Zaštita podataka o ličnosti – aktuelno stanje i izazovi

RADOSLAV M. RAKOVIĆ, Inženjerska akademija Srbije, Beograd

Pregledni rad
UDC: 342.738(497.11)
DOI: 10.5937/tehnika2204501R

Osnovni standard za bezbednost informacija ISO 27001 deklariše potrebu očuvanja osnovnih svojstava informacija – poverljivosti, integriteta i rasopoloživosti – i definiše 114 kontrola orijentisanih ka tehničkim, organizacionim i kombinovanim merama koje bi to trebalo da obezbede. Posebno pitanje odnosi se na zaštitu podataka o ličnosti, koje je predmet posebne Opšte regulative za zaštitu ličnih podataka (General Data Protection Regulation-GDPR), koja je počela da se primenjuje u EU od 25.05.2018. godine i posebnog Zakona za zaštitu podataka o ličnosti Republike Srbije, koji je počeo da se primenjuje od 22.08.2019. godine. Nakon sažetog prikaza GDPR i predmetnog zakona, u radu su razmotreni aktuelno stanje tematike zaštite podataka o ličnosti u Srbiji kao i izazovi koji stoje pred nama u toj oblasti.

Ključne reči: *bezbednost informacija, zaštita podataka o ličnosti, Opšta regulativa za zaštitu podataka, Zakon o zaštiti podataka o ličnosti*

„Tehnologija je čudna stvar. Daje vam velike poklone jednom rukom, a zadaje vam udarac sa leđa drugom“

C. P. Snow, New York Times (1971)

1. UVOD

Poslednjih godina bezbednost informacija postaje veoma aktuelno pitanje i u poslovnoj sferi i privatnom životu. Osnovni razlog leži u suštini izreke koja je odabrana za moto ovog rada. Suočeni smo sa burnim razvojem tehnologija, posebno u oblasti informatike.

Vreme „main frame“ računara davno je prošlo, obrada podataka i informacija je u značajnoj meri distribuirana, zahvaljujući PC tehnologiji, mobilnost je sve izraženija (lap topovi, mobilni telefoni koji su sve više računari, a sve manje telefoni) što zahteva primenu bežičnih („wireless“) tehnologija, bez Interneta je gotovo nezamisliv poslovni i privatni život, ljudi su sve familijarniji sa računarima čija je cena takva da su gotovo svima dostupni, itd. Sve to nam, sa jedne strane, značajno olakšava život, ali nam, sa druge strane, donosi probleme koje do sada nismo imali, ili ih bar nismo imali u tom obimu.

Adresa autora: Radoslav Raković, Inženjerska akademija Srbije, Beograd, Kneza Miloša 9
e-mail: rrakovic@ep-entel.com
Rad primljen: 07.07.2022.
Rad prihvaćen: 11.07.2022.

Oblast bezbednosti informacija (BI) kao pristup očuvanju njenih osnovnih svojstava, generalno je regulisana osnovnim standardom ISO 27001 u sklopu serije ISO 27000 [1]-[3]. Osnovna svojstva informacije - CIA – uključuju poverljivost (engl. Confidentiality), da informacija bude dostupna samo onome ko na nju ima pravo, celovitost (engl. Integrity), da informacija bude kompletna i zaštićena od neovlašćenih izmena i raspoloživost (engl. Availability), da informacija bude na raspolaganju onda kada nam je potrebna, pod uslovom da na nju imamo pravo.

Specifičnost standarda ISO 27001 u odnosu na ostale menadžment standarde ogleda u posebnom Aneksu A, koji u sebi sadrži 114 kontrola grupisanih u 14 oblasti i 35 ciljeva kontrole [2], [4] tabela 1.

Tematika vezana za zaštitu podataka o ličnosti tretirana je u okviru standarda ISO 27001 na nekoliko mesta. U delu A.7 razmatra se bezbednost vezana za ljudske resurse pre, za vreme i nakon angažovanja, a u delu A.8 kroz upravljanje informacionom imovinom koja obuhvata i humanu informacionu imovinu – osoblje. Pored toga, kontrola pristupa u delu A.9 podrazumeva definisanje postupaka autentifikacije (engl. Authentification) tj. dokazivanja prava za pristup i autorizacije tj. definisanje onoga što korisnik može da uradi u sistemu nakon uspešne autentifikacije.

Uz to, zaštita podataka o ličnosti pojavljuje se kroz razgraničenje odgovornosti, deo A.12, upravljanje incidentima vezanim za bezbednost informacija, deo A.16 i obezbeđenje kontinuiteta poslovanja, deo A.17.

Na najneposredniji način, ova tema vidljiva je u delu A.18, u tački A.18.1.4, koja se odnosi na privatnost i zaštitu informacija koje identifikuju ličnost.

Tabela 1. Aneks A standarda ISO 27001:2013 [4].

	Oblast BI	Ciljevi	Kontrole
A5	Politika BI	1	2
A6	Organizacija BI	2	7
A7	Bezbednost vezana za ljudske resurse	3	6
A8	Upravljanje imovinom	3	10
A9	Kontrola pristupa	4	14
A10	Kriptografija	1	2
A11	Fizička i bezbednost radnog okruženja	2	15
A12	Bezbednost operacija	7	14
A13	Bezbednost komunikacija	2	7
A14	Akvizicija, razvoj i održavanje sistema	3	13
A15	Odnosi sa isporučiocima	2	5
A16	Upravljanje bezbednosnim incidentom	1	7
A17	Bezbednosni aspekti kontinuiteta poslovanja	2	4
A18	Usklađenost	2	8
		35	114

2. OPŠTA REGULATIVA ZA ZAŠTITU PODATAKA O LIČNOSTI (GDPR)

Opšte regulativa za zaštitu podataka 2016/679 (engl. General Data Protection Regulative – GDPR), [5] usvojena je od strane Evropskog Parlamenta i Veća 27.04.2016, objavljena je u Službenom glasniku Evropske unije (engl. Official Journal of the European Union) još 4.05.2016, a počela je da se primenjuje od 25.05.2018. godine. Period od dve godine od donošenja do primene predmetne regulative bio je ispunjen mnoštvom nedoumica oko njenog sadržaja i mogućnosti za primenu, što je prisutno i danas. Sama regulativa ima ukupno 88 strana od kojih se na prvih 31 nalazi preambula sa 173 stavke, koja deklariše osnovne elemente koji su sadržani u regulative, koja je izložena na preostalih 57 strana, sadrži ukupno 99 članova koji su grupisani u 11 glava, od kojih neke imaju sekcije. Sažeti prikaz strukture ove regulative dat je u tabeli 2 po glavama i sekcijama (gde postoje). U predmetnoj tabeli, brojevi u zagradama označavaju članove regulative koji se odnose na pojedine segmente.

Uporedo sa ovom uredbom, doneta je direktiva 2016/680 [6] koja ograničava primenu GDPR u slučajevima vezanim za obradu podataka o ličnosti od strane nadležnih organa u svrhe sprečavanja, istrage, otkrivanja i gonjenja krivičnih dela.

Tabela 2. Struktura regulative 2016/679

I	Opšte odredbe (1-4)
II	Principi (5-11)
III	Prava subjekta podataka (12-23)
1	Transparentnost i modaliteti (12)
2	Informacija i pristup ličnim podacima (13-15)
3	Ispravka i brisanje (16-20)
4	Pravo na žalbu i automatsko individualno donošenje odluka (21-22)
5	Ograničanja (23)
IV	Rukovalac i obrađivač (24-43)
1	Opšte obaveze (24-31)
2	Bezbednost ličnih podataka (32-34)
3	Ocenjivanje uticaja na zaštitu podataka i prethodne konsultacije (35-36)
4	Odgovorno lice za zaštitu podataka (37-39)
5	Pravila ponašanja i sertifikacije (40-43)
V	Transfer ličnih podataka trećim zemljama ili međunarodnim organizacijama (44-50)
VI	Nezavisni nadzorni organi (51-59)
1	Status nezavisnosti (51-54)
2	Nadležnost, zadaci i ovlašćenja (55-59)
VII	Saradnja i konzistentnost (60-76)
1	Saradnja (60-62)
2	Konzistentnost (63-67)
3	Evropski odbor za zaštitu podataka (68-76)
VIII	Pravni lek, odgovornost i kazne (77-84)
IX	Odredbe vezane za specifične situacije obrade (85-91)
X	Akti delegiranja i implementacije (92-93)
XI	Završne odredbe (94-99)

Interesantno je analizirati u kakvom je odnosu uredba GDPR prema standardu za menadžment bezbednošću informacija ISO 27001:2013. Analiza pokazuje [7], [8] da korektno implementiran sistem menadžmenta bezbednošću informacija prema standardu ISO 27001:2013 ipak nije dovoljan za usaglašenost sa uredbom GDPR.

Iako između ovih dokumenata postoji dosta sličnosti, postoje i značajne razlike. Pre svega, ovi dokumenti razlikuju se po svom karakteru – uredba je pravno obavezujući dokument čije nesprovođenje povlači određene kazne, dok je primena standarda dobrovoljna, sve dok se organizacija za njega ne opredeli.

U smislu GDPR, „lični podaci“ su bilo koja informacije pomoću kojih se fizičko lice („subjekt podataka“) može identifikovati direktno ili indirektno, posebno u odnosu na identifikator kao što je ime, identifikacioni broj, lokacija, ili jedan ili više faktora specifičnih za fizički, psihološki, genetski, mentalni,

ekonomski, kulturni ili društveni identitet tog fizičkog lica.

Pod „obradom ličnih podataka“ podrazumeva se bilo koja operacija ili skup operacija koje se vrše nad ličnim podacima ili skupom ličnih podataka bez obzira da li se koriste ili ne automatska sredstva, kao što je prikupljanje, zapisivanje, organizovanje, struktuiranje, memorisanje, pretraživanje, korišćenje, obelodanjivanje putem prenosa, razglašavanja ili drugog oblika stavljanja na raspolaganje, svrstavanje ili kombinovanje, ograničavanje, brisanje ili uništavanje.

Posebno značajan pojam vezan za obradu ličnih podataka predstavlja „profilisanje“. U pitanju je bilo koji oblik automatske obrade ličnih podataka koji se sastoji u korišćenju ličnih podataka radi vrednovanja nekih ličnih aspekata koji se odnose na fizičko lice, naročito za analizu ili predviđanje aspekata koji se tiču performansi pojedinca na poslu, ekonomske situacije, zdravlja, ličnih sklonosti, interesa, pouzdanosti, ponašanja, lokacije ili kretanja.

U sprovođenju obrade ličnih podataka ključni učesnici su „Rukovalac“ i „Obrađivač“. „Rukovalac“ (engl. Controller) je fizičko ili pravno lice, javni organ, agencija ili drugo telo koje, samostalno ili u saradnji sa drugima, određuje svrhu i sredstva obrade ličnih podataka, dok je „Obrađivač“ (engl. Processor) fizičko ili pravno lice, javni organ, agencija ili drugo telo koji obrađuje lične podatke u ime rukovaoca.

U okviru GDPR jedna od ključnih institucija jeste „pristanak“ subjekta podataka na obradu ličnih podataka. To predstavlja bilo koji oblik slobodno iskazane volje subjekta podataka kojom on ili ona, izjavom ili jasno afirmativnom akcijom potpiše sporazum o obradi ličnih podataka koji se odnose na njega ili nju.

Ključni problem koji nastaje u obradi ličnih podataka je „narušavanje ličnih podataka“ (engl. Breach), koje predstavlja narušavanje bezbednosti koje dovodi do slučajnog ili nezakonitog uništavanja, gubitka, izmene, neautorizovanog obelodanjivanja ili pristupa ličnim podacima koji se prenose, skladište ili obrađuju na drugi način.

2.1. Principi zaštite ličnih podataka

Principi koji se odnose na obradu ličnih podataka član 5 [5] su:

- Zakonitost, korektnost i transparentnost: Lični podaci treba da budu obrađivani u skladu sa zakonom, korektno i na transparentan način u odnosu na subjekta podataka.
- Ograničenje svrhe: Lični podaci treba da budu prikupljeni za specificirane, eksplicitne i legitimne svrhe i da ne budu obrađivani za druge svrhe. Obrada u svrhe arhiviranja od javnog interesa, u svrhu naučnih i istorijskih istraživanja ili u statističke svrhe ne smatra se nekompatibilnom sa inicijalnom svrhom.
- Minimizacija podataka: Lični podaci treba da budu adekvatni, relevantni i ograničeni na ono što je potrebno u odnosu na svrhu zbog koje su prikupljeni.
- Tačnost: Lični podaci treba da budu tačni i, kada je potrebno, ažurirani. Ako nisu, mora se preduzeti svaki razuman korak da se izbrišu ili isprave bez odlaganja.
- Ograničenje čuvanja: Lični podaci treba da budu držani u obliku koji dopušta identifikaciju subjekta podataka ne više od neophodnog za svrhu za koju se lični podaci obrađuju. Lični podaci mogu se čuvati u dužem periodu u onoj meri u kojoj će biti obrađivani jedino za arhiviranja od javnog interesa, u svrhu naučnih i istorijskih istraživanja ili u statističke svrhe.
- Integritet i poverljivost: Lični podaci treba da budu obrađeni na način koji osigurava odgovarajuću bezbednost ličnih podataka, uključujući i zaštitu od neautorizovanog pristupa ili nezakonite obrade i od slučajnih gubitaka, uništenja ili oštećenja, primenom odgovarajućih tehničkih ili organizacionih mera.
- Krajnja odgovornost: Rukovalac je odgovoran za usklađenost sa odredbama ove Regulative i on definiše svrhu obrade i okvire u kojima deluje obrađivač.

Suština je jasna – lični podaci mogu se prikupljati i obrađivati samo u skladu sa svrhom za koju su namenjeni i to u najmanjem mogućem obimu, pri čemu moraju biti zaštićeni od svih oblika zloupotrebe. Jednostavnim rečima, u obradi ličnih podataka treba „naći pravu meru“, a znamo koliko je to teško u mnogim oblastima života.

2.2. Prava subjekta podataka

Prava subjekta podataka navode se u Glavi III, članovi 12-23 [5]:

- Pravo da bude informisan o obradama njegovih ličnih podataka. To je obaveza rukovaoca, a informacija treba da bude data u sažetom, transparentnom, razumljivom i pristupačnom obliku. Kada rukovalac ima nameru dalje obrade ličnih podataka za svrhe drugačije od onih koje su bile prisutne prilikom prikupljanja ličnih podataka, mora o tome obavestiti subjekta.
- Pravo da od rukovaoca dobije potvrdu da li su ili nisu obrađivani lični podaci koji se odnose na njega ili nju, i, tamo gde je to slučaj, pristup ličnim podacima (član 15) i informacijama o svrsi obrade, kategoriji ličnih podataka na koje se ona odnosi, primaocima ili kategorijama primalaca

kojima su lični podaci obelodanjeni, ili će biti obelodanjeni, naročito primaoci iz trećih zemalja ili međunarodne organizacije, predviđeni period u kome će lični podaci biti čuvani, ili, ako to nije moguće, kriterijumi koji se koriste za određivanje tog perioda itd.

- Pravo na ispravku tj. da od rukovaoca dobije, bez nepotrebnog odlaganja, ispravku netačnih ličnih podataka. Uzimajući u obzir svrhu obrade, subjekt podataka ima pravo da kompletira nekompletne lične podatke.
- Pravo na brisanje („pravo na zaborav“) tj. da mu rukovalac obezbedi brisanje ličnih podataka koji se odnose na njega ili nju bez nepotrebnog odlaganja u slučajevima kada lični podaci više nisu potrebni u odnosu na svrhu za koju su prikupljeni ili na drugi način obrađeni, kada subjekt podataka povuče saglasnost na osnovu koga je obrada vršena, u slučaju prigovora subjekta podataka na obradu itd.
- Pravo da traži od rukovaoca ograničenje obrade u slučajevima kada je tačnost ličnih podataka osporena od strane subjekta podataka, za period koji omogućuje rukovaocu da verifikuje (proveri) tačnost ličnih podataka, kada je obrada nezakonita i subjekt podataka se protivi brisanju ličnih podataka i zahteva organičavanje njihovog korišćenja i kada je subjekt podataka je uložio prigovor na obradu koji nije razrešen i zahteva proveru da li su legitimni osnovi neuvažavanja prigovora.
- Pravo na prenosivost podataka tj. da dobije lične podatke koji se odnose na njega ili nju, koje su on ili ona obezbedili rukovaocu u strukturnom, uobičajeno korišćenom i mašinski-čitljivom formatu, i ima pravo da prenese te podatke drugom rukovaocu.
- Pravo na prigovor, na osnovama koje se odnose na njegovu ili njenu posebnu situaciju, u bilo koje vreme u obradi ličnih podataka koji se odnose na nju ili njega, uključujući profilisanje. Prigovor znači da rukovalac ne bi trebalo više da obrađuje lične podatke ukoliko ne pokaže izuzetne zakonske osnove za obradu koja ne uvažava interese, prava i slobode subjekta podataka.
- Pravo da ne bude subjekat odluka zasnovanih samo na automatskoj obradi, uključujući i profilisanje, koje proizvodi pravne posledice koje se tiču njega ili nje ili slične efekte na njega ili nju.

Regulativa jasno razdvaja obradu ličnih podataka koji su prikupljeni od subjekta podataka (član 13 [5]) i onih koji nisu prikupljeni na taj način (član 14 [5]). Značajnu stavku predstavlja pristanak subjekta podataka na obradu njegovih ličnih podataka, pri čemu je naglašeno da dokument o pristanku treba da bude podnet jednostavnim rečima i da ćutanje ili neaktivnost ne znače odobravanje već se mora obezbediti jasan i pozitivan pristanak za obradu ličnih podataka.

Poseban segment posvećen je pristanku roditelja ili lica sa tim statusom odgovornosti za decu mlađu od 16 godina, pri čemu zemlje članice EU mogu sniziti ovu granicu, ali ne ispod 13 godina (član 8 [5]).

Regulativom GDPR predviđene su veoma visoke kazne za narušavanje bezbednosti podataka o ličnosti. Član 83 Regulative [6] navodi dva nivoa administrativnih kazni za narušavanje ove regulative:

- Administrativna kazna do 20 miliona €, ili u slučaju preduzeća, do 4 % ukupnog godišnjeg prihoda u prethodnoj finansijskoj godini, koje god da je više za narušavanje obaveze rukovaoca ili obrađivača, obaveze sertifikacionog tela i obaveze tela za praćenje, prema odgovarajućim članovima.
- Administrativna kazna do 10 miliona €, ili u slučaju preduzeća, do 2 % ukupnog godišnjeg prihoda u prethodnoj finansijskoj godini, koje god da je više za narušavanje osnovnih principa za obradu, uključujući uslove za pristanak, prava subjekta podataka, transfera ličnih podataka primaocima u trećim zemljama ili međunarodnim organizacijama, bilo koje obaveze prema zakonu Zemlje članice usvojenom prema Glavi 9 kao i neusaglašenosti sa nalogom ili privremenim ili trajnim ograničenjem obrade ili suspenzije toka podataka od strane nadzornog organa ili propust da se obezbedi pristup.

2.3. Kazne za nepoštovanje zaštite podataka o ličnosti

U nastavku su navedeni primeri kažnjavanja rukovalaca zbog nepoštovanja odredaba GDPR u Evropi i u svetu, na osnovu podataka raspoloživih u literaturi [9].

- Google je kažnjen sa 50 miliona € u Francuskoj zbog nejasne svrhe obrade podataka o ličnosti i prosleđivanja ličnih podataka u marketinške svrhe bez pristanka subjekata.
- British Airways je kažnjen sa 20 miliona € u Velikoj Britaniji, zbog gubitka podataka za 500 hiljada klijenata usled kompromitovanja web sajta.
- Facebook je kažnjen sa 100 miliona € u Belgiji jer je „like“ dugme korišćeno za profilisanje korisnika kako bi im bile dostavljane reklame.
- Facebook je kažnjen sa 10 miliona € u Italiji zbog prodaje podataka o korisnicima.
- Facebook je kažnjen sa 565 hiljada € u Velikoj Britaniji jer je omogućio kompaniji Cambridge Analytics da koristi podatke iz ankete 300 hiljada korisnika u izbornoj kampanji Donalda Trampa.

- Pošta u Austriji kažnjena je sa 10 miliona € zbog profilisanja korisnika u političke svrhe i prodaje podataka političkim strankama.
- Kompanija Deutche Wohnen kažnjena je sa 14 miliona € zbog toga što je predugo i bez zakonskog osnova čuvala podatke o korisnicima.
- Krajem maja 2022. godine američka Federalna komisija kaznila je Twitter sa 150 miliona € jer je ta kompanija davala korisničke informacije oglašivačima, uključujući brojeve telefona i e-mailove, u periodu od maja 2013. do septembra 2019. Godine, jer je time obmanula korisnike da štiti njihove lične podatke.

2.4. Ključne razlike standarda USO 27001 i GDPR

Mnoge institucije koje postoje u GDPR ne postoje u okviru standarda ISO 27001. To se pre svega odnosi na pristanak za obradu ličnih podataka (članovi 7 i 8 GDPR), pravo na brisanje tj. „na zaborav" (čl. 17 GDPR), pravo na ograničenje obrade (čl. 18 GDPR), prenosivost podataka (čl. 20 GDPR) i pravo na prigovor (čl. 21 GDPR), dok međunarodni transfer ličnih podataka iz čl. 46 GDPR-a delimično postoji u standardu ISO 27001, ali pre svega se odnosi na poslovne podatke. Pored toga, standard sadrži detalje o održavanju nivoa zaštite informacija, čega u GDPR-u nema.

3. ZAKON O ZAŠTITI PODATAKA O LIČNOSTI

Novembra 2018. godine donet je novi Zakon o zaštiti podataka o ličnosti Republike Srbije - ZZPL [10]. Ustavni osnov za donošenje predmetnog Zakona sadržan je u čl. 42 Ustava [11] koji proklamuje da je zaštita podataka o ličnosti zajemčena, da se prikupljanje, čuvanje, obrada i korišćenje podataka o ličnosti uređuju posebnim zakonom, da svako ima pravo da bude obavešten o prikupljenim podacioma o svojoj ličnosti i ima pravo na sudsku zaštitu u slučaju njihove zloupotrebe. Pored toga, ovom temom bavi se i čl. 97 Ustava u sklopu zaštite sloboda i prava građana.

Razlozi za donošenje novog Zakona o zaštiti podataka o ličnosti leže kako u unutrašnjim potrebama tako i u kontekstu pridruživanja Evropskoj uniji. U prvom segmentu to se odnosi na potrebu dogradnje postojećeg pravnog sistema da bi bolje obezbedio zaštitu ličnih podataka, jer postojeći zakon donet pre desetak godina, nije u mogućnosti da ispuni ono što se u ovoj oblasti zahteva. U drugom segmentu donošenje ovog Zakona predstavlja deo međunarodnih obaveza države i obaveza usklađivanja sa zakonodavstvom EU u procesu evrointegracija. Potreba za izmenom ovog Zakona navedena je 2016. godine u sklopu izveštaja o napretku Srbije u procesu pridruživanja EU.

U tabeli 3 prikazana je struktura ZZPL [12]. Zakon je suštinski objedinio u sebi regulativu 679/2016 - GDPR [5] i Direktivu 680/2016 [6].

Tabela 3. Struktura ZZPL [12]

	Naziv	Čl.	GDPR
I	Osnovne odredbe	1-4	I
II	Načela	5-20	II
III	Prava lica na koje se podaci odnose (subjekta podataka)	21-40	III
IV	Rukovalac i obrađivač	41-62	IV
V	Prenos podataka o ličnosti u druge zemlje i međunarodne organizacije	63-72	V
VI	Poverenik (Nezavisni nadzorni organi)	73-81	VI
VII	Pravna sredstva, odgovornost i kazne	82-87	VIII
VIII	Posebni slučajevi obrade	88-94	IX
IX	Kaznene odredbe	95	VIII
X	Prelazne i završne odredbe	96-102	XI

Već prvi pogled na tabelu 3 ukazuje da u odnosu na strukturu regulative GDPR nedostaju dve sekcije VII „Saradnja i konzistentnost" i X „Akti delegiranja i implementacije" što je posledica činjenice da Srbija još uvek nije članica EU.

Načela ZZPL (u GDPR Principi) i prava subjekta podataka u oba dokumenta preklapaju se u značajnoj meri. Postoje određene razlike između između tih dokumenata [12]:

- Oba dokumenta sadrže po 26 definicija od kojih se 22 preklapaju, a po 4 se razlikuju. Zakon je definisao „lice na koje se podaci odnose" (u GDPR je to „subjekt podataka", ali ne figuriše kao zasebna definicija), „multinacionalnu kompaniju", „organe vlasti" i „nadležne organe", a izostavio je definicije „glavno postavljenje nadzornog organa", „nadležni nadzorni organ", „prekogranična obrada" i „relevantan razuman prigovor".
- Ulogu nadzornog organa u Zakonu preuzima „Poverenik za informacija od javnog značaja i ZPL".
- Po Zakonu, samostalan pristanak za obradu podataka o ličnosti može dati lice sa 15 godina starosti (u GDPR je preporučeno, 16, ali ne niže od 13 godina.
- Zakon predviđa pravo na „pritužbu" Povereniku, što je preuzeto iz Zakona o inspekcijskom nadzoru [13], iako GDPR predviđe pravo na ulaganje prigovora – žalbe. Pravnici su jedinstveni u stavu da pravno dejstvo pritužbe i prigovora – žalbe nije isto.
- Za povredu Zakona predviđene su prekršajne kazne u novčanim iznosima od 50 hiljada do 2 miliona RSD za 32 slučaja kao i 6 slučajeva sa fiksnom kaznom od 100 hiljada RSD. To je drastično različito od GDPR-a jer se raspon kazni kreće od 430 € do 17 hiljada €, a to je na određeni način u

suprotnosti sa stavom da kaznena politika treba da deluje destimulativno za počinioce. U slućaju Zakona visina kazne daleko je ispod štete koja može biti naneta kršenjem Zakona i dobiti koja se na taj način može ostvariti, pa je prekršioci kalkulišu kao „trošak“ poslovanja!

4. IZAZOVI I DILEME

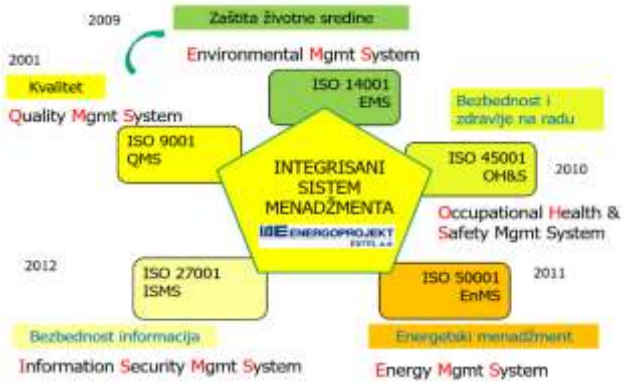
U praktičnoj primeni Zakona ima mnoštvo dilema, nedoslednosti i izazova, od kojih su nastavku navedene samo najznačajnije [9], [14]:

- Zakon je nametnuo nove obaveze organima vlasti i Povereniku, ali je ostavljen veoma kratak interval od 9 meseci od stupanja na snagu ZZPL do njegove primene. U slučaju GDPR taj interval iznosio je 2 godine.
- Zbog nespremnosti institucija predviđenih u ZZPL da preuzmu svoje odgovornosti, Poverenik je tražio odlaganje primene ZZPL od 22.08.2019. godine ali to nije prihvaćeno.
- Organi vlasti često ne obaveštavaju Poverenika o relevantnim pitanjima iz njegove nadležnosti i često preduzimaju korake bez njegove saglasnosti (npr. Iznošenje velike količine podataka o građanima Srbije u inostranstvo, bez odobrenja Poverenika).
- Još uvek ne postoji dovoljna svest ljudi o značaju podataka o ličnosti. Najčešće se smatra da oni kao obični ljudi nisu važni da bi neko imao nešto od njihovih podataka, da nemaju šta da kriju i sl. Isto tako, sami ljudi u različitim oblicima (društvene mreže, ulične ankete, javna mesta i gradski prevoz i sl.) daju svoje lične podatke na uvid drugima bez ikakve potrebe, što je posebno izraženo kod starije populacije.
- U toku je rad na izmenama i dopunama ZZPL i na donošenju Strategije zaštite podataka o ličnosti do 2030. godine u kojoj je planirano uvođenje edukacije o zaštiti podataka o ličnosti u osnovnim i srednjum školama.
- Samo u toku 2021. godine Povereniku je upućeno preko 200 žalbi na narušavanje podataka o ličnosti, a sprovedeno je 303 inspekcijska nadzora.
- U praksi postoji dosta slučajeva zloupotrebe podataka o ličnosti u cilju diskriminacije osetljivih grupa, npr. žena kojima prilikom zapošljavanja poslodavac traži podatke koji nisu od interesa za posao poput informacija o bračnom ststusu i planiranju porodice ili pripadnika LGBT populacije u pogledu kriterijuma za davaoce reproduktivnih ćelija i embriona.
- U bankama ili hotelima često se traži lična karta koja se, umesto elementarne identifikacije, bez ikakve potrebe očitava, štampa i ulaže u neke registratore, ili drži na recepciji u toku boravka gosta sa obrazloženjem da im to traže iz MUP-a.
- Podzakonski akti nisu razrešili pitanje video nadzora na otvorenim i/ili zatvorenim prostorima (tehnologije prepoznavanja lica), niti pitanje neovlašćene upotrebe fotografija na društvenim mrežama.
- U periodu od januara 2015. do jula 2020. Analizirane su aktivnosti javnog tužilaštva i sudova vezane za čl. 146 Krivičnog zakona koji se odnosi na neovlašćeno prikupljanje podataka o ličnosti. Rezultati pokazuju [14] da je od 66 sudova u 14 bilo ukupno 28 predmeta vezanih za taj član, donete su 4 oslobađajuće presude, 2 osuđujuće (obe uslovno), a ostalih 22 predmeta su odbijeni kao neosnovani, odbačeni ili obustavljeni. U istom periodu Poverenik je podneo 17 krivičnih prijava, ali ni jedna od njih nije dobila epilog, posebno zbog činjenice da oštećeni često nemaju advokate zbog svog socijalnog i ekonomskog statusa.
- U periodu od avgusta 2019. do juna 2021. godine Poverenik je uputio 8 zahteva za pokretanje prekršajnih postupaka, samo su dva okončana (jedan sa kaznom, a drugi zbog zastarelosti).
- U okviru jedinstvenog informacionog sistema (JIS) u prosveti postoji ogroman broj podataka u obliku registra đaka, njihovih roditelja ili staratelja, registra nastavnika i sl. kao i sistem elektronskog dnevnika. Uočeno je da privatna firma koja održava taj sistem na komercijalnoj osnovi nudi dodatne opcije korisnicima. Sa stanovišta statistike, svi navedeni podaci trebalo bi da budu anonimizovani tj. da se podaci o stvarnim ličnostima mogu videti samo u posebnim bazama, koje nisu široko dostupne.
- U vreme pandemije COVID-19 zdravstvo je došlo u žižu interesovanja jer su u nekim sredinama podaci o zdravstvenom stanju ljudi postali javno dostupni. U ovoj oblasti nije bilo jasno ko je rukovalac, a ko obrađivač, i koji je pravni osnov za prikupljanje, obradu i obelodanjivanje tih podataka.
- Poseban segment vezan za prikupljanje i obradu podataka o ličnosti predstavljaju privredna društva – organizacije koje ove aktivnosti sprovode na osnovu zakonske obaveze evidencije o radnom odnosu, u svrhu ostvarivanja prava zaposlenih i članova njihovih porodica ili iz razloga ostvarivanja poslovnog i legitimnog interesa organizacije (npr. reference zaposlenih kao deo procesa nuđenja i ugovaranja). U tom smislu ključna su načela minimizovanja (prikupljanje samo onoliko podataka koliko je potrebno, ni više ni manje) i svrsishodnosti tj. da za svaki od podataka postoji jasna svrha zbog koga se prikuplja i obrađuje.

5. CASE STUDY: EP ENTEL

Primena zaštite podataka o ličnosti ilustrovana je na primeru preduzeća Energoprojekt Entel a.d. iz Beograda. U pitanju je preduzeće čija je delatnost projektovanje, konsalting i inžejering u oblastima energetike, vodoprivrede, telekomunikacija i zaštite životne sredine. Organizacija ima implemantiran integrisani sistem menadžmenta (IMS) sa pet menadžment standarda – kvalitet, zaštita životne sredine, bezbednost i zdravlje na radu, bezbednost informacija i energetski menadžment, a u skladu sa relevantnim ISO standardima, slika 1 [15].

Polazeći od prethodno iznetog stava da korektno implementiran sistem menadžmenta bezbednošću informacija prema ISO 27001 nije dovoljan za punu implementaciju odredbi GDPR, odnosno ZZPL, organizacija je proširila svoj sistem menadžmenta bezbednošću informacija (definisan procedurom EN-27P-01) posebnom procedurom EN-27P-02 koja je posvećena temi zaštite podataka o ličnosti.



Slika 1 - Prikaz IMS EP ENTEL [15]

Predmetnom procedurom regulisana je analiza (mapiranje) podataka o ličnosti (opis podatka, kategorija, osnov obrade, period čuvanja, medijum/lokacija čuvanja, transfer trećoj strani, rukovalac, obrađivač i detaljniji opis svrhe obrade), procena uticaja na bezbednost podataka o ličnosti, postupak u slučaju ugrožavanja bezbednosti podataka o ličnosti, davanje i opoziv pristanka na obradu podataka o ličnosti, ostvarivanje uvida zaposlenog u podatke o ličnosti koji se o njemu prikupljaju i obrađuju i brisanje podataka o ličnosti. Pored zaposlenih, ovom procedurom obuhvaćeno je prikupljanje i obrada podataka o ličnosti potencijalno zaposlenih (koji konkurišu za posao preko sajta organizacije) i isporučilaca i drugih poslovnih partnera.

6. ZAKLJUČAK

Tema vezana za zaštitu podataka o ličnosti još uvek je nova u našim uslovima i posebno je opterećena sklonošću našeg mentaliteta da izbegava, a ne da sprovodi utvrđena pravila. Ključno je da se preduzimaju mere preventivnog karaktera, a ne da se leče posledice onda kada nastanu problemi. Ima dosta prostora za napredak, ali mora mnogo da se radi, a to zahteva vreme, napor i strpljenje svih.

LITERATURA

[1] ISO 27000: 2016 Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO, 2016)

[2] ISO 27001: 2013 Information technology - Security techniques - Information security management systems - Requirements (ISO, 2013)

[3] ISO 27002:2013 Information technology - Security techniques - Information security management systems - Code of practice (ISO, 2013)

[4] R. Raković: *Bezbednost informacija – Osnove i smernice*, Akademska misao, Beograd, 2017.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation, Official Journal of European Union, L 119/1 to 88, 4 May 2016.

[6] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Official Journal of European Union, 4 May 2016, L 119/89 to 130)

[7] R. Raković, Zaštita ličnih podataka u svetlu regulative GDPR, *Kvalitet & Izvrsnost*, God.VII, br 7-8, str. 19-22, 2018.

[8] R. Raković, ISO 27001 vs GDPR regulativa – sličnosti i razlike *Kvalitet & Izvrsnost*, God.VIII, br 1-2, str. 39-42, 2019.

[9] www.kolega.rs Bilten pravnika – praktičara, br. 9, decembar 2019: „Institucije u Srbiji nisu pripremljene na novi Zakon o zaštiti podataka o ličnosti“ Sagovornik: Andrej Diligenski

[10] Zakon o zaštiti podataka o ličnosti SGRS 87/2018, 13.11.2018.

[11] Ustav Republike Srbije SGRS 98/2006, 115/2021.

[12] R. Raković, Zakon o zaštiti ličnih podataka u svetlu evropske regulative *Kvalitet & Izvrsnost*, God.VIII, br 3-4, str. 47-52, 2019.

[13]Zakon o inspekcijskom nadzoru, SGRS 36/2015, 44/2018-dr. zakon i 95/2018.

[14]Privatnost i zaštita podataka o ličnosti u Srbiji – Analiza odabranih sektorskih propisa i njihove primene, Partneri za demokratske promene Srbija, #EU za tebe, Ministarstvo za ljudska i manjinska prava i društveni dijalog, Beograd, mart 2021.

[15]Dokumenti sistema IMS EP Entel

SUMMARY

PERSONAL DATA PROTECTION – ACTUAL STATUS AND CHALLENGES

Fundamental information security management standard ISO 27001 declares need for protecting basic features of information – confidentiality, integrity and availability - and defines 114 controls oriented to technical, organizational and combined actions that should enable it. Particular issue represents personal data protection that is subject of particular General Data protection Regulation (GDPR) has been appplied in EU from 25.05.2018. and paricular Law on personal data protection of Republic of Serbia has been applied from 22.08.2019. After brief review of the GDPR and the subject law, actual status of personal data protection in Serbia are considered, as well as challenges we will face in the future in this area.

Key Words: *Information Security, personal data protection, General Data Protection Regulative (GDPR), Law on personal data protection*