SIGURNOST OSOBNIH PODATAKA U RAČUNALNOM OBLAKU IZ PERSPEKTIVE VODITELJA ZBIRKE PODATAKA ZAŠTITE NA RADU

Petak, Ivan

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ivan Petak

SIGURNOST OSOBNIH PODATAKA U RAČUNALNOM OBLAKU IZ PERSPEKTIVE VODITELJA ZBIRKE PODATAKA ZAŠTITE NA RADU

ZAVRŠNI RAD

Karlovac, 2020.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Ivan Petak

SECURITY OF PERSONAL DATA IN THE CLOUD COMPUTING FROM PERSPECTIVE OF THE PROCESSOR OF DATA PROCESSING IN SAFETY AT WORK

FINAL PAPER

Karlovac, 2020

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ivan Petak

SIGURNOST OSOBNIH PODATAKA U RAČUNALNOM OBLAKU IZ PERSPEKTIVE VODITELJA ZBIRKE PODATAKA ZAŠTITE NA RADU

ZAVRŠNI RAD

Mentor:

dr.sc. Damir Kralj, prof.v.š.

Karlovac, 2020.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički diplomski stručni studij Sigurnosti i zaštite
(označiti)

Usmjerenje: Zaštita na radu

Karlovac, 24.07.2020.

ZADATAK ZAVRŠNOG RADA

Student: Ivan Petak

Matični broj: 0248050400

Naslov: SIGURNOST OSOBNIH PODATAKA U RAČUNALNOM OBLAKU IZ PERSPEKTIVE VODITELJA ZBIRKE PODATAKA ZAŠTITE NA RADU

Opis zadatka:

- analizirati aktualno stanje i usklađenost europske i hrvatske regulative u području zaštite osobnih podataka podložnih računalnoj obradi, mrežnom prijenosu i pohrani;
- analizirati osnove tehnoloških rješenja za obradu, prijenos i pohranu podataka koja se danas, između ostalog, koriste i za procesuiranje podataka u domeni zaštite na radu, pri čemu težište dati računalstvu u oblaku i njegovoj usklađenosti sa suvremenim regulatornim odredbama;
- na osnovi prethodnih analiza, dati prikaz u hrvatskoj praksi korištenih, programskih rješenja za vođenje evidencija ZNR, poglavito onih zasnovanih na računalstvu u oblaku, analizirati stupanj njihove zaštite osobnih podataka, usklađenosti s aktualnom regulativom te dati preporuke za eventualno unaprjeđenje postojećeg stanja.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
24.07.2020.	04.12.2020.	14.12. 2020.

Mentor:

dr.sc. Damir Kralj, prof.v.š.

Predsjednik Ispitnog povjerenstva:

Filip Žugčić, pred.

PREDGOVOR

Završni sam rad izradio samostalno koristeći pisane i mrežne izvore navedene u popisu literature.

Ovim putem želio bih se zahvaliti mentoru dr.sc. Damiru Kralju, prof.v.š. na izuzetnoj pomoći prilikom vođenja kroz pisanje rada, strpljenju, stručnosti te savjetima pruženim prilikom izrade ovog završnog rada. Želim se zahvaliti i svim profesorima i kolegama Veleučilišta u Karlovcu, Odjela sigurnosti i zaštite, na stručnom vodstvu kroz godine studija, na pomoći, podršci i prenesenom znanju tijekom studiranja, koje sam primijenio prilikom pisanja ovog završnog rada i koje ću kroz daljnja stjecanja iskustva u rada primjenjivati.

SAŽETAK

Voditelj zbirke osobnih podataka podataka ima visok stupanj odgovornosti s obzirom na osjetljivost svojih aktivnosti, a to je obrada i pohrana osobnih podataka. Uobičajeno je, danas, pohranjivati prikupljene podatke na računalu te ih na računalu i obrađivati. Računala umnogome pojednostavljuju i ubrzavaju rad voditelja zbirke podataka, ali ujedno uvode i rizik kojeg treba biti svjestan. U ovisnosti o načinu pohrane podataka razlikuju se i rizici i prijetnje pohranjenim podacima čije zanemarivanje može dovesti do gubitka, izmjene ili otkrivanja osjetljivih osobnih podataka. Osim lokalne pohrane podataka, u posljednje je vrijeme učestala pohrana podataka u oblaku (eng. *cloud*). Tamo se datoteke obrađuju i spremaju, što znači da se podaci spremaju na fizički udaljene poslužitelje. U tim podacima mogu postojati i osobni podaci. Prema trenutnoj europskoj i hrvatskoj zakonodavnoj regulativi, s osobnim podacima se mora pažljivo postupati, pravno i tehnički. Zbog toga se u ovom završnom daje pregled prijetnji i rizika korištenja računalne tehnologije u području zaštite na radu, načini zaštite pohranjenih podataka te sigurnosnih i pravnih aspekata zaštite podataka u oblaku.

KLJUČNE RIJEČI: zaštita na radu, računalstvo u oblaku, zaštita osobnih podataka, pravna regulativa, voditelj zbirke osobnih podataka

SUMMARY

The processor of the personal data collection has a high degree of responsibility with regard to the sensitivity of his activities, which is the processing and storage of personal data. It is common today to store the collected data on a computer and process it on a computer. Computers greatly simplify and speed up the work of database managers, but they also introduce a risk to be aware of. Depending on the method of data storage, there are risks and threats to stored data, the neglect of which can lead to the loss, alteration or disclosure of sensitive personal data. In addition to local data storage, *cloud* data storage has become more common recently. Unlike the traditional way, data storage and processing power moved from the personal computer to the *cloud*. Files are processed and stored in the *cloud*, which means that data is stored on remote servers physically. In these data there may be personal data. According to the current European and Croatian legal regulations, personal data must be handled with care, legally and in a technically correct way.

KEYWORDS: safety at work, cloud computing, protection of personal data; legal regulations, processor of personal data collection

SADRŽAJ

1. UVOD

Obveze poslodavca u zaštiti na radu proizlaze iz zakonskih regulative. Zaštita na radu je sastavni dio svake organizacije rada i izvođenja radnog procesa. Sukladno Zakonu utvrđena je obveza svakog poslodavca da vodi odgovarajuće evidencije iz zaštite na radu, zaštite od požara i zaštite okoliša s ciljem dugoročnog praćenja podataka i povećanja učinkovitost mjera vezanih uz sigurnost radnika na radnom mjestu. Kako bi se povećala sigurnost na radu te izbjegle kazne, poslodavac je dužan voditi evidencijske kartone, obrasce, očevidnike i izvještaje u kojima, ukoliko se vode u pisanom obliku, postoji mogućnost pogreške. Nadalje, pojavljuje se i niz problema vezanih uz praćenje rokova, potrebno vrijeme za prepisivanje podataka kao i manjak prostora za arhiviranje velike količine podataka. Stoga se danas za vođenje evidencija koriste računalni sustavi s mnoštvom prednosti u odnosu na klasično prikupljanje i pohranu podataka, ali isto tako i s nekim izazovima kojih stručnjak zaštite na radu itekako treba biti svjestan. Osim svjesnosti koja je nužan uvjet, stručnjak zaštite na radu treba poznavati i informacijsko-komunikacijsku tehnologiju (IKT) kako bi mogao prepoznati različite prijetnje i rizike korištenja informacijske tehnologije, a isto tako kako bi mogao djelovati u skladu sa zakonom. Ovo potonje je osobito važno kod korištenja tzv. računalstva u oblaku *(*eng*. cloud computing)* gdje treba biti osobito oprezan pri pohrani osobnih podataka, a što je kod voditelja zbirki podataka gotovo svakodnevica [1].

Cilj ovog rada je na osnovi znanja stečenih tijekom studija i iskustava iz prakse uz oslonac na aktualnu domaću regulativu, EU direktive [2], norme i aktualne projekte, analizirati sigurnost osobnih podataka pri njihovoj pohrani u oblaku s naglaskom na odgovornost i ulogu voditelja zbirke osobnih podataka u procesima pohrane i obrade podataka.

Metodologija predviđena za ostvarenje cilja rada obuhvaća istraživanje i analizu dostupnih pisanih i mrežnih izvora koji sadrže i obrađuju navedene regulativne, normativne i projektne sadržaje te radova koji se bave problemima obrade i pohrane osobnih podataka korištenjem računalstva u oblaku. Također, primjena vlastitih iskustava i znanja stečenih kroz obrazovanje i praktičan rad.

2. RAČUNALSTVO U OBLAKU

Računalni *cloud* ili oblak predstavlja isporuku računalnih usluga preko Interneta. Usluge u oblaku omogućuju pojedincima i tvrtkama korištenje softvera zajedno sa sklopovljem kojim se upravlja od strane trećih entiteta na udaljenim lokacijama. Primjeri *cloud* usluge su mrežna pohrana datoteka, društvene mreže, webmail i aplikacije u svrhu mrežnog poslovanja. Može se reći da je to sljedeća evolucija Interneta. Nakon svjetske mreže stranica (eng. *World Wide Web)* te elektroničke pošte (eng. *e-mail)*, računalstvo u oblaku je najveći korak u toj neprestanoj evoluciji. Koristeći se tehničkim rječnikom, *cloud* predstavlja uređenje gdje su računalni resursi omogućeni na fleksibilnoj i lokacijsko neovisnoj bazi, koja omogućuje brzu dodjelu resursa, po potrebi. Dodjela *cloud* resursa ovisi o kompleksnim višeslojnim aranžmanima između različitih opskrbljivača.Pojam se danas susreće gotovo svugdje od dnevnih novina do blogova, no, samu definiciju pojma je teško odrediti. Sam pojam je došao iz metafore za internet, naime u mnogim shematskim prikazima Interneta, riječ se koristi unutar oblačića. Naravno, poistovjećivanje i izjednačavanje pojmova Internet i *cloud* computing nije točno. Možda bi najbolja definicija bila da je *cloud computing* koncept podjele programskog okruženja koji koristi Internet kao platformu te omogućuje da aplikacije i dokumenti poslani iz bilo kojeg dijela svijeta budu pohranjeni i čuvaju se na za to predviđenim poslužiteljima. Ova vrsta računala koja se zasnivaju na korištenju *weba*, smanjuju potrebu za kupnjom novog sklopovlja i programa te otvaraju nove oblike suradnje. Pristup „podacima u oblaku“ odvija se putem web preglednika ili specijaliziranih aplikacija. Davatelj usluge izvodi isporuku usluge preko tri arhitekturna modela pod nazivom SPI model (engl. *software, platform, and infrastructure as a service*) koji se pojavljuje kao:

- Sas (eng. *Software as a Service*):

  - obuhvaća ponudu gotovih programa u obliku usluge gdje korisnik ima slobodu odabira i konfiguracije softvera kojeg želi koristiti koje korisnik plaća (npr. specifične mogućnosti Google DOS ili Mail usluga);

- Pas (eng. *Platform as a Service*);

  - Oblik usluge koja omogućuje ponudu razvojnog okruženja i aplikacijske platforme. Dakle, njih čine razni uslužni programi, programske biblioteke, softverski servisi i sl. Ovdje pružatelj usluga u oblaku kupuje, nabavlja, održava

tehnologije vezane uz usluge te planira proširenje ako je to potrebno dok korisnik o tome ne mora voditi brigu

- IaaS (eng. *Infrastructure as a Service*):

  - model koji označava ponudu osnovnog softvera (operacijskog sustava upravljačkih programa) i sklopovlja u obliku usluge. Umjesto kupovanja sva oprema se može unajmiti kroz oblak. Infrastruktura kao usluga pomaže tvorcima softverskih aplikacija. kao usluga je način isporuke infrastrukture računalstva u oblaku. To mogu biti poslužiteljska računala, prostori za pohranu podataka, mreže i operacijski sustavi kao usluge po zahtjevu. Umjesto da kupuju računala, softver, uređaje za pohranu podataka, prostor za smještaj sklopovlja i mrežnu opremu, korisnici iznajmljuju uslugu po njihovim potrebama i zahtjevima. Infrastruktura isporučena kao usluga može biti implementirana na nekoliko različitih načina - kao javni ili privatni oblak, kao oblak zajednice ili hibridni oblak.

Slika 1. Cloud computing [3]

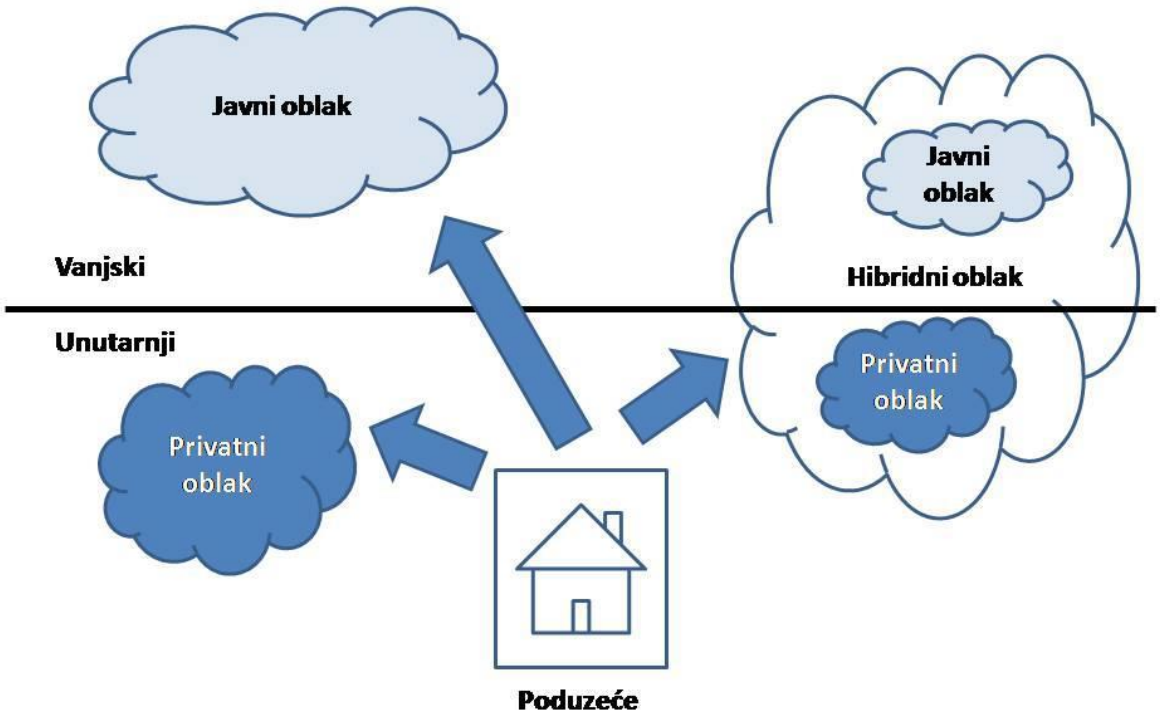
Riječ oblak zapravo govori da se računalstvo bilo kao infrastruktura, bilo kao aplikacijska razina, bilo kao poslovni proces ili kao osobna kolaboracija, može dovesti do krajnjeg korisnika bilo kad i bilo gdje. *Cloud computing* obećava drastična snižavanja kapitalnih ulaganja, a ono što je najbitnije omogućava ljudskim resursima skretanje pozornosti na

važne poslove s održavanja samih IT sustava. Na slici 1 se prikazuje raznolikost uređaja koji mogu koristiti *cloud computing*.

2.1 Modeli pružanja usluge

Postoje četiri modela pružanja usluga u računarstvu u oblaku, a to su: privatni oblak (eng. *Private Cloud*), javni oblak (eng. *Public Cloud*), hibridni oblak (eng. *Hybrid Cloud*), oblak zajednice (eng. *Community Cloud*) (Slika 2.).

Privatni oblak čine središta podataka koja posjeduje ustanova, a koja se temelje na tehnologijama kao i javni oblaci, a namijenjeni su vlastitom korištenju što znači da svaki korisnik može koristiti privatno svoje podatke bez pristupa drugih korisnika. Jedna ustanova može imati više odjela koje koriste svoje računalne resurse i ovisno o trenutnom opterećenju se oni dodjeljuju potrebitim odjelima. Njega posjeduju uglavnom velike kompanije ili javna uprava koje žele nadzirati i upravljati (kontrolirati) svojim podacima i njihovu sigurnost.



Slika 2. Grafički prikaz različitih vrsta usluga u oblaku [4]

Javni oblak je naziv za računalstvo u oblaku općenito u javnom korisničkom pristupu. Ovdje se usluge pružaju široj javnosti i naplaćuju prema korištenju. Ovaj oblak je još nazvan i potrošački oblak, gdje korisnici putem interneta, preko poslužitelja koriste računalne resurse, uslužne aplikacije, resurse poput društvenih mreža, blogova, e-pošte, pohrane podataka ili slika itd. Danas možemo pronaći mnoštvo servisa koje korisnici svakodnevno koriste u svom životu kao npr. Facebook, Twitter, Gmail, Google Docs, Windows Live, Dropbox itd. Najveći problem ovog modela je sigurnost i upravljanje podacima.

Hibridni ili mješoviti oblak je kombinacija privatnog i javnog oblaka gdje neko poduzeće ima mogućnost zadržavanja kritičnih, potrebnih podataka i aplikacija unutar vlastitog vatrozida, dok ostali podaci koji nisu tako važni i mogu biti otvoreni za javnost su pohranjeni u javnom oblaku.

Oblak zajednice je poseban model u kojem više organizacija svojim zahtjevima razmjenjuju infrastrukturu i tako povećavaju svoju funkcionalnost dijeleći troškove.

2.2 Razvoj i trenutna tržišna pozicija

Cloud computing je prošao kroz mnoštvo razvojnih faza koje uključuju distribuiranu računalnu mrežu (eng. *grid*) i računalstvo zasnovano na uslugama (eng. *utility computing*), pružanje programskih usluga (eng. *application service provision, ASP*) i SaaS (eng. *Software as a Service*). Kao počeci *cloud* computinga smatraju se 1960-te godine [5]. Sve je počelo s idejom J.C.R. Licklidera o kompjuterskoj mreži koja povezuje cijeli svijet. On je, među ostalim, odgovoran za omogućavanje razvoja ARPANET-a (eng. *Advanced Research Projects Agency Network*) 1969. godine. Njegova vizija bila je da svi na Zemlji budu međusobno povezani i imaju pristup programima i podacima na svakoj web stranici s bilo koje lokacije na svijetu. To je ideja koja uvelike sliči današnjem *cloud* computingu. Neki stručnjaci pripisuju zasluge stvaranja koncepta *cloud* computinga drugome znanstveniku – Johnu McCarthyu. On je predložio ideju o javno dostupnom računalstvu (eng. *utility computing*). Zaista, *cloud computing* ima slične karakteristike kakve su imale organizacije koje su u šezdesetim godinama prošlog stoljeća pružale usluge obrade podataka na udaljenim poslužiteljima. Termin oblak posuđen je iz telefonije i telekomunikacija, koje su do 1990.-ih primarno nudile točno usmjereni prijenos

podataka, a tada su počele nuditi i usluge VPN-a (eng. *Virtual Private Network*) s usporednom kvalitetom usluge, ali puno nižim troškovima [6]. Prospajanjem prometa, kako bi uravnotežili iskorištavanje, bili su u mogućnosti iskoristiti cjelokupnu propusnost mreže. Simbol oblaka se koristio za označavanje točke grananja poslužitelja od jednog do drugog korisnika. *Cloud* computing širi te granice da bi u potpunosti obuhvatio poslužitelje i infrastrukturu mreže. Od šezdesetih godina *cloud computing* se razvijao u mnogo smjerova (Web 4.0 je primjer najnovije inovacije). Međutim, internet se tek u devedesetim godinama počeo masovnije primjenjivati i imati značajniju propusnost. Jedna od značajnijih prekretnica u *cloud* computingu bio je nastanak Salesforce.coma 1999. godine. Salesforce.com je bio pionir u konceptu dostavljanja aplikacija preko jednostavnih web stranica. Njihovi poslužitelji su popločili put specijaliziranim programskim organizacijama za dostavljanje aplikacija preko Interneta. Amazon je odigrao ključnu ulogu u razvoju *cloud* computinga moderniziranjem svojih podatkovnih centara. Nova arhitektura oblaka rezultirala je značajnim i učinkovitim unutrašnjim poboljšanjima koja omogućuju malim organizacijama lakše i brže dodavanje novih podataka u oblake. Prva njegova značajna inovacija bio je Amazon Web Service (objavljen 2002. godine), koji je pružio *cloud* computing usluge koje uključuju pohranu i obradu, pa čak i ljudsku inteligenciju preko Amazon Mechanical Turka. Amazon je na osnovama utility computinga 2005. godine počeo osiguravati pristup svojim sustavima preko web poslužitelja. Ova osobina razvoja Amazon web poslužitelja ocijenjena je kao izuzetno pojednostavljenje dotadašnjih tehnoloških dostignuća na ovome području. 2006. godine Amazon je objavio EC2 (eng. *Elastic Compute cloud*) kao komercijalni web poslužitelj koji malim organizacijama i individualnim korisnicama omogućuje iznajmljivanje kompjutera na kojima mogu pokretati vlastite aplikacije. [6] Amazon Ec2/S3 je bio prvi komercijalni *cloud* computing poslužitelj. Google, IBM i nekolicina sveučilišta uključila su se 2007. godine u veliki istraživački projekt daljnjeg razvoja *cloud* computinga. To je rezultiralo novim inovacijama na ovom području. Značajna prekretnica pojavila se 2009. godine. Bio je to Web 2.0, koji je tada započeo svoj proboj na tržište. Google i druge organizacije tada su isto počele nuditi aplikacije zasnovane na preglednicima. Tako je nastao Google Apps. Najvažniji doprinos razvoju *cloud* computinga bilo je pojavljivanje uspješnih novih aplikacija objavljenih od strane Microsofta i Googlea. Te dvije organizacije pružale su usluge koje su pouzdane i lake za korištenje, pa su odmah prihvaćene na tržištu. Drugi ključni faktori koji su omogućili razvoj ove tehnologije uključuju razvijanje virtualizacijske tehnologije, razvoj univerzalnih brzih propusnica i univerzalnih programskih standarda. Mnoge organizacije danas prepoznaju prednosti

koje im nudi *cloud* computing. On im omogućuje povećanje mogućnosti pohrane podataka, prilagodljivost i smanjenje troškova. Ali korisnici su i dalje zabrinuti za sigurnost vlastitih podataka pohranjenih u oblaku. *Cloud* computing će doživjeti pravi procvat u praksi tek kada se riješe sigurnosni problemi koje trenutno posjeduje. Analitičari smatraju da će ti sigurnosni problemi uskoro biti riješeni. Kada se riješe sigurnosni problemi, poslužitelji *cloud* computinga omogućiti će korisnicima širenje vlastitih infrastruktura, dodavanje kapaciteta na zahtjev korisnika, povećavanje prilagodljivosti, a u ponudi će biti i sve više različitih resursa (pa će time doći i do značajnih financijskih ušteda). Organizacije će u budućnosti vjerojatno sve više koristiti *cloud* computing. To će se dogoditi kada se na Internetu počne povećavati broj usluga koje se mogu koristiti za obradu i pohranu zahtjevnijih aplikacija. *Cloud* computing donijeti će velike prednosti IT korisnicima. [7]

2.3 Ključne prednosti

Pružatelj usluga teško može anticipirati kako će korisnici koristiti njegove usluge. Neki će korisnik možda uslugu koristiti triput godišnje u vrijeme vršnog poslovanja, dok će drugi možda uslugu koristiti kao primarnu platformu za sve svoje aplikacije. Stoga, servis mora biti dostupan cijelo vrijeme te se mora moći skalirati ovisno o potražnji. Skalabilnost također podrazumijeva da aplikacija može skalirati kada se dodaju novi korisnici i kada se potrebe za aplikacijom mijenjaju. Ova mogućnost izravno ovisi o elastičnosti. Osim toga, samouslužnost je ključna prednost. Korisnik ne mora prolaziti dugotrajnu i kompliciranu proceduru pri povećanju i/ili smanjenju svojih potreba. Korisnik jednostavno zatraži povećanje diskovnog prostora, softvera, procesa ili drugih resursa od svog davatelja usluga. *Cloud* computing povećava brzinu razvijanja aplikacija, pomažući tako u povećavanju broja inovacija koje se pojavljuju na tržištu. Kako je *cloud* computing poprilično nova stvar na IT tržištu, on još nije savršen. Postoje mnoge prednosti koje bi korisnike trebale privući korištenju *cloud* computinga, ali isto tako i problemi koje im korištenje može donijeti. Prije nego što se pojedini korisnik ili organizacija odluče na korištenje ove tehnološke platforme trebali bi se dobro informirati o mogućim nedostacima koje im ova tehnologija može donijeti. Korisnici bi prvo trebali proučiti koji se sve davatelji usluga mogu pronaći na tržištu i koje su njihove međusobne razlike. Zatim bi trebali odrediti koje podatke žele spremati, koliko su ti podatci osjetljivi, koje *cloud* computing usluge ili platforme im najbolje odgovaraju, koliko prostora je potrebno i slično.

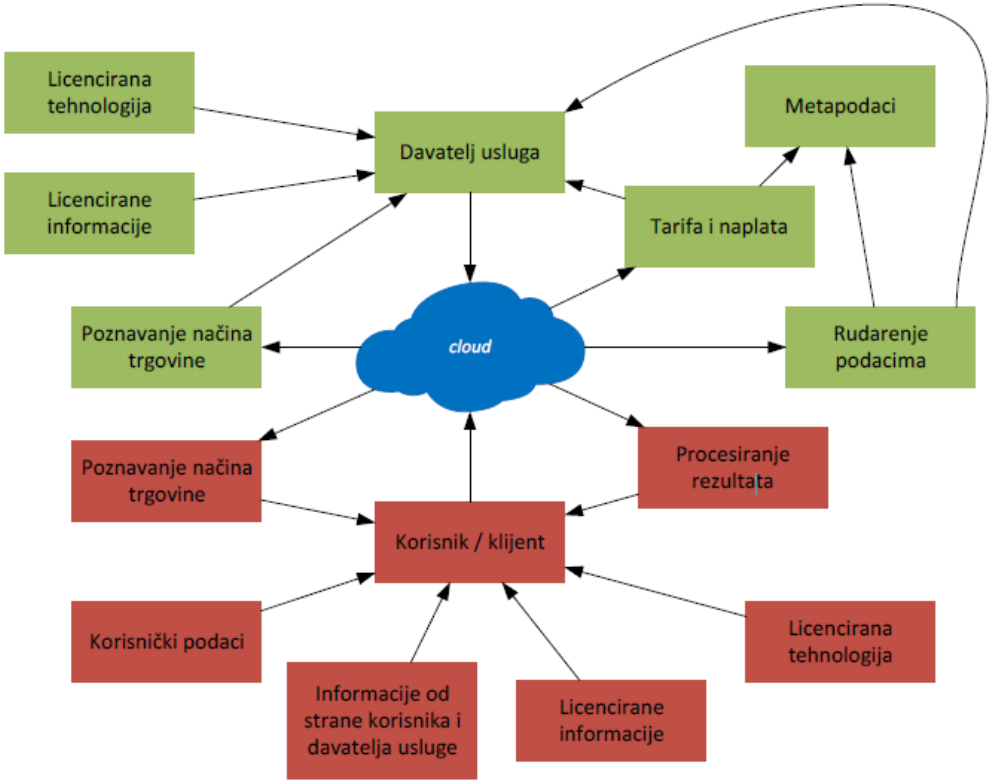
Uvođenje ove tehnologije sigurno nije jednostavna stvar za organizacije. Svaka organizacija prvo bi trebala procijeniti kolike će im financijske uštede donijeti korištenje ovog modela i kako će se one odraziti na sigurnost i konkurentnost organizacije. *Cloud* computing je još uvijek u razvoju i svakim danom se uvode nove promjene, pojavljuju novi poslužitelji, ali isto tako sve više korisnika pristupa ovome konceptu podjele programske podrške koji koristi Internet kao platformu te omogućuje pohranjivanje i čuvanje aplikacija. Aplikacije ili dokumenti mogu biti poslani iz bilo kojeg dijela svijeta. Neke od prednosti korištenja *cloud* computinga su:

- niža cijena sklopovske podrške u smislu da korisnik ne mora kupovati novo sklopovlje, nego ga po potrebi iznajmljuje preko Interneta,
- korisniku je uvijek dostupna posljednja, najnovija inačica programske podrške,
- programska podrška i podaci su dostupni sa svakog računala s kojeg korisnik ima pristup Internetu,
- manji troškovi održavanja i nadogradnje programske podrške. Nema troškova izravno vezanih uz kupovinu sučelja, licenciranih programa, baze podataka, poslužitelja za elektroničku poštu, kao ni troškova vezanih za njihovu instalaciju i konfiguraciju te kasnije održavanje,
- u uslugu je uključena profesionalna antivirusna zaštita,
- dostupnost aplikacija,
- skalabilnost aplikacija - mogućnost opsluživanja velikog broja korisnika,
- fleksibilnost u izmjeni i prilagodbi aplikacija i stalno praćenje rada i održavanje infrastrukture.

2.4 Korisnički sadržaj pohranjen i procesiran u *cloudu*

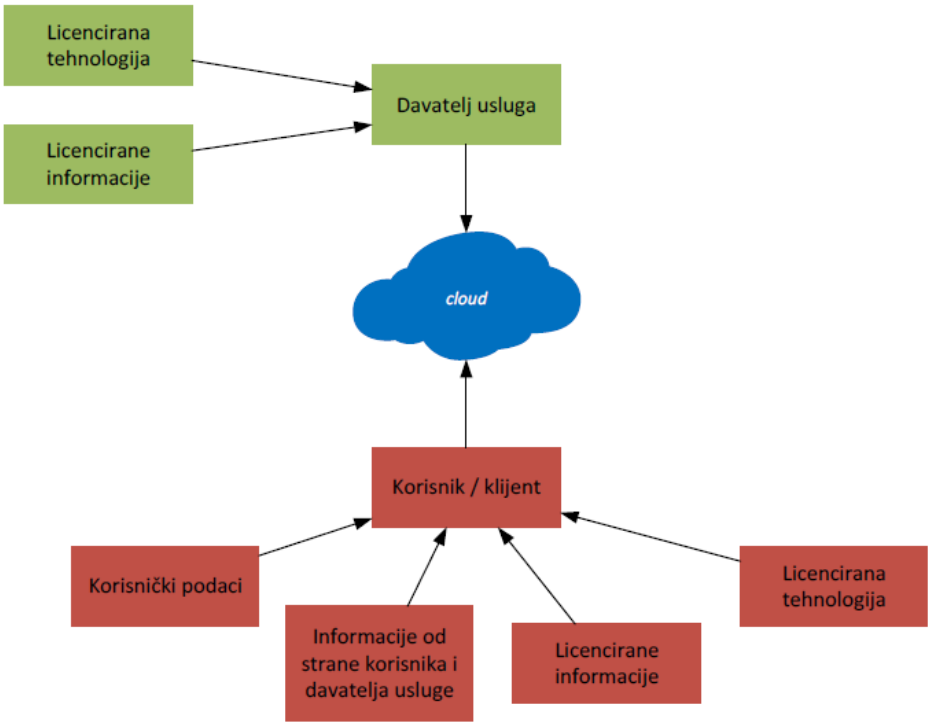
Konceptualna mapa informacijskih tokova između davatelja usluge i korisnika prikazana je na slici 3. Iako mapa izgleda složeno moguće ju je pojednostaviti. Velik dio generiranih informacija su izvan *clouda* (slika 4). Informacije imaju već uspostavljen vlasnički status prije nego li se postave na *cloud*. Međutim, informacije postavljene na *cloud* od strane korisnika mogu postati problematične. Primjer problema je kada milijuni korisnika dijele audio sadržaj putem clouda, isto se odnosi na dijeljenje fotografija putem

društvenih mreža (primjerice: Facebook, Twitter, Instagram, itd.). Ako je inicijalno vlasništvo takvog sadržaja poznato, u praksi kompleksne norme dijeljenje informacija među korisnicima označava dolazak tj. otkrivanje stvarnog vlasnika koji omogućuje cloud usluge postaje gotovo nemoguće [8]. Čini se razumnim tvrditi kako su očekivanja svih sudionika da postavljanje sadržaja na cloud ne bi smjelo izmijeniti status vlasnika.



Slika 3. Prikaz toka podataka u relacijskom modelu clouda [8]

Glavna ideja relacije računalnog *clouda* jest omogućavanje korisniku korištenje *cloud* tehnologije kako bi se procesirale informacije i tako generirali rezultati (eng. *Outputs*).



Slika 4. Generiranje informacija [8]

Međutim, klijent može generirati trgovačke tajne (eng. *Trade secrets*), koje nisu prikazane u niti jednom rezultatu obrade informacija ali su skladištene u strukturama podataka ili procesima koje korisnik uspostavlja korištenjem *clouda*.

2.4.1 Brisanje podataka u *cloud*u

Različiti stupnjevi brisanja podataka postoje u *cloud*u. Ako korisnik obriše podatak, tada se podatak premješta u „koš za smeće“ (eng. *Recycle bin/trash*) ali se određeno vrijeme ne briše u potpunosti, tj. ostaje na raspolaganju korisniku ako treba vratiti podatak, ako mu kojim slučajem zatreba. Kada ugovor između korisnika i davatelja usluga istekne, korisnički podaci ne brišu se odmah, nego nakon određenog razdoblja. Korištenje „koša za smeće“ i brisanje podataka sa vremenom/razdobljem odgode može potencijalno ugroziti ostale elemente sigurnosti kao što su npr. integritet i dostupnost. Problem ponekad nastaje u tome da nakon brisanja podataka u „košu za smeće“ stvarni podaci ostaju jer se brišu reference, točnije pokazivači (eng. *pointers*) koji pokazuju na stvarne podatke koji su pak spremljeni u memoriji na nekom drugom mjestu [9]. Stvarni podaci se zapravo brišu tako da njihovo mjesto zauzimaju nadolazeći, svježi podaci spremljeni od strane istih ili različitih korisnika. Remanentnost podataka odnosno brisanje nominalnih podataka zbog navedenih problema predstavlja podosta velik problem. Kako bi se postigla efektivna povjerljivost podataka potrebno je u više navrata izvršiti aktivnost

brisanja već obrisanih podataka. Krajnja mjera čak navodi demagnetizaciju diska ili sigurnosno uništavanje fizičkog medija. Privatni *cloud* u ovom slučaju pokazuje se kao bolje rješenje jer je jednostavnije zatražiti da se podaci „unište“ do kraja za razliku od javnog modela gdje krajnji korisnik nikada ne može biti siguran je li kakav fragment podataka ostao na dislociranom serveru ili nije.

2.5 Sigurnosni rizici i opasnost u *cloudu*

Podaci su u srži informacijskih sigurnosnih problema za bilo koju organizaciju, bez obzira na oblik infrastrukture koja se pritom koristi. Računani *cloud* to ne mijenja, ali pridonosi dodatnom fokusu zbog distribuirane prirode računalne i *cloud* infrastrukture. Sigurnosni razlozi odnose se i na prijenos kao i na pohranu podataka. U suštini, pitanje koje se odnosi na podatke za računalni *cloud* o različitim oblicima rizika: rizik od krađe ili neovlaštenog otkrivanja podataka, rizik od neovlaštenog ili neovlaštenih izmjena podataka, rizik od gubitka ili nedostupnosti podataka. Također je vrijedno zapamtiti da u slučaju imovine podatka u *cloud*u je moguće uključi stvari kao što su aplikacijski programi ili strojne slike što može imati isti rizik kao i sadržaj baze podataka ili podatke datoteka.Cilj sigurnosti jest spriječiti ono što nije dozvoljeno. Ova jednostavna definicija krije u sebi dodatno pitanje: „A što to nije dozvoljeno?“. To ovisi od sustava koji se štiti i treba biti definirano za svaki konkretan sustav. Zahvaljujući dugogodišnjem civilizacijskom iskustvu u udruživanju ljudi i rješavanju konflikata, države i njihove organizacijske jedinice imaju norme koje definiraju dozvoljena i nedozvoljena ponašanja. Te norme su zakoni. Međutim, nemaju sve države ili čak svi dijelovi iste države iste zakone. Znači da nešto može biti dozvoljeno na jednom mjestu, a zabranjeno na drugom. Stvari mogu izgledati još složenije za osobu koja brine o računalima u nekoj organizaciji. Svaki korisnik računala u organizaciji može imati svoj stav o tome što je dozvoljeno, a što nije. Organizacija koja je vlasnik informacija, odnosno oni koji donose odluke u organizaciji, određuje kome i što je dozvoljeno raditi s tim informacijama. Dokument kojim se ovo iskazuje i koji je polazište za sve što se tiče sigurnosti je: sigurnosna politika. Sigurnosna politika opisuje željeno stanje sustava iz aspekta sigurnosti. Sigurnosna politika u principu navodi što je dozvoljeno, a što nije. Na primjer, u sigurnosnoj politici nekog fakulteta može stajati da prepisivanje na ispitu nije dozvoljeno. U nekoj tvrtki ova politika može navesti da samo generalni i financijski direktor imaju pristup informacijama o trenutnom stanju računa. U sigurnosnoj politici banke može stajati da samo rukovoditelj može mijenjati

stanje računa klijenata. Sigurnosna politika može navesti i kakvu kvalitetu usluge sustav treba pružiti korisnicima. Sigurnosna politika se ne bavi, i ne treba se baviti, načinima na koje se postiže da se u navedenom sustavu odvijaju samo dozvoljene stvari. U navedenim primjerima sigurnosna politika ne treba navoditi na koji način se sprječava prepisivanje studenata, odnosno na koji način se pristup stanju računa kompanije omogućava samo generalnom i financijskom direktoru. Sigurnosni mehanizmi omogućavaju poštivanje sigurnosne politike. Bez sigurnosne politike nema sigurnosti. Prije analize mogućih sigurnosnih rizika i opasnosti u *cloud* okruženju potrebno je analizirati vlasništvo nad informacijama u *cloud* okruženju. Stoga će prva dva potpoglavlja istražiti niz pitanja koja se odnose na to kako se informacije pohranjuju, obrađuju i/ili distribuiraju u *cloud* okruženju. Isto tako obradit će se zahtjevi odnosno problemi koji se nameću samom *cloudu*. Uz normativni mod vlasništva kreiran od strane intelektualnog tipa vlasništva (eng*. Intellectual property*), akcija povjerljivosti ili ona od strane ugovora, istražuje se kakve računarski *cloud* ima implikacije u pogledu otvorenih modela vlasništva. Konačno, zbog autorskih prava i implikacije razvoja *cloud*a kao industrije u cjelini također se istražuju pitanja vlasništva nad sučeljem za programiranje aplikacija (API) koji su neophodni za interoperabilnost *cloud*a. Prvo se usmjerava pozornost pohranjenom i obrađenom sadržaju od strane korisnika (ili kupca) usluge i također, kratko, sadržaja ili informacija koje su pohranjene ili obrađene od strane samog davatelja usluga. Takav sadržaj, bez obzira je li kontroliran od strane korisnika ili usluga bit će proizveden izvan ili unutar oblaka. Jedno od glavnih obilježja *cloud*a je to što omogućuje apstrakciju dok se korisnička funkcionalnost može odvojiti od upravljanja resursa. Ali, oslanjanje na apstraktne resurse koji su kontrolirani od trećih strana i čija se korisnost dijeli predstavlja rizik. Zabrinutost se obično pojavljuje oko smanjenja korisničkih funkcionalisti i povećanja funkcionalnosti davatelja usluge, posebice sigurnosti podataka pogonjena vjerojatno od smanjenja dostupnih informacija prema korisnicima koji se odnose na detalje od strane davatelja komponenti, dobavljača i mehanike. Ko-lokacijski rizik isto tako može postojati, ako se za sklopovlje sumnja da sadrži neprikladne odnosno neprovjerene dijelove tada se podaci povlače od strane zaduženog osoblja [10]. Isto tako, podaci koji se skladište na istoj opremi ili bazi podataka nekog drugog korisnika na kojeg se vrši napad sa udaljene lokacije također mogu biti ugroženi. Neovisno o tome je li meta lokalna ili se pak nalazi na nekoj udaljenoj lokaciji, podaci na koje se vrši napad su uvijek ugroženiji nego podaci koji su isto tako skladišteni na istom resursu ali na koje se napad ne vrši direktno. Primjerice ako postoji osoba A, koja ima spremljene podatke na istom poslužitelju kao i osoba B ali je slučaj da je napad je usmjeren na osobu A isključivo, tada

podaci osobe B mogu ostati sigurni neovisno o tome što je poslužitelj na kojemu se nalaze računi (engl. *Account*) mnogih korisnika cijeli kompromitiran tj. vrši se napad na njega. Generalno sigurnost *clouda* ovisi o tipu odnosno, servisnom modelu i dizajnu (svaka organizacija na drugačiji način izrađuje dizajn: Microsoft, Apple, Google, itd.).

2.5.1 Pojam informacijske sigurnosti

Uloga je informacijske sigurnosti zaštita podataka i informacija bez obzira u kojem se obliku one nalaze, digitalnom ili papirnatom [11]. Osim problema s količinom, pojedince, poslovne organizacije i vladina tijela svakako brine i zaštita podataka i informacija od neovlaštenog pristupa, neovlaštenog uništenja i neovlaštene promjene, što postaje predmetom informacijske sigurnosti.

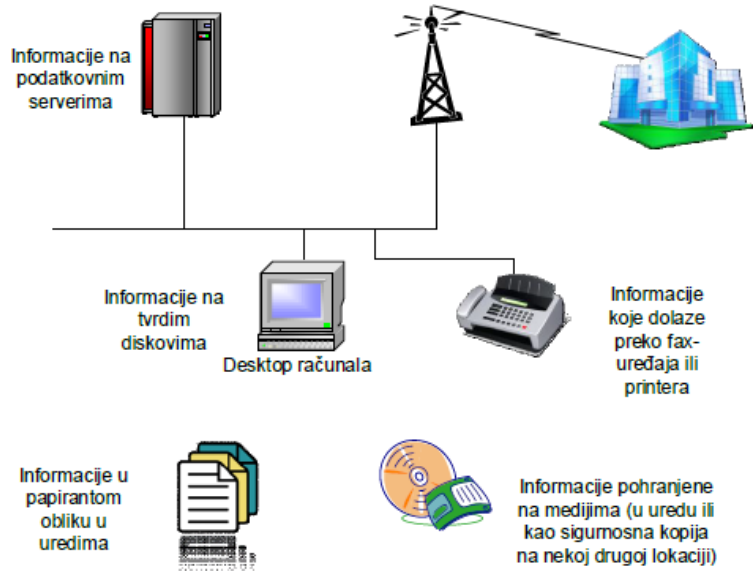
Informacijska sigurnost za pojedince, poslovne organizacije ili državu označava osiguravanje:

- povjerljivosti – da informacije nisu dostupne neovlaštenim korisnicima
- dostupnosti (raspoloživosti) – da su informacije i resursi dostupni i uporabljivi za ovlaštene korisnike, tada kada su potrebni
- cjelovitosti (integriteta) – da je osigurana točnost i potpunost informacija.

Informacijska sigurnost podrazumijeva poduzimanje preventivnih koraka da bi se zaštitili informacijski resursi i vlastiti kapaciteti od prijetnji, pri čemu posebnu pozornost treba obratiti na vlastite ranjivosti. Zaštita različitih podataka vrlo često je i zakonska obveza ako se radi o podacima koji su klasificirani kao povjerljivi ili tajni (Zakon o informacijskoj sigurnosti) odnosno ako su u pitanju osobni podaci (Zakon o zaštiti osobnih podataka). Zakon o informacijskoj sigurnosti primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje se u svojem djelokrugu koriste klasificiranim i neklasificiranim podacima te na pravne i fizičke osobe, koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. Taj zakon informacijsku sigurnost definira kao stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

2.5.2 Sustav informacijske sigurnosti

Dobar sustav sigurnosti podrazumijeva dobru fizičku sigurnost koja je potrebna da bi se zaštitila fizička imovina kao što su papirnati zapisi i sklopovlje. Komunikacijska je sigurnost potrebna da bismo zaštitili podatke prilikom njihova prijenosa. Računalna je sigurnost potrebna da bismo kontrolirali pristup računalnim sustavima, a mrežna je sigurnost potrebna za kontrolu sigurnosti lokalnih mreža. Zajedno ti koncepti pružaju informacijsku sigurnost.



Slika 5. Lokacije, formati, prijenos i pohrana informacija [12]

Na slici 5 su prikazane različite lokacije i formati pohrane informacija i neke od mogućnosti njihova prijenosa, koje je potrebno štititi navedenim mjerama informacijske sigurnosti. Sustav informacijske sigurnosti obuhvaća ljude, procese, infrastrukturu, organizaciju i tehnologiju. U svrhu zaštite podataka Zakon o informacijskoj sigurnosti predviđa donošenje mjera koje se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini, što podrazumijeva sustavan pristup pri planiranju, implementaciji i nadzoru mjera i standarda informacijske sigurnosti. Područja su informacijske sigurnosti za koja se Zakonom propisuju mjere i standardi informacijske sigurnosti:

- sigurnosna provjera
- fizička sigurnost
- sigurnost podatka
- sigurnost informacijskog sustava
- sigurnost poslovne suradnje.

Da bi se postigao optimalan izbor bitnih mjera i postupaka, informacijskom sigurnošću treba sustavno upravljati, stoga se često govori o sustavu upravljanja informacijskom sigurnošću.

2.5.3 Izvori i oblici prijetnji informacijskoj sigurnosti

Informacijski i računalni sustavi mogu biti izloženi prijetnjama na brojne načine. Incidenti mogu biti namjerni (zlonamjerni) ili se mogu dogoditi slučajno. Međutim, bez obzira na to zašto se određeni incident dogodio, činjenica je da on nanosi štetu pojedincu ili organizaciji. Zbog toga se takvi incidenti često nazivaju napadima bez obzira je li bilo zlonamjernosti ili ne.Izvore prijetnja informacijskom sadržaju možemo podijeliti:

- na višu silu kao izvor prijetnja
- na čovjeka s obilježjem namjernosti ili nenamjernosti
- na tehničku pogrešku.

Viša sila kao izvor prijetnja obuhvaća prirodne nepogode koje mogu djelovati svojom snagom, npr. potres, poplava, požar i erupcija. Osim prirodnih nepogoda postoje i druge prijetnje koje nije moguće kontrolirati, npr. rat, epidemija i sl. Prevencija te vrste prijetnja moguća je organizacijskim, građevinskim i tehničkim mjerama ovisno o procijenjenoj vjerojatnosti njihova nastanka. Čovjek s obilježjem namjernosti ili nenamjernosti najčešći je izvor prijetnja informacijskoj sigurnosti. Najveće štete mogu prouzročiti upravo djelatnici, davatelji usluga ili vanjski suradnici koji dobro poznaju organizaciju i funkcioniranje informacijskog sustava. Stoga je ulaganje u radno zadovoljstvo i sigurnost iznimno važno kada se govori o obilježju namjernosti, a kod obilježja nenamjernosti posebnu pozornost treba usmjeriti programima osvješćivanja zaposlenika o informacijskoj sigurnosti. Tehnička pogreška kao prijetnja (primjerice kvarovi na informatičkoj opremi i sl. koji mogu prouzročiti gubitak informacijskog sadržaja) najpredvidljivija je pogreška te se sustavnim upravljanjem informacijskom sigurnošću i primjenom odgovarajućih mjera tehničke prirode posljedice njezina nastanka mogu svesti na minimalnu razinu.

Načini na koje se prijetnje iz navedenih izvora mogu realizirati svakim su danom sve brojniji i složeniji. S obzirom na to da ih je nezahvalno sve navoditi, najčešće se grupiraju s obzirom na posljedice koje njihovim djelovanjem nastaju na informacijskom sadržaju:

- neautorizirani pristup
- neidentificirana i neautorizirana izmjena
- uskraćivanje usluge
- neprihvaćanje.

Realizacija prijetnje u obliku neautoriziranog pristupa nastaje u pokušaju da napadač dođe do informacija kojima nema pravo pristupa. Napadi takve vrste događaju se na bilo kojem mjestu pohrane informacija ili tijekom njihova prijenosa. Riječ je o napadu na povjerljivost informacija. Neautorizirana izmjena podrazumijeva napad u kojem napadač radi izmjene na informacijskom sadržaju za koji nema prava pristupa. Taj oblik napada također se može dogoditi na bilo kojem mjestu pohrane informacija ili tijekom njihova prijenosa, pri čemu je riječ o napadu koji ugrožava integritet informacija. Taj oblik prijetnje može ostaviti najteže posljedice, posebice kada je riječ o poslovnim sustavima koji svoje odluke temelje na promijenjenom informacijskom sadržaju. Neautorizirana izmjena informacijskog sadržaja najčešće se obavlja izmjenom, umetanjem ili brisanjem podataka. Na primjer, promjenom financijskog izvještaja (informacija je i prije postojala samo je neautoriziranom intervencijom izmijenjena), prebacivanje financijskih sredstava s jednog računa na drugi umetanjem nove transakcije (takva informacija nije postojala prije) te brisanjem povijesnih informacija kao što su kazneni bodovi. Napadi uskraćivanjem usluge DoS (eng. *Denial-of-Service*) predstavljaju napade koji uskraćuju korištenje resursa legitimnim korisnicima informacija, informacijskog sustava i resursa. DoS-napadi uglavnom su napadi na računalne sustave i mreže, što ne znači da ne postoje DoS-napadi na informacije u papirnatom obliku, nego da je mnogo lakše provesti napad u elektroničkom okruženju. Moguće je razlikovati napade uskraćivanja pristupa informacijama, aplikacijama, operacijskim sustavima i mrežama. Neprihvaćanje je napad usmjeren prema neporecivosti informacija, a podrazumijeva pokušaje davanja pogrešnih informacija ili poricanja da su stvarni događaj ili transakcija nastali. Pojavni oblici su maskiranje koje se javlja (kada se napadač ponaša ili predstavlja kao netko drugi) u osobnoj komunikaciji, transakcijama ili komunikaciji među sustavima te poricanje da se dogodila aktivnost / transakcija koja je zabilježena (npr. poricanje transakcije obavljene kreditnom karticom u online kupnji). Koncentracija računalnih resursa i korisnika u okruženju računalstva u oblaku predstavlja koncentraciju sigurnosnih prijetnji. Zbog njegove veličine i značajnosti, okruženje računalstva u oblaku je često meta napada.

2.5.4 Pitanja provođenja sigurnosne politike

Zakoni određuju što je društveno prihvatljivo i dozvoljeno ponašanje, a što nije. Na žalost, ne pridržavaju se svi zakona te zbog toga država ima mehanizme, u vidu policije i pravosudnih organa, koji se brinu da se zakoni poštuju i provode. Mđdutim, i pored postojanja mehanizama događaju se kršenja zakona, od kojih neka čak prođu i nekažnjeno. Očigledno je potrebno pronaći adekvatnu ravnotežu između ulaganja i ostvarene sigurnosti. Analogno ovome i provođenje sigurnosne politike računalnih sustava zahtjeva određene resurse, što obavezno povlači troškove, pa se uvijek postavlja i pitanje ekonomske opravdanosti. Ulaganje u sigurnost ne bi smjelo biti veće od vrijednosti onoga što se štiti, zapravo moralo bi biti dovoljno malo, da bi bilo opravdano. Opravdana visina ulaganja u neku mjeru sigurnosti bi trebala biti izračunata.

2.5.5 Upravljanje rizikom

Rizik ima i definiciju koja se koristi i koja uključuje dva nova pojma: prijetnja i slabost. Prijetnja je uzrok nekog incidenta koji narušava sigurnost informacija. Prijetnja se može ostvariti ako postoji neka slabost u sustavu upravljanja sigurnošću informacija. Rizik je vjerovatnost ostvarenja prijetnje i iskorištavanja postojeće slabosti. Eliminacijom bilo prijetnje bilo slabosti može se eliminirati rizik. Na žalost, niti slabosti niti prijetnje se ne mogu u potpunosti ukloniti. Slabosti (eng. *vulnerabilities*), koje se u području sigurnosti često nazivaju i sigurnosnim propustima, nastaju ili kao posljedica odstupanja realizacije od specifikacije, ili kao posljedica odstupanja specifikacije od originalnih zahtjeva na sigurnost. Zahtjevi na sigurnost su iskazani u sigurnosnoj politici. Dizajn procedura koje treba provoditi sigurnosnu politiku predstavlja specifikaciju za realizaciju sigurnosti. Realizacija je konkretni sustav za zaštitu sigurnosti informacija. Postoji brojna literatura koja teoretski razmatra zašto praktične realizacije ne mogu u potpunosti odgovarati specifikacijama, koje opet ne mogu u potpunosti obuhvatiti zahtjeve. Razlozi koji se navode mogu biti ljudski faktor [13], ekonomski faktor, kao i princip da ne postoji testiranje koje bi jamčilo da neka programska podrška (eng. *software*) nema grešaka. Prijetnja je mogućnost narušavanja sigurnosti. Akcije kojima se prijetnje ostvaruju i od kojih se treba štititi nazivaju se napadi. Posljedice prijetnji se mogu podijeliti u četiri kategorije [14]:

• otkrivanje (eng. *unauthorized disclosure*) – neovlašten pristup informacijama

• prijevara (eng. *deception*) – prihvaćanje pogrešnih podataka

• smetnja (eng. *disruption*) – prekidanje ili sprečavanje normalnog rada

• uzurpacija (eng. *usurpation*) – neovlaštena kontrola nekog dijela sustava

Prijetnje dolaze iz različitih izvora, imaju različite uzroke, nepredvidive su, a nekad za njih nema posebnog razloga. Zato ih je teško eliminirati u potpunosti. Prirodna katastrofa je primjer prijetnje koja ugrožava sigurnost, a ne može se niti predvidjeti niti eliminirati. Ljudski postupci su također nepredvidiva, ali česta, prijetnja sigurnosti. Ljudi ugrožavaju sigurnost nekad namjerno, ali jos češće iz neznanja. Pošto je nemoguće u potpunosti ukloniti rizik, razvijena je metodologija upravljanja rizikom. Upravljanje rizikom sastoji se od tri koraka [14]:

• analiza rizika

• proračun rizika

• tretman rizika

2.5.5.1 Analiza rizika

Analiza rizika je sistematična identifikacija izvora rizika i procjena moguće štete. Analiza rizika podrazumjeva identifikaciju i evidentiranje svih resursa organizacije. Za svaki od resursa potrebno je identificirati slabosti te prijetnje koje mogu iskoristiti otkrivene slabosti. Ova analiza i prikupljeni podaci daju osnovu za proračun rizika i njegov tretman.

2.5.5.2 Proračun rizika

Proračun rizika je proces uspoređivanja procijenjenoga rizika sa zadanim kriterijem rizika. Kriterij je skalar koji određuje važnost rizika u odnosu na postavljene prioritete. Prioriteti mogu biti, između ostalog, financijskog, pravnog ili društvenog karaktera. Postoji više načina proračuna rizika, ali se najčešće koristi očekivani godišnji gubitak (eng. *Annualized Loss Expectancy, ALE*) za svaki od potencijalnih slučajeva gubitka. U nastavku je pokazan način ALE. Prvo je potrebno utvrditi vrijednost imovine (eng. *asset value, AV*) koja je izložena riziku. Vrijednost imovine potrebno je izraziti u novčanoj vrijednosti. Ova vrijednost treba uključiti materijalni i nematerijalni trošak koji bi gubitak (uništenje, neupotrebljivost) imovine izazvao. Na primjer ukoliko poslužitelj na kojem se

nalazi baza podataka kupaca bude uništen, gubitak se sastoji od troška nabavke i zamjene servera, ali i troška izazvanog neupotrebljivošću poslužitelja i nemogućnošću davanja usluge, kao i mogućeg troška izazvanog gubitkom podataka čije sigurnosne kopije ne postoje. U slučaju da poslužitelj nije oštećen, ali su podaci s njega neovlašteno preuzeti i distribuirani, potrebno je procijeniti vrijednost ovih podataka, odnosno štetu po organizaciju koju će ova distribucija izazvati. Vrijednost imovine (AV) je potrebno pomnožiti s faktorom izloženosti (eng. *Exposure Factor, EF*) u slučaju događaja za koji se proračunava rizik. Faktor izloženosti nekom riziku je postotak vrijednosti imovine koji će biti uništen u slučaju dogadaja čiji se rizik računa. Ako će u slučaju poplave neki uređaj izgubiti 40%, a u slučaju požara 70% vrijednosti onda je faktor izloženosti za taj uređaj (imovinu) u slučaju poplave 0,4, a u slučaju požara 0,7.

Umnožak ove dvije vrijednosti naziva se očekivani jednokratni gubitak (eng. *single loss expectancy, SLE*).

$$SLE = AV \times EF \quad (1)$$

Potrebno je još utvrditi i godišnju učestalost događanja (ARO – Annual Rate of Occurrence) za događaj čiji se rizik procjenjuje. To je zapravo vjerovatnost da će se taj događaj dogoditi u toku godine za koju se ovaj rizik računa. Recimo, ako se prema povijesnim podacima požar u poslužiteljskoj sobi događa jednom u svakih deset godina, a poplava jednom u svakih pet, onda je ARO za požar 1/10 = 0,1 (10%), a za poplavu 1/5 = 0,2 (20%). Umnožak očekivanog jednokratnog gubitka i godišnje učestalosti događaja je traženi očekivani godišnji gubitak (ALE) :

$$ALE = SLE \times ARO \quad (2)$$

Iznos ALE je procjena koliki će godišnji gubici na nekoj imovini biti od dogadaja za koji se proračunava rizik. Recimo, ako neki uređaj vrijedi 20.000 KN (AV = 20.000 KN) i u slučaju poplave bi bio 40% uništen (EF = 0,4) i ako se statistički poplave u prostorijama u kakvoj se nalazi uredaj dešavaju jednom u pet godina (ARO = 0,2) onda je:

$$SLE = 20000KN \times 0{,}4 = 8000\ KN \quad (3)$$

$$ALE = 8000KN \times 0{,}2 = 1600KN \quad (4)$$

Za slučaj nematerijalne štete od neovlaštenog pristupa i distribucije povjerljivih podataka računica može biti:

vrijednost (šteta od gubitka) svih povjerljivih podataka AV = 100.000 KN, postotak podataka koji bi bio dostupan u slučaju neovlaštenog pristupa nekoj od korisničkih prijava EF = 0,3 (pretpostavljeno je da ni jedna od korisničkih prijava na sustav nema pristup do više od 30% povjerljivih podataka), vjerovatnost ovakvog neovlaštenog pristupa tokom godine ARO = 0,1. U ovom slučaju računica je:

$$SLE = 100000KN \times 0,3 = 30000KN \quad (5)$$

$$ALE = 30000KN \times 0,1 = 3000KN \quad (6)$$

Očekivani godišnji gubitak (ALE) daje informaciju na temelju koje se može prijeći u slijedeću fazu upravljanja rizikom, odnosno njegov tretman. Iz navedenog bi trebalo biti očigledno da proračun rizika nije lako napraviti i da se u ovom proračunu mogu pojaviti mnoge nepoznanice čija se vrijednost može samo pretpostaviti. Ova analiza može biti i kvalitativna, umjesto kvantitativna, bitno je da njen rezultat može biti iskorišten da bi se odgovorilo na pitanje što učiniti.

Nematerijalna šteta počinjena nad podatcima danas se može prilično uspješno spriječiti korištenjem kriptografije. Kriptiranjem podataka onemogućava se neovlaštenim osobama čitanje i korištenje podataka čak i ukoliko dođe do krađe istih.

2.5.5.3 Tretman rizika

Tretman rizika je izbor i provedba mjera za promjenu rizika. Ove mjere mogu biti:

- izbjegavanje rizika
- prihvaćanje rizika
- prijenos rizika
- optimizacija rizika

Odluka o izboru neke od mjera se donosi na temelju proračuna posljedica rizika i proračuna odnosa troškova tretmana rizika i troškova realizacije rizika. Izbjegavanje rizika je odluka da se ne uključi u neku aktivnost ili da se povuče iz neke situacije, ako se procjeni da su povezane sa određenim, prevelikim, rizikom. Na primjer, ako se proračuna da je rizik povezivanja računala s vrijednim podacima na Internet ili računalnu mrežu vrlo veliki, moguće je izbjeći taj rizik nepovezivanjem računala. Prihvaćanje rizika je odluka

da se ne poduzimaju nikakve mjere smanjenja rizika. Ako se proračuna da je rizik za organizaciju od dopuštanja korisnicima da koriste e-poštu u privatne svrhe mali, organizacija može odlučiti prihvatiti taj rizik i ne provoditi dodatne mjere zaštite. Prijenos rizika je prijenos tereta rizika na druge osobe putem osiguranja ili sličnog ugovora. Svake godine prilikom osiguravanja automobila svaki vlasnik ”procijeni“ rizik od krađe i oštećenja svog vozila i odluči koji dio rizika, obavezno ili potpuno osiguranje, će prenijeti na osiguravajuću kuću. Naravno prijenos većeg dijela rizika košta više. Optimizacija rizika je postupak minimiziranja negativnih i maksimizacije pozitivnih posljedica. Optimizacija je jedini postupak koji se bavi smanjenjem posljedica rizika putem provedbe različitih mjera. Ove mjere su zapravo realizacija sigurnosti. Ako je prilikom proračuna rizika ustanovljen očekivani godišnji gubitak (ALE) na razini organizacije za slučaj nekog događaja, onda se ova vrijednost može iskoristiti za donošenje odluke, koja odgovara na pitanje koju od mjera tretmana rizika treba poduzeti. Za rizične događaje uglavnom postoje mjere koje ih mogu spriječiti ili smanjiti njihovu vjerovatnost. Ove mjere imaju svoju cijenu (trošak). Vrijednost neke od mjera zaštite može se izračunati na slijedeći način:

Vrijednost mjere zaštite = ALE (bez mjere) - Trošak(provođenja mjere) = ALE(s mjerom) (7)

Iz ove jednadžbe mogu se izvući i prioriteti pri provođenju mjera te odlučiti koje rizike treba izbjeći, koji se mogu prihvatiti, od kojih se bolje osigurati, a za koje je najbolje provesti mjere sigurnosti. Najpoznatiji standard koji regulira upravljanje sigurnosti informacija, ISO/IEC 27001 [16], zahtijeva da prvi korak u uspostavljanju sustava sigurnosti bude razmatranje rizika. Po ovom standardu, rizik je prvo neophodno identificirati, zatim ga analizirati i procijeniti te odrediti na koji način će se sustav nositi s rizikom. Standard definira mnogo detalja iz ovog područja, ali ono što je bitno je da se prilikom definiranja koraka za identifikaciju rizika definira i okvir za utvrđivanje prijetnji sigurnosti informacija.

2.5.6 Od čega, što i kako zaštititi?

Napadi mogu proizaći iz prijetnji. Najčešće korištena podjela napada je [17]:

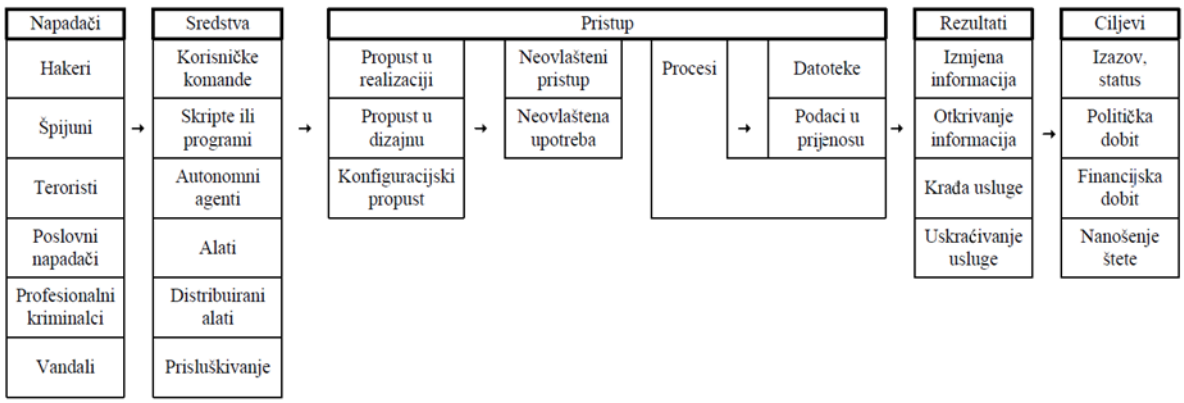
- izviđanje – testiranje potencijalne mete radi prikupljanje informacija. Ovi napadi su česti i uglavnom ne uzrokuju štetu, osim ako se s njima ne otkrije slabost koja se kasnije iskoristi.
- onemogućavanje pružanja usluge (eng. *DoS – denial of service*) – napadi koji imaju za cilj da poremete normalan rad sustava, tako da napadnuto računalo prestane raditi ili da se blokira mrežni promet
- udaljeni pristup (eng. *R2L – remote to local*) – napadi u kojim neovlašteni korisnik zaobilazi normalan proces provjere identiteta i izvršava naredbu na napadnutom računalu.
- podizanje privilegija (eng. *U2R – user to root*) – napadi kojima ovlašteni korisnik sustava zaobilazi normalan proces provjere identiteta da bi dobio privilegije drugog korisnika, najčešće onog s najvećim privilegijama.

Slijed događaja prilikom napada može se razdvojiti u tri faze [17]:

1. Vrijeme prije napada kada napadač izviđa sustav u potrazi za slabostima koje bi mogao iskoristiti.

2. Izvođenje napada koristeći pronađenu slabost.

3. Iskorištavanje uspješno izvedenog napada putem izvođenja radnji od strane napadača koje inače ne bi bile moguće.



Slika 6. CERT sistematizacija [18]

Na slici 6. data je sistematizacija i način povezivanja svih faktora u sekvenci ugrožavanja sigurnosti koju koristi CERT (eng. *Computer Emergency Response Team*). Napadači

imaju ciljeve i ostvaruju ih koristeći sredstva koja im omogućavaju pristup kojim postižu rezultate koji ostvaruju cilj. CERT sistematizacija sa slike 6 ukazuje na to što je zapravo ono što treba štititi. Različiti napadači koristeći različita sredstva pokušavaju postići mali skup rezultata. Ti rezultati su: izmjena informacija, otkrivanje informacija, uskraćivanje usluge i krađa usluge. Iz ovog skupa je očigledno što treba spriječiti, odnosno koja svojstva informacija treba očuvati. Informacije treba zaštiti od neovlaštenog otkrivanja, neovlaštene izmjene i uskraćivanja ovlaštenim subjektima. Krađa usluge zapravo omogućava svaki od prethodna tri rezultata. Sigurnost računalnih sustava se obično realizira kroz tri procesa. To su: potvrdivanje identiteta (eng. *authentication*), provjera ovlaštenja (eng. authorization) i evidentiranje (eng. accounting). Potvrđivanje identiteta je provjera da je identitet subjekta zaista onaj koji subjekt kaže da jest. Provjera ovlaštenja je provjera prava pristupa objektima za subjekt utvrđenog identiteta. Evidentiranje je čuvanje podataka o svim akcijama subjekata. Potvrđivanje identiteta i provjera ovlaštenja omogućavaju pristup informacijama samo onim subjektima koji na to imaju pravo, što jamči povjerljivost informacija. Pored toga, procedure utvrđivanja identiteta i provjere ovlaštenja dozvoljavaju promjenu informacija samo ovlaštenim subjektima na ovlašteni način, što osigurana integritet informacija. Ova dva procesa, dakle, ne samo da omogućavaju ovlaštenim subjektima odgovarajući pristup informacijama, već i sprječavaju pristup neovlaštenim subjektima što izravno utječe na dostupnost informacija. Evidentiranje akcija subjekata omogućava provjeru je li došlo da narušavanja principa povjerljivosti, integriteta i dostupnosti informacija, i ako jest na koji način. Za pristup i promjenu informacija od strane ovlaštenog subjekta vezani su i pojmovi odgovornosti (eng. *accountability*) i neporicanja (eng. *non-repudiation*). Odgovornost i nemogućnost poricanja su svojstva sigurnog računalnog sustava i uglavnom se ostvaruju utvrđivanjem identiteta i evidentiranjem akcija. Evidentiranje omogućava da svaki subjekt bude odgovoran za svoje akcije te da ih ne može poreći. Spomenuti procesi zaštite sigurnosti informacija postižu se realizacijom kontrola. Kontrole se obično dijele na administrativne, logičke i fizičke. Administrativne kontrole su primarno politike i procedure uspostavljene da bi se definiralo dozvoljeno ponašanje i načini provođenja politike. Tehničke, ili logičke, kontrole su uređaji, procesi, protokoli i druge mjere za zaštitu informacija. Fizičke kontrole su uređaji i sredstva za fizičku kontrolu pristupa i zaštitu dostupnosti informacija. Drugi način podjele kontrola sigurnosti je na preventivne, detektivne i korektivne. Preventivne kontrole sprječavaju narušavanje sigurnosti. Kada ove kontrole ne uspiju spriječiti neko narušavanje sigurnosti, detektivne kontrole otkrivaju da je došlo do narušavanja sigurnosti. Korektivne kontrole ispravljaju posljedice narušavanja sigurnosti, tako da

prekinu događaj koji je narušio sigurnost, ili tako da povrate sustav na stanje koje je bilo prije događaja ili, što je najbolje, tako da omoguće da sustav nastavi da sigurno funkcionira i tokom ovakvog događaja. Sigurnosna politika sustava provodi se pomoću sigurnosnih mehanizama. Sigurnosni mehanizam je metoda, sredstvo ili procedura koji provodi neki dio sigurnosne politike [19]. Sigurnosni mehanizmi su realizacija kontrola. Sigurnosni mehanizmi mogu biti tehnički i netehnički. Sredstva su primjer tehničkih, dok su procedure primjer netehničkih sigurnosnih mehanizama. Sigurnosnih mehanizama ima mnogo, a mogu se grupirati u mehanizme za utvrđivanje identiteta; mehanizme za kontrolu pristupa; i mehanizme za evidentiranje. Jedan od osnovnih principa dizajna u računalnoj znanosti je odvajanje mehanizama od politike, u smislu da mehanizmi ne bi trebali diktirati ili ograničavati politiku [20]. Politika sustava, naime, ne smije ovisiti od nekog konkretnog skupa mehanizama jer politika definira što je dozvoljeno i što nije, a ne kako će se to provesti u djelo. Ovaj princip je originalno postuliran za računarstvo, a može se izravno primjeniti i na sigurnost informacija.

Osiguravanje fizičke sigurnosti uređaja, kao i isticanje važnosti posjedovanja procedure za izradu sigurnosne kopije, oslanja se na važeće standarde za upravljanje informacijskom sigurnošću. Značajke procedure i stvaranje sigurnosne kopije podataka kao i njezino obnavljanje i provjera valjanosti, prezentiraju se kroz standardne funkcije operacijskog sustava. Postoje različite vrste imovine kojima pojedina organizacija može raspolagati (informacije, softverski paketi, fizička imovina, usluge, osoblje te nematerijalna imovina) stoga je važno da organizacija vodi popise imovine da bi se mogla osigurati njezina učinkovita zaštita. Popisivanje lokacija i dijelova opreme važnije je u kontekstu poslovnih organizacija s obzirom na to da je takav popis važan preduvjet upravljanja sigurnosnim rizicima, pri čemu je važno da se točno zna tko preuzima rizik za, na primjer, gubitak uređaja ili njegovo uništenje. Osiguranje fizičke sigurnosti uređaja potrebno je radi smanjena rizika od neovlaštenog pristupa informacijama i zaštite od njihova gubitka ili oštećenja. Pozornost se treba obratiti na smještaj uređaja radi zaštite od prijetnji i opasnosti koje mogu doći iz okruženja, na primjer: potrebno je smanjiti rizike od potencijalnih fizičkih prijetnji poput požara, poplave, potresa, prekida fizičkog napajanja, utjecaja temperature i vlage izolirati uređaje koji trebaju posebnu zaštitu i slično. Poznavanjem lokacija na kojima su smješteni uređaji s procijenjenim visokim sigurnosnim rizikom moguće je primijeniti neke od mjera fizičke zaštite kao što su određivanje granica fizički sigurnog prostora i kontrole fizičkog pristupa. Pod određivanje granica fizički sigurnog prostora podrazumijeva se postojanje jasno definiranih granica

sigurnog prostora u kojem se nalaze uređaji s osjetljivim podacima, postojanje recepcija ili sigurnih ulaza, ugradnja sustava za detekciju provale, pridržavanje pravila protupožarne zaštite i slično. Međutim, sigurno područje može biti i ured koji se zaključava. Na kontroli ulaska u sigurna područja potrebno je evidentirati vrijeme dolaska i odlaska te nadzirati posjetitelje, osim ako nemaju prethodno odobreno dopuštenje za pristup uređajima s osjetljivim podacima. Prava na pristup sigurnim područjima trebaju se redovito ažurirati. Oprema koja se nalazi u uredima može se dodatno fizički zaštititi zaključavanjem u ormare, montiranjem kablovskih brava kojima se periferna oprema pričvršćuje za računalo ili bravama s lozinkama. Da bi se osigurala neprekidna dostupnost uređaja, potrebno je redovito održavanje, a posebnu važnost treba obratiti na sigurnost uređaja koji se iznose izvan prostora organizacije.

2.5.6.1 Sigurnosne kopije podataka

Ukoliko se nedovoljna pažnja posveti rizicima koji ugrožavaju računalne sustave, u organizacijama su moguće situacije koje mogu uzrokovati zastoje u poslovanju. I da se ne bi dogodio neplanirani zastoj, organizacije i korisnici moraju redovito obavljati procedure za izradu i održavanje sigurnosnih kopija. U protivnom može doći do katastrofalnih posljedica kako za korisnike tako i za organizaciju. Uzrok tome je što je poslovanje ovisno u informacijskim tehnologijama. Pred informatičke podatke se postavljaju visoki kriteriji zaštite koji su jednaki ili čak veći od kriterija zaštite zapisa u poslovnim knjigama. Informacijski sustav je dio infrastrukture organizacije te je stoga nedostupnost istog ili uništenje podataka veliki rizik za koji treba planirati mjere kontrole i obavljati postupke kojima se povećava potpuno, sigurno i jeftino vraćanje podataka. Izrada sigurnosnih kopija (eng. *backup*) je osnovna pretpostavka koja se postavlja pred sustav koji mora zadovoljavati sigurnosne zahtjeve. Postupak izrade sigurnosnih kopija zajedno s postupkom povratka podataka, predstavlja osnovnu proceduru kojom se sustav zaštićuje od gubitka podataka i osigurava brza obnova podataka u slučaju nepravilnosti u radu sustava kao što su npr. prekidi u radu računalnog sustava, infekcije virusima ili pak prirodne katastrofe poput poplava i požara. Jedan od glavnih razloga za izradu sigurnosnih kopija je raspoloživost sustava. No, za potrebe ovog rada razmatra se cjelovitost i integritet podataka. Još jedan razlog za izradu sigurnosnih kopija je zakonska obveza čuvanja financijskih i drugih sličnih podataka.

Donošenje odluke o tome za koje podatke je potrebno izrađivati sigurnosne kopije ovisi kako od osobe do osobe tako i od organizacije do organizacije. U osnovi, za sve podatke koje nije jednostavno, lako ili ih uopće nije moguće zamijeniti u slučaju gubitka, treba raditi sigurnosne kopije. U nastavku slijedi popis podataka za koje se preporuča izrada sigurnosnih kopija:

• elektronička pošta,

• bankovni podaci i drugi financijski podaci kao što su npr. ugovori,

• digitalne fotografije

• programi koji su skinuti s Interneta ili kupljeni,

• osobni i organizacijski projekti,

• adresar iz aplikacije za elektroničku poštu,

• kalendar rada, itd…

2.5.6.2 Kriptografija kao mjera zaštite clouda

Neautorizirani ulazak može se spriječiti tako da korisnici kriptiraju svoje podatke prije nego što ih pohrane na *cloud*. Kriptografski programi mogu transformirati cjelokupni set podataka tako da primjene adekvatni kriptografski algoritam na tu skupinu podataka. Na primjer, informacija se translatira u neki drugi jezik tako da samo oni koji poznaju jezik mogu razumjeti napravljenu translaciju. Jednosmjerna kriptografija aplicira jednosmjernu funkciju na podatke i tako producira fiksnu zaštitu (engl. *hash*) ili zaštitnu vrijednost. Funkcionalnost izvedena je tako da je nemoguće vratiti podatak u prvobitno stanje [21]. Za razliku od jednosmjernih funkcija za zaštitu podataka, primjenom dvosmjerne funkcije u zaštiti podataka oguće je vratiti podatak u prvobitno stanje ali samo od strane ovlaštenih osoba, pod striktno definiranim uvjetima. Bitni faktori koji utječu na kriptiranje podataka ovise o jačini odnosno intenzitetu enkripcije, duljini enkripcijskog ključa (dulji ključevi su uglavnom manje podložni napadima nego kraći) i raspolaganje ključevima.[20] Generalno podaci se smatraju dobro kriptiranim ako se kriptografske metode pokažu efikasnim i sigurnim u realnom svijetu. Kriptografiju je moguće primijeniti na podatke unutar elektroničkog dokumenta, datoteke, baze podataka ili neke druge kolekcije informacija. Korisnici mogu primijeniti kriptografiju na dijelove ili još češće na cjelokupne skupine

podataka prije nego što ih pohrane na *cloud*. Primjerice jednosmjerna ili dvosmjerna kriptografija može se primijeniti samo na imena dok ostali podaci mogu ostati netaknutima u pogledu kriptografije. Dekriptiranje te ponovna enkripcija podataka reducira performanse, što predstavlja veliku manu kriptografiji. Nadalje, isto tako s podacima koji su kriptirani vrlo moćnim kriptografskim algoritmima poput vojnih podataka i podataka od iznimne državne važnosti moraju proći proces dekriptiranja kako bi se nad njima mogla vršiti daljnja obrada u pogledu dodatne analize, sortiranje podataka, indeksiranje, optimizacija i sl. Dekriptiranje podataka može dovesti do kompromitacije istih zato se uvijek nastoji prilikom dekriptiranja pohraniti kriptirane podatke na siguran sustav (primjerice *offline* računalo) te tek tada izvršiti potpuno dekriptiranje. Neovlašteni pristup je isto tako moguć ako se podaci presretnu prilikom transmisije na sam *cloud*. Ako korisnik šalje ne kriptirane podatke putem kriptiranog kanala, davatelji usluga će opet dobiti ne kriptirane podatke. Obrnuto, kriptirani kanali nisu potrebni za pouzdanu transmisiju od već snažno kriptiranih podataka, iako netko tko nadzire kanal ionako može samo presresti kriptirane podatke koji nisu od nikakvog značaja.

3. ZAKONSKA REGULATIVA U PODRUČJU ZAŠTITE NA RADU

Zaštita na radu je skup tehničkih, zdravstvenih, pravnih, psiholoških, pedagoških i drugih djelatnosti pomoću kojih se otkrivaju i otklanjaju opasnosti što ugrožavaju život i zdravlje osoba na radu i utvrđuju mjere, postupci i pravila da bi se otklonile ili smanjile te opasnosti. Na temelju toga "svrha zaštite na radu je stvarati sigurne uvjete kako bi se spriječile ozljede na radu, profesionalne bolesti i nezgode na radu. Sve navedeno se mora provoditi u skladu sa zakonima i propisima u Republici Hrvatskoj, ali također obratiti pažnju na usklađivanje sa europskim direktivama i normama. Zaštita na radu unutar Europske Unije područje je rada Europske agencije za sigurnost i zdravlje na radu (EU-OSHA), Occupational Safety and Health Administration. Njihov cilj je promoviranje važnosti zaštite kroz pristup prevencije opasnosti i eliminiranja rizika na radnom mjestu. Agencija se bavi istraživanjem opasnosti i predlaganjem mjera poboljšanja zaštite na radu na radnom mjestu, dok u svom radu sudjeluju sa vladama zemalja članica, organizacijama radnika i zaposlenika, regulativnim EU tijelima i privatnim tvrtkama. [22]

EU-OSHA provodi istraživanja i prati rezultate primjene mjera zaštite na radu te na temelju tih rezultata predlaže izmjene i poboljšanja. provode ankete među zaposlenicima i poslodavcima sa područja Europske Unije te se obrađuju rezultati i prati statistika stanja zaštite na radu u zemljama članicama. Zaštita na radu u zemljama Europske Unije prvi puta je uređena Direktivom 89/391 EEC koja je prihvaćena 1989. godine s ciljem poboljšanja zaštite i zdravlja radnika na radnom mjestu. Direktivom je donešen okvir mjera čiji je cilj unaprijeđenje sigurnosti rada. Implementacija ove Direktive u zemljama članicama Europske Unije, prema izvještaju Povjerenstva 2004. godine, pridonijela uvođenju kulture prevencije opasnosti na radnom mjestu te pojednostavnjenju i racionalizaciji zakonske legislative pojedinih zemalja članica.

Mjere i propisi iz područja zaštite na radu uređeni su OSHA standardom. Taj standard uređuje zahtjeve kojima mora udovoljavati radna oprema, okolina, objekt. Definirani su zahtjevi koji se tiču samog objekta kao što su zahtjevi za radne površine i površine za hodanje pa tako imamo za primjer propis za uređenje visine ograda na stubištu ili na prostorima na kojima se radi na povišenom. Ostali propisi tiču se predloženih mjera za evakuaciju i spašavanje, zaštitu zdravlja i opasnosti koje prijete iz radne okoline, opasnih radnih tvari, osobnih zaštitnih sredstava, obaveza iz područja prve pomoći (poput pribora za prvu pomoć), zaštite od požara i uvjetima koje moraju zadovoljiti sustavi za dojavu i

gašenje požara, mjerama za skladištenje i rukovanje opremom pod tlakom, mjerama zaštite koje moraju ispunjavati strojevi s povećanim opasnostima te uvjetima koje mora zadovoljiti ručni i prijenosni alat, uređaji za zavarivanje, mjere kojima mora udovoljavati električna instalacija (od izolacije vodiča do izvođenja vodiča), uvjeti rada ako se radi o radovima ispod površine zemlje. Ovaj standard osnova je modernih zakona o zaštiti na radu članica Europske unije [23].

Republika Hrvatska (RH), prije ulaska u Europsku uniju (EU) morala je svoje zakone, propise, norme i regulative uskladiti sa zakonima, propisima, regulativama i normama EU. Osnovni zakonski propis koji uređuje zaštitu na radu u Republici Hrvatskoj je Zakon o zaštiti na radu (N. N. br. 59/96., 94/96., 114/03., 100/04., 86/08., 116/08.). Svrha ovog zakona je sprečavanje ozljeda na radu, profesionalnih bolesti, drugih bolesti u svezi s radom te zaštita radnog okoliša. Zakon utvrđuje subjekte, njihova prava, obveze i odgovornosti glede provedbe zaštite na radu, kao i sustav pravila zaštite na radu čijom se primjenom u najvećoj mogućoj mjeri postiže svrha navedenog Zakona. Prethodno spominjajući primoranost usklađivanja zakona RH sa zakonima EU taj cilj je postignut preko okvirne Direktive 89/391/EEC kao i sa dodacima na koje se ona poziva.

Europska Okvirna direktiva o sigurnosti i zdravlju na radu (Direktiva 89/391 EEZ) donesena 1989. bila je važna prekretnica za poboljšanje sigurnosti i zdravlja na radu, međutim stupila je na snagu 1. siječnja 1997. godine. Direktivom se jamče minimalni zahtjevi u vezi sa zdravljem i sigurnošću diljem Europe, a istovremeno se državama članicama dopušta da zadrže ili uvedu strože mjere. Okvirnu direktivu bilo je potrebno do kraja 1992. prenijeti u nacionalno pravo. Posljedice koje je prenošenje imalo za nacionalne pravne sustave razlikovale su se među državama članicama. U nekim je državama članicama prenošenje Okvirne direktive imalo velike pravne posljedice zbog neodgovarajućeg nacionalnog zakonodavstva, dok u drugim državama članicama nisu bile potrebne veće prilagodbe.[24]

U Narodnim novinama 71/14., objavljen je novi Zakon o zaštiti na radu, a stupio je na snagu 19. lipnja 2014. godine. Novi Zakon uvodi odredbe o osnivanju Zavoda za unaprjeđivanje zaštite na radu koji preuzima dio poslova postojećeg Hrvatskog zavoda za zaštitu zdravlja i sigurnosti na radu, koji će zadržati svoje djelatnosti koje se odnose na zdravstvene aspekte zaštite na radu. Novi Zavod za unaprjeđivanje zaštite na radu koji će u provedbenom smislu biti u okvirima nadležnosti Ministarstva rada i mirovinskoga sustava, nadležan za praćenje stanja i predlaganje mjera za unapređenje zaštite na radu i preuzima segment sigurnosti u zaštiti na radu, koji će, između ostaloga, pružati stručnu

pomoć u provođenju mjera zaštite na radu i prevenciji nezgoda, ozljeda poslodavcima, a osobito malim i srednjim, kao provedbeno i savjetodavno tijelo. Novi Zakon po prvi puta uvodi odredbe o mjerama zaštite radnika od psihosocijalnih rizika, ponajprije se pod uzročnicima psihosocijalnih rizika smatra stres i psihofizioloških napora na radu, sve u cilju prevencije i edukacije svih dionika [25].

3.1 Zaštita osobnih podataka i opća uredba o zaštiti osobnih podataka (GDPR)

Digitalizacija je okosnica razvoja razmjene informacija te otvara kompleksnost zaštite privatnosti i informacijske sigurnosti. Liberalizacija se ponajprije odnosi na otvorenost neograničenog komunikacijskog prostora s pratećim procesom kulturne globalizacije. Globalizacija pak, uz podršku informacijskih i komunikacijskih tehnologija i otvorena globalnog prostora, svjetske trendove premješta u lokalne okvire. Preduvjet za ovakav razvoj interneta bila je otvorena, decentralizirana, interaktivna mrežna arhitektura, zatim mrežni protokoli koji također moraju biti otvoreni i koji se mogu jednostavno modificirati, te institucije/strukture upravljanja i razvoja Interneta koji moraju biti u skladu s principima otvorenosti i suradnje kako ga ne bi kočile. trenutku identifikacijom može postati koristan, ili pak opasan osobni podatak, koji se na bilo koji način mora zaštititi od javnosti, ili od moguće zlouporabe. Otvorenost arhitekture Interneta i njegov stalni razvoj u kojemu su korisnici bili istovremeno i kreatori i pridonosili njegovu daljnjem razvoju, bile su njegove glavne snage razvoja [26]. Nezaustavljivi trend informacijskog društva unaprjeđuje kvalitetu komunikacija, oplemenjuje razvoj tehnologija, ali ima važan zadatak – uspostavljanje modela zaštite podataka, osobito zaštite osobnih podataka, najvrjednijeg dijela osobnosti i koncepta individualnosti i nasuprot globalnoj univerzalnosti jedan je od ključnih ciljeva reforme regulative zaštite podataka koja je usvojena u travnju 2016. godine. Opća EU uredba o zaštiti podataka 2016/679 (engl. *General Data Protection Regulation* – dalje GDPR), unosi velike promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje raspolažu osobnim podacima građana Europske unije. Nadalje, kao članica Europske unije, Hrvatska je preuzela obvezu uskladiti svoje zakonodavstvo s novodonesenom regulativom EU za područje zaštite podataka, kao i sve ostale države članice EU, do 2018. Važnost ove reforme proizlazi upravo iz njenog temeljnog cilja donošenja, a to je ustanoviti granice i maksimalno zaštititi protok podataka s naglaskom na obradu osobnih podataka i zaštitu privatnosti građana

na području Europske unije u suvremenom informacijskom društvu čime se cjelokupna pravna i sigurnosna zaštita dižu na višu razinu sigurnosti i zaštite u suvremenom informacijskom društvu. Uz navedenu Opću uredbu, sastavni dio usvojena zakonodavnog paketa je i Direktiva o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka 2016/680.

Tablica 1. Usporedba razlika između Direktive 95/46/EZ i Opće uredbe o zaštiti podataka [27]

Direktiva 95/46/EZ	GDPR
• Identitet kontrolora • Svrhe obrade • Obaveza odgovoriti na subjekta podataka • Pravo pristupa, ispravaka i prigovora • Primatelji • Prijenos podataka	• Identitet kontrolora i DPO-a • Svrha • Razdoblje čuvanja podataka • Pravo pristupa, ispravaka, ograničenja i prigovora • Pravo na podnošenje žalbe • Primatelji • Prijenosi • Pravo povlaćenja suglasnosti u bilo kojem trenutku • Legitiman interes kontrolora ili treće osobe (ako je relevantno) • Informacije o profiliranju • Sve ostale informacije koje jamče zakonitost prerade

Tom se Direktivom ujednačava zaštita osobnih podataka koje obrađuju pravosudna i policijska tijela u državama članicama Europske unije. Ona jasno definira mogućnosti obrade osobnih podataka ispitanika, uključujući njihovo iznošenje u treće zemlje, pri čemu se osiguravaju visoki standardi zaštite pojedinaca razmjerno s potrebama provedbe odgovarajućih policijskih i pravosudnih postupaka. Ovom Direktivom jasno se određuje nadzor neovisnog tijela za zaštitu osobnih podataka nad njihovom obradom[24]. Važno je istaknuti kako GDPR zamjenjuje Direktivu 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka te stupa na snagu danom donošenja i izravno se primjenjuje u svim državama članicama EU-a.

3.1.1 Definicija osobnog podatka prema GDPR-u

Nova EU Uredba donosi bitne promjene u pravilima koja definiraju osobne podatke i samu obradu podataka u cjelini. Prvi Zakon o zaštiti osobnih podataka (NN, 103/03, 118/06, 41/08, 130/11, 106/12 – dalje ZZOP) u Hrvatskoj je donesen još 2003. godine (zadnje izmjene i dopune 2012.), a ova je Uredba prvi odmak u zakonskoj definiciji na razini Europske unije još 1995. godine. Iscrpna pravna definicija osobnog podatka dana je u ZZOP-u prema kojem: "osobni podatak predstavlja svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati odnosno osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet" (ZZOP, čl. 2. st. 1.). Nova Uredba dodaje izrijekom dopunu pravne definicijie prema kojem je osobni podatak svaki podatak kojim se "osoba može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;" (GDPR, čl. 4. st. 1.). Odnosno definicija izravno uvodi pojam mrežni identifikator te se nadalje u tekstu Uredbe po prvi put definiraju (i zakonski uređuju) genetski podaci" i biometrijski podaci kao osobni podaci. Naime, genetski podaci predstavljaju osobne podatke "koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca"; (GDPR, čl. 4. st. 13.) dok se pod pojmom. biometrijski podaci podrazumijevaju se "osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci". (GDPR, čl. 4. st. 14.). Kao i ranije, ključan dio za obradu osobnih podataka jest "privola" osobe na korištenje njenih osobnih podataka koja se smatra jasnim činom odobrenja. Naime, "privola" ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje, pristanak za obradu osobnih podataka koji se na njega odnose. (GDPR, čl. 4. st. 11.). Novina je činjenica da su u slučaju proboja sigurnosti podataka tvrtke dužne obavijestiti nadležne službe, ali i pojedinca čiji su osobni podaci povrijeđeni što ranije nije bio slučaj. Budući da se na osnovu prikupljenih osobnih podataka identificirane osobe dalje mogu raditi daljnja istraživanja i analize, neki su podatci, naravno iznimno u slučajevima predviđenim svim nacionalnim i međunarodnim

normama, dodatno prošireno na iznimnu dozvolu ispitanika, te u slučaju kada je potrebno radi zaštite njegovog zdravlja ili života, zaštićeni od daljnjih obrada. Možda se svi i neće složiti s kategorijom osjetljivih podataka, jer netko bi radije zaštitio nekakve druge podatke, ali u tu kategoriju podataka prema Zakonu o zaštiti osobnih podataka pripadaju slijedeći podaci. " Zabranjeno je prikupljanje i daljnja obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku."Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12 čl.8.) izuzimajući situaciju kada je sam ispitanik objavio takve podatke te postavljajući jasnu granicu povjerljivosti podataka i daljnjih korisnika ograničavajući se na nadležna tijela i svrhu u koju je podatak prikupljen. Ovdje je jasno kako u pogledu osjetljivih podataka nedovoljnom pažnjom ispitanik može iznijeti u javnost dio takvih podataka, pogotovo u današnje vrijeme kada je dovoljan samo jedan „sviđa mi se" (eng. *like*) na nekoj od društvenih stranica da ga poveže s nekom pripadnom skupinom ili rasom, a da on toga nije niti svjestan. Međutim, to ipak ne znači da će odmah biti stigmatiziran ili će uslijediti nekakva zlouporaba takvih podataka, ali u svakom slučaju ostavlja otvorene mogućnosti.

Obrada osobnih podataka znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje (članak 4. Opće uredbe).

3.1.1 Europska regulativa o zaštiti podataka u oblaku

Europska unija ne donosi zakone već direktive kao jedan od pravnih akata. Direktive su pravni akti Unije upućeni svim ili nekim državama članicama a koje države članice moraju usvojiti odnosno, do nekog određenog roka prenijeti u vlastito zakonodavstvo. Direktive imaju posredan učinak. Iznimno, direktive imaju neposredan učinak ako direktiva nije u roku pretočena u nacionalno pravo i ako je sadržajno bezuvjetna i jasno određena te ako iz nje pojedinac stječe neko pravo prema državi [28]. Niti jedan pravni akt se ne odnosi konkretno na zaštitu korisničkih podataka u oblaku već se odnosi na općenitu zaštitu osobnih podataka u elektroničkim komunikacijama.

Europski parlament donio je najprije Direktivu iz 1995. godine a zatim zbog potreba pojašnjavanja i nadopunjavanja direktive iz 1995. godine, Direktivu iz 2002. godine.

Direktiva 2002/58/EZ najprije donosi pregled definicija koje se primjenjuju u njoj [31]:

- korisnik;
- podaci o prometu;
- podaci o lokaciji;
- komunikacija;
- poziv;
- pristanak;
- usluga s dodatnom vrijednosti;
- elektronička pošta.

Korisnik predstavlja svaku fizičku osobu koja koristi elektroničke komunikacije u privatne i/ili poslovne svrhe. Korisnik prema Direktivi ne mora biti nužno i pretplatnik. Podaci o prometu označavaju podatke koji se obrađuju u svrhu prijenosa odnosno komunikacije na elektroničkoj komunikacijskoj mreži ili za njeno naplaćivanje. Podaci o lokaciji označavaju podatke koji su obrađeni u elektroničkoj komunikacijskoj mreži, koji naznačuju zemljopisni položaj korisničkog terminala, javno dostupne elektroničke komunikacijske usluge. Komunikacija je definirana kao svaka informacija koja se razmjenjuje ili prenosi između ograničenog broja strana putem javno dostupne elektroničke komunikacijske usluge. Komunikacija ne uključuje bilo koju informaciju prenesenu kao dio usluge emitiranja za javnost osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju a koji se može identificirati. Poziv predstavlja uspostavljenu vezu putem javno dostupne telefonske usluge, a koja omogućuje stvarno vremensku dvosmjernu komunikaciju. Pristanak korisnika ili pretplatnika predstavlja proces prihvaćanja. Usluga s dodatnom vrijednosti definirana je kao svaka usluga koja zahtijeva obradu podataka o prometu ili lokaciji, osim podataka o prometu koji nisu nužno potrebni za prijenos komunikacije ili za njeno naplaćivanje. Elektronička pošta je svaka tekstualna, glasovna, zvučna ili slikovna poruka, poslana preko javne komunikacijske mreže a koja se može pohraniti u mreži ili u primateljevom terminalu sve dok ju primatelj ne preuzme. U članku 3. određeno je kako će se Direktiva odnositi na obradu osobnih podataka, vezano s pružanjem javno dostupnih elektroničkih komunikacija, u javnim komunikacijskim mrežama u Zajednici.

Sigurnost podataka određena je člankom 4. Direktive. Prema članku 4., davatelj usluga elektroničkih komunikacija dužan je poduzeti odgovarajuće tehničke i organizacijske mjere, kako bi se zaštitila sigurnost svojih usluga, odnosno sigurnost mreže. Za provođenje tih aktivnosti, davatelj usluga dužan je surađivati s pružateljem javne komunikacijske mreže. Također, u ovom članku predviđeno je kako davatelj usluge mora pratiti trendove, odnosno poduzimati odgovarajuće mjere zaštite, ovisno o razini mogućih prijetnji. Nadalje, ovim člankom se određuje kako je davatelj javno dostupne elektroničke komunikacije usluge dužan obavijestiti pretplatnike o određenoj sigurnosnoj opasnosti i poduzeti sve mjere za otklanjanje opasnosti. Povjerljivost komunikacija opisana je člankom 5. Prema tom članku države članice moraju osigurati povjerljivost komunikacija i s time povezanih podataka o prometu, koji se šalje preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga. Članak nalaže državama članicama da zabrani svim neautoriziranim osobama: slušanje, prisluškivanje, pohranjivanje ili bilo koji drugi oblik presretanja i nadzora nad komunikacijama, a za kojeg nemaju pristanak korisnika. Prema članku 6. podaci o korisničkom prometu, nakon obrade i pohrane moraju se brisati ili učiniti anonimnima, u trenutku kada više nisu potrebni za prijenos komunikacije. Članak, nadalje, predviđa mogućnost obrade podataka o korisničkom prometu u cilju naplate usluga. Međutim, tada se podaci o prometu mogu obrađivati samo u razdoblju, dok postoji mogućnost pravnog pobijanja računa. Članak 9. opisuje podatke o lokaciji. Prema tom članku podaci o lokaciji, a koji nisu podaci o prometu, a odnose se na korisnike javnih komunikacijskih mreža, mogu se obrađivati, ali samo kada su ti podaci učinjeni anonimnima. Međutim, članak predviđa mogućnost obrade takvih podataka, a da nisu anonimni samo kada korisnik da pristanak za obradu podataka. Osim zaštite podataka, Direktiva određuje i druge elemente komunikacija kao što su: imenici pretplatnika, neželjene komunikacije, automatsko prosljeđivanje poziva i drugo [27]. Zaštita osobnih podataka, opisana je Uredbom zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka. Tom Uredbom ažurirana su i osuvremenjena načela sadržana u Direktivi o zaštiti podataka iz 1995. godine. Njome su utvrđena prava pojedinaca i obveze organizacija koje obrađuju osobne podatke, ali i obveze odgovornih za osobne podatke. U Uredbi se navode pojačana prava pojedinaca. Tim pravima pojedincima se daje više kontrole nad njihovim osobnim podacima. Kontrola je dana pomoću [30]:

- potrebe za jasnim pristankom pojedinaca na obradu osobnih podataka;
- lakšeg pristupa pojedinaca njegovim ili njezinim osobnim podacima;

- prava na ispravljanje, brisanje i „zaborav“;
- prava na prigovor, pa i za upotrebu osobnih podataka za potrebe izrade profila;
- prava na prenosivost podataka s jednog poslužitelja na drugi.

Uredba, također, donosi opće obveze voditelja obrade odnosno, osobe zadužene za obradu podataka. Jedna od obveza voditelja obrade je pružanje transparentnih i lako dostupnih informacija o ispitanicima i obradi njihovih podataka. Također, voditelj obrade ima obvezu provoditi odgovarajuće sigurnosne mjere, koje moraju biti usklađene s prisutnim rizikom, pri obradi podataka. Od voditelja obrade može se zatražiti izvješće o mogućoj povredi osobnih podataka. Nadalje, Uredba obvezuje organizacije, koje obavljaju određene rizične radnje obrade podataka, na imenovanje službenika za zaštitu podataka. Uredba previđa potrebu svake države članice da na nacionalnoj razini uspostavi neovisno nadzorno tijelo. Cilj uspostave takvog nadzornog tijela je, uz zaštitu osobnih podataka, uspostaviti mehanizam za osiguravanje dosljednosti u primjeni prava o zaštiti podataka, diljem EU. U RH to nadzorno tijelo je Agencija za zaštitu osobnih podataka. Također, Uredba prepoznaje mogućnost ispitanika za podnošenjem pritužbe određenom nadzornom tijelu, a posljedično i pravo na pravni tijek, naknadu i odgovornost. Zbog potrebe zbližavanja pojedinaca i nadzornih tijela, vezanih za odluke ispitanici imaju pravo da odluku nadzornog tijela ispita određeni sud (Upravni sud za RH). Protiv prekršitelja ove Uredbe određene su administrativne sankcije. Sankcije predstavljaju novčanu kaznu, kojom će se kazniti voditelji obrade podataka, i to u iznosu do 20 milijuna EUR ili do 4% ukupnog godišnjeg prihoda. Veličinu administrativnih uvoditi i određivat će tijela za zaštitu podataka [30].

3.2 Hrvatsko zakonodavstvo

Zaštita osobnih podataka u RH predviđena je Ustavom RH i Zakonom o zaštiti osobnih podataka (dalje: ZZOP) [29]. Pitanje osobnih podataka Ustavom je određeno člankom 37. Ustav predviđa svakom građaninu RH sigurnost i tajnost osobnih podataka. Nadalje, Ustav zabranjuje prikupljanje, obrađivanje i korištenje osobnih podataka, a da to nije određeno zakonom ili da građanin nije dao pristanak. Također, Ustav zabranjuje uporabu osobnih podataka, na način koji je suprotan utvrđenoj svrsi prikupljanja osobnih podataka. [30] Temeljitije uređenje zaštite osobnih podataka, ali i nadzora nad prikupljanjem, obradom i korištenjem osobnih podataka te iznošenjem iz RH provedeno

je ZZOP-om. Prema ZZOP-u vrha zaštite osobnih podataka je zaštita privatnosti ljudskog života i ljudskih prava te temeljnih sloboda, u koje se može ući: prikupljanjem, obradom i korištenjem osobnih podataka. Zaštita osobnih podataka, prema ZZOP-u, omogućena je svakoj fizičkoj osobi, bez obzira na: rasu, boju kože, spol, jezik, političko ili drugo uvjerenje, nacionalno ili socijalno podrijetlo, imovinu, rođenje, naobrazbu, društveni položaj ili neko drugo svojstvo ili obilježje. Člankom 2, ZZOP, daje značenje određenim pojmovima [31]:

- osobni podatak;
- obrada osobnih podataka;
- zbirka podataka;
- ispitanik;
- voditelj zbirke osobnih podataka;
- privola ispitanika.

Osobni podatak jest svaki podatak ili informacija, koja se odnosi na fizičku osobu (pravna osoba je isključena iz definicije), koja se pomoću te informacije može identificirati, izravnim ili neizravnim putem, preko jednog ili skupine podataka. ustanove, udruženja ili bilo kojeg drugog neprofitnog tijela, koje je neposredno vezano uz takve podatke, a koji se moraju odnositi na njihove članove. Zbirke osobnih podataka ne smiju sadržavati posebne kategorije podataka. Proces prikupljanja osobnih podataka vrlo je jasno definiran čak u odnosu na uobičajenu praksu, ZZOP uvodi značajna ograničenja. Po pitanju opsega osobnih podataka ZZOP nalaže da traženi podaci moraju biti bitnu u svrhu prikupljanja, odnosno da ispitanik može svo prikupljane podatke odbiti dati. Primjer takvih prikupljenih podataka su spol i godina rođenja. Također, ZZOP jasno definira potrebu za određivanjem svrhe i informiranja ispitanika. Cilj ove definicije je spriječiti neprimjereno i prekomjerno korištenje osobnih podataka. Temeljem toga ispitanik mora biti jasno i nedvosmisleno upoznat sa svrhom prikupljanja osobnih podataka, temom i opsegom. ZZOP zabranjuje davanje prikupljenih podataka trećim stranama. Nadalje, ZZOP inzistira na točnosti, potpunosti i ažurnosti osobnih podataka. Ako treća strana želi koristiti osobne podatke, mora podnijeti voditelju zbirke osobnih podataka pisani zahtjev. U zahtjevu mora biti jasno navedena svrha i pravni temelj korištenja podataka. Korištenje podataka, voditelj zbirke, može odobriti samo za obavljanje poslova utvrđenih zakonom. Voditelj zbirke dužan je voditi evidenciju davanja osobnih podataka, sa svrhom davanja. Svaki

ispitanik ima pravo uvida u evidenciju korištenja njegovih osobnih podataka. Iako se takvi podaci smatraju osobnima, dani podaci ne smiju omogućiti identifikaciju pojedinaca. ZZOP predviđa mogućnost iznošenja osobnih podataka izvan teritorija RH. To je jako bitno za *cloud* okruženje, zato što se *cloud* poslužitelji većinom ne nalaze na teritoriju RH. Voditelj zbirke osobnih podataka može staviti podatke na raspolaganje na teritoriju izvan RH. Međutim, država u koju se ti podaci „iznose“ mora imati jasno i kvalitetno uređenu zaštitu osobnih podataka. Ako postoji sumnja u uređenost zaštite osobnih podataka, voditelj zbirke dužan je zatražiti AZOP-ovo mišljenje. Prema ZZOP-u, ispitanik ima pravo, zatražiti od voditelja zbirke na vlastiti zahtjev, a u vremenskom roku od 30 dana:

- potvrdu u kojoj je navedeno obrađuju li se ispitanikovi osobni, ili ne;
- obavijest u razumljivom obliku, o podacima koji se odnose na ispitanika, čija je obrada u tijeku i izvor tih podataka;
- uvid u evidenciju zbirke osobnih podataka i uvid u osobne podatke, sadržane u zbirci osobnih podataka;
- izvatke, potvrde ili ispise osobnih podataka, koji su sadržani u zbirci osobnih podataka;
- ispis podataka o tome tko je i s kojom svrhom te po kojem pravnom temelju dobio na korištenje ispitanikove osobne podatke;
- obavijest o logici automatske obrade osobnih podataka;
- dopunjavanje, izmjenu ili brisanje osobnih podataka, koji su: netočni, nepotpuni ili neažurni.

Sve zbirke osobnih podataka nalaze se u evidenciji osobnih podataka. Vođenje evidencije osobnih podataka spada pod nadležnost AZOP-a. Zaključno, može se reći kako pravno uređene države paze na privatnost, odnosno osobne podatke svakog građanina, kako u klasičnim okruženjima tako i u *cloud* okruženju. Organizacijama koje se bave *cloud* okruženjem zabranjeno je prikupljanje podataka o svojim klijentima, osim ako to krajnji korisnik ne dozvoli. Organizacije najčešće traže različita dopuštenja za prikupljanje podataka u ugovoru o korištenju (eng. *User agreement*) a korisnici najčešće daju pristanak zato što ne čitaju ugovor.

3.3 Voditelj i izvršitelj obrade osobnih podataka

Od 25. svibnja 2018., u svim državama članicama Europske unije izravno se primjenjuje Opća uredba o zaštiti (u daljnjem tekstu: Opća uredba) kojom se prije svega utvrđuju pravila povezana sa zaštitom pojedinca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka. Uredba ne obuhvaća obrada podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući naziv i oblik pravne osobe i kontakt podatke.

Voditelj obrade (eng. *controller*) je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka (članak 4. Opće uredbe). Primjeri voditelja obrade: trgovačka društva ili obrti koji obrađuju podatke svojih radnika; financijske institucije koje obrađuju osobne podatke svojih stranaka/klijenata; udruge koje obrađuju podatke svojih članova; škole ili fakulteti koji obrađuju osobne podatke učenika, studenata ili nastavnika/svojih radnika; bolnice koje obrađuju osobne podatke svojih pacijenata; državna tijela ili tijela jedinica lokalne/regionalne samouprave koja obrađuju osobne podatke građana.

Izvršitelj obrade (eng. *processor*) je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom (članak 4. Opće uredbe). Primjeri izvršitelja obrade: knjigovodstveni servis koji obrađuje podatke o plaćama radnika za poslodavca; trgovačka društva ovlaštena za obavljanje privatne zaštite; agencije za naplatu potraživanja temeljem sklopljenog ugovora o poslovnoj suradnji.

Voditelj obrade nije u obvezi imati izvršitelja obrade. Naime Opća uredba daje mogućnost voditelju obrade da povjeri izvršitelju obrade obavljanje samo nekih točno ugovorenih poslova u ime i za račun voditelja obrade.

Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade. U slučaju općeg pisanog odobrenja, izvršitelj obrade obavješćuje voditelja obrade o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom drugih izvršitelja obrade kako bi time voditelju obrade omogućio da uloži prigovor na takve izmjene. Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom (mora biti u pisanom obliku, uključujući i elektronički oblik) u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade,

vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. Tim se ugovorom ili drugim pravnim aktom osobito određuje da izvršitelj obrade:

- obrađuje osobne podatke samo prema zabilježenim uputama voditelja obrade, među ostalim s obzirom na prijenose osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, osim ako to nalaže pravo Unije ili pravo države članice kojem podliježe izvršitelj obrade; u tom slučaju izvršitelj obrade izvješćuje voditelja obrade o tom pravnom zahtjevu prije obrade, osim ako se tim pravom zabranjuje takvo izvješćivanje zbog važnih razloga od javnog interesa;
- osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim obvezama o povjerljivosti;
- uzimajući u obzir prirodu obrade, pomaže voditelju obrade putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika koja su utvrđena u poglavlju III. Opće uredbe o zaštiti podataka;
- pomaže voditelju obrade u osiguravanju usklađenosti s obvezama uzimajući u obzir prirodu obrade i informacije koje su dostupne izvršitelju obrade;
- po izboru voditelja, briše ili vraća voditelju obrade sve osobne podatke nakon dovršetka pružanja usluga vezanih za obradu te briše postojeće kopije osim ako sukladno pravu Unije ili pravu države članice postoji obveza pohrane osobnih podataka;
- voditelju obrade stavlja na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obveza utvrđenih u ovom članku i koje omogućuju revizije, uključujući inspekcije, koje provodi voditelj obrade ili drugi revizor kojeg je ovlastio voditelj obrade, te im doprinose.

Uzimajući u obzir obvezu izvršitelja obrade kojom mora osigurati da su se osobe ovlaštene za obradu osobnih podatatka obvezale na poštivanje povjerljivosti ili da podliježu zakonskim obvezama povjerljivosti ne znači da izvršitelj obrade eventualno potpisane izjave o povjerljivosti svojih zasposlenika koji neposredno sudjeluju u obradi osobnih podataka, mora iste ako su potpisane dostavljati voditelju obrade s kojim se sklapa ugovor. Naime, njegova obveza je jamčiti da će se osobni podaci prema točno danim uputama voditelja obrade obrađivati, te je na taj način dužan osigurati povjerljivost u skladu s obvezama koje proizlaze iz ugovora.

Iz samog odnosa voditelja i izvršitelja obrade proizlazi da izvršitelj obrade poduzima određene radnje u obradi u ime i za račun voditelja obrade. Stoga, voditelj obrade može povjeriti pojedine poslove i obveze koje proizlaze iz Opće uredbe o zaštiti podataka konkretnom izvršitelju obrade, pa tako izvršitelj obrade može primjerice prikupljati i obrađivati osobne podatke u točno određenu svrhu, prema danim uputama voditelja obrade. Upravo iz tog razloga za postojanje pravne osnove i zakonite svrhe prilikom obrade osobnih podataka odgovoran je voditelj obrade, dok izvršitelj obrade samo obrađuje podatke u njegovo ime i za njegov račun. Izvršitelj obrade mora jamčiti zaštitu i povjerljivost obrade osobnih podataka te provoditi odgovarajuće mjere zaštite kako bi osigurao i mogao dokazati da se obrada provodi u skladu sa Općom uredbom.

Voditelj obrade u trenutku prikupljanja osobnih podataka obvezan je ispitaniku pružiti informacije:

- svom identitetu,
- o službeniku za zaštitu podataka (kontakt podaci službenika),
- upoznati sa svrhom i pravnom osnovom za obradu osobnih podataka,
- o primateljima ili kategorijama primatelja osobnih podataka,
- o prenošenju osobnih podataka trećoj zemlji ili međunarodnoj organizaciji (koje nisu članice EU),
- o legitimnom interesu,
- o vremenskom roku pohrane osobnih podataka te kriterijima kojima se utvrđuje razdoblje pohrane,
- o postojanju prava da se od voditelja obrade zatraži pristup osobnim podacima, ispravak, brisanje osobnih podataka ili ograničavanje obrade koja se na njega odnose, prava na ulaganje prigovora na obradu takvih podataka te na prenosivost njegovih podataka drugom voditelju obrade,
- pravu da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena,
- o pravu na podnošenje prigovora nadzornom tijelu (Agenciji za zaštitu osobnih podataka)
- je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže,

- o postojanju automatiziranog donošenja odluka, što uključuje izradu profila te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika.

Nadalje, svaki voditelj i izvršitelj obrade dužan je poduzimati i provoditi odgovarajuće tehničke i organizacijske mjere zaštite koje imaju za cilj osigurati sigurnost i povjerljivost obrade osobnih podataka, odnosno sprječavanje neovlaštenog pristupa ili neovlaštenog raspolaganja osobnim podacima kao i tehničkoj opremi kojom se koriste voditelji i izvršitelji obrade. Provođenjem odgovarajućih mjera zaštite osigurava se da osobni podaci nisu automatski dostupni neograničenom broju osoba koje nisu ovlaštene za njihovu obradu. U vrijeme određivanja sredstava obrade i u vrijeme same obrade obveza je svakog voditelja obrade da ovisno o prirodi/naravi, opsegu i svrsi obrade osobnih podataka odredi mjere zaštite koje jamče sigurnu, poštenu i zakonitu obradu osobnih podataka te učinkovitu primjenu načela zaštite podataka (osobito uzimajući u obzir nužnost obrade podataka za svaku posebnu svrhu, smanjenje količine prikupljanih podataka kao i opsega podataka prilikom obrade, određivanje rokova čuvanja podataka, njihovu dostupnost i dr.).

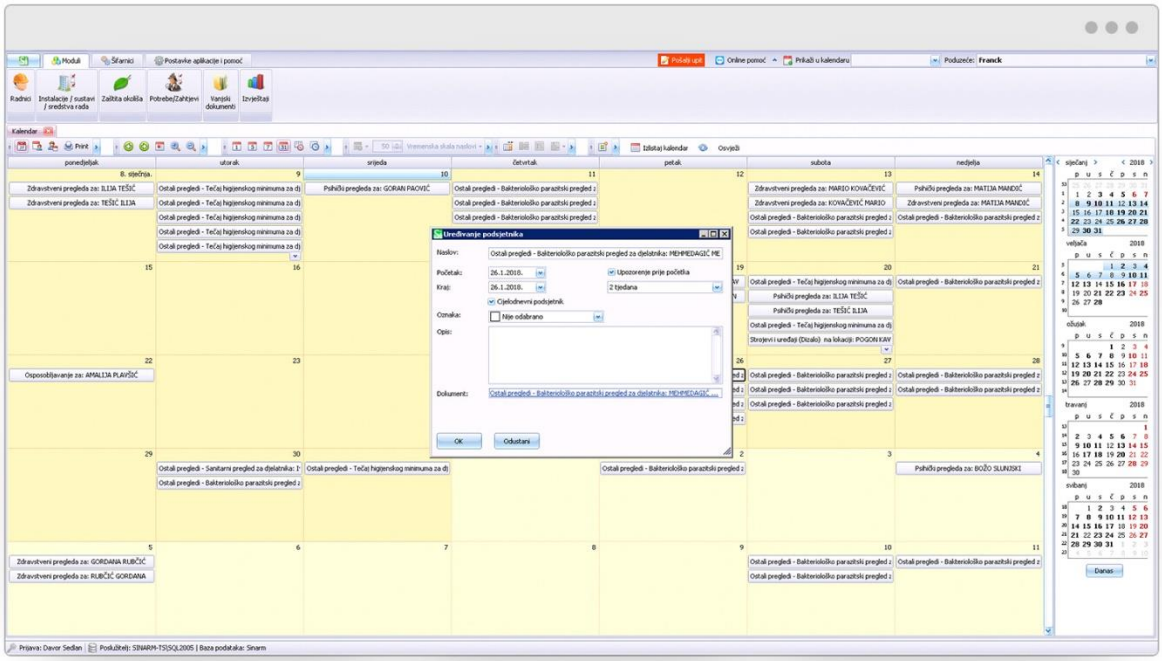
Preporuka je da se dokumentacija u papirnatom obliku koja sadrži osobne podatke pohrani, primjerice u ormare ili ladice pod ključem koja će biti pod nadzorom ovlaštenih osoba voditelja obrade, da pristup osobnim podacima pohranjenim u elektroničkom obliku bude omogućen uporabom korisničkog imena i lozinke. Također, izrada sigurnosnih kopija od strane ovlaštenih osoba, bilježenje pristupa podacima, potpisivanje izjava o povjerljivosti osoba koje su u obradi osobnih podataka te pseudonimizacija ili enkripcija osobnih podataka- osobito ako se radi o posebnim kategorijama (primjerice: podataka o zdravlju). [30]

4. PREGLED *CLOUD* RJEŠENJA NA HRVATSKOM TRŽIŠTU

Iako je na tržištu dostupno mnoštvo rješenja za pohranu podataka u oblaku od kojih su neki I spomenuti ranije u ovom radu, iz perspektive stručnjaka zaštite na radu mogu se izdvojiti programska rješenja dostupna na hrvatskom tržištu. Sva vodeća rješenja dijele neke iste značajke, a zajednička im je pohrana podataka u oblaku.

4.1 Sinarm

Sinarm (slika 7) je cloud aplikacija koja informatizira vođenje evidencija, ispisivanje podataka u forme propisane zakonom te generiranje izvještaja potrebnih za obavljanje poslova vezanih uz zaštitu na radu, zaštitu od požara i zaštitu okoliša.



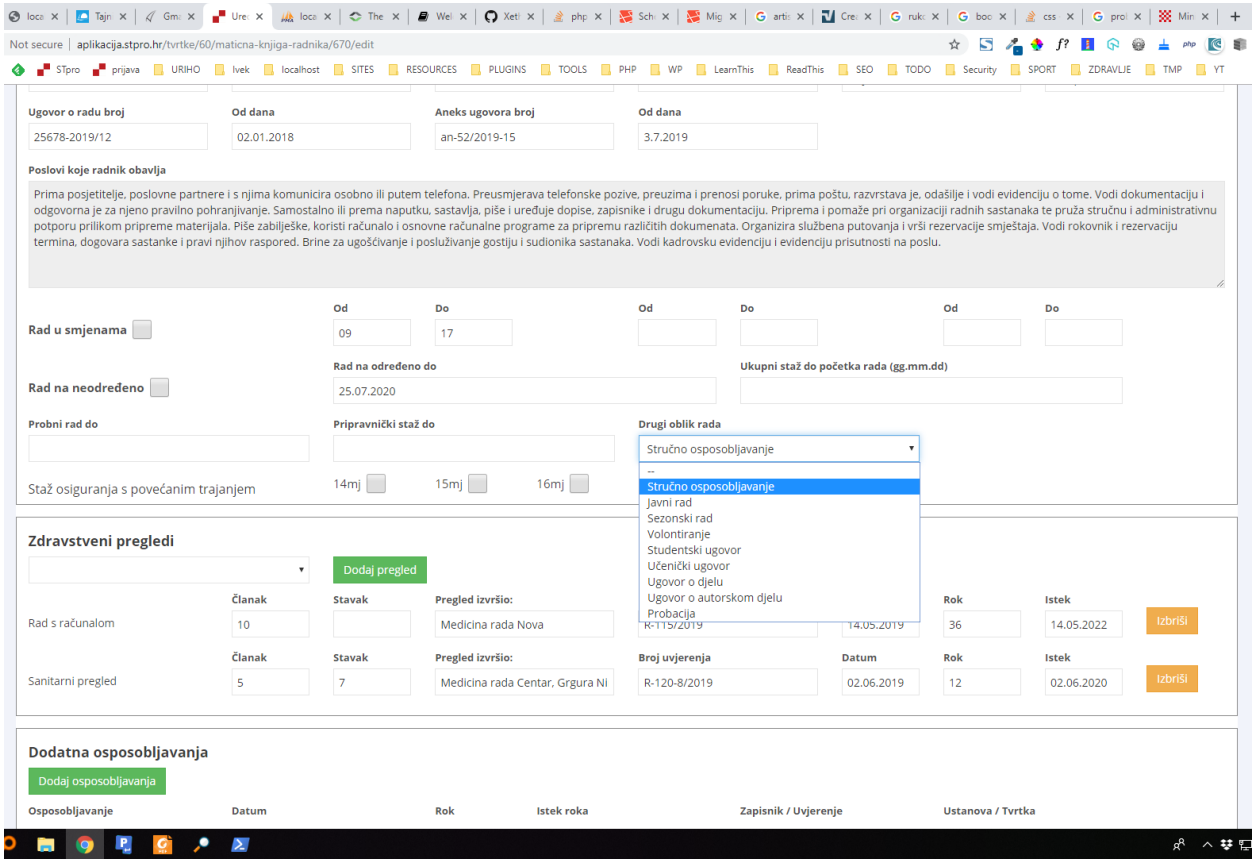
Slika 7. Sučelje Sinarma [33]

Sinarm je programsko rješenje koje omogućava korisniku vođenje svih potrebnih evidencija iz područja ZNR ZOP i ZO na jednom mjestu uz mogućnost prilaganja vanjskih dokumenata (uvjerenja, svjedodžbe i slično). Dizajniran je tako da zadovoljava potrebe malih poduzetnika za jednostavnošću, ali se može koristiti i u velikim tvrtkama u kojima

istovremeno radi veći broj korisnika. Iznimno je korisno što Sinarm pruža mogućnost kreiranja personaliziranih izvještaja, pri čemu korisnik sam odabire, grupira i sortira podatke za izvještaj. Treba istaknuti da je u program moguće. integrirati korisnikove postojeće digitalne podatke ili izraditi modul za povezivanje s kadrovskom evidencijom. Rad u programu moguć je s različitih lokacija za jednog ili više korisnika uz detaljno podešavanje prava pristupa što znači da je svakom pojedinom korisniku moguće definirati različite ovlasti. Također, Sinarm donosi rješenje i za sve one koji vode evidenciju za nekoliko različitih tvrtki. Oni tako na vrlo jednostavan način i bez napuštanja programa, istovremeno mogu obavljati više poslova i postići maksimalan učinak. Sinarm korisničko sučelje podijeljeno je na sljedeće cjeline i omogućava vođenje evidencija za: radnike, vatrogasne aparate, instalacije, strojeve i uređaje, radnu okolinu, gospodarenje otpadom, kemikalije, ispuštanja onečišćenja u zrak i vode [33]. U kontekstu pohrane osjetljivih podataka važno je zamijetiti kako ova aplikacija u smislu licence dolazi u dva oblika: kupnja ili najam. Ukoliko se želi potpuna kontrola nad pohranjenim podatcima, tada je jedina opcija kupnja programa gdje se on instalira na poslužitelj kupca, odnosno organizacije. Voditelj zbirke podataka u tom smislu ne mora brinuti oko korištenja osjetljivih podataka od treće strane. Svakako valja istaknuti, kako je u radu opisana sigurnosna pohrana podataka, da program Sinarm u licenci najma nudi dnevne sigurnosne pohrane. U tom slučaju, stručnjaci zaštite na radu ne moraju brinuti o gubitku podataka.

4.2 STpro

Programsko rješenje STPro se nudi isključivo kao web aplikacija te ne zahtjeva instalaciju na računala organizacije. Ono što razlikuje aplikaciju STPro od prethodno navedene jest što se nudi kao isključivo web aplikacija, a to podrazumijeva kako su svi podaci pohranjeni u oblaku. Osim pohrane u oblaku nudi i izradu sigurnosnih kopija. Za organizaciju to znači smanjivanje troškova, no za voditelja zbirke osobnih podataka podrazumijeva svjesnost o poštivanju zakonskih propisa oko pohrane osjetljivih podataka na računalne sustave izvan vlastite organizacije. U tom smislu valja istaknuti kako je spomenuta aplikacija redovno nadograđivana kako bi poštovala sve zakonske propise, a pri tome se koristi i uslugama Zavodu za unapređivanje zaštite na radu. Jedna od uloga STpro je praćenje rokova ispitivanja, liječničkih pregleda i osposobljavanja radnika te automatsko popunjavanje obrazaca i generiranje izvješća [33].



Slika 8. Sučelje aplikacije Stpro[33]

Objedinjavanjem svih rokova na jednom mjestu postiže se lakše planiranje, organiziranje i praćenje rokova. STpro je izrađen kako bi krajnjem korisniku omogućio jednostavan rad i praćenje svih rokova zaštite na radu i zaštite od požara. STpro korisnike rješava glavobolje od praćenja rokova kao što su: liječnički pregledi, osposobljavanja, ispitivanja radne opreme i instalacija te servisiranja opreme i održavanja.

Prednosti STpro-a:

• Drugačiji od drugih-jednostavnost korištenja programa od strane korisnika

• Rad i kvaliteta- traženje novih putova i rješenja

• Korisnička podrška- podrška od 09 do 19 sati putem telefona ili emaila

• Iskustvo i vještine- o programu skrbe stručnjaci sigurnosti, informatike i dizajna

• Sigurnost podataka- podaci u oblaku što znači veća razina sigurnosti i dostupnosti

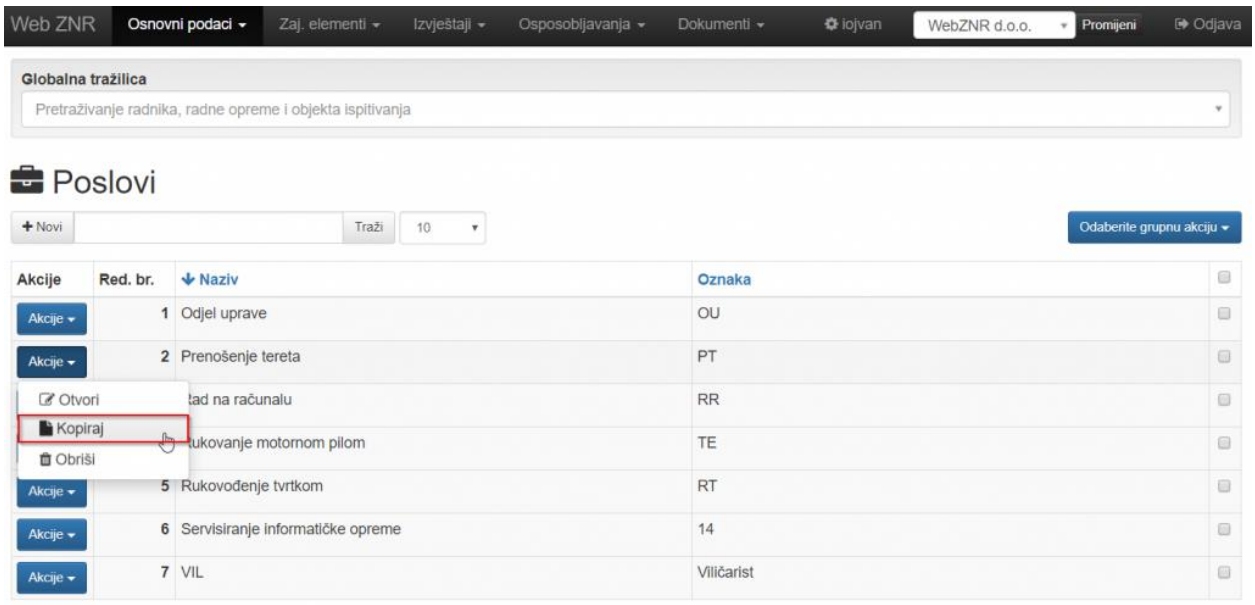
• Zajamčena sigurnost- svi podaci su zaštićeni i uključuju automatsku izradu sigurnosnih kopija

4.3 Web ZNR

Web ZNR je cloud aplikacija čiji se podatci pohranjuju na certificiranim poslužiteljima koji su geografski odvojeni kako bi se se spriječio gubitak podataka uslijed prirodnih katastrofa I sličnih nepoželjnih događaja. Namijenjena djelatnicima zaduženima za vođenje zaštite na radu i zaštite od požara [34]. Pomoću aplikacije korisnici vode podatke potrebne za ispunjenje evidencija propisanih Zakonima i Pravilnicima s područja zaštite na radu i zaštite od požara. Temeljni podaci odnose se na evidencije podataka kao što su podaci o djelatnicima, predmetima ispitivanja i njihovi pregledi, raznim obrascima, radnim mjestima te organizacijskoj strukturi. Osnovna zadaća aplikacije je izvješćivanje korisnika o isteku rokova za ponavljanje osposobljavanja i ispitivanja. Kako bi osigurali poštivanje rokova, korisnici prilikom pristupa aplikaciji te putem email poruka dobivaju obavijesti o isteku rokova za željeni broj dana unaprijed kao i za sve istekle rokove ukoliko oni nisu produženi. Bilo da se radi o liječničkom pregledu djelatnika, ispitivanju stroja, ispitivanju vatrogasnog aparata ili izdavanju zaštitnog sredstva aplikacija će se pobrinuti da niti jedan rok ne prođe nezamijećeno. Aplikacija korisnika putem kalendara i email obavijesti na vrijeme obaviještava o nadolazećim obavezama. Tako će korisnik moći na vrijeme planirati svoje djelovanje i istek nekog roka dočekati spreman. Što se tiče jednostavnog popunjavanja obrazaca, svaki stručnjak zaštite na radu zna da je najveći gubitak vremena ponovno upisivanje podataka o zaposleniku ili uređaju u sve potrebne obrasce. Aplikacija WebZNR će korisniku omogućiti da liječničke uputnice RA-1, RO-1, RO-2, NR-1, prijava ozljede na radu OR i EK-3, prijave profesionalne bolesti PB, obavijesti o događaju koji je izazvao smrt, težu ozljedu dvaju ili više zaposlenika OIR-1, godišnji izvještaj o ozljedama na radu, korisnik popuni tako da podaci koji su već uneseni u aplikaciju (poput osobnih podataka zaposlenika i sl.) budu uneseni automatski u navedene obrasce. Na korisniku tada ostaje da popuni dijelove obrazaca koji traže njegovu ekspertizu i da ih snimi ili ispiše. Aplikacija uvelike pojednostavljuje postupak upravljanja ZNR-a i ZOP-a koji zna biti izazovan pogotovo u velikim kolektivima s velikim brojem korisnika i uređaja [34]. Aplikacija WebZNR omogućuje da svi podatci budu uvijek dostupni s bilo kojeg uređaja koji se može spojiti na internet. Podaci u aplikaciji bit će uvijek ažurni, a popunjavanje izvještaja jednostavno i brzo. Iz same aplikacije dobiva se mogućnost kreiranja velikog broja izvještaja koje korisnici mogu kreirati zahvaljujući mogućnosti filtriranja i grupiranja svih podataka koji se nalaze u aplikaciji. Generiranje evidencijskih kartona i liječničkih uputnica obavlja se na temelju evidentiranih podataka pomoću kojih je omogućena izrada evidencijskih kartona

EK-1(o osposobljenosti radnika za rad na siguran način), EK-2(o radniku raspoređenom na poslove s posebnim uvjetima rada), EK-4(o ispitivanju strojeva i uređaja s povećanim opasnostima), EK-5(o ispitivanju radne okoline), EK-6(o pregledu ili ispitivanju osobnog zaštitnog sredstva), liječničkih uputnica te spomenutih izvještaja. Evidencijski kartoni i liječničke uputnice pri tome imaju zakonom propisanu formu i u samoj aplikaciji kako bi snalaženje u njima bilo što jednostavnije za korisnika aplikacije. Ispis istih je također u skladu sa zakonom propisanim formama s mogućnošću ispisa na A4 i A3 papir i snimanje u velikom broju formata datoteka. Uz evidentirane podatke mouće je priložiti datoteke poput skeniranih uvjerenja, uputa za siguran rad, procjena opasnosti i slično u formatima .jpg, Word, Excel ili PDF datoteka. Sve postojeće datoteke i dokumente koji su do sada bili raspodijeljeni na različitim mjestima moguće je pohraniti na jedno mjesto poput digitalne arhive. Aplikacija tako omogućava da se uz zaposlenika prilože skenirana osobna iskaznica, uz uređaj uvjerenje o ispitivanju ili možda uz organizacijsku jedinicu evakuacijski plan. Svi ti dokumenti će tako postati uvijek dostupni i korisniku na raspolaganju bez obzira gdje se nalazi u tom trenutku. Aplikacija WebZNR omogućava kontrolu pristupa podacima u samoj aplikaciji od strane zaposlenika vlastite tvrtke ili vanjskih suradnika (kontrolne kuće i sl.). Unutar same aplikacije jednostavno se može. kontrolirati pristup pojedinim dijelovima aplikacije s pravima čitanja ili uređivanja. Na ovaj način npr. kontrolne kuće mogu same unositi rezultate ispitivanja uređaja u aplikaciju korisnika i tako štedjeti njegovo vrijeme koristeći njegovu aplikaciju, a da pri tome ne mogu vidjeti niti uređivati podatke za koje korisnik to ne želi. Aplikacija WebZNR omogućava da kroz nju tvrtke koje to žele mogu same izvršavati teorijsko i praktično osposobljavanje svojih zaposlenika. Kroz aplikaciju korisnici sami mogu pratiti osposobljavanje te na kraju i izdavati uvjerenja o osposobljavanju koja više nisu zakonski obavezna ali predstavljaju svojevrsnu potvrdu zaposleniku da je osposobljen. Iz ove evidencije generira se matična knjiga osposobljavanja. Aplikacija omogućuje praćenje i planiranje troškova. U samoj aplikaciji omogućen je unos cijene za pojedino ispitivanje, liječnički pregled ili ispitivanje uređaja. Na temelju tog podatka i rasporeda potrebnih radnji u pojedinom vremenskom razdoblju korisnik će biti u mogućnosti izraditi troškovnike, budžete za naredno razdoblje, procjene troškova i slično, doslovno u par klikova. Aplikacija omogućava svojim korisnicima jednostavni uvoz podataka iz postojećih baza (obično su to razne aplikacije kadrovske službe). Kreiranjem jednostavne CSV datoteke imate mogućnost uvoza podataka o zaposlenicima čime značajno olakšavate si prijelaz na novu aplikaciju. Za veće sustave gdje je fluktuacija zaposlenika veća i gdje je potrebna automatska sinkronizacija njihovi stručnjaci će napraviti sinkronizacijske

aplikacije koje će podatke sinkronizirati automatski. Od početka 2016. godine izašao je i novi mogul procjene rizika unutar aplikacije WebZNR. Ovaj modul omogućava generiranje Word dokumenta na temelju upisanih podataka nakon čega se može nastaviti obrada dokumenta prema željama korisnika. Također je bitno za istaknuti i korisnički portal putem kojeg stručnjak zaštite na radu može dozvoliti kontrolirani pristup podacima iz evidencije. Korisnički portal djeluje kao interna stranica za ZNR i ZOP što omogućava svim zaposlenicima pristup informacijama o nekom stroju, radnom mjestu ili organizacijskoj jedinici, a pri tome stručnjak zaštite na radu cijelo vrijeme ima potpunu kontrolu nad tim koji podaci se prikazuju na korisničkom portalu. Aplikacija se može izvoditi na vlastitom poslužitelju ili na poslužitelju proizvođača aplikacije. S obzirom kako aplikacija poštuje stroga pravila za siguran pristup podacima svakako je oportuno koristiti poslužitelj proizvođača, time se i smanjuju troškovi. Svakako valja istaknuti kako se WebZNR može isprobati na rok od 15 dana.



Slika 9. Sučelje aplikacije WebZNR [34]

S obzirom na način instalacije, stručnjak zaštite na radu treba biti svjestan korištenja aplkacije na poslužitelju izvan vlastite organizacije.

4.4 Data collector

Zavod za unaprjeđenje zaštite na radu (ZUZNR), prije nego je postao dio Ministarstva rada i mirovinskog sustava, predstavio je u siječnju 2016. godine program pomoću kojega bi unaprijedio ZNR, zdravlje i produktivnost radnika u Republici Hrvatskoj, Data Collector. Razvoj Središnjeg nacionalnog informacijskog sustava zaštite na radu predviđen je u dvije faze. Prva faza podrazumijeva uspostavljanje Informacijskog sustava zaštite na radu Zavoda za unapređivanje zaštite na radu (u daljnjem tekstu: IS ZNR ZUZNR) kao temeljnog modula Središnjeg nacionalnog informacijskog sustava zaštite na radu putem kojega će Zavod razmjenjivati podatke sa središnjim sustavom. Druga faza podrazumijeva integraciju baza podataka pojedinih institucija koje djeluju na području zaštite na radu i zaštite zdravlja na radu u svrhu uspostavljanja jedinstvene baze podataka dostupne korisnicima s definiranim ovlastima u skladu s potrebama, a što će ujedno omogućiti predlaganje i poduzimanje pojedinačnih i zajedničkih aktivnosti na poboljšanju i unapređivanju ukupnog stanja zaštite na radu. Putem IS ZNR Zavoda pratit će se podaci svih pravnih i fizičkih osoba koje imaju registriranu djelatnost na teritoriju Republike Hrvatske (poslodavci), ovlaštenih pravnih i fizičkih osoba za obavljanje poslova zaštite na radu te registar stručnjaka zaštite na radu [35]. Podaci iz IS ZNR Zavoda koristit će se za nadzor nad radom ovlaštenih osoba za poslove zaštite na radu, praćenje stanja zaštite na radu kod poslodavaca, izradu stručnih mišljenja iz zaštite na radu za različite subjekte, provođenje statističkih istraživanja iz zaštite na radu, izrađivanje programa, vodiča, metoda i modela zaštite na radu, utvrđivanje kriterija i postupaka u vezi s organizacijom rada, pružanje pomoći udruženjima poslodavaca, sindikatima, osobama ovlaštenim za poslove zaštite na radu te tijelima uprave, provođenje akcija s pojedinih područja zaštite na radu i zaštite zdravlja na radu te za unapređivanje ukupnog stanja zaštite na radu. Središnji nacionalni informacijski sustav zaštite na radu nazvan Data Collector (Središnji nacionalni informacijski sustav zaštite na radu) uspostavlja se s ciljem podizanja kvalitete ukupnog stanja zaštite na radu u Republici Hrvatskoj putem integriranja podataka vezanih za područje zaštite na radu u jedinstvenu funkcionalnu bazu. Trenutni problem korištenja Data Collectora je nepostojanje mogućnosti integracije podataka koji onemogućuje sagledavanje šire slike u području zaštite na radu i zaštite zdravlja, a time i samo predlaganje i poduzimanje efektivnih zajedničkih aktivnosti na poboljšanju i unapređivanju ukupnog postojećeg stanja. Glavno tijelo nadležno za razvoj, primjenu te pravilno funkcioniranje Data Collectora inicijalno se smatrao Zavod za unapređivanje zaštite na radu koji je u međuvremenu ukinut i postao je jedna od uprava

MRMS nadležna za ZNR. Zadaća mu je inicijalno bila uspostavljanje, vođenje i održavanje Data Collectora kao sveobuhvatnog, informatičkog i mrežnog temeljnog rješenja za praćenje stanja zaštite na radu. Prethodnim analizama postojećeg stanja zaštite na radu u Republici Hrvatskoj, utvrđeno je da su primarni korisnici podataka o zaštiti na radu Ministarstvo rada i mirovinskog sustava (MRMS), Služba za zaštitu na radu i Inspektorat rada, Hrvatski zavod za zdravstveno osiguranje (HZZO), Zavod za unapređivanje zaštite na radu (ZUZNR), Hrvatski zavod za zaštitu zdravlja i sigurnost na radu (HZZZSR) te Hrvatski zavod za javno zdravstvo (HZJZ). U ovom pretpostavljenom skupu korisnika više nisu istaknuti već spomenuti ZUZNR i HZZZSR koji je na sličan način postao dio HZJZ. Bitno za istaknuti je da će uz prethodno navedene institucije krajnji korisnici Data Collector-a biti poslodavci obveznici unosa podataka iz ovog područja te pravne i fizičke osobe ovlaštene za obavljanje poslova zaštite na radu. Također, osim uspostavljanja jedinstvene baze podataka o ozljedama na radu i profesionalnim bolestima, sustav će omogućiti generiranje različitih cjelovitih podataka iz područja zaštite na radu (slika 10).

Slika 10 Blok shema cjelokupnog SNIS ZNR [36]

Prikupljeni podaci koristit će se za praćenje stanja zaštite na radu, izradu stručnih elaborata iz zaštite na radu za različite subjekte, provođenje statističkih istraživanja iz zaštite na radu..

5. ZAKLJUČAK

Pohrana podataka evoluirala je u obradu i pohranu u oblaku. Računalstvo u oblaku nudi obilje mogućnosti obrade, pohrane i prijenosa podataka u okviru poslovnog sustava zaštite na radu. Iako takav način pohrane nudi značajnu fleksibilnost, efikasnost i brzinu vođenja podataka, voditelj zbirke osobnih podataka s obzirom na razinu odgovornosti u organizaciji, treba kod prikupljanja i pohrane podataka imati u vidu i rizike i prijetnje takve pohrane. Također, trebao bi biti informatički obrazovan te poznavati tehnologije koje se koriste kod takve pohrane. Svjesnošću o rizicima te mogućim gubitcima podataka voditelj zbirke podataka može prevenirati takve pojave. Gubitak podataka se može spriječiti korištenjem sigurnosnih kopija. Procesom stvaranja sigurnosnih kopija i povratom podataka smanjuju se rizici kojima je izložen informacijski sustav. Iako pohrana podataka u oblaku značajno podiže sigurnost organizacije te ju načelno oslobađa brige o sigurnosnim kopijama, za potpunu sigurnost valja izrađivati i lokalne sigurnosne kopije podataka jer potpuno prepuštanje brige o sigurnosti podataka trećoj strani može ugroziti podatke s obzirom kako napadi na tvrtke koje pružaju usluge u oblaku nisu rijetkost. Osim sigurnosnih kopija, voditelj zbirke podataka treba uvijek voditi računa o zakonskim propisima i aktima kod prikupljanja i pohrane podataka, napose ukoliko je riječ o pohrani u oblaku. Iako pohrana u oblaku smanjuje rizik gubitka podataka, ona nudi izazove usklađenja s važećim zakonima s kojima voditelj zbirki podataka treba neprestano biti upoznat kako bi maksimalno iskoristio mogućnosti pohrane u oblaku, a usto osigurao zaštitu osobnih podataka što je osobito važno i zbog rigorozne zakonske regulative. Korištenjem oblaka uvelike se pojednostavljuje upotreba i promet podataka vezanih za poslovanje poduzeća i njihovog sustava zaštite na radu, a pohrana podataka i njihovo upravljanje je sistematizirano na višu razinu. Prednosti korištenja računalstva u oblaku su te što je zaposlenicima i ostalim djelatnicima u poduzeću omogućeno pristupiti potrebnim dokumentima i podacima sa bilo kojeg mjesta i u bilo koje vrijeme te za to nije potreban dodatno sklopovlje i/ili programska podrška, već postojeća strojna podrška kao što je tablet, računalo ili pametni telefon. U skladu s preporukama Europske unije te usklađivanjem regulativa EU sa regulativama Republike Hrvatske, došlo je do unaprjeđivanja sustava zaštite na radu i početka primjene europskih direktiva zaštite na radu od kojih najveće značenje ima direktiva 89/391/EEC o uvođenju mjera za poticanje poboljšanja sigurnosti i zdravlja radnika na radu. Doprinos računalstva u oblaku se može očitati i u pripremi početka realizacije projekta Središnjeg nacionalnog informacijskog

sustava ZNR tzv. Data Collectora. Sustav se uspostavlja s ciljem podizanja kvalitete ukupnog stanja zaštite na radu u Republici Hrvatskoj putem integriranja do sada autonomno lociranih podataka vezanih za područje zaštite na radu u jedinstvenu nacionalnu funkcionalnu bazu. Ciljevi Data Collectora koji su važni za ostvarenje prilikom uporabe samog sustava u zaštiti na radu mogu se podijeliti na dnevno-operativne ciljeve kojima je zadaća izdavanje uputnica, izvješća o povredama i vođenje osnovnih evidencija vezanih za zaštitu na radu. Osim toga, postoje i taktički ciljevi za koje je zaduženo niže i srednje rukovodstvo i strateške koji će rezultirati izgradnjom SNIS ZNR koji bi integrirao podatke vezane uz zaštitu na radu u jedinstvenu bazu s ciljem podizanja kvalitete ukupnog stanja zaštititе na radu u Republici Hrvatskoj. Unaprijeđivanje sustava u domeni ZNR se svakako vidi u povećanju edukacija svih dionika u sustavu napose u smjeru informatizacije, a svakako valja podići svijest o značaju osobnih, a i svih ostalih podataka koji se pohranjuju u računalnim sustavima što podrazumijeva poznavanje zakonske regulative u tom području.

6. LITERATURA

[1] Vlada RH, „Strategija "Informacijska i komunikacijska tehnologija - Hrvatska u 21. stoljeću", dostupno na: https://narodnenovine.nn.hr/clanci/sluzbeni/2002_09_109_1753.html (10. kolovoza 2020.)

[2] Europska komisija., „EU data protection rules“, dostupno na: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en (10. kolovoza 2020.)

[3] Kilibarda N., „Računarstvo u oblaku“, dostupno na: https://raduoblaku.wordpress.com/ (3. kolovoza 2020.)

[4] Ogrizek Biškupić I., Banek Z. M., „Web tehnologije“, Zagreb, 2014

[5] Kepes B., „Understanding the *Cloud* Computing Stack: SaaS, PaaS, IaaS“, 2016. dostupno na: https://support.rackspace.com/white-paper/understandingthe-*cloud*-computing-stack-saas-paas-iaas/ (5. srpnja 2020.)

[6] Amazon documents, dostupno na: https://docs.aws.amazon.com/ (2. kolovoza 2020.)

[7] Hlebec, D. „Primjena računalstva u oblaku u poslovanju“, završni rad, Sveučilište Jurja Dobrile u Puli, Odjel za informacijsko-komunikacijske tehnologije, Pula, Hrvatska, 2016., str. 21-50.

[8] Millard C., „Cloud Computing Law“, Oxford: Oxford University Press, 2013., str.113-171.

[9] Google inc., „Google Apps for Business (Online) Agreement“, dostupno na: https://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html. (5.srpnja 2020.)

[10] Urquahrt J., „FBI seizures highlight law as cloud impediment“,2009., dostupno na: http://www.cnet.com/news/fbi-seizures-highlight-law-as*cloud*-impediment/ (6. srpnja 2020.)

[11] Središnji državni ured za e-Hrvatsku: „Nacionalni program

Informacijske sigurnosti u Republici Hrvatskoj“, Zagreb, 2015., str. 10-60.

[12] CARNet, „Sustavi za upravljanje (osobnim) podacima, informacijama i digitalnim sadržajem, Zagreb, 2018., str. 41-62.

[13] Castells M., „The Internet Galaxy: Reflections on the Internet, Business, and Society“, Oxford University Press, Chicago , 2001.

[14] Cerf V. Kahn R., „A protocol for packet network interconnection“, IEEE Trans. Comm. Tech.,“ Berlin, 1974., str. 56-71.

[15] Jones A., Wulf W.: „Towards the design of secure systems. Software: Practice and Experience“, London, 1975.. str.113-160.

[16] Weber D., „A taxonomy of computer intrusions“. Master’s thesis, Massachusetts Institute of Technology, Massachusets, 1998., str. 25-54.

[17] CERT. CERT Statistics (Histrorical), dostupno na: http://www.cert.org/stats/, 2009. (5. srpnja 2020.)

[18] Anderson R., „A guide to building dependable distributed Systems“, Wiley, 2008., str. 64-91

[19] Christian V. Lundestad and Anique Hommels: „Software vulnerability due to practical drift. Ethics and Information Technology“, Stockholm, 2007., str. 101-145

[20] Europske direktive o sigurnosti i zdravlju na radu, dostupno na: https://osha.europa.eu/hr/safety-and-health-legislation/european-directives (16. kolovoza 2020.)

[21] „Zaštita na radu - propisi, cijene, obveze, ponude“, dostupno na: https://www.zastitanaradu.com.hr/novosti/Zastita-na-radu-u-Europskoj-uniji-39 (7. kolovoza 2020.)

[22] Europska agencija za zaštitu na radu, dostupno na: https://osha.europa.eu/hr/safety-and-health-legislation/european-directives (6. kolovoza 2020.)

[23] Hrvatski Sabor, „Zakon o izmjenama i dopunama Zakona o zaštiti na radu“, Narodne novine, dostupno na: http://narodnenovine.nn.hr/clanci/sluzbeni/2018_10_94_1819.html (12. kolovoza 2020.)

[24] Europsko vijeće, „Opća uredba o zaštiti podataka“, 2016. dostupno na: http://www.consilium.europa.eu/hr/policies/data-protectionreform/data-protection-regulation/. (12. kolovoza 2020.)

[25] CARNet, „Zakon o zaštiti osobnih podataka“, dostupno na: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-07-234.pdf. (12. kolovoza 2020.)

[26] Gumzej N., „Uredba o zaštiti osobnih podataka“, dostupno na: https://bib.irb.hr/datoteka/951269.Nina_Gumzej_Uredba_o_zatiti_osobnih_podataka_FP2017_1.pdf (11. lipnja 2020).

[27] Službeno priopćenje Europskog parlamenta na temu usklađivanja zakonodavnog paketa, dostupno na: http://www.europarl.europa.eu/news/hr/news-room/20160407IPR21776/Reforma-za%C5%A1tite-podataka-EP-odobrio-nova-pravila (5. lipnja 2020).

[28] Voigt, P., Bussche von Dem, A., „The EU General Data Protection Regulation (GDPR): A Practical Guide“, Springer, 2017., str. 12-60

[29] Zaštita osobnih podataka u RH, dostupno na: https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (05 lipnja 2020.).

[30] Ustav Republike Hrvatske, dostupno na: https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske%20 (6. lipnja 2020.)

[31] Zakon o zaštiti osobnih podataka, dostupno na: https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka (6. lipnja 2020.)

[29] Europski parlament i Vijeće: „Opća uredba o zaštiti osobnih podataka“, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/ (05. lipnja 2020.).

[30] McKenzie B., „Unpacking the European Commission General Data Protection Regulation - Getting into the Nitty Gritty of How to Comply”, dostupno na https://m.acc.com/chapters/wash/.../BM-Unpacking-the-GDPR-FINAL-June-2017.ppt (10. srpnja 2020).

[31] Hrvatski Sabor, „Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka NN. br. 139/04,“ dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/313073.html. (14. kolovoza 2020.)

[32] Sinarm, dostupno na: http://www.sinarm.net/o-programu/, (12. kolovoza 2020.)

[33] STpro, dostupno na: https://www.stpro.hr/o-programu (20. kolovoza 2020.)

[34] WebZNR-vodeće rješenje za evidenciju zaštite na radu, dostupno na: https://www.zastitanaradu.hr/isznr/ (20. kolovoza 2020.)

[35] Ministarstvo rada i mirovinskog sustava, dostupno na: http://uznr.mrms.hr/znr/is-znr/ (20. kolovoza.2020.)

[36] ZUZNR, „Zajedno za zaštitu na radu, zdravlje i produktivnost , Zagreb, 15.01.2016.“, dostupno na: http://www.hzos.hr/upload_data/site_files/zuznr_hzos_sijecanj_2016.pptx (06. kolovoz 2020.)

7. POPIS SKRAĆENICA

AZOP - Agencija za zaštitu osobnih podataka

CSA - *Cloud* Security Alliance

CSCC - The *Cloud* Standards Customer Council

EC2 - Elastic Compute *Cloud*

EK - Europska komisija

EU - Europska unija

IaaS - Infrastructure as a service

IEC - International Electrotechnical Commission

IKT – Informacijsko-komunikacijska tehnologija

ISO - International Organization for Standardization

IT - Information Technology

LAN - Local Area Network

NaaS - network as a service

OCC - Open Commons Consortium

OCCI - Open *Cloud* Computing Interface

PaaS - Platform as a service

SaaS - Software as a service

ZZOP - Zakon o zaštiti osobnih podataka

8. POPIS SLIKA

9. POPIS TABLICA