PROCJENA UČINKA NA ZAŠTITU LIČNIH PODATAKA

PRIVACY IMPACT ASSESSMENT

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

JEL Kategorija rada: K22, M15

Apstrakt

Integracija zahtjeva privatnosti u dizajn informacionog sistema nije jednostavan zadatak. Kao prvo, privatnost je sama po sebi složen, višestruk i kontekstualni pojam. Osim toga, pitanje privatnosti uglavnom nije primarni zahtjev sistema, a ponekad čak ovaj zahtjev može doći i u sukob s drugim (funkcionalnim ili nefunkcionalnim) zahtjevima sistema. Stoga je od najveće važnosti da se precizno definišu ciljevi privatnosti u procesu realizovanja privatnosti po dizajnu. Jedan od načina da se definišu ciljevi informacionog sistema u smislu zahtjeva privatnosti je provođenje procjene učinka na zaštitu podataka ili analize rizika privatnosti. Provođenje procjene učinka na zaštitu podataka u skladu je i sa načelima tehničke i integrisane zaštite podataka iz člana 25. Opšte uredbe o zaštiti podataka EU - GDPR. U skladu s načelima tehničke i integrisane zaštite podataka procjenu učinka na zaštitu podataka trebalo bi provesti prije same obrade, a s ciljem korištenja iste kao pomoćnog alata za donošenje odluka o obradi, a posebice izbora odgovarajućih mjera tehničke i integrisane zaštite. Iako Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost u smjernicama Radne skupine za zaštitu podataka iz članka 29 EU navedene su preporuke za korištenje međunarodnih standarda. U radu je ukratko predstavljena metoda procjene učinka na zaštitu podataka temeljem preporuka francuske agencije za zaštitu privatnosti podataka i preporuka međunarodnih standarda ISO/IEC 29134 i ISO/IEC 27005.

Ključne reči: *privatnost, lični podaci, zaštita podataka, procjena učinka na privatnost, GDPR, PIA, ISO/IEC 29134*

Abstract

Integrating the privacy requirement in the information system design is not an easy task. First of all, privacy is a complex, multiple, and contextual concept in itself. In addition, the issue of privacy is not a primary requirement of the system, and sometimes even this requirement can come into conflict with other (functional or non-functional) requirements of the information system. Therefore, it is of utmost importance to precisely define the objectives of privacy in the process of realizing privacy by design. One way to define the objectives of the information system in terms of the privacy requirement is to conduct a privacy impact assessment or a privacy risk analysis. Conducting a privacy impact assessment is in line with the principles of technical and integrated

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

data protection under Article 25 of the General Data Protection Regulation – GDPR. In accordance with the principles of technical and integrated data protection, a privacy impact assessment should be carried out before the processing itself with the aim of using it as a tool for decision-making, in particular for the selection of appropriate technical protection measures. Although the General Data Protection Regulation does not prescribe any specific methodology or standard for privacy impact assessment in the guidelines of the Article 29 Working Group on Data Protection, there are recommendations for the use of international standards. This paper presents the method of privacy impact assessment based on the recommendations of the French Data Protection Agency and the recommendations of international standards ISO/IEC 29134 and ISO/IEC 27005.

Keywords: *privacy, personal data, data protection, privacy impact assessment, GDPR, PIA, ISO/IEC 29134*

1. UVOD

Opšta uredba o zaštiti podataka EU - Uredba, koja je na snazi od 25. maja 2018. uvodi koncept procjene učinka na zaštitu podataka. Procjena učinka na zaštitu podataka je postupak osmišljen za opisivanje obrade, procjenu njezine nužnosti i proporcionalnosti te pružanje pomoći u upravljanju rizicima za prava i slobode pojedinaca koji nastaju obradom ličnih podataka, njihovom procjenom i određivanjem mjera za njihovo uklanjanje. Provođenje procjene učinka na zaštitu podataka važno je za odgovornost, jer pomaže voditeljima obrade da se usklade sa zahtjevima Opšte uredbe o zaštiti podataka i da dokažu da su poduzete potrebne mjere za osiguravanje usklađenosti s Uredbom. Drugim riječima, procjena učinka na zaštitu podataka postupak je za uspostavu i dokazivanje usklađenosti, naglašava se iz Radne skupine za zaštitu podataka iz članka 29. (Smjernica, 2017) (Uredba, 2016)

U skladu s Opštom uredbom o zaštiti podataka neusklađenost sa zahtjevima procjene učinka na zaštitu podataka može rezultirati novčanim kaznama koje izriče nadležno nadzorno tijelo. Propust u provođenju procjene učinka na zaštitu podataka u slučaju da obrada podliježe njezinu provođenju, neispravno provođenje procjene učinka na zaštitu podataka, ili nesavjetovanje s nadležnim nadzornim tijelom kad je to potrebno može rezultirati upravnim novčanim kaznama do najviše 10 miliona EUR ili, u slučaju preduzeća, do 2% ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, ovisno o tome koji je iznos viši. (Smjernica, 2017) (Uredba, 2016)

Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost. Međutim, u smjernicama Radne skupine za zaštitu podataka iz člana 29 EU (eng. Article 29 Working Party - Art. 29 WP)) prezentirane su neke preporuke, kao što je ISO/IEC 29134, Informaciona tehnologija – Sigurnosne tehnike - Smjernice za procjenu utjecaja na privatnost. U nastavku rada predstavljemo osnovne smijernice za provođenje procjena učinka na zaštitu podataka temeljem dobrih praksi predstavljenih od strane francuske agencije za zaštitu privatnosti podataka (CNIL) i međunarodnih standarda.

2. OBAVEZA PROVOĐENJA PROCJENE UČINKA NA ZAŠTITU PODATAKA

U skladu s pristupom temeljenim na riziku, utvrđenim u Opšoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obavezno za svaki postupak obrade. Procjena učinka na zaštitu podataka potrebna je ako će obrada vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca: „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“. (član 35. stav 1. Uredbe)

Jedna procjena učinka na zaštitu podataka može se upotrijebiti za procjenu višestrukih postupaka obrade koji su slični s obzirom na prirodu, opseg, kontekst, svrhu i rizike. To može biti slučaj ako se koristi slična tehnologija za prikupljanje iste vrste podataka u iste svrhe. Art. 29 WP navodi kao primjer, skupinu opštinskih tijela, od kojih svako postavlja sličan sistem kamera televizije zatvorenog kruga (CCTV), gdje se može provesti jedna procjena učinka na zaštitu podataka koja obuhvaća postupke pojedinačnih voditelja obrade

ili primjer željezničkog prijevoznika (jedan voditelj obrade) gdje se mogu jednom procjenom učinka na zaštitu podataka obuhvatiti sve nadzorne kamere na svim željezničkim stanicama. To može biti primjenjivo i u sličnim postupcima obrade koje provode razni voditelji obrade podataka. U tim je slučajevima referentnu procjenu učinka na zaštitu podataka potrebno zajednički upotrebljavati ili učiniti javno dostupnom, moraju se provesti mjere opisane u procjeni učinka na zaštitu podataka, a provođenje jedne procjene učinka na zaštitu podataka potrebno je obrazložiti, navode iz Art. 29 WP. (Smjernica, 2017)

Procjena učinka na zaštitu podataka može biti korisna i u procjeni učinka nekog tehnološkog proizvoda na zaštitu podataka, na primjer neke opreme ili nekog računarskog programa, koje će različiti voditelji obrade podataka vjerojatno upotrebljavati za provođenje različitih postupaka obrade. Art. 29 WP naglašava da u ovom slučaju voditelj obrade podataka koji upotrebljava proizvod i dalje mora provesti vlastitu procjenu učinka na zaštitu podataka s obzirom na specifičnu provedbu, ali te se informacije mogu nalaziti i u procjeni učinka na zaštitu podataka koju prema potrebi priprema dobavljač proizvoda. (Smjernica, 2017)

U smjernicama Radne skupine za zaštitu podataka iz članka 29 se navodi i pojašnjava sljedećih devet kriterija koje je potrebno uzeti u obzir prilikom procjene da li namjerava obrada zahtijeva provođenje procjene učinka na zaštitu podataka. Predmetne kriterije detaljno navodimo u nastavku (Smjernica, 2017):

"1. Procjena ili bodovanje, uključujući izradu profila i predviđanje, posebno na temelju aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, ličnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja. Primjeri mogu obuhvaćati finansijsku instituciju koja provjerava svoje klijente u referentnoj bazi podataka o kreditnoj sposobnosti, u bazama podataka o suzbijanju pranja novca i financiranja terorizma ili u bazi podataka o prijevarama; biotehnološko preduzeće koje izravno svojim kupcima nudi genetska testiranja radi procjene i predviđanja bolesti/zdravstvenih rizika ili preduzeće koje izrađuje bihevioralne i marketinške profile utemeljene na upotrebi ili pregledavanju njihove internetske stranice.

2. Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom. Obrada čiji je cilj donošenje odluka o ispitanicima proizvodeći pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca. Na primjer, obrada može rezultirati isključivanjem ili diskriminacijom pojedinaca. Obrada čiji je učinak na pojedince neznatan ili nikakav ne odgovara ovom specifičnom kriteriju.

3. Sistemsko praćenje. Obrada koja se koristi za posmatranje, praćenje ili kontrolu ispitanika, uključujući podatke prikupljene putem mreža ili „sistemskog praćenja javno dostupnog područja". Ova je vrsta praćenja jedan od kriterija jer se lični podaci mogu prikupljati u situacijama u kojima ispitanici nisu svjesni tko prikuplja njihove podatke i u koje će svrhe ti podaci biti upotrijebljeni. Usto, pojedinci možda neće moći izbjeći takvu obradu na javnim (ili javno dostupnim) mjestima.

4. Osjetljivi podaci ili podaci vrlo lične prirode. Ovo uključuje posebne kategorije ličnih podataka, kako je utvrđeno u članu 9. Uredbe (na primjer informacije o političkim mišljenjima pojedinaca), kao i lične podatke koji se odnose na krivične osude ili kažnjiva djela, kako je utvrđeno u članu 10 Uredbe. Primjer je opšta bolnica koja čuva medicinsku dokumentaciju pacijenata ili privatni istražitelj koji čuva pojedinosti o prijestupnicima. Osim onoga što je obuhvaćeno odredbama Opšte uredbe o zaštiti podataka, za neke se kategorije podataka može smatrati da povećavaju mogući rizik za prava i slobode pojedinaca. Ti lični podaci smatraju se osjetljivima (kako se uobičajeno i shvaća ovaj pojam) jer su povezani s kućanstvom i privatnim aktivnostima (poput elektronske komunikacije čija povjerljivost treba biti zaštićena) ili zato što utječu na ostvarivanje temeljnog prava (poput lokacijskih podataka čije prikupljanje dovodi u pitanje slobodu kretanja) ili zato što njihova povreda očito podrazumijeva ozbiljne učinke na svakodnevni život ispitanika (poput finansijskih podataka koji mogu biti upotrijebljeni za prijevaru u platnom prometu). U tom pogledu može biti važno je li te podatke

već javno objavio ispitanik ili treća strana. Činjenica da su lični podaci javno dostupni može se smatrati činjenicom u procjeni ako se očekivalo daljnje korištenje tim podacima u određene svrhe. Taj kriterij može obuhvaćati i podatke poput ličnih dokumenata, e-pošte, dnevnika, bilježaka s e-čitača na kojima se mogu praviti bilješke i vrlo ličnih informacija sadržanih u aplikacijama za bilježenje životnih događaja.

5. Opsežna obrada podataka. U Opštoj uredbi o zaštiti podataka nije određeno što obuhvaća pojam „opsežno", ali se u uvodnoj izjavi 91. nalaze određene smjernice. U svakom slučaju, Radna skupina za zaštitu podataka iz članka 29. preporučuje da se, pri utvrđivanju je li obrada opsežna, posebno razmotre slijedeći elementi:
   a. broj uključenih ispitanika, bilo kao određeni broj ili udio relevantnog stanovništva;
   b. količina podataka i/ili niz različitih podataka koji se obrađuju;
   c. trajanje ili stalnost postupka obrade podataka;
   d. zemljopisni opseg aktivnosti obrade.
6. Podudarajući ili kombinirani skupovi podataka, na primjer oni koji potječu iz dva postupka obrade ili više njih, a koji su provedeni u različite svrhe i/ili koje su proveli različiti voditelji obrade podataka na način koji može premašiti razumna očekivanja ispitanika.
7. Podaci koji se odnose na osjetljive ispitanike (uvodna izjava 75.). brada ove vrste podataka jest kriterij zbog povećane neravnoteže moći između ispitanika i voditelja obrade podataka, što znači da pojedinci ne mogu jednostavno dati saglasnost ili se usprotiviti obradi svojih podataka ili ostvarivati svoja prava. Osjetljivi ispitanici mogu biti djeca (smatra se da ne mogu svjesno i promišljeno dati pristanak ili se usprotiviti obradi podataka), zaposlenici, osjetljivije skupine stanovništva koje trebaju posebnu zaštitu (osobe s duševnim smetnjama, tražitelji azila ili starije osobe, pacijenti itd.). Time su obuhvaćene i situacije u kojima se može utvrditi neravnoteža između položaja ispitanika i voditelja obrade.
8. Inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja, poput kombiniranja otisaka prstiju i prepoznavanja lica radi poboljšane kontrole fizičkog pristupa itd. Iz Opšte je uredbe o zaštiti podataka jasno (član 35. stav 1. i uvodne izjave 89. i 91.) da upotreba nove tehnologije, definisane u skladu s postignutim nivoom tehnološkog znanja (uvodna izjava 91.) može dovesti do potrebe za provođenjem procjene učinka na zaštitu podataka. To je zato što upotreba takve tehnologije može obuhvaćati inovativne oblike prikupljanja i upotrebe podataka s mogućim visokim rizikom za prava i slobode pojedinaca. Doista, lične i društvene posljedice implementacije nove tehnologije još nisu posve poznate. Procjena učinka na zaštitu podataka pomoći će voditelju obrade podataka u razumijevanju takvih rizika i postupanju s njima. Na primjer, određene aplikacije „internet stvari" mogu znatno utjecati na svakodnevni život i privatnost pojedinaca; stoga je potrebno provesti procjenu učinka na zaštitu podataka.
9. Situacija u kojoj sama obrada sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora (član 22. i uvodna izjava 91.). To uključuje i postupke obrade kojima se ispitanicima dopušta, mijenja ili odbija pristup pojedinoj usluzi ili sklapanje ugovora. Primjer je banka koja provjerava klijente u referentnoj bazi podataka o kreditnoj sposobnosti pri odlučivanju o dodjeli kredita."

U većini slučajeva, voditelj obrade podataka može smatrati da obrada koja ispunjava bar dva od prethodno navedenih kriterija zahtijeva provođenje procjene učinka na zaštitu podataka. Općenito, Radna skupina za zaštitu podataka iz članka 29 smatra da što je više kriterija ispunjeno obradom, to je veća mogućnost da ona predstavlja visok rizik za prava i slobode ispitanika i stoga je nužno provođenje procjene učinka na zaštitu podataka, bez obzira na mjere koje voditelj obrade namjerava donijeti. (Smjernica, 2017)

Međutim, u određenim slučajevima voditelj obrade podataka može smatrati da je zbog obrade koja ispunjava samo jedan od tih kriterija nužno provesti procjenu učinka na zaštitu podataka. (Smjernica, 2017)

U slijedećim je primjerima prikazano na koji se način trebaju upotrijebiti kriteriji kako bi se procijenilo da li je za određeni postupak obrade nužno provesti procjenu učinka na zaštitu podataka. (Smjernica, 2017)

Primjer obrade 1

Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacijski sistem).

Mogući relevantni kriteriji:
- Osjetljivi podaci ili podaci vrlo lične prirode.
- Podaci koji se odnose na osjetljive ispitanike.
- Opsežne obrade podataka

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebni - DA

Primjer obrade 2

Upotreba sistema nadzornih kamera za praćenje ponašanja vozača na autocestama. Voditelj obrade namjerava upotrijebiti sistem pametne video analize za izdvajanje automobila i automatsko prepoznavanje registarskih tablica.

Mogući relevantni kriteriji:
- Sistemsko praćenje.
- Inovativna upotreba ili primjena tehnoloških ili organizacijskih rješenja.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 3

Preduzeće sistemski prati aktivnosti svojih zaposlenika, uključujući praćenje radne stanice, aktivnost na internetu itd.

Mogući relevantni kriteriji:
- Sistemsko praćenje.
- Podaci koji se odnose na osjetljive ispitanike.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 4

Prikupljanje podataka s javnih društvenih medija za izradu profila.

Mogući relevantni kriteriji:
- Procjena ili bodovanje.
- Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom.
- Sprečava ispitanika u ostvarivanju prava, korištenju uslugom ili ugovorom.
- Osjetljivi podaci ili podaci vrlo lične prirode.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 5

Internetski časopis čiji se urednici koriste popisom adresa za slanje generičkih dnevnih novosti svojim pretplatnicima.

Mogući relevantni kriteriji:
- Osjetljivi podaci.
- Podaci koji se odnose na osjetljive ispitanike.
- Sprečava ispitanike u ostvarivanju prava, korištenju uslugom ili ugovorom.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 6

Pohrana u svrhu arhiviranja pseudonimiziranih ličnih osjetljivih podataka koji se odnose na osjetljive ispitanike u okviru istraživačkih projekata ili kliničkih ispitivanja.

Mogući relevantni kriterij:
- Opsežna obrada podataka.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - NIJE NUŽNO

Primjer obrade 7

Internetska stranica e-trgovine koja prikazuje reklame za dijelove oldtajmera, što obuhvaća i ograničenu izradu profila na temelju pregleda ili kupnji na vlastitoj internetskoj stranici.

Mogući relevantni kriterij:
- Procjena ili bodovanje.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - NIJE NUŽNO

Ako nije jasno je li procjena učinka na zaštitu podataka potrebna, Art. 29 WP preporučuje da se ona ipak provede jer voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka. (Smjernica, 2017)

3. OBAVEZA SAVJETOVANJA SA NADZORNIM TIJELOM

Procjenu učinka na zaštitu podataka potrebno je provesti prije obrade. To je u skladu s načelima tehničke i integrisane zaštite podataka: “Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina 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 …" (Uredba, 2016 – Član 25) (Hamidović, 2019)

Radna skupina za zaštitu podataka iz članka 29 navodi da bi procjenu učinka na zaštitu podataka trebalo posmatrati kao pomoćni alat za donošenje odluka o obradi, te preporučuje da bi s provođenjem procjene učinka na zaštitu podataka trebalo započeti što je prije moguće tijekom planiranja postupka obrade, čak i ako su neki postupci obrade još uvijek nepoznati. Ažuriranjem procjene učinka na zaštitu podataka tijekom trajanja projekta osigurat će se da se vodi računa o zaštiti podataka i privatnosti i potaknut će se iznalaženje rješenja kojima se potiče usklađenost. Pojedine će korake procjene možda biti potrebno ponoviti u tijeku postupka razvoja jer odabir određenih tehničkih ili organizacijskih mjera može utjecati na ozbiljnost i vjerojatnost rizika koje predstavlja obrada. (Smjernica, 2017)

Činjenica da će procjena učinka na zaštitu podataka možda trebati biti ažurirana nakon što obrada stvarno započne nije valjan razlog za odgodu ili neprovođenje procjene učinka na zaštitu podataka. Procjena učinka na zaštitu podataka kontinuiran je proces, posebno ako je postupak obrade dinamičan i podložan stalnim promjenama. Procjena učinka na zaštitu podataka provodi se kontinuirano, a ne jednom. (Smjernica, 2017)

U smjernicama Radne skupine za zaštitu podataka iz članka 29 se navodi kao primjer pohranjivanje ličnih podataka u prijenosni računar uz upotrebu prikladnih tehničkih i organizacijskih sigurnosnih mjera (učinkovito kriptanje cijelog diska, sigurno upravljanje ključem, prikladni nadzor pristupa, zaštićene sigurnosne kopije itd.) uz postojeće politike (obavijest, saglasnost, pravo pristupa, pravo na prigovor itd.). U navedenom primjeru prijenosnog računara, ukoliko voditelj obrade podataka smatra da je rizik dovoljno umanjen te u skladu s tekstom člana 36. stavka 1. i uvodnih izjava 84. i 94., obrada se može nastaviti bez savjetovanja s nadzornim tijelom. Samo u slučajevima u kojima utvrđene rizike voditelj obrade podataka ne može ukloniti na odgovarajući način, (tj. preostali rizici su i dalje visoki), voditelj obrade podataka mora potražiti savjet nadzornog tijela. (Smjernica, 2017)

U vezi sa prethodno navedenim primjerom Radna skupina za zaštitu podataka iz članka 29 napominje da pseudonimizacija i enkripcija osobnih podataka (kao i minimizacija podataka, mehanizmi nadzora itd.) nisu nužno odgovarajuće mjere. Riječ je samo o primjerima. Odgovarajuće mjere ovise o kontekstu i rizicima koji su specifični za postupke obrade.

Primjer neprihvatljivog visokog preostalog rizika uključuje slučajeve u kojima se ispitanici mogu suočiti sa znatnim ili čak nepopravljivim posljedicama, koje možda neće moći ukloniti (npr. neovlašteni pristup podacima kojim se može ugroziti život ispitanika, otpuštanje, financijski rizik) i/ili ako je očito da će doći do pojave rizika (npr. ako se ne može smanjiti broj osoba koje pristupaju podacima zbog razmjene podataka, njihove upotrebe ili načina distribucije ili ako dobro poznata slabost nije uklonjena). (Smjernica, 2017)

Ako voditelj obrade podataka ne može pronaći odgovarajuće mjere za smanjenje rizika na prihvatljiv nivo (tj. ako su preostali rizici i dalje visoki), mora se savjetovati s nadzornim tijelom, a temeljem zahtjeva iz Člana 35 Uredbe "Voditelj obrade savjetuje se s nadzornim tijelom prije obrade ako se procjenom učinka na zaštitu podataka iz članka 35. pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika." (Uredba, 2016)

Trebalo bi međutim istaknuti da, bez obzira na to je li savjetovanje s nadzornim tijelom potrebno s obzirom na nivo preostalog rizika, čuvanje zapisa o procjeni učinka na zaštitu podataka i pravodobno ažuriranje procjene učinka na zaštitu podataka i dalje su nužni. (Smjernica, 2017)

4. PRIMJER METODE PROCJENE RIZIKA

Francuska agencija za zaštitu privatnosti podataka (CNIL) navodi u svojim smjernicama da, što se tiče oblasti privatnosti, primarni rizici koje treba uzeti u obzir su oni koji predstavlja obrada ličnih podataka za privatnost. Ti rizici se sastoje od događaja kojih se plašimo (eng. feared event) (čega se plašimo?) i svih prijetnji koje ih mogu omogućiti (kako se to može dogoditi?) (CNIL, 2012)

Primjeri događaja od kojih strahujemo:

- Podaci o navikama zaposlenih nezakonito se prikupljaju i koriste od strane njihovih nadređenih za usmjeravanje istraživačkih dokaza s ciljem otpuštanja uposlenika.
- Koordinate se preuzimaju i koriste u komercijalne svrhe (spam, ciljano oglašavanje…).
- Identiteti su lažirani za vršenje nezakonitih aktivnosti u ime subjekata podataka, koji se suočavaju sa krivičnim gonjenjem.
- Nakon neželjene modifikacije zdravstvenih podataka, pacijenti su neadekvatno zbrinuti, pogoršava im se stanje što može da uzrokuje invalidnost ili smrt.
- Prijave za socijalnu pomoć nestaju, čime se korisnici lišavaju ovih pogodnosti i prisiljava ih se da ponove administrativne formalnosti.

Da bi se desio događaj od koga strahujemo, mora postojati jedan ili više izvora rizika koji ga uzrokuju, bilo slučajno ili namjerno. Izvori rizika mogu uključivati:

- Osobe koje pripadaju organizaciji - korisnik, kompjuterski stručnjak ...
- Osobe izvan organizacije - primalac, provajder, konkurent, ovlašteno treće lice, vladina organizacija …
- Ne-ljudski izvori - kompjuterski virus, prirodna katastrofa, zapaljivi materijali, epidemija, glodari…

Izvori rizika će djelovati, slučajno ili namjerno, na različite komponente informacionog sistema, na koje se oslanjaju primarna sredstva (procesi i podaci). Ova podržavajuća sredstva mogu uključivati:

- Hardver - računari, komunikacijski releji, USB uređaji, hard diskovi ...
- Softver - operativni sistemi, poruke, baze podataka, poslovne aplikacije…
- Mreže - kablovska, bežična, optička ...
- Ljudi - korisnici, administratori, top menadžment…
- Papirni mediji - štampanje, fotokopiranje ...
- Kanali prijenosa papira - pošta, radni procesi (eng. workflow) ...

Djelovanje izvora rizika na sredstva podrške može se dogoditi kroz različite prijetnje:

- Zloupotreba funkcija - pomoćna sredstva se preusmjeravaju iz svoga namjeravanog konteksta upotrebe bez promjene ili oštećenja istih;
- Špijunaža - prateća sredstva se posmatraju bez oštećenja istih;
- Prekoračene granice operacije - sredstva podrške su preopterećena, pretjerano eksploatisana ili korištena pod uslovima koji im ne dozvoljavaju da pravilno funkcionišu;
- Oštećenje - sredstva podrške su djelomično ili potpuno oštećena;
- Promjene - sredstva podrške se transformišu;
- Imovinski gubici - sredstva podrške su izgubljena, ukradena, prodata ili predata, tako da više nije moguće ostvarivati imovinska prava.

Primjeri prijetnji:

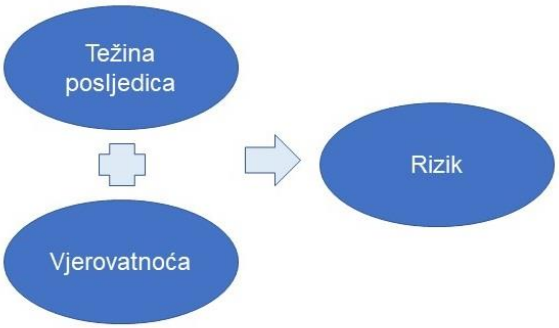
- Zlonamjerni napadač ubacuje neočekivane upite u formu na web lokaciji.
- Tržišni suparnik koji inkognito posjećuje preduzeće i pri tome ukrade prenosivi hard disk.
- Član osoblja greškom uklanja tabele iz baze podataka.
- Štete od vode uzrokuju uništavanje računarskih servera i telekomunikacijske opreme.

CNIL navodi da rizik predstavlja scenarij koji opisuje kako izvori rizika mogu iskoristiti ranjivosti podržavajućih sredstava što vodi do izazivanja incidenta na primarnoj imovini i uticaja na privatnost.

Nivo rizika se procjenjuje u smislu ozbiljnosti i vjerovatnoće.

Ozbiljnost u suštini zavisi od stepena identifikacije ličnih podataka i nivoa posljedica potencijalnih utjecaja.

Vjerovatnoća predstavlja izvedivost dešavanja rizika, i u suštini zavisi od stepena ranjivosti podržavajućih sredstava koji se suočavaju sa nivoom mogućnosti izvora rizika da ih iskoriste.



Slika 1. Određivanje nivoa rizika (CNIL, 2012)

Slika 2 predstavlja sintezu prethodno spomenutih pojmova.

CNIL navodi sljedeću skalu koja se može koristiti za procjenu ozbiljnosti neželjenih događaja (CNIL, 2018):

Slika 2. Komponente rizika (CNIL, 2012)

Tabela 1 Primjeri nivoa utjecaja na temelju vrste ličnih podatak

Vrsta ličnih podataka	Nivo utjecaja
Javno dostupni lični podaci (npr. telefonski direktorij, imenik ili selekcijske liste).	1
Lični podaci koji zahtijevaju opravdani interes za pristup (npr. ograničene javne datoteke ili članovi distribucijskog popisa).	2
Lični podaci čija neovlaštena objava može utjecati na reputaciju nosioca podataka (npr. podaci o prihodima, socijalne naknade, porez na imovinu ili kazne).	3
Lični podaci čija neovlaštena objava, izmjena, gubitak ili uništenje može utjecati na postojanje ili zdravlje, slobodu i život nosioca podataka (npr. informacije o pripadnosti stranci, lične sklonosti, podaci o zdravlju, nepodmireni dugovi, ili ako je pak nositelj podataka pod rizikom da postane žrtva u krivičnom predmetu).	4

1. *Zanemarivo* - Subjekti podataka neće biti pogođeni ili će možda naići na nekoliko neugodnosti koje će moći prevazići bez ikakvih problema, kao na primjer u slučaju gubitaka vremena u ponavljanju već obavljenih formalnosti ili prijema neželjene pošte.
2. *Ograničeno* - Subjekti podataka mogu naići na značajne neugodnosti, koje će moći prevazići uprkos nekoliko poteškoća, kao na primjer u slučaju propuštenih prilika za udobnost (otkazivanje odmora, kupovine, ukidanje online računa), propuštenih prilika za napredovanja u karijeri, prijema neželjenih ciljanih poruka koje bi mogle da oštete reputaciju subjekata podataka.
3. *Značajano* - Subjekti podataka mogu naići na značajne posljedice, koje bi trebali biti u stanju prevazići iako sa stvarnim i ozbiljnim poteškoćama, kao na primjer u slučaju zloupotrebe novca subjekta podataka koji nije nadoknađen, gubitka zaposlenja ili razvoda.
4. *Maksimalno* - Subjekti podataka mogu osjetiti značajne, ili čak i nepovratne, posljedice koje oni ne mogu prevazići, kao na primjer u slučaju oboljevanja od dugotrajnih ili trajnih fizičkih bolesti (zbog zanemarivanja kontraindikacija), oboljevanja od dugotrajne ili trajne psihološke bolesti ili u slučaju krivične odgovornosti subjekta podataka.

U međunarodnom standardu ISO/IEC 29134 se navodi primjer nivoa utjecaja na temelju vrste ličnih podataka (Tabela 1).

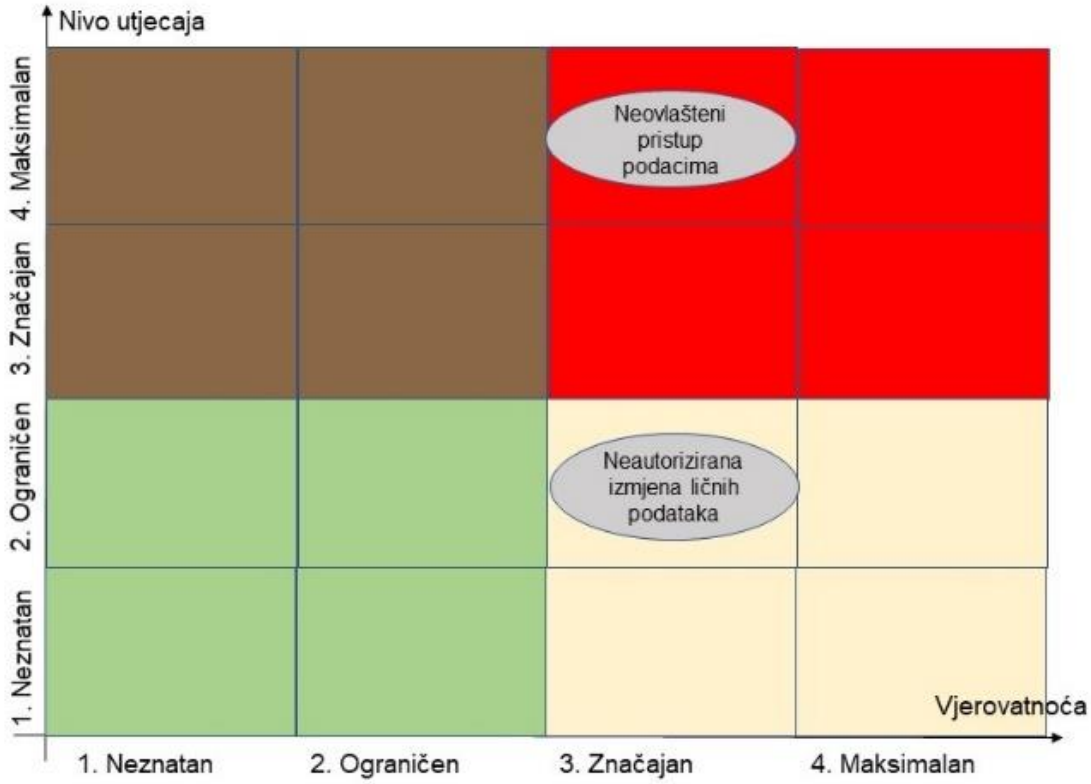
Što se tiče prijetnji, njihova vjerovatnoća se izračunava iz ranjivosti podržavajuće imovine (u

kojoj mjeri se karakteristike podržavajuće imovine mogu iskoristiti da bi se izvršila prijetnja) i sposobnosti izvora rizika (napadači) da iskoriste ove ranjivosti (vještine, raspoloživo vrijeme, financijski resursi, bliskost sa sistemom, motivacija, itd.).

ISO/IEC 29134 navodi sljedeću skalu koja se može koristiti za izražavanje stupanj do kojeg prijetnja može iskoristiti ranjivosti podržavajuće imovine:

1. *Neznatan stupanj*. Izvršavanje prijetnje ne čini se moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u sobi koja je zaštićena čitačem i pristupnim kodom).
2. *Ograničen stupanj.* Izvršavanje prijetnje čini se teško moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u sobi koja je zaštićena čitačem – badge reader).
3. *Značajan stupanj*. Izvršavanje prijetnje čini se moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u uredu kojem se ne može pristupiti prije prethodne prijave na recepciji)
4. *Maksimalni stupanj*. Izvršavanje prijetnje čini se ekstremno lagano za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u predvorju

Svaki rizik privatnosti koji se sastoji od neželjenih događaja i povezanih prijetnji može biti iscrtan u dvodimenzionalnom (vjerovatnoća i ozbiljnost) prostoru, kao na primjeru sa slike 3.



Slika 3. Primjer mape rizika

U zavisnosti od pozicije u ovom prostoru, rizik se može klasificirati kao „potrebno je u potpunosti ga izbjeći", „potrebno je da se ublaži" (kako bi se umanjila vjerovatnoća i/ili utjecaj), ili „prihvatljiv“ (vrlo vjerovatno i sa manjim uticajem).

Nakon procjene rizika, analitičar rizika privatnosti može odrediti kako reagirati. Vrsta odgovora mora uzeti u obzir ograničenja resursa u stvarnom svijetu, kao što su vrijeme, novac i ljudi, kao i sami rizici. Analitičar ima četiri izbora kada odgovara na rizik (Breaux, 2015):

- Prihvatite rizik. Ako je rizik nizak, onda može biti razumno i potrebno prihvatiti rizik.
- Prenesite rizik. Ako postoje drugi subjekti koji mogu bolje upravljati rizikom, transfer rizika može biti najbolja opcija. Na primjer, korišćenje usluga trećih strana koje mogu da upravljaju platnim spiskovima, plaćanjem i drugim finansijskim uslugama koristeći visoke standarde privatnosti i bezbjednosti može biti poželjnije od internog razvoja ekvivalentnog sistema od temelja.

- Ublažiti rizik. Ublažavanje je najbolja opcija kada razvojni inženjer može implementirati kontrole privatnosti koje smanjuju rizik. To može na primjer biti kroz softversku komponentu ili kroz promjenu poslovnih procesa.
- Izbjegavajte rizik. Izbjegavanje nastaje kada se može izbjeći nepovoljan događaj promjenom dizajna sistema ili poslovnog procesa.

Kontrole rizika spadaju u tri kategorije (Breaux, 2015):
- administrativne kontrole, koje upravljaju poslovnom praksom organizacije;
- tehničke kontrole koje upravljaju softverskim procesima i podacima; i
- fizičke kontrole, koje npr. regulišu fizički pristup štampanim kopijama podataka i sistemima koji obrađuju i čuvaju elektronske kopije.

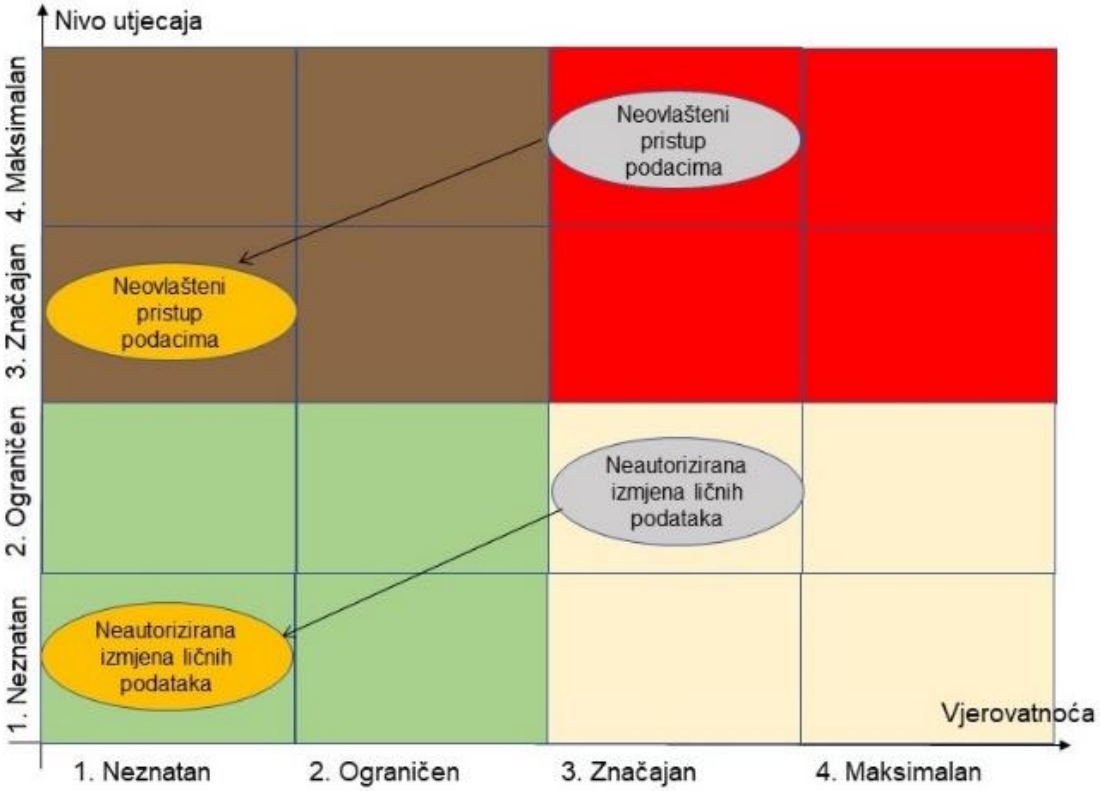
U oblasti zaštite privatnosti, primjer administrativnih kontrola uključuju:
- Imenovanje službenika za privatnost koji je odgovoran za koordiniranje dobrih praksi zaštite privatnosti na nivou cijele organizacije;
- Razvoj i dokumentiranje procedura privatnosti i sigurnosti;
- Obuka osoblja u oblasti zaštite privatnosti;
- Kreiranje inventara ličnih informacija radi praćenja praksi zaštite podataka…

Tehničke kontrole ciljaju informacione sisteme i treba da budu u fokusu softver inženjera prilikom dizajniranja sistema za očuvanje privatnosti. One uključuju:

- Implementacija mehanizama kontrole pristupa;
- Audit pristupa informacijama;
- Kriptanje osjetljivih podataka;
- Upravljanje individualnim pristankom;
- Objavljivanje obaveštenja o privatnosti…

Navedene mjere moraju se formalno odrediti, provesti, redovno pregledati i stalno poboljšavati.

Nakon implementiranja mjera za kontrolu rizika potrebno je procijeniti ozbiljnost i vjerovatnoću preostalih rizika (tj. rizika koji ostaju nakon provedbe odabranih mjera). Rizici se zatim mogu repozicionirati na mapi rizika, kao na Slici 4.



Slika 4. Mapa rizika nakon implementiranja mjera za kontrolu rizika

Za obavljanje procjene učinka na privatnost može se koristiti i matrica za određivanje rizika predstavljena međunarodnim standardom ISO/IEC 27005.

Kvalitativnom metodom odabire se jedna od pet opisnih nivoa vjerojatnosti, odnosno mogućnosti pojave rizika (ZIH, 2019):

1 - *vrlo niska* (nije vjerojatno da bi se razmatrani rizik mogao dogoditi, odnosno vjerojatnost njegove pojave je otprilike jednom u pet godina, ne postoje slučajevi, statistike ili motivi koji bi naznačili njegovo ostvarivanje, povezane ranjivosti procesa ili tehnologije se teško mogu iskoristiti, postojeće kontrole koje mogu spriječiti takav događaj su vrlo učinkovite),
2 - *niska* (malo vjerojatno da bi se razmatrani rizik mogao dogoditi, odnosno vjerojatnost njegove pojave je otprilike jednom u dvije godine, ali postoje slučajevi, statistike ili motivi koji bi naznačili njegovo ostvarivanje, povezane ranjivosti procesa, postojeće kontrole koje mogu spriječiti takav događaj su učinkovite),
3 - *srednja* (vjerojatnost pojave razmatranog rizika je jednom u godini, postoje slučajevi, statistike ili druge informacije koje ukazuju na to da se ovaj ili sličan događaj dogodio, ili postoji naznaka da bi mogli postojati neki razlozi za realizaciju scenarija; povezane ranjivosti bi se mogle iskoristiti; postojeće kontrole su uglavnom učinkovite),
4 - *visoka* (vjerojatnost pojave razmatranog rizika je jednom do dva puta u godini, postoje slučajevi, statistike ili druge informacije koje ukazuju na to da se ovaj ili sličan događaj nedavno dogodio (unutar godine dana), povezane ranjivosti bi se mogle lako iskoristiti; postojeće kontrole nisu dovoljno učinkovite),
5 - *vrlo visoka* (vjerojatnost pojave razmatranog rizika je više puta u godini, očekuje se pojava, odnosno postoje slučajevi, statistike ili druge informacije koje ukazuju na to da će se razmatrani scenarij vjerojatno pojaviti ili postoje jaki razlozi ili motivi za realizaciju scenarija; povezane ranjivosti se mogu vrlo lako iskoristiti; nisu implementirane kontrole, vjerojatnost pojave događaja je više puta u godini).

Treba odabrati jedan od pet nivoa utjecaja na ostvarenje ciljeva, koja najbolje opisuje kako će ostvareni rizik djelovati na organizaciju:

1 – *vrlo nizak*. Nema utjecaja na privatnost pojedinaca
2 – *nizak*. Zanemariv utjecaj na privatnost pojedinaca
3 – *srednji*. Manji utjecaj na privatnost – pojedinačni slučajevi ugrožavanja osobnih podataka
4 – *visok*. Značajniji utjecaj na privatnost – veći broj slučajeva ugrožavanja ličnih podataka
5 – *vrlo visok*. Vrlo veliki utjecaj na privatnost – vrlo veliki broj slučajeva ugrožavanja ličnih podataka.

Nivo rizika se izračunava po formuli:

*Nivo rizika = Vjerojatnost ostvarenja rizika * Utjecaj na ostvarenje ciljeva*

Nakon izračuna vrijednosti rizika isti se unosi u matricu procjene rizika sa slike 5.

	Vjerojatnost incident scenarija	Vrlo niska	Niska	Srednja	Visoka	Vrlo visoka
	Vrlo niska	0	1	2	3	4
	Niska	1	2	3	4	5
	Srednja	2	3	4	5	6
	Visoka	3	4	5	6	7
Utjecaj	Vrlo visoka	4	5	6	7	8

Slika 5. Matrica procjene rizika (Hamidović, 2010) (ISO/IEC, 2018)

Pri tom je skala ukupne ocjene rizika izražena kao:

- *Nizak rizik*: 0-2
- *Srednje rizičan*: 3-5
- *Visok rizik*: 6-8

5. ZAKLJUČCI

U skladu s pristupom temeljenim na riziku, utvrđenim u Opšoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obavezno za svaki postupak obrade, već samo ukoliko će obrada vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca. No, ukoliko nije jasno je li procjena učinka na zaštitu podataka potrebna, Radna skupina za zaštitu podataka iz članka 29 preporučuje da se ona ipak provede, jer voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka.

U skladu s načelima tehničke i integrisane zaštite podataka procjenu učinka na zaštitu podataka trebalo bi provesti prije same obrade, a s ciljem korištenja iste kao pomoćnog alata za donošenje odluka o obradi, a posebice izbora odgovarajućih mjera tehničke i integrisane zaštite.

Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost, no u smjernicama Radne skupine za zaštitu podataka iz članka 29 navedene su preporuke za korištenje međunarodnih standarda kao što je ISO/IEC 29134. U radu je predstavljena i CNIL metoda za procjenu učinka na privatnost, a koja je u velikoj mjeri usklađena sa preporukama ISO/IEC 29134. Iako je sama CNIL metoda prilično opšta i na visokom nivou, ista je dopunjena katalogom dobrih praksi koje mogu pomoći voditeljima obrade podataka u njihovom zadatku (za procjenu uticaja neželjenih događaja, na identifikaciju izvora rizika, odabir mjera proporcionalno rizicima, itd.).

CITIRANA DJELA

Breaux T. (2015). Introduction to IT Privacy: A Handbook for Technologists, International Association of Privacy Professionals (IAPP)

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

CNIL. (2012). Methodology for Privacy Risk Management. 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. (2010). Priručnik za izradu i reviziju plana sigurnosti osobnih podataka u automatskoj obradi, Info Press, Zagreb,

Hamidović, H. (2019). Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka. FBIM Transactions, 15 04, 7(1), pp. 67-73

Smjernica. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Article 29 Working Party

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 27005:2018 Information technology -- Security techniques -- Information security risk management. 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

ZIH. (2019). Seminar - Primjena Uredbe o zaštiti osobnih podataka – Radni materijali, Zavod za informatičku djelatnost Hrvatske, Zagreb