Odgovor Poverenika za javne informacije i zaštitu podataka o ličnosti na pitanje:

Da li postoji obrazac Pravilnika koji bi svaka institucija-operator interneta trebala da poseduje garantujuci istovremeno njegovu primenu?

Poštovani gospodine Ignjatoviću,

Pre nego što smo pristupili koncipiranju odgovora na postavljena pitanja, izvršili smo dosta detaljan uvid u sadrža internet stranice http://www.ipb.ac.rs/index.php/sr/ kako bi smo stekli jasniju predstavu o radu ove naučno-istraživačke ustanove i obimu obrade podataka o ličnosti koja se vrši.

Shodno odredbama Zakona o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012, dalje: ZZPL), sa kojim se detaljnije možete upoznati nahttp://www.poverenik.org.rs/sr.html , OBRADA PODATAKA je *svaka radnja* preduzeta u vezi sa podacima kao što su: prikupljanje, beleženje, prepisivanje, umnožavanje, kopiranje, prenošenje, pretraživanje, razvrstavanje, pohranjivanje, razdvajanje, ukrštanje, objedinjavanje, upodobljavanje, menjanje, obezbeđivanje, korišćenje, stavljanje na uvid, otkrivanje, objavljivanje, širenje, snimanje, organizovanje, čuvanje, prilagođavanje, otkrivanje putem prenosa ili na drugi način činjenje dostupnim, prikrivanje, izmeštanje i na drugi način činjenje nedostupnim, kao i sprovođenje drugih radnji u vezi sa navedenim podacima, bez obzira da li se vrši automatski, poluautomatski ili na drugi način; PODATAK O LIČNOSTI je *svaka informacija koja se odnosi na fizičko lice*, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i sl.), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i sl, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl.), ili bez obzira na drugo svojstvo informacije, a FIZIČKO LICE je čovek na koga se odnosi podatak, čiji je identitet *određen ili odrediv* na osnovu ličnog imena, jedinstvenog matičnog broja građana, adresnog koda ili drugog obeležja njegovog fizičkog, psihološkog, duhovnog, ekonomskog, kulturnog ili društvenog identiteta itd.

U napred navedenom smislu podaci o ličnosti jesu i objavljene fotografije članova Istraživačkih oblasti, njihovi kontakt podaci i kratke biografije, pa čak i sami mail nalozi, kao npr. sijacki@ipb.ac.rs koji dovoljno govori o tom fizičkom licu čineći njegov identitet *odredivim* (prezime+skraćenica institucije), a ukrštanjem sa drugim podacima na webu, i vrlo *određenim.*

U značenju datom ZZPL, Institut za fiziku, Pregrevica 118, 11080 Beograd (dalje: Institut), ne samo da podleže atributu Rukovaoca podataka (*Rukovalac podataka je fizičko ili pravno lice, odnosno organ vlasti koji obrađuje podatke*), već i atributu Organa vlasti (*Organ vlasti je državni organ, organ teritorijalne autonomije i jedinice lokalne samouprave, odnosno drugi organ ili organizacija kojoj je povereno vršenje javnih ovlašćenja*), u značenju ovih izraza datom ZZPL, iz kog razloga se Institut i nalazi u Katalogu organa vlasti (videti: http://www.poverenik.org.rs/sr/zakon-i-podz-akti-.html).

U tom smislu, Institut nesumnjivo vrši obradu određenog broja podataka o ličnosti koja je propisana zakonom (kao npr. Kadrovska evidencija, odnosno Evidencija zaposlenih), kako zaposlenih, tako i trećih lica, ali po svemu sudeći i obradu koja se ad hoc vrši u skladu sa potrebama Instituta i kao takva za svoj osnov crpe, ili bi barem trebalo da crpe, iz pristanka lica čiji se podaci obrađuju, najčešće u vidu pisane saglasnosti u skladu sa čl. 10. i 15. ZZPL (npr. obrada u vidu sačinjavanja spiska i dalje obrade podataka o ličnosti učesnika pojedinih seminara, dodela priznanja, stručnih putovanja isl.). Naravno, ovo su hipotetički primeri, ali po pravilu obrada je je uvek hibridnog karaktera. U jednom delu propisuju ju je zakoni (vrstu podataka, svrhu prikupljanja i dalje obrade isl.), dok se u određenom delu ista vrši i u situacijama koje ne reguliše zakon, a kako treba obezbediti pravni osnov, on je najčešće sadržan u pisanom pristanku. Zašto najčešće – zato što ZZPL poznaje i tzv. "obradu bez pristanka" od strane organa vlasti, u članu 13. Zakona, ali o tome možda bolje neki drugi put.

Najzad, uz preporuku da neko vičan pravu dobro iščita ZZPL i markira obaveze Instituta po tom Zakonu (npr. obaveze ka Centralnom registru Poverenika http://registar.poverenik.rs/onlineusers/search), evo da Vam odgovorimo na postavljena pitanja.

Institut ne podleže KONKRETNOM postupku nadzora koji se vodi prema Operatorima, ali svakako, kao Rukovalac podataka, podleže nadzoru koji potencijalno može biti otvoren radi utvrđivanja dozvoljenosti obrade koju vrši, odnosno sprovođenja i izvršavanja ZZPL (npr. obaveze iz čl. 48. i 51. ZZPL u vezi Centralnog registra, Institut - nije izvršio!).

Donošenje Pravilnika o radu institutskog servisa elektronske poste svakako je dobar potez i iako njegovo donošenje (za sada) nije obavezujuće, u skladu je sa obavezama koje rukovalac podataka ima prema čl. 47. ZZPL:

"*Podaci moraju biti odgovarajuće zaštićeni od zloupotreba, uništenja, gubitka, neovlašćenih promena ili pristupa.*
Rukovalac i obrađivač dužni su da preduzmu ***tehničke, kadrovske i organizacione mere*** *zaštite podataka,u skladu sa utvrđenim standardima i postupcima, a koje su potrebne da bi se podaci zaštitili od gubitka, uništenja, nedopuštenog pristupa, promene, objavljivanja i svake druge zloupotrebe, kao i da utvrde obavezu lica koja su zaposlena na obradi, da čuvaju tajnost podataka".*

Donošenje navedenog Pravilnika predstvaljalo bi ***organizacionu*** meru Instituta, kao Rukovaoca podataka.

U tom smislu, svi rukovaoci podataka, pa tako i Operatori, Institut itd. koji vrše obradu podataka o ličnosti, posebno kada je u pitanju tzv. automatizovana obrada, dužni su da vode računa o primeni čl. 47. ZZPL koji nije razrađen u zakonu, ali nesumnjivo ukazuje na sve one aspekte zaštite i bezbednosti podataka na koje ukazuju važeći standardi (npr. **SRPS** ISO/IEC 27001:2011) koji su svoj izraz našli i prilikom formulisanja Upitnika.

ISO/IEC 27001:2005 predstavlja standard koji se odnosi na informacionu zaštitu (ISMS standard), a isti su ustanovile Međunarodna organizacija za standrdizaciju ISO i Međunarodna elektrotehnička komisija IEC.

Pogledati na adresi:

http://www.iso.org/iso/catalogue_detail?csnumber=42103 i http://www.iec.ch/.

Kao usvojeni srpski standard ISO/IEC 27001:2005 u katalogu Instituta za standardizaciju Srbije nosi oznaku SRPS ISO/IEC 27001:2009 i ICS broj: 35.040.

Pored navedenih , postoji i određeni broj standarda koji se odnose na specifične sektore i dopuna su seriji ISO/IEC 27000 standarda.

S druge strane, ukazali bi smo vam na CobiT (*skraćenica od CONTROL OBJECTIVES for INFORMATION and RELATED TECHNOLOGY*) kao skup najbolje prakse *(pogledati na adresi* http://www.isaca.org/) koju stvaraju *Information Systems Audit and Control Association* (ISACA) i *IT Governanc Institute* (ITGI). Sa nizom opšte donetih mera, pokazatelja, procesa i najbolje prakse, CobiT obezbeđuje rukovaocima podataka oruđe za upravljanje i maksimiziranje koristi dobijenih upotrebom informacionih tehnologija.

Najzad, tu je i *The Information Technology Infrastructure Library* (ITIL) koja sadrži detaljan opis brojnih važnih IT praksi sa spiskovima, nalozima i postupcima, koje je moguće prilagoditi za sve IT vrste organizacija *(pogledati na adresi:* http://www.itil-officialsite.com).

Prema tome, ne postoji "*... obrazac Pravilnika koji bi svaka institucija-operator interneta trebala da poseduje garantujuci istovremeno njegovu primenu*", ali postojanje istog svakako je poželjno i dobrodošlo.

Da li se primenjuju mere, na žalost, Poverenik često saznaje kasno - kada se već dogodi incident (npr. slučaj "Sex kod Arene").

Međutim, prilikom redovnih nadzora Poverenik ne propušta da iskontroliše i ovaj aspekt obrade podataka o ličnosti (postojanje tehničkih, kadrovskih i organizacionih mera).

Slikovito rečeno, nije dovoljno definisati samo nivoe pristupa određenoj bazi podataka, već i arhivskom prostoru gde se na papiru kao nosaču informacija mogi nalaziti ti isti podaci, ili čak u daleko većem obimu.

Zahvaljujemo na interesovanju za pravilnu primenu ZZPL.

Srdačno,

Radoje Gvozdenović
Viši savetnik
Načelnik Odeljenja za nadzor nad zaštitom podataka u organima vlasti
Sektor za nadzor
Služba Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti
11 000 Beograd
Bulevar kralja Aleksandra 15
Tel. +381 11 3408 910
E-mail: radoje.gvozdenovic@poverenik.rs
Web: www.poverenik.org.rs