ISO 27001 I ZAKON O ZAŠTITI LIČNIH PODATAKA

ISO 27001 AND PERSONAL DATA PROTECTION LAW

Enver Delić, dipl.oec., 27001 Lead Auditor
IPI – Institut za privredni inženjering
Zenica

Dragana Agić, dipl.iure
IPI – Institut za privredni inženjering
Zenica

REZIME
Implementacija sistema upravljanja zaštitom informacija (skr. ISMS – Information Security Management System) je proces koji će mnoge organizacije koje u radu koriste povjerljive informacija morati proći tokom narednih godina s ciljem približavanja evropskim integracijama. Iako rad na implementaciji može biti poprilično intenzivan, postignuti rezultati umnogome opravdaju uloženi trud.

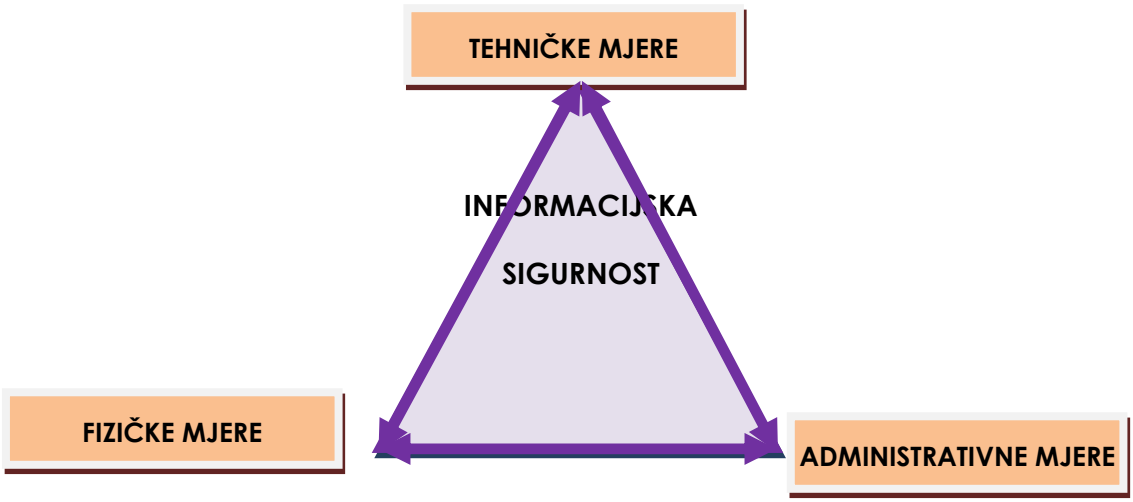
Ključne riječi: ISO/IEC 27001, ISMS, zaštita informacija

ABSTRACT
Implementation of the Information Security Management System (ISMS) is a process that organizations that use confidential data will have to go through in the near future. Besides being one of the conditions for membership in the EU, it will also help organizations, as the results of the successful implementation show worthy of time and effort invested.

Keywords: ISO/IEC 27001, ISMS, information security

1. UVOD

Sigurnost informacija u nekom sistemu je realnost i potreba. Izgradnja „upravljivog" sistema sigurnosti je nužnost u svim organizacijama koje vrše prikupljanje, obradu ili distribuciju povjerljivih podataka. Moderni državni i ekonomski subjekti sve više ovise o kompjuterskoj i komunikacijskoj infrastrukturi. To dovodi do pojave velikog protoka informacija među subjektima, ali ujedno izlaže informacije i njima pripadajuće informacijske sisteme brojnim prijetnjama.
Pojam informacijske sigurnosti ne odnosi se isključivo na tehničke mjere zaštite (korisnička imena, lozinke, enkripciju, prava pristupa i slično), već podrazumijeva administrativne (sigurnosne politike, pravilnici, procedure) i fizičke (video nadzor, zaštita prostorija, fizička kontrola pristupa) mjere.



Slika 1. Korelacija mjera informacijske sigurnosti

Danas se u sve većoj mjeri prepoznaje potreba za uspješnim upravljanjem sigurnošću informacija, te se razvijaju brojni standardi koji daju preporuke za uspostavljanje sistema upravljanja sigurnošću informacija.
Na međunarodnom nivou sve je prihvaćenija norma ISO/IEC 27001 koja daje preporuke za uspješnu implementaciju efikasnog sistema upravljanja. Ovaj sistem je jako fleksibilan, definira upravljački okvir, a ne zadire u konkretnu tehničku implementaciju, što ga čini primjenjivim u različitim organizacijama. To je sistem koji pruža sistemski pristup upravljanju osjetljivim informacijama u 3 glavna aspekta: povjerljivost, integritet i raspoloživost. Norma ISO/IEC 27001 predstavlja širok spektar smjernica za implementaciju sigurnosnih kontrola, pokriva sigurnosne politike, pravne, organizacijske, fizičke i ljudske komponente informacijskih sistema.
Prilikom implementacije sistema za upravljanje sigurnošću informacija po standardu ISO/IEC 27001 potrebno je voditi računa i o primjenjivim zakonskim rješenjima i ugovornim aspektima. U Bosni i Hercegovini se tokom implementacije mora voditi računa o sljedećim zakonskim normama: Zakon o agenciji koji se odnosi na Agenciju za identifikacione dokumente, evidenciju i razmjenu podataka (IDDEEA- nekadašnji CIPS), Zakon o slobodi pristupa informacijama u Bosni i Hercegovini (2000. godina) i Zakon o izmjeni Zakona o slobodi pristupa informacijama u Bosni i Hercegovini (2006. godina).
Iz navedenih Zakona na ovu oblast se posebno odnose pojedini članovi. Tako se kod Zakona o agenciji za ISO/IEC 27001 kao najvažniji članovi mogu smatrati član 9. (pristup, prijenos i razmjena podataka) i član 11. (Tajnost i osiguranje podataka), dok su kod Zakona o slobodi pristupa informacijama u Bosni i Hercegovini najvažniji članovi 1. (Cilj), 4. (Pravo pristupa) i 5. (Utvrđivanje izuzetaka).

2. POTREBA ZA USPOSTAVLJANJEM ISMS-A

Pored zakonskih i ugovornih obaveza potrebno je voditi računa i o propisima nadležnih agencija ili strukovnih udruženja kojima organizacija pripada poput propisa Agencije za bankarstvo koja zahtjeva da sve finansijske institucije implementiraju plan neprekidnosti poslovanja i oporavka u slučaju katastrofe (*business continuity and disaster recovery plan*) ili Etički kodeks za medicinske odnosno zdravstvene informatičare, koji je Svjetska udruga za medicinsku informatiku izdala 2002. godine. Ispunjavanjem uslova standarda se u potpunosti zadovoljavaju i principi i obaveze ovog kodeksa, a uvođenje EU normi o zaštiti ličnih

podataka nameće i svim državnim ustanovama implementaciju većeg dijela kontrola iz Aneksa A standarda ISO/IEC 27001. U Hrvatskoj, koja je na dobrom putu za prijem u EU je donesen zakon o zaštiti ličnih podataka koji se u 95% posto sadržaja podudara sa ISO/IEC 27001. Kako bi bili sigurni da su im podaci zaštićeni u skladu sa najboljim svjetskim normama pojedine županije, kao što je Primorsko-goranska, su certificirale svoje informacione sisteme koje sadrže osjetljive podatke naspram standarda. IPI - Institut za privredni inženjering je prepoznao potencijale ovog standarda i prvi u Bosni i Hercegovini ga implementirao na kompleksnom informacionom sistemu.
„Institut za privredni inženjering“ Zenica je firma za istraživanje i eksperimentalni razvoj, planiranje i projektovanje, konsalting i edukaciju. Osnovan je sa idejom da se promovišu naučni i stručni potencijali, akumulirana znanja i iskustva i infrastruktura Mašinskog fakulteta i Univerziteta u Zenici. IPI čine dvije jedinice: poslovna jedinica „Inžinjering“ i poslovna jedinica „Centar za vozila“.

PJ Inženjering
Aktivnosti ove poslovne jedinice su sljedeće:

- izrada: studija i elaborata, razvojnih i biznis planova, programa, projekata i druge tehničke dokumentacije;
- konsalting: o tehničko-tenološkim i ekonomsko-finansijskim pitanjima, uvođenju i razvoju proizvoda, izboru opreme i investiranju, tržišnom nastupu i promocionim aktivnostima;
- laboratorijske usluge obrade i ispitivanja;
- izvođenje programa obuke i osposobljavanja.

PJ Centar za vozila
Odlukom Vlade FBiH, između Federalnog ministarstva prometa i komunikacija i IPI – Instituta za privredni inžinjering, sklopljen je Ugovor o međusobnim pravima i obavezama, a kojim su na IPI – Institut preneseni sljedeći poslovi:

- stručno osposobljavanje kontrolora tehničke ispravnosti vozila, voditelja stanica tehničkog pregleda i drugih osoba koje rade na stručnim poslovima tehničkog pregleda;
- periodična provjera znanja kontrolora tehničke ispravnosti vozila i drugih osoba koje rade na stručnim poslovima tehničkog pregleda;
- kontrola izvršenog baždarenja opreme kojom se vrši kontrola tehničke ispravnosti vozila
- obrada podataka i izrada analiza iz oblasti tehničkog pregleda vozila;
- izrada pisanih uputstava, informacija i stručnih publikacija iz oblasti tehničkog pregleda vozila;
- uvezivanja stanica za tehnički pregled vozila i drugih zainteresovanih subjekata u jedinstven informatički sistem, vezan za poslove tehničkog pregleda vozila;
- praćenje propisa iz oblasti kontrole ispavnosti vozila koje donose susjedne zemlje, Evropska unija i druge međunarodne organizacije;
- saradnja sa stručnim, naučnim organizacijama, institutima, preduzećima i drugim pravnim licima iz oblasti tehničkog pregleda vozila.

Najkompleksnija obaveza iz prenesenih oblasti je dizajn, implementacija i razvoj informacionog sistema pod imenom a|TEST čiji je cilj prikupljanje podataka o registrovanim vozilima i njihovim vlasnicima sa stanica tehničkog pregleda u realnom vremenu, obrada tih podataka i pružanje statističkih informacija ovlaštenim subjektima. Dio informacija, koje su se odlukom Vlade prikupljale i analizirale, je zaštićen Zakonom o zaštiti ličnih podataka koji je stupio na snagu 2006. godine.

3. ZAKON O ZAŠTITI LIČNIH PODATAKA I ISO/IEC 27001:2005

ISO/IEC 27001 je međunarodna norma koja preporučuje dobru praksu za upravljanje informacijskom sigurnošću. Ova norma ujedno propisuje organizaciju sigurnosnih procesa kako u poslovanju organizacije u cjelini tako i unutar samog informacijskog sistema. Pored uslova standarda, za kompletnu implementaciju potrebno je voditi računa i o zakonskim i ugovornim obavezama subjekta.

Bosna i Hercegovina je 2006. godine donijela Zakon o zaštiti ličnih podataka koji je stupio na snagu objavljivanjem u Službenom glasniku Bosne i Hercegovine br. 49/06. Ovaj se Zakon primjenjuje na osobne podatke koje obrađuju sva javna tijela, fizičke i pravne osobe. Potrebno je razjasniti i neke pojmove koji će se ubuduće sve češće upotrebljavati:

- nositelj podataka je fizička osoba čiji se identitet može ustanoviti ili identificirati, neposredno ili posredno, osobito na temelju jedinstvenog matičnog broja te jednog ili više faktora svojstvenih za fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet te osobe;
- kontrolor je svako javno tijelo, fizička ili pravna osoba, agencija ili drugo tijelo koje samostalno ili zajedno s drugim vodi, obrađuje i utvrđuje svrhu i način obrade osobnih podataka na temelju zakona ili propisa;
- obrađivač je fizička ili pravna osoba, javno tijelo, agencija ili drugo tijelo koje obrađuje osobne/lične podatke u ime kontrolora

Prilikom implementiranja sistema **a|TEST** morali smo, kao obrađivač podataka na osnovu ugovora sa kontrolorom podataka, Ministarstvom saobraćaja i komunikacija, voditi računa o sljedećim stavkama Zakona:

1. Obrađivati samo vjerodostojne i tačne osobne podatke, te ih ažurirati kada je to potrebno; osobne podatke koji su netačni i nepotpuni, s obzirom na svrhu zbog koje su prikupljeni ili se dalje obrađuju, izbrisati ili preinačiti;
2. Kontrolor podataka i, u okviru svoje nadležnosti, obrađivač podataka brinu se o sigurnosti podataka te poduzimaju sve tehničke i organizacijske mjere i utvrđuju pravila postupka koji su nužni za provođenje ovoga Zakona i drugih propisa u vezi sa zaštitom i tajnošću podataka.
3. Kontrolor i obrađivač dužni su poduzeti mjere protiv neovlaštenog ili slučajnog pristupa osobnim podacima, mijenjanja, uništavanja ili gubitka podataka, neovlaštenog prijenosa, drugih oblika nezakonite obrade podataka, kao i mjere protiv zloupotrebe osobnih podataka. Ova obveza ostaje na snazi i nakon završetka obradbe podataka.
4. Kontrolor i, u okviru svoje nadležnosti, obrađivač podataka dužni su sačiniti plan za osiguranje podataka kojim se određuju tehničke i organizacijske mjere za sigurnost ličnih podataka.
5. Obrada podataka preko obrađivača mora biti regulirana ugovorom između kontrolora i obrađivača u kojem se navode: opseg, svrha i rok na koji je sporazum zaključen, te odgovarajuća jamstva obrađivača u vezi s tehničkom i organizacijskom zaštitom osobnih podataka.
6. Uposlenici kontrolora ili obrađivača, ostale fizičke osobe koje obrađuju osobne podatke na temelju ugovora zaključenog s kontrolorom ili obrađivačem i ostale osobe koje u sklopu primjene zakonom propisanih prava i obavljanja dužnosti dođu u kontakt s osobnim podacima u prostorijama kontrolora ili obrađivača, dužne su čuvati tajnost osobnih podataka i pridržavati se utvrđenog načina osiguranja.
7. Osobni podaci koje obrađuju kontrolor ili obrađivač podataka za uposlenike predstavljaju službenu tajnu.
8. Obaveza čuvanja tajnosti osobnih podataka ostaje na snazi i nakon prestanka radnoga odnosa, odnosno određene zadaće.

Unutar sistema a|TEST ove zakonske norme su zadovoljene kroz sljedeće karakteristike:

- Podaci koji se unose sa ličnih dokumenata prolaze kroz aplikaciju koja očekuje isključivo slova ili brojeve, uz ograničenje polja ukoliko je te moguće. Sve osobe koje unose podatke u sistem su prethodno obučene za taj posao. Uneseni podaci se zatim upoređuju sa podacima iz CIPS baze kako bi se potvrdio njihov integritet. Ukoliko se podaci ne podudaraju, korisnik se obavještava o problemu a aplikacija kreira izvještaj. Ukoliko se greška ponovi još jednom sistem automatski šalje E-mail i SMS saradniku za nadzor. Svi podaci se čuvaju u skladu sa zahtjevima Vlade Federacije Bosne i Hercegovine.
- Kako bi zaštitili povjerljivost i dostupnost podataka implementiran je niz tehničkih i organizacijskih mjera od „Politike sigurnosti“ i „Kontrole pristupa“ do mrežnih i lokalnih sistema za detekciju i prevenciju upada (HIDS/NIDS). Pored toga vrši se kontinuirana provjera dostupnosti klijenata i lokalnih resursa sa automatskom notifikacijom administratora ukoliko se desi problem iznad predefinisanog nivoa opasnosti.
- Kroz analizu rizika smo uvidjeli da je najveća opasnost koja prijeti povjerljivosti podataka ljudski faktor. Pored uposlenika Kontrolora i Obrađivača do povjerljivih informacija mogu doći i treća lica (lica koja rade na održavanju opreme, dobavljači, električari, čuvari, čistači). Kako bi spriječili curenje podataka kroz Kontrolu pristupa su razdvojena pristupna prava kako niko ne bi imao tzv. superprivilegije, a pored toga sva lica koja mogu doći u kontakt sa povjerljivim podacima moraju potpisati Sporazum o čuvanju informacija ukoliko klauzule o čuvanju sigurnosti informacija nisu već uključene u ugovor. Osobe koje nemaju dozvolu za pristup povjerljivim podacima do njih ne mogu doći slučajno.
- Svi podaci su klasifikovani u skladu sa internom i zakonskom regulativom i njihova klasifikacija je jasno vidljiva na naslovnici dokumenta ili medija. Podaci se u na osnovu klasifikacije pohranjuju na odgovarajući zaštićene lokacije.

4. ZAKLJUČAK

Trenutno u svijetu ima više hiljada ISMS-ova implementiranih u javnim organima, sudskim, obrazovnim i medicinskim ustanovama, telekomunikacionim firmama, projektnim i advokatskim i IT firmama i svim ostalim organizacijama koje u svojem radu prikupljaju, obrađuju ili na bilo koji drugi način koriste povjerljive podatke.
S obzirom da je ISO/IEC 27001 jedini standard koji u potpunosti obuhvata ne samo IT nego i druge aspekte sigurnosti podataka, trenutno je nezamjenjiv prilikom implementacije sistema upravljanja sigurnošću informacija. Implementacijom ovog standarda ne samo da ispunjavamo norme koje je pred nas stavila direktiva EU 95/46/EC i Zakon o zaštiti ličnih podataka već nam omogućava da u slučaju da se i desi neki sigurnosni incident, pošto, kao što znamo, nijedan sistem nije 100% siguran, znamo ko je odgovoran za propust i omogućava nam da dođemo do uzroka nesigurnosti i u prihvatljivom roku ga eleminišemo.
Sigurnost informacije u službi kvaliteta doprinosi poslovnom uspjehu.

5. LITERATURA

[1] ISO/IEC 27001:2005, Zahtjevi za sistem upravljanja sigurnošću informacija (ISMS)
[2] Zakon o agenciji za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine.,
[3] Zakon o slobodi pristupa informacijama u Bosni i Hercegovini, 2000.,
[4] Zakon o izmjeni Zakona o slobodi pristupa informacijama u Bosni i Hercegovini, 2006.,
[5] Zakon o zaštiti ličnih podataka (Službeni glasnik Bosne i Hercegovine br. 49/06).,
[6] Directive 9S/46/EC of the European Parliament and of the council Of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal of the European Communities, 23. 11. 95).,
[7] IMIA Code of Ethics for Health Information Professionals. International Medical Informatics Association. http://www.imia.org/English_code_of_ethics.html