama posla.

SAVET

Najbolja implementacija ovlašćenja u okviru velikih sistema je upotreba kvalifikovanih digitalnih sertifikata. U sertifikat se zapisuju sve relevantne informacije o zaposlenom kao što su ime, prezime, radna pozicija, korisničko ime, mejl adresa i delovi sistema kojima taj korisnik ima pravo pristupa. Sadržaj digitalnog sertifikata je potpisan elektronskim potpisom odgovorne osobe (direktor ili rukovodilac organizacione jedinice).

DVOSTRUKA PROVERA

Jak sistem autentifikacije podrazumeva više od jednog zahteva prilikom pristupa - ne samo korisničku lozinku, već i kvalifikovani sertifikat.

Dvostruka provera podrazumeva zahtev za potvrdu identiteta lozinkom i sertifikatom. Prednost korišćenja ovakvog sistema nalazi se u dodatnoj prepreci, u slučaju da je lozinka ukradena.

Pored IS organa vlasti, dvostruku proveru bi trebalo koristiti i za ostale naloge zaposlenog (mejl, nalozi na društvenim mrežama, finansijske aplikacije i slično).

SAVET

Digitalni sertifikati se mogu primeniti na više načina, ali je najjednostavnije distribuirati ih u obliku smart kartica ili USB tokena. Ukoliko se koriste sertifikati u obliku kartica, za njihovu upotrebu neophodni su odgovarajući čitači, dok se USB tokeni koriste preko postojećeg USB ulaza na računaru.

LOGOVANJE

Log je registar svih događaja u okviru jednog sistema, odnosno svih aktivnosti korisnika - od prijave, preko unosa podataka do njihovih promena, štampanja, brisanja i drugih postupaka.

Logovi mogu beležiti aktivnosti u različitim delovima sistema. Osnovni oblik je pristupni log (access log), a njegovu strukturu, kao i strukturu svih logova, podešava administrator IS. Prilikom podešavanja treba imati na umu da log treba da bude dovoljno detaljan da omogući jasno utvrđivanje zloupotreba (neovlašćeni pristupi i druge aktivnosti), ali da ne bude previše kompleksan za analizu ili skladištenje.

Svaki pristupni log bi trebalo da sadrži informacije o:
- korisniku koji je pristupio bazi podataka;
- datumu i vremenu pristupa;
- IP adresi sa koje je pristupljeno bazi podataka;
- **resursu** kojem je pristupljeno (set podataka o ličnosti, dosije kojem je pristupljeno);
- **vrsti obrade** podatka (pregled/unos/izmena/brisanje/izvoz/štampa);

Logove je potrebno čuvati najmanje godinu dana, a ukoliko postoji mogućnost i duže. Pored toga, informacioni sistem je neophodno projektovati tako da se za svaki podatak o ličnosti, od trenutka nastanka, odnosno unosa, pa sve do trenutka brisanja, pamte sve izmene. Dakle, prilikom svake obrade podatka o ličnosti potrebno je čuvati informacije o:
- **korisniku** koji je obradio podatak;
- **vrsti obrade** (unos/izmena/brisanje);
- **datumu i vremenu** obrade;
- **vrednosti podatka.**

SKLADIŠTENJE PODATAKA

Skladištenje podataka je metoda kojom se analizira i obrađuje velika količina podataka koja pomaže organizaciji i upravljanju u organu vlasti. U logičkom smislu, skladištenje predstavlja centralizovanu bazu podataka. Podaci se izvlače iz različitih izvora i sinhronizuju u bazu podataka prema unapred definisanom modelu.

BEZBEDNOST BAZE PODATAKA

ENKRIPCIJA I HEŠOVANJE

Zaštitu podataka pohranjenih u bazi, omogućava enkripcija odnosno šifrovanje podataka tako da ih je nemoguće rastumačiti bez šifre. Budući da računar sve sadržaje tretira kao brojeve, bez obzira da li je reč o tekstu ili slikama, proces šifrovanja praktično prevodi podatke u veliki skup besmislenih znakova koji se obrnutim procesom, uz pomoć jedinstvenog ključa, vraćaju u prvobitni oblik. S obzirom na važnost podataka koje organi vlasti obrađuju, enkripcija bi trebalo da bude standardna mera zaštite servera.

Podjednako važna mera zaštite je hešovanje, što podrazumeva računanje numeričke vrednosti na osnovu sadržaja, odnosno podataka koji se obrađuju. Za svaki set podataka, ova vrednost je unikatna. Osnovna funkcija heša jeste kalkulisanje vrednosti koja je za određeni set podataka konstantna i skladišti se na bezbednom mestu. Prilikom korišćenja podataka, ponovo se radi obračun vrednosti. Ukoliko su obe vrednosti iste, sadržaj podataka je ostao nepromenjen. U suprotnom, ukoliko se vrednosti razlikuju, podaci su korumpirani. Bilo koji podatak se hešovanjem preračunava u nečitljivi niz bajtova i to uvek fiksne dužine. Veoma je mala verovatnoća da će dva različita podatka (šifre) dati dva jednaka heša. Iz heširanog podatka se nikako ne može doći do originala.

SAVET

Zbog implementacije najsavremenijih tehnologija za zaštitu baza podataka, važno je da organi vlasti koriste ažurirane verzije baza podataka. Najčešće korišćene vrste baze podataka su MySQL, Oracle, Microsoft SQL Server i IBM DB2.

MySQL je relaciona baza otvorenog koda, koja se po učestalosti korišćenja u svetu nalazi na drugom mestu. Najviše korišćena je kao klijent-server model otvorenog koda relacionih baza podataka. MySQL se najčešće koristi kao baza podataka za veb aplikacije.

Oracle baza podataka je objektno-orijentisana baza. Ova baza podataka predstavlja identifikator alfanumeričkog sistema (system identifier - SID) koji obuhvata jednu instancu aplikacije zajedno sa skladištem podataka.

Microsoft SQL server je relacioni sistem za upravljanje bazama podataka. Kao server baze podataka, Microsoft SQL server je softverski proizvod sa primarnom funkcijom čuvanja i pronalaženja podataka koje zahtevaju druge softverske aplikacije.

IBM DB2 je porodica servera baze podataka koja podržava relacione modele, ali takođe i objektno-orijentisane strukture podataka.

ZAHTEVI GRAĐANA

KOJA PRAVA IMAJU GRAĐANI?

Pored toga što su organi vlasti dužni da uvek obrađuju podatke o ličnosti u skladu sa ZZPL-om, drugim zakonima i načelima obrade, oni imaju obavezu da na transparentan način obrađuju podatke, te da građanima omoguće da se upoznaju sa svim aspektima obrade podataka o ličnosti.

U tom smislu građanima se moraju obezbediti sledeća prava:

- **Pravo na obaveštenje** o obradi podataka koje organ vlasti poseduje;
- **pravo na uvid** u podatke koje organ vlasti poseduje;
- **pravo na izdavanje kopije** podataka koje organ vlasti poseduje;
- **prava povodom izvršenog uvida.**

U skladu sa tim pravima građani će redovno upućivati zahteve organima vlasti. Jedan zahtev se može odnositi samo na jedno od navedenih prava, ali treba imati u vidu da građani često upućuju zahteve kojim traže ostvarenje dva ili više prava.

PRIMER:

Jovan Petrović jednim zahtevom od Doma zdravlja u Požegi traži da ga obaveste koje sve podatke o njemu poseduju, te da izvrši uvid u te podatke, kao i da mu Dom zdravlja izda kopiju podataka koji se odnose na njega.

Bitno je razumeti da je svako od ovih prava zasebno i da organ vlasti mora postupiti po svakom od ovih prava, te da se, na primer, dostavljanjem kopije podataka ne oslobađa obaveze da licu omogući uvid u podatke.

OBRAZAC ZA PODNOŠENJE ZAHTEVA

ZZPL jasno ističe da ne postoji obaveza organa vlasti da propiše obrazac za podnošenje zahteva, a čak i u slučaju da je organ vlasti propisao obrazac, građani nisu dužni da ga koriste.

Ipak, razlozi efikasnosti svakako preporučuju da se pristupi izradi obrasca za podnošenje zahteva, jer bi se na taj način olakšalo građanima da ostvare svoja prava, dok bi sa druge strane državnom organu bilo znatno olakšano postupanje po zahtevu, jer bi se predupredile brojne nejasnoće koje mogu da nastanu ako bi građani sami izrađivali zahteve, te bi se smanjilo vreme koje je potrebno da se po zahtevu postupi.

Obrazac bi na vidljivom mestu trebalo objaviti na sajtu državnog organa, u formatu koji omogućava građanima da ga lako prilagode svojim potrebama (npr. MS Word dokument), a trebalo bi da postoji i u papirnom obliku koji bi građani mogli da preuzmu u prostorijama organa vlasti.

POSTUPANJE ORGANA VLASTI U VEZI SA ZAHTEVIMA

PRIJEM ZAHTEVA

Od izuzetne je važnosti da postoji **lice u organu vlasti koje je nadležno za postupanje po zahtevima građana,** kako bi nakon prijema zahteva organ vlasti u propisanim rokovima i na ispravan način rešio zahtev. To bi trebalo da bude lice koje je zaduženo za zaštitu podataka o ličnosti, čije su nadležnosti opisane u organizacionom delu ovog Vodiča.

FORMA I OBAVEZNI ELEMENTI ZAHTEVA

Zahtev za obaveštenje, uvid i kopiju se po pravilu podnosi u pisanoj formi, ali organ vlasti može prihvatiti i usmeni zahtev građana. S druge strane, zbog posledica koje mogu nastupiti, zahtev za ostvarivanje prava povodom uvida može se podneti samo u pisanoj formi.

Zbog same prirode zahteva, ali i zbog kasnije komunikacije sa podnosiocima zahteva, ZZPL-om su propisani **obavezni elementi zahteva** koji se odnose na podatke o identitetu podnosioca zahteva i to su: a) ime i prezime, b) ime jednog od roditelja, c) datum i mesto rođenja, d) JMBG i e) adresa prebivališta, odnosno boravišta, kao i drugi podaci neophodni za kontakt.

UTVRĐIVANJE IDENTITETA LICA I AKTIVNA LEGITIMACIJA PODNOSIOCA

Građani imaju navedena prava samo na podatke koji se na njih odnose, a nikako nemaju pravo da traže kopiju ili izmenu podataka koji se odnose na druga lica.

Iz obrazloženja odluke Poverenika u predmetu broj 07-00-03994/2014-06 od 27.11.2014. godine: "Ovo stoga što ostvarivanje prava u vezi sa obradom podataka o ličnosti, kao i ostvarivanja prava povodom izvršenog uvida pripada fizičkom licu na koje se podaci odnose, koje pravo lice može ostvariti lično ili preko punomoćnika, a kako žalilac nije podnetim zahtevom tražio podatke koji se odnose na njega, već za drugo lice, to se u konkretnom slučaju ne radi o ostvarivanju prava u vezi sa podacima o ličnosti."

Iz tog razloga neophodno je da organ vlasti, pre nego što postupi po zahtevu, utvrdi identitet lica kako ne bi došao u situaciju da ustupi podatke o ličnosti osobi na koju se ti podaci ne odnose, odnosno koja nema pravo da takvim podacima pristupi, čime bi došlo do povrede prava na zaštitu podataka o ličnosti i odgovornosti. Sama identifikacija se može vršiti uvidom u lične dokumente podnosioca zahteva, a ukoliko se sa podnosiocem zahteva opšti samo pisanim putem, onda se moraju podudarati podaci za kontakt iz zahteva sa podacima za kontakt iz evidencija koje vodi državni organ.

Treba istaći da postoje određene situacije kada podnosilac zahteva može biti lice na koje se ti podaci ne odnose i tada organ vlasti mora postupiti po ovim zahtevima:

- ZZPL izričito predviđa da zahtev koji se odnosi na podatke umrlog lica može podneti njegov zakonski naslednik, te se u ovom slučaju prilažu i podaci o identitetu umrlog, izvod iz knjige umrlih kao i dokaz o srodstvu podnosioca sa umrlim.
- Ovlašćeni punomoćnik određenog lica može podneti zahtev koji se odnosi na podatke zastupanog lica (lice ovlasti advokatsku kancelariju da u njegovo ime podnese zahtev za brisanje podataka).
- Zakonski zastupnik određenog lica može podneti zahtev koji se odnosi na podatke zastupanog lica (maloletne dece, lica kojima je oduzeta poslovna sposobnost i slično).

Praksa Poverenika, broj predmeta 07-00-04235/2014-06: "Zahtev za ostvarivanje prava u vezi sa obradom podataka koji se odnosi na maloletnu decu podnose oba roditelja koji vrše roditeljska prava, osim ukoliko imaju potpisan sporazum, odnosno pravosnažnu sudsku odluku o samostalnom vršenju roditeljskog prava."

NERAZUMLJIV I NEPOTPUN ZAHTEV

Ukoliko organ vlasti primi zahtev po kome ne može da postupi zato što je zahtev nerazumljv ili nepotpun (nije jasno na šta se odnosi zahtev, nema obaveznih podataka o identitetu podnosioca i slično), on je dužan da pouči podnosioca kako da otkloni nedostatke da bi se po zahtevu moglo postupiti. Tek ako podnosilac u određenom roku ne otkloni nedostake, a nedostaci su takvi da se po zahtevu ne može postupati, organ vlasti će zaključkom odbaciti zahtev kao neuredan.

ODLUČIVANJE PO ZAHTEVU ZA OSTVARIVANJE PRAVA NA OBAVEŠTENJE O OBRADI

Ukoliko je primio potpun i razumljiv zahtev, podnet od strane ovlašćenog lica, organ vlasti je dužan da **istinito i potpuno obavesti podnosioca zahteva o sledećim aspektima obrade podataka o ličnosti:**

- **da li organ vlasti obrađuje podatke o njemu** i koju radnju obrade vrši;
- **koje podatke** obrađuje o njemu;
- **od koga su prikupljeni** podaci o njemu, odnosno ko je izvor podataka;
- u **koje svrhe** obrađuje podatke o njemu;
- po kom **pravnom osnovu** obrađuje podatke o njemu;
- u kojim **zbirkama podataka** se nalaze podaci o njemu;
- ko su **korisnici podataka** o njemu;
- **koje podatke,** odnosno koje vrste podataka o njemu koriste;
- u **koje svrhe** se koriste podaci o njemu;
- po kom **pravnom osnovu** koristi podatke o njemu;
- kome se **podaci prenose**;
- **koji podaci** se prenose;
- u **koje svrhe** se podaci prenose;
- po kom **pravnom osnovu** se podaci prenose;
- u kom **vremenskom periodu** se podaci obrađuju.

Organ vlasti je dužan da pruži traženo obaveštenje bez odlaganja, a najkasnije **u roku od 15 dana** od dana podnošenja zahteva. Ipak, ako iz opravdanih razloga nije u mogućnosti da postupi u roku od 15 dana, može produžiti rok za **još 30 dana**, ali je dužan da o tome obavesti podnosioca. Obaveštenje o produženju roka bi moralo biti saopšteno, odnosno dostavljeno podnosiocu u prvobitno postavljenom roku od 15 dana od dana podnošenja zahteva, moralo bi da sadrži novi rok, ali i detaljno obrazloženje o razlozima za produženje, s obzirom da Poverenik može proveravati razloge za produženje .

Obaveštenje se daje u pisanom obliku i to direktno podnosiocu zahteva ili poštom/elektronskom poštom na adresu koju je podnosilac naveo u zahtevu, a u izuzetnim situacijama obaveštenje se može dati i usmeno, i to samo ako se podnosilac nesumnjivo saglasi sa tim.

Kada je pružio obaveštenje, organ vlasti je dužan da o tome sačini belešku.

ODLUČIVANJE PO ZAHTEVU ZA UVID

Ukoliko je primio potpun i razumljiv zahtev za uvid, podnet od strane ovlašćenog lica, organ vlasti je dužan da podnosiocu omogući da izvrši uvid u svoje podatke u roku od 30 dana od dana podnošenja zahteva. Ovaj rok se, kao i kod odlučivanja po zahtevu za ostvarivanje prava na obaveštenje o obradi, može iz opravdanih razloga produžiti za **još 30 dana.**

Pre nego što omogući uvid, organ vlasti je dužan da podnosioca obavesti o:

- **vremenu** kada će mu biti omogućen uvid (u roku od 30 dana od dana podnošenja zahteva, a samo iz opravdanih razloga još 30)
- **mestu** gde će uvid biti izvršen (po pravilu u prostorijama organa vlasti)
- **načinu** na koji će uvid biti omogućen (pregled i čitanje dokumentacije u papirnoj formi, uvid u informacioni sistem koji sadrži podatke, gledanje snimka video nadzora i slično)

Ovo obaveštenje se može dati u pisanom ili usmenom obliku, ali podnosilac mora nesumnjivo i potpuno biti obavešten.

Samo vršenje uvida će se po pravilu vršiti u prostorijama organa vlasti i od ovoga se može odstupiti samo izuzetno (na primer, arhiva državnog organa se nalazi u prostorijama privatne kompanije koja ih izdaje za potrebe arhiviranja dokumentacije državnog organa). Čak i ako je organ vlasti utvrdio tačno vreme za vršenje uvida (na primer, 3. mart u 12h), u slučaju da iz opravdanih razloga podnosilac zahteva da se uvid izvrši u drugo vreme, organ vlasti će morati da obavesti podnosioca o novom vremenu u kome će mu biti omogućen uvid.

Prilikom ostvarivanja ovog prava, podnosiocu se moraju učiniti dostupnim svi podaci koji se na njega odnose i to **u razumljivom** obliku. Ako se podaci čuvaju u različitim oblicima (npr. podaci o licu se nalaze u papirnoj prijavi koju je predao organu vlasti, ali su potom uneseni u informacioni sistem organa vlasti), podnosilac može izabrati kojim podacima će pristupiti, a ovo pravo se može ograničiti samo kada je potpuno neizvodljivo.

SAVET

Imajući u vidu da se sve veći broj podataka vodi u elektronskoj formi, organi vlasti bi na zahtev lica morali omogućavati da se izvrši uvid u podatke koji se nalaze u informacionom sistemu državnog organa. Ovakav uvid bi se sa jedne strane mogao ostvariti preko računara zaposlenog u državnom organu i uz korišćenje njegovog korisničkog imena i šifre, te bi se ovakav uvid iz razloga bezbednosti morao vršiti uz stalno prisustvo zaposlenog u državnom organu. S druge strane, građanima može putem elektronskog servisa biti omogućen pristup informacionom sistemu i njihovim podacima, ali se u tom slučaju moraju preduzeti mere zaštite podataka o ličnosti i neovlašćenog pristupa informacionom sistemu, u skladu sa standardima tehničke zaštite.

Organ vlasti ne sme ni na koji način naplaćivati vršenje uvida, niti na bilo koji sličan način uslovljavati vršenje prava na uvid.

Kada je omogućio pravo na uvid organ vlasti je dužan da o tome sačini belešku.

ODLUČIVANJE PO ZAHTEVU ZA KOPIJU

Ukoliko je primio potpun i razumljiv zahtev za kopiju podataka, podnet od strane ovlašćenog lica, organ vlasti je dužan da podnosiocu izda kopiju podataka **u roku od 30 dana** od dana podnošenja zahteva. Ovaj rok se kao i kod odlučivanja po zahtevu za ostvarivanje prava na obaveštenje o obradi, može iz opravdanih razloga produžiti za **još 30 dana.**

Treba istaći da pravo na kopiju podataka ne podrazumeva samo u praksi uobičajeno fotokopiranje papirne dokumentacije, već i umnožavanje audio i video zapisa, digitalnih dokumenata i slično. Ovakva vrsta kopija će se po pravilu izdavati na flash memoriji, CD-u, kaseti ili slanjem digitalnog formata putem elektronske pošte

Ukoliko poseduje tehničke kapacitete, organ vlasti će sam pristupiti izradi kopije i obavestiti podnosioca o preuzimanju kopije. Poželjno je da se kopija podataka preda podnosiocu lično, imajući u vidu da bi slanjem kopije podataka poštom ili elektronskom poštom podaci mogli da dođu do lica koje nije podnosilac. Ipak, ukoliko razlozi ekonomičnosti i efikasnosti to zahtevaju i ukoliko se podnosilac sa tim saglasi, kopije podataka bi se mogle slati poštom ili elektronskom poštom, ali uz preduzimanje mera kako bi podaci stigli direktno podnosiocu.

Ukoliko organ vlasti ne poseduje tehničke kapacitete za izradu kopije, on je dužan da obavesti podnosioca o tome i da ga upozna sa mogućnošću da upotrebom svoje opreme izradi kopiju. U ovom slučaju, mora se vršiti nadzor nad podnosiocem dok izrađuje kopiju kako ne bi došlo do oštećenja originalnog dokumenta koji sadrži podatke.

Sve nužne troškove izrade kopije, bez obzira ko izrađuje kopiju, dužan je da snosi podnosilac zahteva. U tom smislu, organ vlasti može uslovljavati izdavanje kopije uplatom sredstava. Ipak, organ vlasti ne sme zloupotrebljavati ovo pravo, i tražiti uplatu iznosa koji prevazilazi nužne troškove. U ovom slučaju nužni troškovi bi bili cena fotokopiranja papirne dokumentacije, cena umnožavanja video snimka i slično.

Kada je izdao kopiju podataka, organ vlasti je dužan da o tome sačini belešku.

KADA ORGAN VLASTI MOŽE OGRANIČITI PRAVA PO ZAHTEVU ZA OBAVEŠTENJE, UVID I KOPIJU?

Članom 23 ZZPL-a predviđeni su brojni razlozi zbog kojih se ova prava mogu ograničiti i koje bismo mogli grupisati u sledeće celine:

- Lice traži obaveštenje o podacima koji su **već dostupni javnost**i, ili o kojima je već obavešteno od strane državnog organa. Lice je **već izvršilo uvid i dobilo kopiju podataka.** Lice **zloupotrebljava svoja prava** ili bi organ vlasti bio onemogućen u vršenju svojih poslova ukoliko bi udovoljio zahtevu.
- Davanje ovabeštenja bi **ugrozilo druge bitne interese** kao što su javna bezbednost, krivične istrage, finansijski interes države, čuvanje tajne, te privatnost ili drugi važan interes drugih lica.
- Podaci se koriste samo za **naučno-istraživačke svrhe.**

Treba naglasiti da se svi navedeni razlozi moraju usko tumačiti i da se uvek moraju stavljati u odnos sa pravom građana na obaveštenje, uvid i kopiju pa tek ako neki drugi interes preteže, ova prava se mogu ograničiti. Veoma je bitno da se u obrazloženju rešenja kojim se ograničava pravo detaljno obrazloži razlog za takvo postupanje, jer će se u eventualnom drugostepenom postupku pred Poverenikom ovo obrazloženje uzeti u obzir prilikom odlučivanja da li je organ vlasti postupio u skladu sa zakonom.

Dodatno, svi navedeni razlozi pre svega predstavljaju osnov za ograničenje, ali ne i potpuno uskraćivanje prava građana.

PRIMER:

Lice traži forokopiju zapisnika u kome se pored njegovih podataka nalaze i podaci o ličnosti drugih lica. U ovom slučaju bi davanjem kopije zapisnika u integralnoj verziji bila povređena prava na zaštitu podataka o ličnosti drugih lica. Ipak, organ vlasti neće biti ovlašćen da u potpunosti odbije zahtev podnosioca, već je dužan da u kopiji zapisnika izvrši anonimizaciju podataka drugih lica i da tako anonimizovanu verziju zapisnika dostavi podnosiocu zahteva.

REŠENJE O ODBIJANJU ZAHTEVA ZA OSTVARIVANJE PRAVA NA OBAVEŠTENJE, UVID I KOPIJU

Ukoliko postoji neki od razloga iz člana 23 ZZPL-a, ili neki drugi razlog zbog kog organ vlasti smatra da ne treba udovoljiti zahtevu podnosioca, organ vlasti je **dužan da donese rešenje** i da ga dostavi podnosiocu.

Ovo rešenje mora da sadrži pouku da podnosilac na njega može izjaviti žalbu Povereniku **u roku od 15 dana** od dana prijema rešenja.

Rešenje bi takođe trebalo da sadrži detaljno obrazloženje razloga iz kojih je odbijen zahtev podnosioca. To je bitno jer će se u eventualnom drugostepenom postupku pred Poverenikom ovo obrazloženje uzeti u obzir prilikom odlučivanja da li je organ vlasti postupio u skladu sa zakonom.

ODLUČIVANJE PO ZAHTEVU ZA OSTVARIVANJE PRAVA POVODOM IZVRŠENOG UVIDA

Nakon što je licu omogućen uvid u podatke koji se na njega odnose, čime se to lice adekvatno informisalo o svojim podacima koje obrađuje organ vlasti, ono ima sledeća prava:

- Pravo da zahteva **ispravku, dopunu i ažuriranje** podataka
- Pravo da zahteva **brisanje** podataka
- Pravo da zahteva **prekid i privremenu obustavu** obrade podataka

Ova prava su jasno propisana zakonom i ona pre svega proističu iz načela zakonitosti i pravičnosti, načela tačnosti i načela transparentnosti.

Kod zahteva povodom izvršenog uvida specifično je da se takav zahtev podnosi samo u pisanoj formi, jer postupanje po ovakvom zahtevu može imati daleko veće posledice nego postupanje po zahtevima za obaveštenje, uvid i kopiju. U tom smislu, ukoliko nakon postupanja po zahtevu zainteresovano lice ima primedbe, organ vlasti će imati dokaz da je postupao u skladu sa zahtevom.

Ukoliko je primio potpun i razumljiv zahtev za ostvarivanje prava povodom izvršenog uvida, u pisanoj formi, podnet od strane ovlašćenog lica, i smatra da je taj zahtev osnovan, organ vlasti je dužan da **u roku od 15 dana** od prijema zahteva označi podatak kao osporen i privremeno obustavi njegovu obradu. Ovo je bitno iz razloga što organ vlasti ne bi trebalo da potpuno obriše podatak koji je netačan ili zastareo, jer je moguće da su upravo na osnovu netačnog ili zastarelog podataka donete određene odluke. Zbog toga je važno da ostane trag podatka i u obliku koji je netačan ili zastareo, ali on mora biti osporen i njegova obrada se mora obustaviti, u smislu da se na osnovu takvog podatka ne mogu donositi nikakve odluke, niti nanositi bilo kakva šteta licu na koje se podaci odnose.

REŠENJE O ODBIJANJU ZAHTEVA POVODOM IZVRŠENOG UVIDA

Organ vlasti neće postupiti i ispraviti, dopuniti, ažurirati i brisati podatke, odnosno prekinuti obradu ako :

- **nije istekao rok** za obavezno čuvanje podataka;
- je očigledno da bi postupanje po zahtevu **nanelo ozbiljnu štetu** interesima drugih lica;
- je zbog posebnog načina čuvanja podataka postupanje po zahtevu nemoguće, ili iziskuje **prekomerni utrošak vremena ili sredstava.**

PRIMER:

Ukoliko lice zahteva da se obrišu njegovi podaci iz matične evidencije koje vodi PIO fond, a nije istekao rok propisan zakonom da se ti podaci čuvaju najmanje 30 godina od dana sticanja prava utvrđenih na osnovu podataka, PIO fond će odbiti takav zahtev.

Ukoliko iz ovih razloga organ vlasti ne postupi po zahtevu, dužan je da donese rešenje koje obavezno sadrži razloge za odbijanje zahteva, kao i razloge za dozvoljenost obrade. Ovo je bitno jer će se u eventualnom drugostepenom postupku pred Poverenikom ovo obrazloženje uzeti u obzir prilikom odlučivanja da li je organ vlasti postupio u skladu sa zakonom.

ZAHTEVI PO ZZPL-U I ZAHTEVI PO ZAKONU O SLOBODNOM PRISTUPU INFORMACIJAMA OD JAVNOG ZNAČAJA

Imajuću u vidu slična procesna pravila (opšti rok od 15 dana), identičan naziv pojedinih prava (pravo na uvid, pravo na kopiju) kao i identičan drugostepeni organ (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti), organi vlasti često ne razumeju najbolje razliku između zahteva građana po ZZPL-u i zahteva po Zakonu o slobodnom pristupu informacijama od javnog značaja (ZSPIJZ). Ovome doprinosi i činjenica da je često ista osoba u organu vlasti ovlašćena za postupanje za obe vrste zahteva.

	Zahtevi po ZZPL	Zahtevi po ZSPIJZ
Na šta se zahtev odnosi	Pravo fizičkog lica na zaštitu podataka o ličnosti (lično pravo)	Interes javnosti da zna
Vrednost koja se štiti	Na podatke o ličnosti	Na bilo koje informacije koje poseduju organi vlasti
Ovlašćeni podnosilac	Fizičko lice i to samo u odnosu na svoje podatke	Bilo koje pravno ili fizičko lice bez obzira na predmet zahteva
Ko ima obavezu da postupa po zahtevu	Bilo koje fizičko ili pravno lice koje je rukovalac podataka o ličnosti	Organi javne vlasti

Ipak, razlika između ove dve vrste zahteva je značajna, kako je prikazano u tabeli:

U praksi može doći do potencijalnog ''sukoba'' između prava na pristup informacijama od javnog značaja i prava na zaštitu podataka o ličnosti. Na primer, pitanje je kako bi organ vlasti trebalo da postupa u slučaju kada jedan dokument istovremeno sadrži i podatke o ličnosti određene osobe i informacije od javnog značaja. Ukoliko je uvid i kopiju takvog dokumenta tražilo ovlašćeno lice u skladu sa ZZPL-om, onda organ vlasti ne bi trebalo da ima dileme, s obzirom da takvo lice ima pravo na pristup svojim podacima o ličnosti, ali i pravo na pristup bilo kojoj informaciji od javnog značaja. S druge strane, ukoliko je takav dokument tražen u skladu sa ZSPIJZ-om, onda je situacija nešto komplikovanija. Naime, i sam ZSPIJZ ovlašćuje organ vlasti da uskrati ostvarivanje ovog prava ukoliko bi se time povredilo pravo na privatnost lica na koje se informacija odnosi (samim tim i pravo na zaštitu podataka o ličnosti, kao uži element prava na privatnost). Ipak, činjenica da određeni dokument sadrži konkretne podatke o ličnosti ne znači da organi vlasti po automatizmu treba da odbijaju ovakve zahteve. Ovde se uvek mora vagati između dva naizgled suprostavljena interesa, prava javnosti da zna i prava na privatnost. Ukoliko su, na primer, u pitanju dokumenti koji prvenstveno predstavljaju informacije ličnog karaktera (zdravstveni kartoni), onda teško da može prevagnuti interes javnosti da zna. Kada određeni dokumenti sadrže informacije od interesa za javnost, uz lične podatke kojima se garantuje zaštita, takva situacija se može prevazići anonimizacijom podataka o ličnosti u dokumentu, čime organ vlasti može udovoljiti tražiocu zahteva po ZSPIJZ, a da pritom ne dođe do povrede privatnosti i povrede prava na zaštitu podataka o ličnosti.

SAVETI ZA ANONIMIZACIJU[4]

- Kada se sprovodi anonimizacija potrebno je imati na umu njenu dvojaku svrhu: da se isključi mogućnost identifikacije lica, a da ostale informacije pružene u dokumentaciji zadrže izvorno značenje i smisao, te da dokumentacija bude lako čitljiva i kontekstualno razumljiva.
- Kada se u dokumentaciji koja postoji u elektronskom obliku podaci prekrivaju crnom bojom, potrebno je obratiti pažnju da nije dovoljno pretvoriti dokument iz .doc formata u .pdf format. U tom slučaju kopiranjem teksta iz .pdf dokumenta u .doc dokument biće moguće identifikovati lice. Zato pri ovakvom postupku preporučujemo čuvanje anonimizovanog dokumenta u formatu koji odgovara slici (na primer .jpeg ili .png).
- Ukoliko dokumentacija postoji samo u papirnom obliku, preporučujemo da se dokument prvo fotokopira, zatim primeni anonimizacija i potom ponovo fotokopira (ili skenira). Na taj način sprečava se mogućnost skidanja traga korektora ili čitanja teksta ispod crnog flomastera.
- Ukoliko dokumentacija postoji samo u papirnom obliku, a potrebno je anonimizovati podatke o više lica, treba primeniti postupak anonimizacije na osnovu kojeg bi bilo moguće sagledati ulogu svakog lica u predmetu, uz istovremenu zaštitu identiteta tih lica. Jedan od načina da se to postigne je brisanje dela imena i prezimena, te ostavljanje pojedinih slova (na primer, ''osiguranik Milan Petrović'' - ''osiguranik Milan Petrović''), i sl.

04 Više o pojmu i metodama anonimizacije možete naći u Analizi: ''Anonimizacija podataka u sudskim odlukama u Srbiji – ka usaglašenim pravilima i praksi'' koju je izradila organizacija Partneri za demokratske promene Srbije, dostupno na: http://www.partners-serbia.org/category/multimedija/publikacije/

SHARE FOUNDATION - 2016