FBIM Transactions

OBAVEZA PODUZIMANJA TEHNIČKIH MJERA ZAŠTITE PODATAKA TEMELJEM EU UREDBE O ZAŠTITI PODATAKA

OBLIGATION TO IMPLEMENT TECHNICAL MEASURES FOR DATA PROTECTION BASED ON EU GDPR

Haris Hamidović
MKF/MKD EKI Sarajevo, Sarajevo, Bosna i Hercegovina

JEL kategorija rada: **K22, M15**

Apstrakt

25. maja 2018. godine u svim zemljama Evropske unije stupila je na snagu Uredba o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka - Uredba). Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere radi osiguravanja poštovanja uslova ove Uredbe. Za kršenje odredbi koje se odnose na sigurnost obrade predviđene su upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu. U ovom radu predstavljamo obaveze provođenja odgovarajućih tehničkih i organizacijskih mjera zaštite ličnih podataka i mogućnost korištenja međunarodnih standarda za dokazivanje sukladnosti.

Ključne reči: *informacijska sigurnost, privatnost, GDPR, ISMS, PIMS, ISO/IEC 27001, ISO/IEC CD 27552*

Abstract

On 25 May 2018 in all countries of the European Union came into force The General Data Protection Regulation – GDPR. The protection of the rights and freedoms of individuals with regard to the processing of personal data requires that appropriate technical and organizational measures be taken to ensure compliance with the requirements of this Regulation. For breaches of the provisions relating to the security of processing, administrative fines of up to EUR 10 000 000 are envisaged, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. In this paper, we present the obligations of carrying out the appropriate technical and organizational measures for the protection of personal data and the demonstration of conformity with the use of international standards.

Keywords: *information security, privacy, GDPR, ISMS, PIMS, ISO/IEC 27001, ISO/IEC CD 27552*

Adresa autora:
Haris Hamidović
haris.hamidovic@eki.ba

1. UVOD

Sukladno tekstu preambule Opšte uredbe o zaštiti podataka svaka obrada ličnih podataka trebala bi biti zakonita i poštena. Za pojedince bi trebalo biti transparentno kako se lični podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti lični podaci obrađuju ili će se obrađivati. Načelom transparentnosti traži se da svaka informacija i komunikacija u vezi s obradom tih ličnih podataka bude lahko dostupna i razumljiva te da se upotrebljava jasan i jednostavan jezik. To se načelo posebno odnosi na informacije ispitaniku o identitetu voditelja obrade i svrhama obrade te daljnje informacije radi osiguravanja poštenosti i transparentnosti obrade s obzirom na pojedince o kojima je riječ i njihovo pravo da dobiju potvrdu i na obavješetenje o ličnim podacima koji se obrađuju, a koji se odnose na njih. Pojedinci bi trebali biti upoznati s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom ličnih podataka i načinom ostvarenja svojih prava u vezi s obradom. Posebno, određena svrha u koju se lični podaci obrađuju trebala bi biti izrijekom navedena i opravdana te određena u vrijeme prikupljanja ličnih podataka. Lični podaci trebali bi biti primjereni, bitni i ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju. Zbog toga je posebno potrebno osigurati da je razdoblje u kojem se lični podaci pohranjuju ograničeno na strogi minimum. Lični podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima. Radi osiguravanja da se lični podaci ne drže duže nego što je nužno, voditelj obrade trebao bi odrediti rok za brisanje ili periodično preispitivanje. Trebalo bi poduzeti svaki razumno opravdani korak radi osiguravanja da se netačni lični podaci isprave ili izbrišu. I na kraju, a što je i tema ovog rada, lične podatke bi trebalo obrađivati uz odgovarajuće poštovanje sigurnosti i povjerljivosti ličnih podataka, što obuhvaća i sprečavanje neovlaštenog pristupa ličnim podacima i opremi kojom se koristi pri obradi podataka ili njihove neovlaštene upotrebe. (Uredba, 2016)

2. TEHNOLOŠKI RAZVOJ I IZAZOVI U ZAŠTITI LIČNIH PODATAKA

Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti ličnih podataka, navodi se u preambuli Opšte uredbe o zaštiti podataka. Opseg prikupljanja i razmjene ličnih podataka značajno se povećava. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje upotreba ličnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje lične informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i privredu i društveni život te bi trebala dalje olakšavati slobodan protok ličnih podataka u Evropskoj uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visok nivo zaštite ličnih podataka. (Uredba, 2016)

Pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli, kao što su adrese internetskog protokola, identifikatori kolačića ili drugim identifikatorima poput oznaka za radiofrekvencijsku identifikaciju. Tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju, a što je i prepoznato odredbom člana 4. Opšte uredbe o zaštiti podataka koja proširuje definiciju „ličnih podataka" na sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi - izravno ili neizravno, posebno uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više elemenata svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. (Uredba, 2016)

Temeljem člana 6. Opšte uredbe o zaštiti podataka obrada ličnih podataka je zakonita i ukoliko je ispitanik dao privolu za obradu svojih ličnih podataka u jednu ili više posebnih svrha. Privola bi se trebala davati jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu ličnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili

usmene izjave, navodi se u preambuli Opšte uredbe o zaštiti podataka To bi moglo obuhvaćati označivanje polja kvačicom pri posjetu internetskim stranicama, biranje tehničkih postavaki usluga informacijskog društva ili drugu izjavu ili ponašanje koje jasno pokazuje u tom kontekstu da ispitanik prihvaća predloženu obradu svojih ličnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom. Bitno je napomenuti da ukoliko se obrada temelji na privoli ispitanika, voditelj obrade trebao bi moći dokazati da je ispitanik dao privolu za postupak obrade. (Uredba, 2016)

Obrada ličnih podataka je zakonita i ukoliko je nužna i proporcionalna za potrebe osiguravanja sigurnosti mreže i informacija, odnosno sposobnosti mreže ili informacijskog sistema da se odupre, na danom stepenu povjerljivosti, slučajnim događajima ili nezakonitim ili zlonamjernim radnjama koje ugrožavaju dostupnost, autentičnost, integritet i povjerljivost pohranjenih ili prenesenih ličnih podataka te sigurnost povezanih usluga koje nude ili koje su dostupne putem tih mreža i sistema, koju provode tijela javne vlasti, jedinice za hitne računarske intervencije (CERT-ovi), jedinice za računarske sigurnosne incidente (CSIRT-ovi), pružatelji elektroničkih komunikacijskih mreža i usluga te davatelji sigurnosnih tehnologija i usluga. To bi, na primjer, moglo uključivati sprečavanje neovlaštenog pristupa elektroničkim komunikacijskim mrežama i širenja zlonamjernih kodova te zaustavljanje napada „uskraćivanjem usluge" te sprečavanje štete na računarskim i elektroničkim komunikacijskim sustavima, navodi se u preambuli Opšte uredbe o zaštiti podataka. (Uredba, 2016)

Nadalje, kako bi se osiguralo da pojedincima nije uskraćena zaštita na koju imaju pravo temeljem Opšte uredbe o zaštiti podataka, na obradu ličnih podataka ispitanika koji se nalaze u Evropskoj uniji, a koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Evropskoj uniji, trebala bi se primjenjivati ova Uredba i ako su aktivnosti obrade povezane s ponudom robe ili usluga takvim ispitanicima, bez obzira na to ima li ta ponuda veze s plaćanjem. Kako bi se utvrdilo nudi li takav voditelj obrade ili izvršitelj obrade robu ili usluge ispitanicima koji se nalaze u Evropskoj uniji, trebalo bi utvrditi je li očito da voditelj obrade ili izvršitelj obrade namjerava ponuditi usluge ispitanicima koji se nalaze u jednoj ili više država članica Evropske unije. Iako su sama dostupnost internetskih stranica voditelja obrade, izvršitelja obrade ili posrednika u Evropskoj uniji ili adrese elektroničke pošte i drugih kontaktnih podataka ili korištenje jezikom koji je općenito u upotrebi u trećoj zemlji u kojoj voditelj obrade ima poslovni nastan nedovoljni za utvrđivanje takve namjere, elementi kao što je korištenje jezikom ili valutom koji su općenito u upotrebi u jednoj ili više država članica s mogućnošću naručivanja robe i usluga na tom drugom jeziku, ili spominjanje kupaca ili korisnika koji se nalaze u Evropskoj uniji, mogu jasno pokazati da voditelj obrade namjerava nuditi robu ili usluge ispitanicima u Evropskoj uniji. (Uredba, 2016)

Temeljem člana 35. Opšte uredbe o zaštiti podataka ako je vjerojatno da će neka vrsta obrade, posebno putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu ličnih podataka. U slučajevima gdje nije jasno da li je procjena učinka na zaštitu podataka potrebna, EU WP29 radna grupa preporučuje da se ipak provede, zato što je ona koristan alat koji pomaže voditeljima obrade da budu u skladu sa zahtjevima Opšte uredbe o zaštiti podataka. Zahtjevi Opšte uredbe o zaštiti podataka ne diktiraju neki određeni metodološki ili standardni pristup kako bi se izvodila procjena učinka na zaštitu podataka, no koriste smjernice se mogu naći u međunarodnim standardima kao što je ISO/IEC 29134 ili ISO 22307. (Hamidovic, 2010) (Babić, 2018)

3. TEHNIČKE I ORGANIZACIJSKE MJERE ZAŠTITE

Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere radi osiguravanja poštovanja uslova Opšte uredbe o zaštiti podataka. Radi dokazivanja sukladnosti sa Uredbom voditelj obrade trebao bi uvesti interne

politike i provesti mjere koje osobito ispunjavaju načela tehničke zaštite podataka i integrirane zaštite podataka. (Hamidović, 2013) (Uredba, 2016) Takve mjere mogle bi se, među ostalim, sastojati od smanjenja količine obrade ličnih podataka, pseudonimizacije ličnih podataka što je prije moguće, transparentnosti u vezi s funkcijama i obradom ličnih podataka, omogućavanja ispitaniku da prati obradu podataka, omogućavanja voditelju obrade da stvara i poboljšava sigurnosne značajke. Prilikom razvijanja, osmišljavanja, odabira i upotrebe aplikacija, usluga i proizvoda koji se temelje na obradi ličnih podataka ili obrađuju lične podatke kako bi ispunili svoju zadaću, proizvođače proizvoda, usluga i aplikacija trebalo bi poticati da uzmu u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija i da uzimajući u obzir najnovija dostignuća osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka. Načela tehničke i integrirane zaštite podataka trebalo bi također uzeti u obzir u kontekstu javnih natječaja. (Uredba, 2016)

Temeljem člana 83. Opšte uredbe o zaštiti podataka za kršenja odredaba u vezi zaštite ličnih podataka mogu se izreći upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, ovisno o tome što je veće. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna pozornost, između ostalog, posvećuje se (Uredba, 2016):

(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s članovima 25. i 32.

Predmetni članovi Opšte uredbe o zaštiti podataka glase:

Član 25. Tehnička i integrirana zaštita podataka

1. Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih nivoa vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.

2. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo lični podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih ličnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Tačnije, takvim se mjerama osigurava da lični podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.

3. Odobren mehanizam certificiranja sukladno članu 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavaka 1. i 2. ovog člana.

Član 32. Sigurnost obrade

1. Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih nivoa vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajući nivo sigurnosti s obzirom na rizik, uključujući prema potrebi:

(a) pseudonimizaciju i enkripciju ličnih podataka;

(b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sistema usluga obrade;

(c) sposobnost pravodobne ponovne uspostave dostupnosti ličnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;

(d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

2. Prilikom procjene odgovarajućeg nivoa sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ličnih podataka ili neovlaštenog pristupa ličnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

3. Poštovanje odobrenog kodeksa ponašanja iz člana 40. ili odobrenog mehanizma certificiranja iz člana 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavka 1. ovog člana.

4. Voditelj obrade i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću voditelja obrade ili izvršitelja obrade, a koji ima pristup ličnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obvezan učiniti prema pravu Unije ili pravu države članice.

Osim toga, kako bi se osiguralo poštovanje zahtjeva iz Opšte uredbe o zaštiti podataka u vezi s obradom koju provodi izvršitelj obrade u ime voditelja obrade, pri povjeravanju aktivnosti obrade izvršitelju obrade, voditelj obrade trebao bi angažirati samo izvršitelje obrade koji u zadovoljavajućoj mjeri jamče, osobito u pogledu stručnog znanja, pouzdanosti i resursa, provedbu tehničkih i organizacijskih mjera koje udovoljavaju zahtjevima iz Uredbe, među ostalim u pogledu sigurnosti obrade. (Uredba, 2016)

4. DOKAZIVOST USKLAĐENOSTI SA ZAHTJEVIMA UREDBE

Opštom uredbom o zaštiti podataka države članice, nadzorna tijela, Odbor i Komisija se potiču na uspostavu mehanizama certificiranja zaštite podataka te pečata i oznaka za zaštitu podataka u svrhu dokazivanja da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s ovom Uredbom.

Određeni mehanizami certificiranja postoje već izvjesno vrijeme na EU tržištu. Jedan od njih je i EuroPriSe certifikat namijenjen proizvođačima i prodavačima IT proizvoda i IT servisa. Proizvodi koji se mogu certifikovati su hardverski (kao npr. firewall) i softverski (kao npr. baza podataka). IT servisi su servisi kao naprimjer online bankarstvo, email servisi i slično. Predmet certifikovanja može biti proizvod u cjelini, dio proizvoda te više proizvoda zajedno, a isto se odnosi i na IT servise. EuroPriSe je certifikat koji izdaje nezavisna treća strana i koji potvrđuje da su IT proizvodi i IT bazirani servisi u skladu sa evropskim regulativama o privatnosti i sigurnosti podataka. Projekat je pokrenut u junu 2007. godine sa fondom od 1,3 miliona eura, a finansiran je od strane Evropske komisije. U martu 2009. EuroPriSe je preuzet od strane ULD (Unabhängiges Landeszentrum für Datenschutz - Nezavisni Centar za zaštitu podataka), Ured povjerenika za zaštitu podataka i slobodu informacija Schleswig-Holstein, Njemačka.

U EuroPriSe navode da se prilikom procesa tehničke evaluacije potrebna dubina tehničke kontrole može znatno smanjiti ukoliko podnositelj zahtjeva za EuroPriSe certifikat posjeduje široko priznat certifikat kao što je ISO / IEC 27001, koji je aktualan i relevantan za predmetni cilj procjene. Osim toga, navodi se da će budući međunarodni standard ISO / IEC 27552 ("PIMS standard") bit će još korisniji u ovom pogledu nego što je ISO / IEC 27001 danas. (Meissner, 2017) Korisne smjenice u vezi kontrola sigurnosti takođe se mogu naći i u ISO/IEC 27018 i ISO/IEC 29151.

Korištenje međunarodnih standarda kao okvira za implementaciju i procjenu zahtjeva informacijske sigurnosti već je korištena praksa od strane EU regulatora u sektoru telekomunikacija. (Hamidović, 2012) Dokument „Tehničke smjernice za minimalne sigurnosne mjere" predstavlja smjernice za nacionalna regulatorna tijela u vezi provedbe članka 13a EU Direktive 2009/140/EC, a posebno u vezi sigurnosnih mjera koje pružatelji javnih komunikacijskih usluga moraju poduzeti kako bi se osigurala sigurnost i integritet njihovih mreža. Ovaj dokument navodi minimalne sigurnosne mjere koje nacionalna regulatorna tijela trebaju uzeti u obzir prilikom ocjenjivanja usklađenosti pružatelja javnih komunikacijskih usluga sa stavkama 1. i 2. članka 13a EU Direktive 2009/140/EC. Minimalne sigurnosne mjere izvedene su iz skupa međunarodnih i nacionalnih standarda koji se

obično koriste u telekomunikacijskim organizacijama, kao što su:

- ISO/IEC 27001 i ISO/IEC 27002 za sistem upravljanja informacijskom sigurnošću,
- ISO/IEC 27005 za upravljanje rizikom informacijske sigurnosti,

BS 25999-1 i BS 25999-2 za upravljanje kontinuitetom poslovanja i dr

Sukladno tekstu preambule Opšte uredbe o zaštiti podataka osoba sa stručnim znanjem prakse zaštite podataka trebala bi pomagati voditelju obrade ili izvršitelju obrade pri praćenju unutarnje usklađenosti s ovom Uredbom. (Uredba, 2016) Osim korištenja međunarodnih standarda kao okvira za implementaciju sistema informcijske sigurnosti u vezi zaštite ličnih podataka, francuska nacionalna Agencija za zaštitu privatnosti i podataka korisnika – CNIL preporučuje da se i prilikom procjene stručnosti pojedinaca koji se bave pitanjima tehničke zaštite ličnih podataka koriste poznate i priznate certifikacijske sheme kao što su CISSP - Certified Information Systems Security Professional, CISM - Certified Information Security Manager, ISO 27001 Auditor i dr. (CNIL, 2018)

5. ZAKLJUČCI

Rizik za prava i obaveze pojedinaca, različitih vjerojatnosti i ozbiljnosti, može proizaći iz obrade ličnih podataka koja bi mogla prouzročiti fizičku, materijalnu ili nematerijalnu štetu, posebno ako ta obrada može dovesti do diskriminacije, krađe identiteta ili prijevare, finansijskog gubitka, štete za ugled, gubitka povjerljivosti ličnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije, ili bilo koje druge znatne ekonomske ili društvene štete.

Opšta uredbe o zaštiti podataka adresira, između ostalog, rješavanje pitanja rascjepkanosti provedbe zaštite podataka u Evropskoj uniji, pravne nesigurnosti i rasprostranjenog javnog mišljenja da osobito kod internetskih aktivnosti postoje znatni rizici povezani sa zaštitom pojedinaca.

Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere zaštite ličnih podataka. Uredbom se od organizacija zahtijeva dokaziva usklađenost, a što se može realizovati i kroz akreditirane mehanizme certifikacije.

Budući da je Sporazumom o stabilizaciji i pridruživanju Bosna i Hercegovina preuzela obavezu usklađivanja svog zakonodavstva vezano za zaštitu ličnih podataka s pravom Zajednice i drugim evropskim i međunarodnim zakonodavstvom o privatnosti, privredni subjekti u Bosni i Hercegovini, ali i drugim državama kandidatkinjama za pristup EU, bi trebali izvršiti procjenu implementiranih tehničkih i organizacijskih mjera zaštite ličnih podataka i njihove usklađenosti sa zahtjevima iz Opšte uredbe o zaštiti podataka. Kao okvir za implemantaciju i procjenu tehničke usklađenosti mogu se koristiti priznati međunarodni standardi iz oblasti informacijske sigurnosti kao što su ISO/IEC 27001, a posebno standard u razvoju ISO/IEC 27552.

CITIRANI RADOVI

Babić. T. (2018). Procjena rizika i procjena učinka na zaštitu podataka Preuzeto sa: http://www.gdpr-simpozij.com/assets/00---procjena-rizika-i-procjena-ucinka-na-zastitu-podataka.pdf Pristupljeno 24.08.2018

CNIL. (2018). Privacy Impact Assessment (PIA) 3 : knowledge bases. Commission Nationale de l'Informatique et des Libertés

Hamidovic, H. (2010). An Introduction to the Privacy Impact Assessment Based on ISO 22307. ISACA Journal. Volume 4, 2010, The Information Systems Audit and Control Association

Hamidović, H. (2012). EU smjernice iz oblasti informacijske sigurnosti u sektoru telekomunikacija. Telekomunikacije. God.11, br. 37, 2012, Bosanskohercegovačko udruženje za telekomunikacije Sarajevo

Hamidović, H. (2013). Opći model upravljanja zakonskim zahtjevima informacijske sigurnosti. Zbornik radova sa Treće internacionalne naučne konferencije "Ekonomija integracija" ICEI 2013 „Znanjem od recesije ka prosperitetu", održane od 6. – 7. decembar 2013. god. Tuzla, Bosna i Hercegovina, Univerzitet u Tuzli

Meissner S. (2017). Experiences from data protection certification and the use of standards orthe lack thereof Preuzeto sa: https://www.enisa.europa.eu/events/enisa-cscg-2017/enisa-cscg-2017-agenda Pristupljeno 23.08.2018

Standard. (2013). ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Standard. (2014). ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Standard. (2017). ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Standard. (2017). ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Standard. (2018). ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Uredba. (2016, maj 4). Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Službeni list Europske unije, L 119/1