FILOZOFSKI FAKULTET SVEUČILIŠTA U ZAGREBU

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

AK. GOD. 2017./2018.

Lovro Šikić

ZAŠTITA OSOBNIH PODATAKA

Završni rad

Mentorica : dr.sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

Sažetak

Podaci su u konstantnom opticaju u današnje vrijeme te su lako dostupni svima. Krađa i zloupotreba podataka nije rijetka pojava i može se svakome u jednom trenutku dogoditi, na nama je da se pravovremeno i na ispravan način zaštitimo. U ovom radu ću se baviti zaštitom osobnih podataka, posljedicama krađe i načinima prevencije. Krađa identiteta je spomenuta kao jedan od najvećih zločina povezanih s krađom podataka. S obzirom na činjenicu da je u posljednjih 20 godina došlo do razvoja tehnologije tako je došlo i do povećanja učestalosti kriminala povezanog s osobnim podacima. Doneseni su novi zakoni i nove regulative, točnije GDPR koji jasno definira naša prava i na koji način smo zaštićeni od zlouporabe podataka. Agencija za zaštitu osobnih podataka jasno definira naša prava i služi tome da kontinuirano nadgleda rad i provođenje nove regulative.

Ključne riječi: *osobni podatak, sigurnost osobnih podataka, obrada osobnih podataka*

Abstract

Data is constantly in circulation today and are easily accessible to everyone. Theft and misuse of data is not a rare occurrence and can happen to anyone at some point, it is up to us to protect ourselves in a timely and correct manner. In this paper I will deal with the protection of personal data, consequences of theft and methods of prevention. Identity theft is mentioned as one of the biggest crimes related to data theft. Given the fact that technology has evolved over the last 20 years, there has been an increase in frequency of crime related to personal data. New laws and new regulations have been adopted, namely the GDPR that clearly defines our rights and how we are protected from data misuse.The Personal Data Protection Agency clearly defines our rights and serves to continuously monitor the work and implementation of the new regulation.

Keywords: *personal data, personal data security, personal data processing*

1 Uvod

Ovaj rad daje kratki osvrt i pregled zakona i regulative koji se tiču zaštite osobnih podataka u Republici Hrvatskoj, ali isto tako i svim zemljama članicama Europske Unije te svim zemljama koje surađuju sa zemljama članicama.

S obzirom na to da je tijekom prošlog, ali ne tako davnog razdoblja došlo do velikog informacijskog napretka tako je došlo i do novih poslova, masovnog korištenja u svrhu ostvarenja novih izvora prihoda, promicanja znanosti, ali isto tako i do novih do tada nepoznatih informatičkih problema, kriminalnih aktivnosti, a samim time i do potrebe za usvajanjem novih zakona kako bi se sankcionirala već počinjena, odnosno spriječila nova kaznena djela.

Europska Direktiva o zaštiti osobnih podataka 95/46/EZ, koja je na snazi bila punih 20 godina promijenila se usvajanjem nove Direktive Europske unije (EU) 2016/679, koja je na snagu stupila početkom svibnja 2018.godine. U proteklom periodu od 20 godina tehnologija je, osobito razvojem interneta, doživjela svoj najveći napredak (posebice društvene mreže kao npr. Facebook, Instagram i dr.) i bilo je jasno da je bilo neophodno poduzeti nove mjere kako bi se zaštitili svi oni korisnici čiji su osobni podaci na bilo koji način izloženi neovlaštenom korištenju, a samim time i njihovoj zlouporabi. Korisnici kojih je danas jako puno, u velikom broju, nisu upoznati sa zaštitom osobnih podataka te su zbog toga podložni potencijalnim opasnostima koje vrebaju iza svakog kuta interneta. Većina korisnika bez previše razmišljanja objavljuje svoje osobne fotografije, mjesta na kojima se nalaze ili općenito podatke iz osobnog života poput preslika osobnih iskaznica, vozačkih dozvola, putovnica ili fotografija svoje djece.

E-bay kao jedna od najpopularnijih internetskih stranica na svijetu zahtijeva, prilikom kupnje ponuđenih proizvoda, unos osobnih podataka potrebnih za dostavu naručene robe, podaci koji se šalju nekoj potpuno nepoznatoj osobi ne razmišljajući pri tome da takav način komuniciranja može dovesti do raznih i ne baš zanemarivih šteta.

2 Važnost zaštite osobnih podataka

Sama svrha zaštite osobnih podataka je ujedno i zaštita kako privatnog života svake individualne fizičke osobe tako i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. [5] U Republici Hrvatskoj svaka fizička osoba ima pravo na zaštitu osobnih podataka neovisno o razlikama u prebivalištu, državljanstvu, spolu, rasi, jeziku, vjeri, socijalnom ili nacionalnom podrijetlu, imovini, društvenom položaju, rođenju, naobrazbi, boji kože ili drugim osobinama.

"Pravo na privatnost ili češće spominjano, prema anglo-američkoj inačici, kao *„Right to privacy*" predstavlja elementarno čovjekovo pravo, kako međunarodno, tako i ustavno pravo javno-pravnog značenja te osobno pravo civilno-pravnog značaja". [1]

U posljednje 2 godine je brzim napretkom tehnologije došlo do stvaranja novih problema oko zaštite osobnih podataka. Zaštita osobnih podataka je važna više nego ikada prije. U ovo doba ubrzanog razvoja informacijske i komunikacijske tehnologije je bitno da zaštitimo svoje osobne podatke kako u realnom tako i virtualnom svijetu.

2.1 Osobni podaci

"Osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati."[5] Svaka osoba može po nekom svom obilježju biti identificirana. To može biti ili prema OIB-u ili nekakvom socijalnom, fizičkom, mentalnom, kulturnom odnosno gospodarskom identitetu. Izuzev naprijed navedenog, osobnim podacima se mogu smatrati i osobne fotografije, adresa stanovanja, elektroničke pošte, odabir stranke itd.

Slika 1. Osobni podatak

Ako više različitih informacija, prikupljenih u jednoj cjelini mogu identificirati određenu osobu, te informacije se također smatraju osobnim podacima. Pseudonimizirani, šifrirani i neidentificiran podaci koji se i dalje mogu upotrijebiti za identifikaciju osobe, ostaju osobni podaci. Osobnim podacima se više ne smatraju podaci koji su anonimizirani, odnosno koji su učinjeni anonimnima tako da se pojedina osoba ne može više preko njih identificirati. Da bi ti podaci uistinu bili anonimni, taj proces anonimizacije mora biti nepovratan.

Najosjetljiviji osobni podaci su:

- Ime i prezime
- Broj bankovnog računa
- Broj osobne iskaznice ili putovnice
- OIB

Sigurnost osobnih podataka

Pravo na sigurnost osobnih podataka podrazumijeva zakonsko pravo građana koje se odnosi na sprečavanje odnosno sankcioniranje zlouporaba osobnih podataka. Identitet pojedinca može se provjeriti izravno ili neizravno, a prije svega prema jednom ili više obilježja vezanih za njegov fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet. Identitet je nešto što pojedinca izdvaja od ostalih na temelju njegovih karakteristika (dob, spol, rasa). Identitet se uglavnom, ali ne nužno, utvrđuje uvidom u javne isprave.

2.2 Posebne kategorije osobnih podataka

Posebne kategorije osobnih podataka zahtijevaju veći stupanj pažnje i brige te posebnu zaštitu s obzirom na njihovu posebnu osjetljivost (politička stajališta, vjerska ili druga uvjerenja, zdravlje, etničko podrijetlo i dr.). Obrada ovog tipa podataka nije dozvoljena, osim u iznimnim slučajevima propisanima u "Zakonu o zaštiti osobnih podataka", a i tada obrada treba biti posebno označena i zaštićena.[4]

Primjer povrede zaštite posebnih kategorija osobnih podataka i neadekvatno ophođenje istim zbio se u incidentu između bolnice i žene koja je u ono vrijeme bila tamošnji pacijent. Naime, njen suprug je zatražio medicinsku dokumentaciju za sina vođenog kao novorođenče u medicinskoj dokumentaciji bolnice. Suprugu nije dostavljena samo dokumentacija tražena za novorođeno dijete već i medicinska dokumentacija njegove supruge. Nakon tog događaja podnesen je zahtjev za zaštitu prava koji je naposljetku i prihvaćen, te je bolnica bila obvezna

poduzeti odgovarajuće mjere, odnosno poboljšati zaštitu svoje medicinske dokumentacije kako ne bi došlo do "curenja" povjerljivih i osjetljivih podataka.

2.3 Krađa identiteta

Krađa identiteta je bilo koja radnja koju netko koristi u svrhu prikupljanja i obrade osobnih podataka bilo koje fizičke osobe, protivno njihovoj volji i ujedno protivno zakonu. Krađa identiteta kao nesporna činjenica povrede privatnosti može se očitovati na više načina od kojih su najviše u primjeni: otvaranje lažnog profila na društvenim mrežama i lažno predstavljanje prema trećima u ime i na račun druge fizičke osobe. Takav način povrede prava na zaštitu osobnih podataka ujedno je i kazneno djelo za koje se može odrediti kazna zatvora u trajanju od jedne godine. Zlouporaba osobnih podataka uobičajeno je usmjerena u svrhu nanošenja štete određenoj osobi.[12]

Kao primjer može se navesti slučaj kada neka osoba otvori lažan profil na društvenoj mreži, koristeći se tuđim osobnim podacima poput osobnih fotografija, imena i prezimena, adrese stanovanja i dobi te osobe kojoj želi nauditi pritom objavljujući vulgaran i neprimjeren sadržaj na toj društvenoj mreži. Na takav način šteti se ugledu i časti osobe te se povređuje njezina privatnost. U određenim slučajevima tuđi osobni podaci se koriste radi počinjenja kaznenih djela (npr. prevara u gospodarskom poslovanju zaključenjem ništetnih ugovora) što je sankcionirano Kaznenim zakonom koji primjerice u svom članku 146. stavak 1. propisuje:

„Tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba kaznit će se kaznom zatvora do jedne godine.“ [9]

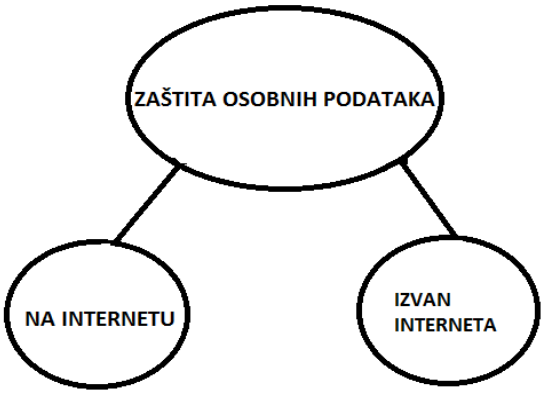
Do krađe identiteta se dolazi na razne načine, a između ostalog i neopreznim raspolaganjem vlastitim podacima od strane osoba čiji su ti podaci do nedostatne i nezadovoljavajuće te neadekvatne primjene mjera zaštite osobnih podataka od strane voditelja zbirki osobnih podataka koji samostalno obrađuju osobne podatke.

Postoje i mnogi načini zaštite od krađe identiteta. Najbolji način za to je instaliranje aplikacije koja se o brine o zaštiti podataka, a time i identiteta. Jedna od funkcija koje te aplikacije imaju je upozoravanje na to da se dogodila značajna promjena na bankovnom računu. Još jedna opcija koju te aplikacije nude je tim koji se brine za sprječavanje situacija koje bi mogle dovesti do financijske štete. Ako je npr. u tijeku velika transakcija poput kupnje automobila, osoba čiji su podaci iskorišteni pri kupnji će biti obaviještena o toj transakciji te će biti upitana da li je to stvarno ona ta koja obavlja transakciju, a u slučaju da nije, tim će pokrenuti

istragu i poduzeti sve potrebne mjere da se ta transakcija zaustavi. Osim instaliranja aplikacija postoje i neke jednostavnije i brže metode kao što su promjena lozinke. Što je kompliciranija lozinka to ju je teže razotkriti. No lozinka nije jedino na što se treba pripaziti tijekom korištenja interneta odnosno društvenih ili poslovnih stranica. Jedan od načina za krađu identiteta je kopanje po nečijem smeću, a to se može razriješiti tako da se osigura uništavač dokumenata, eng. shredder, s kojim se lako može ukloniti bilo kakav fizički dokument na kojem se nalaze podaci. Prije svega neophodno je voditi računa o tome komu se daju osobni podaci i iz kojeg razloga. Jednako tako nužno je paziti i gdje se ostavljaju ti podaci, odnosno da se ne ostavljaju na bilo kojoj društvenoj ili poslovnoj mreži ili na nekom trećem lako dostupnom mjestu, jer se na takav način ti podaci čine lako dostupnima te lako dolazi do njihove zlouporabe.

2.4 Zaštita osobnih podataka

Zaštitu osobnih podataka možemo promatrati obzirom na to radi li se o podacima na internetu ili izvan interneta. U nastavku poglavlja opisane su specifičnosti ova dva slučaja.



Slika 2. Zaštita osobnih podataka

2.4.1 Zaštita osobnih podataka na internetu

Internet je podatkovna mreža koja povezuje milijune računala i računalne mreže korištenjem istoimenog protokola (internetski protokol odnosno IP). Internet kao "mreža svih mreža" se sastoji od milijuna kućnih, poslovnih i svakakvih drugih mreža među kojima se razmjenjuju informacije i usluge kao što su elektronička pošta, chat i prijenos datoteka te povezane stranice i dokumenti World Wide Weba. Dok ga neki ljudi koriste za posao drugi ga mogu koristiti za zabavu. Internet gotovo da nema granica što se tiče mogućnosti rada ili zabave na njemu. Prilikom korištenja interneta, valja biti na oprezu jer je općepoznato da na internetu

ostaju sačuvane radnje koje su poduzimane pa tako i ostavljene osobne podatke. Uz svu tu razvijenu i lako dostupnu tehnologiju vrlo je teško ostati potpuno anoniman. Jedini način na koji bi se zadržala potpuna anonimnost je da se uopće niti ne koristi postojećom tehnologijom.

Sama sigurnost pojedinca u stvarnosti može biti ugrožena objavljivanjem krivih stvari na internetu.[Slika 2.] U svakom slučaju treba uvijek biti na oprezu kada se radi o bilo kakvom objavljivanju, bilo to anonimno na forumima ili javno na društvenim mrežama. Postoje različite metode kojima se mogu prikupljati podaci na internetu među kojima je i tzv. Spoofing attack metoda. Spoofing je falsificiranje tuđih podataka, a može se iskoristiti za nanošenje štete osobama čiji su podaci iskorišteni. Postoji nekoliko različitih Spoofing metoda.

Jedna od metoda je tzv. E-mail spoofing koja implicira izrađivanje e-mail poruka s krivotvorenom adresom pošiljatelja. Često spam[1] i phishing[2] elektroničke pošte koriste takav spoofing kako bi prevarile primatelja pošte o porijeklu same te pošte. Na primjer osoba je dobila zaraženu elektroničku poštu i otvorila ju je. Virus unutar elektroničke pošte može pretražiti adresar osobe čije je računalo zaraženo i može nekoj drugoj osobi poslati isti takav e-mail u ime osobe čije je računalo zaraženo što odmah povećava vjerojatnost širenja otvaranog zaraženog e-maila.

Još jedna metoda je Website spoofing. Website spoofing je izrada lažne internetske stranice s namjerom da se prevari čitatelje implicirajući da je stranica stvorena od strane neke druge osobe ili organizacije. Tako je moguće da napadač stvori kopiju World Wide Weba kroz koju može dobiti sve osjetljive informacije osobe koja je tom metodom pogođena. GPS spoofing pokušava zavarati GPS prijamnik emitirajući netočne GPS signale. Takav napad započinje emitiranjem signala koji se sinkronizira s pravim signalima koje dobiva primatelj te se onda ti lažni signali postepeno pojačavaju tako da bi se primatelja odvuklo od pravih signala prema lažnima. Primjer takvog napada je kada je uhvaćen dron Lockheed RQ-170 u sjeveroistočnom Iranu 2011. godine.

Login spoofing je još jedna od metoda spoofing napada. To uključuje tehnike kojima se pokušavaju ukrasti korisničke lozinke. Korisnik se pokušava ulogirati sa svojim korisničkim

[1] Spam ili junk mail. Neželjena pošta. Dosta spam pošte sadrži sakrivene linkove koje vode na phishing stranice ili na stranice koje sadrže malware.
[2] Pokušaj da se dobiju osjetljive informacije poput korisničkih imena i kreditnih kartica prerušavanjem u povjerljivi entitet u elektroničkoj komunikaciji.

imenom i lozinkom u naizgled običnu stranicu koja je ustvari lažna verzija originalne stranice napravljena od strane napadača s namjerom da dođe do lozinke.

Peta metoda je tzv. DNS spoofing, nazvan i trovanjem DNS predmemorije. To je oblik hakiranja u kojima napadač dolazi do cjelokupnog internetskog prometa žrtve.

Šesta metoda je IP spoofing tj. tehnika kojom se promijeni polazišna adresa IP paketima. Jedan od ciljeva ove tehnike je lažiranje IP adrese što omogućuje napadaču da zaguši računalo osobe čija se adresa krivotvori tj. da se onemogući usluga, eng. Denial of service. [6]

2.4.2 Zaštita osobnih podataka izvan interneta

Uz zaštitu osobnih podataka izvan interneta najviše je vezana krađa identiteta. Ako dođe do gubitka ili krađe osobne iskaznice potrebno je nadležnim organima, odnosno policiji, što prije prijaviti nestanak. U slučaju da neka druga osoba dođe u vlasništvo tuđe osobne iskaznice može nanijeti materijalnu štetu. Čest primjer nanošenja takve materijalne štete je lažno predstavljanje u ime te druge osobe, čija je iskaznica, putem telefona. Preko osobne iskaznice jednostavno se dolazi do OIB-a koji se može iskoristiti za lažno predstavljanje. Jedan takav primjer lažnog predstavljanja bi bio da se putem telefona naruče novi mobilni uređaji na ime osobe čija je osobna iskaznica te da ih se tako i materijalno ošteti. [Slika 2.]

Kao što postoje načini prikupljanja podataka na internetu tako postoje i u svakodnevnom životu. Nije teško doći do osobnih podataka, a jedna od tehnika koja najbolje funkcionira je tzv. socijalni inženjering temeljen na pojedincima tj. na ljudskom faktoru. Informacije se mogu prikupljati na različite načine, koristeći ljudsko povjerenje, znatiželju, nemarnost itd. Cilj socijalnog inženjeringa je da se nanese novčana šteta prevarenim osobama. Primjer bi bila infiltracija na radno mjesto osobe koju se napada te pregledavanjem službene dokumentacije u poslovnim prostorijama ili čak prekopavanja smeća te osobe na koji način se može doći do nekakvih privatnih i tajnih informacija koje se mogu iskoristiti protiv žrtve. Jedna od najjednostavnijih tehnika je tzv. Shoulder surfing, tj. otkrivanje lozinke pristupa osobnom računalu dok se napadač nalazi u blizini žrtve koja upisuje svoju lozinku, a da to žrtva ni ne zna. Jedna od popularnijih tehnika je kopanje po smeću, eng. Dumpster diving. Ovo implicira prekopavanje smeća kako bi se našle osjetljive informacije ili lozinke za ulaz u sustav ili bilo koji drugi podaci koji bi pomogli neovlaštenom ulazu u računalo žrtve. Također, žrtve mogu biti prevarene od strane napadača. Napadač može preuzeti tuđi identitet i lažno se predstaviti. Najčešće se to zna dogoditi putem telefona kada se napadač može

predstaviti kao ovlašteni serviser te tako iskoristi nepažnju i naivnost žrtve kako bi došao do lozinke ili nekih drugih povjerljivih informacija.

3 Direktiva 95/46/EZ Europskog parlamenta i Vijeća

Sustavi za obradu podataka su osmišljeni da služe čovjeku; moraju poštivati njihova temeljna prava i slobode, prava na privatnost te doprinositi razvitku gospodarstva i socijalnom aspektu. [8] Data protection Directive (Direktiva 95/46/EZ) uvedena je 24. listopada 1995. godine u svrhu zaštite individualnih osoba u smislu zaštite njihovih osobnih podataka.

Pravo na privatnost je visoko razvijeno područje prava u Europi. Sve države članice su isto tako potpisale i Konvenciju za zaštitu ljudskih prava i temeljnih sloboda 4. studenog 1950. uzimajući u obzir Opću deklaraciju o ljudskim pravima proglašenu 10. prosinca 1948. godine. Cilj potpisane konvencije je bilo da se ustanove ljudska prava, odnosno prava na život i slobodu osim ako sudskom presudom nije izrečena zatvorska odnosno smrtna kazna. Direktiva o zaštiti osobnih podataka regulira obradu osobnih podataka bilo da je takva obrada automatska ili ne. Obrada osobnih podataka ne bi smjela biti dopuštena, osim u slučaju zadovoljavanja određenih uvjeta. Ti uvjeti spadaju u 3 kategorije: transparentnost, legitimna svrha i proporcionalnost.

Transparentnost

osoba čiji se podaci obrađuju ima pravo biti obaviještena u slučaju da se njeni podaci obrađuju. Podaci se smiju obraditi samo ako je barem jedna od navedenih konstatacija istinita:

- Osoba čiji se podaci obrađuju je dala dopuštenje.
- Kada je obrada podataka bitna za sklapanje ugovora.
- Kada je obrada neophodna za poštivanje zakonske obveze.
- Kada je obrada podataka potrebna da bi se zaštitili vitalni(neka druga riječ možda) interesi nositelja podataka(osobnih podataka osobe)(osobe u pitanju)(data subject)
- Kada je obrada neophodna za obavljane zadataka u svrhu javnog interesa ili u obavljanju
- službene ovlasti dodijeljene trećoj strani kojoj se podaci otkrivaju.
- Ako je obrada neophodna u svrhu legitimnih interesa koje provodi kontrolor ili treća strana ili stranke kojima se podaci otkrivaju, osim u slučaju da su takvi interesi nadmašeni interesima za temeljna ljudska prava i slobode nositelja podataka. Subjekt podataka(Osoba čiji su podaci) ima pravo na pristup svim obrađenim podacima o njemu, te također ima pravo tražiti ispravljanje, brisanje ili blokiranje podataka koji su nepotpuni, netočni ili nisu u skladu s pravilima zaštite podataka.

Legitimna svrha

Osobni podaci mogu biti obrađivani samo u legitimne svrhe te se ne smiju dalje obrađivati na bilo koji način koji je nekompatibilan s tim ciljevima. Osobni podaci moraju biti zaštićeni od zlouporabe i moraju imati poštovanje za određena prava vlasnika podataka koja su zajamčena pravom EU.

Proporcionalnost

Obrađivanje osobnih podataka je dopušteno samo ako su prikladni podaci relevantni i ne prelaze svrhu za koju su prikupljani i dalje obrađivani. Prikupljeni podaci moraju biti točni i ažurni te se moraju poduzeti svi koraci kako bi se osiguralo da se svi netočni ili nepotpuni podaci s obzirom na svrhu u koju su prikupljani budu izbrisani ili ispravljeni. Ti isti podaci ne smiju biti čuvani na takav način koji dopušta identifikaciju subjekta odnosno vlasnika tih podataka duže nego što je potrebno u svrhe za koje su prikupljeni. Zaštitne mjere moraju biti propisane od strana država članica za osobne podatke koji se čuvaju u razne svrhe tj. za statističku, povijesnu ili znanstvenu uporabu. Pri obradi osjetljivih podataka, odnosno vjerskih uvjerenja, političkih mišljenja, zdravlja, rasa itd., dodatna ograničenja moraju biti primijenjena.

4 Reforma zaštite osobnih podataka u EU

Nedvojbeno je da postoji golema količina podataka, a velika većina tih podataka je javna i dostupna svima. Nesporno je da je veliki dio tih podataka osobne naravi poput imena i prezimena te adrese pojedine osobe, njegove zdravstvene povijesti, fotografije, video snimke itd. Većini ljudi je u interesu da zadrže određenu razinu privatnosti i kontrole nad svojim osobnim podacima, a cilj GDPR-a je da to osigura, odnosno da pomogne u očuvanju tih podataka i da pojača prava vezana uz osobne podatke.

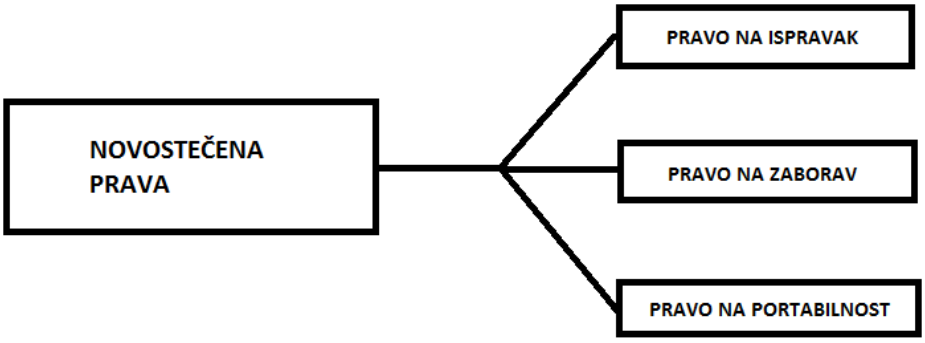
Slika 3. General Data Protection Regulation

GDPR ili General Data Protection Regulation je regulativa koja je stupila na snagu 25. svibnja 2018. godine. GDPR je regulativa Europske unije pa se tako odnosi na sve zemlje članice EU, uz napomenu da su novom regulativom zahvaćene i zemlje koje posluju na teritoriju EU ili s građanima EU. Kao primjer može se istaknuti društvena mreža Facebook koja mora pratiti odredbe europske regulative unatoč tome što je američka kompanija. Kako bi pravne odnosno fizičke osobe čije podrijetlo odnosno boravište nije na teritoriju EU mogle obavljati poslove s članovima EU, moraju se pridržavati pravila koja propisuje GDPR. Ta regulativa ima utjecaj na pohranjivanje, obrađivanje, pristup i transfer podataka. Prema GDPR-u svaka organizacija koja nadgleda podatke na nekoj većoj razini, mora imenovati službenika za zaštitu podataka. Isto tako se implementira i ideja pseudonimizacije[3]. Svi čiji su podaci korišteni i koji su pod zaštitom GDPR-a imaju pravo na prigovor, tj. mogu tražiti da se njihovi podaci prestanu obrađivati i koristiti. To znači da organizacije koje se koriste tim podacima sada imaju pravnu obvezu pokazati kako imaju legalan i uvjerljiv razlog za obradu podataka. Svaka zemlja koja je članica EU ima nadzorna tijela koja provode GDPR. Neprestanim razvojem tehnologije

[3] Obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija

nastaju problemi koje GDPR nastoji riješiti. Što više postajemo ovisni o tehnologiji, o sakupljanju, obradi, i dijeljenju podataka to se više javlja potreba da zaštitimo te podatke.

4.1 Novostečena prava



Slika 4. Podjela novostečenih prava

4.1.1 Pravo na ispravak

Pravo na ispravak znači da vlasniku osobnih podataka mora biti omogućen uvid u njegove osobne podatke te mu se mora pružiti mogućnost ispravka. Odnosno u slučaju uočavanja greške na osobnim podacima npr. ime, prezime, adresa itd. moguće je obratiti se centru za korisnike u kojem se ti podaci čuvaju, da se ta greška korigira. Problem i mana je u heterogenim IT sustavima s kompleksnom organizacijom u velikim tvrtkama. Velike firme mogu prikupljati osobne podatke iz različitih razloga te se ti osobni podaci, unatoč tome što se odnose na jednu istu osobu, mogu razlikovati. Npr. Zagrebački holding može imati različite podatke za odvoz smeća i isporuku plina. Što više se podaci obrađuju to više može doći do pobune i negativnog učinka u smislu da nastane zbrka oko točnosti podataka, a isto tako može doći i do zbrke oko OIB-a i JMBG-a pa sve to može dovesti do izmjene digitalnog identiteta u nekom IT sustavu.[3]

4.1.2 Pravo na zaborav

Pravo na zaborav – Ovo je najzahtjevnije pravo koje je nova regulativa donijela. Ako vlasnik osobnih podataka odluči da više ne želi imati svoje podatke u sustavu neke tvrtke on ih može zatražiti da ih ta tvrtka i obriše. Primjer toga bio bi da je neka osoba prije bila klijent neke banke te je došlo do raskida odnosa, u tom slučaju osoba koja više nije klijent banke može tražiti da se njegovi podaci izbrišu. Brisanje osobnih podataka iz nekog sustava može narušiti i samu strukturu sustava, te je zbog toga tehnički zahtjevno. Većina sustava, napravljena je

prije GDPR-a i nije imala implementiranu opciju brisanja podataka, te zbog toga uglavnom većina tih sustava ima samo mogućnost označivanja podataka kao da su neaktivni dok se svi podaci zadržavaju, no to nije dovoljno dobro za GDPR pa nastaju problemi. Pravo na zaborav se uglavnom odnosi na podatke koje je neka osoba dala nekome na korištenje i obrađivanje uz privolu. Ovim se pravom ne samo osigurava to da svaki novi sustav mora imati kao preduvjet opciju za brisanje podataka nego i povećava iznimno puno i samu sigurnost tih podataka.[3]

4.1.3 Pravo na portabilnost

Pravo na portabilnost znači da se vlasniku osobnih podataka omogući njihov prijenos u elektroničkom obliku. Primjerice ako se želi promijeniti dobavljač struje, od trenutnog dobavljača se može zatražiti izvoz potrošnje za sve prošle periode u namjeri da novi dobavljač može izračunati uštedu.[3]

4.2 Načela obrade osobnih podataka

Opća uredba o zaštiti podataka (GDPR) (EU) 2016/679 uredba je Europske unije kojom se regulira zaštita podataka i privatnost individualaca unutar Europske unije, a donosi i propise vezane za iznošenje podataka u treće zemlje. Glavni su ciljevi GDPR-a vratiti građanima nadzor nad njihovim osobnim podacima i pojednostaviti regulatorno okruženje za međunarodne korporacije ujednačavanjem propisa u cijeloj Uniji. Stupanjem GDPR-a na snagu prestaje važiti Direktiva 95/46/EC. Uredba je usvojena 27. svibnja 2016. godine, čime je počelo teći prijelazno razdoblje od dvije godine. GDPR je na snagu stupio 25. svibnja 2018. Ova uredba, u području osobnih podataka, predstavlja veliki napredak. Uredba se odnosi na obradu osobnih podataka koja je u cijelosti automatizirana te isto tako i na neautomatiziranu obradu osobnih podataka koji su obuhvaćeni sustavom pohrane ili su namijenjeni biti dio sustava pohrane. Jedan od bitnijih članaka ove uredbe (Članak 5.), odnosi se na obradu podataka odnosno kako se prema podacima treba odnositi i na koji način smiju biti obrađivani. Iz te uredbe slijedi 6 načela:

1. Zakonitost, poštenosti, transparentnost - Osobni podaci se moraju pošteno, zakonito i transparentno obrađivati s obzirom na osobu čiji su podaci.
2. Ograničavanje svrhe - Ako su podaci zakonski uz privolu ispitanika prikupljeni i obrađeni u jednu svrhu, ne smiju se obrađivati u neku drugu.

3. Smanjenje količine podataka - Mora se obratiti pažnja na to da podaci budu primjereni, relevantni i ograničeni na svrhu u koju se obrađuju.
4. Točnost - Točnost podataka i njihova ažurnost ne smije biti zanemarena.
5. Ograničenje pohrane - Prikupljeni podaci moraju moći identificirati ispitanika samo na ono vrijeme koje je potrebno za obrađivanje u neku svrhu. Iznimno se podaci smiju čuvati na dulji period ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.
6. Cjelovitost i povjerljivost - Podaci moraju biti na takav način obrađivani kako bi se sačuvao njihov integritet i osigurala njihova sigurnost. [13]

4.3 Zakonitost obrade

Obrađivanje podataka je dopušteno i zakonito ako su ispunjeni određeni uvjeti od kojih je najvažniji da je osigurana privola ispitanika za obradu njegovih osobnih podataka. No uz taj najbitniji uvjet postoje i drugi uvjeti koji, ako su zadovoljeni, omogućavaju obradu osobnih podataka. Ako je ispitanik stranka u nekakvom ugovoru i ako je obrada bitna za izvršenje tog ugovora, dopušteno je obrađivanje podataka. Osim stjecanje privole osobe, čiji su osobni podaci prikupljeni odnosno obrađeni, daljnji uvjeti za stjecanje prava na prikupljanje i obradu osobnih podataka su:

1. Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
2. Obrada je nužna radi poštovanja pravnih obveza voditelja obrade
3. Obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe
4. Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade
5. Obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.
   [7]

5 Agencija za zaštitu osobnih podataka – AZOP

Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima. AZOP ima viziju uspostavljanja i očuvanja visoke razine zaštite osobnih podataka kao jednog od temeljnih ljudskih prava. AZOP namjerava u suradnji s akterima tj. voditeljima obrade, izvršiteljima obrade, primateljima i drugima, osigurati zaštitu osnovnih ljudskih prava i pravo na slobodu svakog pojedinca u području privatnosti, te pogotovo njihovo pravo na zaštitu i privatnost osobnih podataka.

Misija Agencije za zaštitu osobnih podataka je uspješno izvršavanje nadzora nad provođenjem propisa o zaštiti osobnih podataka. AZOP se brine o sprječavanju zlouporabe prikupljanja osobnih podataka. Agencija se također brine o izradi i davanju preporuka za unapređenje zaštite osobnih podataka kod voditelja obrade i o davanju savjeta kada je riječ o stvaranju novih zbirki osobnih podataka, pogotovo ako je riječ o uvođenju neke nove informacijske tehnologije. Također se brine o suradnji s nadležnim državnim tijelima u izradi prijedloga propisa koji se odnose na zaštitu osobnih podataka. Agencija također prati uređenja zaštita osobnih podataka u drugim zemljama te suradnju s tijelima koja su nadležna nad zaštitom osobnih podataka u njima.[5]

Strateški plan Agencije za zaštitu osobnih podataka ima jasno definirane ciljeve, a to su: podizanje razine zaštite osobnih podataka i osiguravanje učinkovite provedbe zakona i propisa o zaštiti osobnih podataka. Pokazatelj učinka, odnosno ostvarivanja tih ciljeva je smanjen broj uočenih zlouporaba. Ovi ciljevi se planiraju ostvariti na nekoliko načina :

1. Nadzorom provedbe zaštite osobnih podataka
2. Podizanjem razine svijesti građana i popularizacije područja zaštite osobnih podataka
3. Rješavanje povodom zahtjeva za utvrđivanje povrede prava zajamčenih Zakonom o zaštiti osobnih podataka
4. Provođenjem nadzora prema Uredbi o Hrvatskom viznom informacijskom sustavu
5. Donošenjem zakonskih i podzakonskih akata odnosnih na područje zaštite osobnih podataka

Indikator da se nadzire provedba zaštite osobnih podataka će biti kontinuirana realizacija planiranih nadzora po službenoj dužnosti i nadzora po zahtjevu za zaštitu prava. Podizanje razine svijesti građana će biti očitovano kroz kontinuirano održavanje različitih oblika osvještavanja javnosti i edukacija za osobe zaslužne za brigu osobnih podataka. Rješavanje

povodom zahtjeva za utvrđivanje povrede prava zajamčenih Zakonom o zaštiti osobnih podataka će biti vidljivo iz dvije stvari, a to su: kontinuirano rješavanje neupravnih predmeta u predviđeno vrijeme zakonskih rokova i kontinuirano praćenje tih istih predmeta i njihovo rješavanje. Provođenje nadzora prema Uredbi o Hrvatskom viznom informacijskom sustavu će biti očitano kroz kontinuiranu realizaciju planiranih nadzora diplomatskih misija i konzularnih ureda RH u svijetu na godišnjoj razini. I na kraju iz čega će biti vidljivo da donošenje zakonskih i podzakonskih akata koji se odnose na područje zaštite osobnih podataka djeluje su izmjene i dopune tih zakonskih i podzakonskih akata koje su objavljene u Narodnim novinama i koje su stupile na snagu.

6 Zaključak

U izradi ovog završnog rada, bilo je potrebno osvrnuti se na zaštitu osobnih podataka i na sve nove odredbe i regulative koje je propisala Europska unija kako bi zaštitila svoje građane od zlonamjernih napada i nedozvoljenog korištenja osobnih podataka i nemarnog ophođenja osobnim podacima svake osobe. U današnje vrijeme, kontinuiranim razvojem informacijskih tehnologija dolazi do sve veće potrebe o brizi za osobne podatke. Današnja tehnologija omogućava brzu i neprestanu obradu osobnih podataka što ju ostavlja ranjivijom nego ikada prije. No tehnologija ne donosi samo negativne posljedice, već i dosta pozitivnih. Možemo se zaštititi od napadača na internetu i u stvarnosti kako ne bi došlo do negativnih posljedica. Agencija za zaštitu osobnih podataka vrlo je važna za građane Republike Hrvatske s obzirom na to da joj je jedna od glavnih zadaća kako briga o određenim pravima građana tako i briga o implementaciji novih prava i obveza nametnutih Republici Hrvatskoj kao punopravnoj članici Europske unije i Vijeća Europe.

Jako je puno primjera kako su pojedinci bili povrijeđeni počevši od nemarnog odnosa prema svojim osobnim podacima ili nepažljivim ostavljanjem svog računala otvorenog i spremnog za rad preko objavljivanja osobnih ili fotografija članova obitelji na društvenim mrežama sve do gubitka osobnih podataka krađom na internetu ili u stvarnom svijetu na veliki broj načina. Naša je zadaća, kao vlasnika svojih osobnih podataka, voditi primjerenu brigu o njima kako ti podaci ne bi pali u krive ruke i nanijeli nam štetu. Problem predstavlja neinformiranost i neznanje velike većine nas kao pojedinaca kako o načinu ophođenja osobnim podacima tako i osobito o načinu i postupcima njihove zaštite.

7 Literatura

Popis internetskih izvora

1. Boban, M. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu. // Zbornik radova Pravnog fakulteta u Splitu 49(2012.), str. 575.-598. Dostupno na: https://hrcak.srce.hr/file/129212 (01.08.2018)

2. Caroll, B. Computer Crime [prezentacija]. Dostupno na: http://crystal.uta.edu/~carroll/cse3316/uploads/750BCADD-CDF6-3D91-4781-9AD587B37296_.pdf (02.09.2018)

3. Cerin, S. ICT Business : Usklađivanje IT sustava i upravljanja IT sustavima. // Velika škola GDPR-a lekcija 6. Dostupno na: https://www.ictbusiness.info/kolumne/velika-skola-gdpr-a-lekcija-6-uskladivanje-it-sustava-i-upravljanja-it-sustavima (03.09.2018)

4. Cerin, S. ICT Business : Utjecaj na društvo i poslovanje. // Velika škola GDPR-a ICTbusiness portala. Dostupno na: https://www.ictbusiness.info/kolumne/velika-skola-gdpr-a-ictbusiness-portala-lekcija-prva-utjecaj-na-drustvo-i-poslovanje (02.09.2018)

5. Djelatnost i unutarnje ustrojstvo Agencije // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/djelatnost-agencije (25.08.2018)

6. Dolenc D, Lazić M, Mudražija M. Zaštita osobnih podataka u RH. // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (29.08.2018)

7. DuPaul, N. SPOOFING ATTACK: IP, DNS & ARP. // Veracode. Dostupno na: https://www.veracode.com/security/spoofing-attack (29.08.2018)

8. Europski parlament. Članak 6. : "Zakonitost obrade". // Opća uredba o zaštiti podataka. Dostupno na: http://www.privacy-regulation.eu/hr/6.htm (29.08.2018)

9. Europski parlament; Vijeće Europe. Direktiva o zaštiti pojedinaca glede obrade osobnih podataka i o slobodnom kretanju takvih podataka. // Službeni list L 281(1995.), str. 31–50. Dostupno na: http://www.azlp.gov.ba/images/PropisiHR/Direktiva%2095-46-EC%20Europskog%20parlamenta%20i%20Vije%C4%87a%20od%2024.10.1995.pdf (01.08.2018)

10. Hrvatski sabor. Članak 146. : Nedozvoljena uporaba osobnih podataka. // Kazneni zakon. Dostupno na: https://zakonipropisi.com/hr/zakon/kazneni-zakon/146-clanak-nedozvoljena-uporaba-osobnih-podataka# (29.08.2018)

11. Intersoft consulting [Internet]. [Pristupljeno 16.08.2018]; Dostupno na: https://gdpr-info.eu/art-1-gdpr/

12. Klarić, M. Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda. Zbornik radova Pravnog fakulteta u Splitu 53, 4 (2016.). Dostupno na: https://hrcak.srce.hr/169037 (25.08.2018)

13. Neovlašteno prosljeđivanje osobnih podataka radnika. // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/rjesenja-agencije/detaljnije/obrada-osjetljivih-podataka (10.08.2018)

14. Politika o zaštiti podataka. // Splitska banka. Dostupno na: https://www.splitskabanka.hr/Portals/8/docs/Politika%20o%20za%C5%A1titi%20podataka.pdf (07.09.2018)

15. Posebne kategorije osobnih podataka-osobni podaci koji zahtijevaju posebnu zaštitu. // AZOP : Agencija za zaštitu podataka. Dostupno na: http://azop.hr/prava-ispitanika/detaljnije/posebne-kategorije-osobnih-podataka (19.08.2018)

16. Prikupljanje i obrada osobnih podataka radnika prilikom evidentiranja radnog vremena. // AZOP : Agencija za zaštitu podataka. Dostupno na: http://azop.hr/info-servis/detaljnije/prikupljanje-i-obrada-osobnih-podataka-radnika-prilikom-evidentiranja-radno (01.09.2018)

17. Reforma zaštite podataka - EP odobrio nova pravila. // Europski parlament : Vijesti. Dostupno na: http://www.europarl.europa.eu/news/hr/press-room/20160407IPR21776/reforma-zastite-podataka-ep-odobrio-nova-pravila (02.09.2018).

18. Reforma zaštite osobnih podataka u EU-usvojen novi zakonodavni paket zaštite osobnih podataka. // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/aktualno/detaljnije/europska-unija-usvojila-zakonodavni-paket-zastite-osobnih-podatak (10.08.2018)

19. Strateški plan Agencije za zaštitu osobnih podataka za razdoblje 2017.-2019. godine. // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/images/dokumenti/217/strateski-plan-azop.pdf (15.08.2018)

20. System and method for early detection and prevention of identity theft. // United States Patent. Dostupno na: https://patentimages.storage.googleapis.com/9b/66/37/ff6cfedf890278/US7548886.pdf (03.09.2018)

21. Što je krađa identiteta? // AZOP : Agencija za zaštitu podataka. Dostupno na: http://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi (02.09.2018)

22. The European Parlament; The Concil of EU. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. // Eur-lex : Official Journal. Dostupno na: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (03.09.2018)

23. Uvid u natječajnu dokumentaciju. // AZOP : Agencija za zaštitu podataka. Dostupno na: https://azop.hr/uvid-osobni-podaci/detaljnije/uvid-u-natjecajnu-dokumentaciju1 (10.08.2018)

24. Vijeće Europe. (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda. // Zakon.hr. Dostupno na: https://www.zakon.hr/z/364/(Europska)-Konvencija-za-za%C5%A1titu-ljudskih-prava-i-temeljnih-sloboda (03.09.2018)

25. Zaštita osobnih podataka. // Obrazovna grupa Zrinski. Dostupno na: http://www.zrinski.org/nikola/o-nama/info/zastita-osobnih-podataka-2438/ (02.09.2018)

Popis literature

26. Bračić, M.; Krehić, T. GDPR Master course – posljednja provjera uoči implementacije. // Hrvatski institut za finacije. Dostupno na: http://hif.hr/gdpr-master-course-posljednja-provjera-uoci-implementacije/

27. Kaelble S. GDPR Compliance for dummies. New Jersey: John Wiley & Sons; 2018.