Usporedba savjetnika za informacijsku sigurnost prema Zakonu o informacijskoj sigurnosti i službenika za zaštitu osobnih podataka prema Općoj uredbi o zaštiti podataka

Crnković, Kristijan

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Law / Sveučilište u Zagrebu, Pravni fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:199:632573

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-01-18**

Repository / Repozitorij:

Repository Faculty of Law University of Zagreb

Pravni fakultet Zagreb
Katedra za pravo informacijskih tehnologija i informatiku

Kristijan Crnković

USPOREDBA SAVJETNIKA ZA INFORMACIJSKU SIGURNOST PREMA ZAKONU O INFORMACIJSKOJ SIGURNOSTI I SLUŽBENIKA ZA ZAŠTITU PODATAKA PREMA OPĆOJ UREDBI O ZAŠTITI PODATAKA

Diplomski rad

mentor izv. prof. dr. sc. Tihomir Katulić

Zagreb, lipanj 2024.

Izjava o izvornosti

Ja, Kristijan Crnković, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor diplomskog rada, da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima do onih navedenih u radu.

Kristijan Crnković, v.r.

Sadržaj

1. Uvod

Područje informacijske sigurnosti i pravo zaštite osobnih podataka iznimno su aktualne teme u današnjem okruženju. Svakodnevno se susrećemo, ali i koristimo informacijskim tehnologijama gdje se prikupljaju naši podatci, od najbanalnije kupovine namirnica u internetskoj trgovini pa sve do mobilnog bankarstva i raznih servisa koje nude sustavi poput e-Građani. S pogodnostima koje nose informacijske tehnologije dolaze i ugroze za informacijsku sigurnost i zaštitu osobnih podataka. Također se s razvojem tehnologije razvijala, i još se razvija, pravna zaštita na područjima informacijske sigurnosti i zaštite podataka na međunarodnoj razini, ali i u nacionalnim zakonodavstvima.

Središnji dio rada započinje poglavljem o informacijskoj sigurnosti. Donosi povijesni razvoj toga područja, ali i ono što predstavlja danas. Slijede poglavlja o zakonodavnom okviru informacijske sigurnosti u Republici Hrvatskoj i poziciji savjetnika za informacijsku sigurnost koja je u hrvatski pravni poredak uvedena 2008. godine donošenjem Zakona o informacijskoj sigurnosti. Nezaobilazno je poglavlje o području prava zaštite podataka, odnosno povijesti i razvoju prava zaštite podataka te povezanosti s pravom na privatnost. Rad donosi i odgovor na pitanje kako je pravo na zaštitu podataka uređeno danas s naglaskom na Opću uredbu o zaštiti podataka koja od 2018. (2016.) godine uređuje to područje u Europskoj uniji. Naposljetku, detaljnije se izlaže o poziciji službenika za zaštitu podataka, njegovim pravima i obvezama te ulozi koju ima unutar organizacije voditelja ili izvršitelja obrade.

U zaključku se daje završna misao o poziciji savjetnika za informacijsku sigurnost i o poziciji službenika za zaštitu podataka.

2. Informacijska sigurnost

2.1. Povijesni razvoj

Iako je pojam informacijske sigurnosti nastao nedavno, nije pogrešno reći da je osnovna njegova smisao u ljudskoj civilizaciji prisutna još od davnih vjekova. U svakom razdoblju postojali su određeni podatci, informacije za koje su ljudi smatrali da su važne i koje su na poseban način željeli zaštititi. Svaka nova era donosila je sa sobom nove tehnologije, nova otkrića, nove tajne i samim time nove informacije koje su se štitile na poseban način, što je zapravo smisao informacijske sigurnosti danas.

Povijest informacijske sigurnosti ne počinje s razvojem interneta, telegrafa i telefona, nego puno prije,[1] još od drevnih egipatskih hijeroglifa (koje su ponekad stari Egipćani pisali na nestandardni način kako bi zavarali neprijatelje), ali i starih Grka (koji su se služili primitivnim štapom *skytale* koji je funkcionirao tako da se pergament motao oko štapa određenog promjera na koji se zatim pisala poruka razumljiva samo onome koji je imao štap istog promjera). Sve su to bili primitivni načini kojima su ljudi pokušavali zaštititi svoje važne informacije, što je ujedno važno za razumijevanje pojma informacijske sigurnosti danas.[2]

Suprotno navedenim tezama, većina autora smatra da je razvoj informacijske sigurnosti počeo puno kasnije u povijesti, tek u 20. stoljeću.[3] Uzima se da je povijest informacijske sigurnosti počela zapravo s konceptom i razvojem računalne sigurnosti.[4] Potreba za računalnom sigurnosti pojavila se sredinom 20. stoljeća, točnije u Drugom svjetskom ratu kada su se razvila prva računala koja su koristila za dešifriranje poruka nacistički kriptografski stroj Enigmu.[5] Implementirale su se razne sigurnosne mjere poput ograničavanja pristupa samo ljudima koji su imali ključ ili značku; ili su zaštitari odobravali pristup na temelju prepoznavanja lica.[6] U početku su sve mjere računalne sigurnosti bile usmjerene na zaštitu računala, osoblja i ostale opreme od vanjskih, fizičkih prijetnji poput krađe, špijunaže, sabotaže i slično. Tek se kasnijim

[1] De Leeuw, Karl; Bergstra, Jan. *The history of information security, a comprehensive handbook*, Elsevier, Amsterdam, 2007., str. 1.
[2] Ibid. Slična teza iznijeta je u citiranoj knjizi gdje se na kratkoj crtici iz Nizozemske povijesti objašnjava kako su se već tada, u 17. st., ljudi brinuli za podatke i protok informacija jer su razumjeli da ako određena informacija dođe u pogrešne ruke može doći do ozbiljnih posljedica, što je zapravo važno za suvremeno razumijevanje pojma informacijske sigurnosti.
[3] Whitman, Michael E.; Mattord, Herbert J. *Principles of Information Security*, Cengage, Boston, 2021., str 3.
[4] Ibid.
[5] Ibid.
[6] Ibid.

razvojem tehnologije shvatilo da treba, osim samog računala, štititi i sam računalni sustav.[7] Jedan od prvih zabilježenih problema na računalnom sustavu, koji nije imao veze s fizičkom, vanjskom prijetnjom, dogodio se početkom šezdesetih godina 20. stoljeća kada je računalo zbog pogreške u programu zamijenilo dvije datoteke (jedna je bila i ona sa zaporkama) na kojima su radili administratori, što je prouzročilo da datoteka sa zaporkama bude objavljena.[8]

Šezdesete godine su godine u kojima se razvio ARPANET, preteča današnjeg interneta, radi lakše i učinkovitije razmjene informacija između računala koja je koristila američka vojska.[9] Premda koristan i za svoje vrijeme napredan, imao je mnogo mana u pogledu mrežne sigurnosti. Bio je česta meta napada tako da se njegova mrežna sigurnost počela nazivati mrežna nesigurnost.[10] Kako to obično biva, svi nedostatci i sve pogreške koje donosi jedan sustav pridonose tome da sljedeći sustav bude napredniji. Tako se može reći za izvještaj RAND R-609 iz 1970. godine (dok mu je oznaka povjerljivosti skinuta tek 1979. godine kada je i objavljen) da je bio prvi rad koji je pokušao definirati razne kontrole i mehanizme važne za zaštitu podataka obrađenih unutar računalnog sustava. U njemu je prepoznata važnost zaštite samog računalnog sustava. Prije rada narativ je bio na fizičkoj zaštiti računala i lokaciji na kojoj se ono nalazilo.[11] U radu se tako napominje da se mora obratiti veća pažnja na osiguranje podataka, da se moraju ograničiti neodobreni i slučajni pristupi podatcima te da se u osiguranje informacijske sigurnosti mora uključiti osoblje sa svih hijerarhijskih razina organizacije.[12] Ovaj se rad ujedno smatra kao začetak proučavanja računalne sigurnosti.[13]

Kako se razvijala tehnologija i sustavi sigurnosti, počeli su se razvijati i pravni instrumenti koji će uređivati i štititi to područje. Tako je sredinom osamdesetih godina 20. st. zakonodavac u SAD-u donio nekoliko zakona kojima je priznata važnost računalne sigurnosti.[14] Godine 1988. osnovan je prvi CERT u sklopu Ministarstva obrane SAD-a, dok je preteča današnjeg CERT-a u Republici Hrvatskoj osnovan 1996. godine kao odjel unutar CARNETA.[15]

---

[7] Ibid.
[8] Salus, Peter. *Net Insecurity: Then and Now* (1969–1998). Sane '98 Online. November 19, 1998., www.sane.nl/events/sane98/aftermath/salus.html., pristupljeno 7. studenoga 2023.
[9] Op.cit. (bilješka 3.), str. 4.
[10] Ibid.
[11] Ibid.
[12] Ibid. str. 5.
[13] Ibid.
[14] Ibid. str. 7. Radi se o The Computer Fraud and Abuse Act iz 1986. godine te o *Computer Security act* iz 1987. godine
[15] Ibid. CERT je akronim za Computer Emergency Response Team. Više o Hrvatskom CERT-u bit će riječ dalje u tekstu.

Devedesetih godina internet je postao dostupan široj javnosti. Do tada je bio rezerviran isključivo za djelatnike vlade, akademsku zajednicu i sl. U početku se internet malo brinuo o sigurnosti, zapravo mnogi problemi koji se tiču sigurnosti na internetu danas vuku svoje korijene još u rane faze interneta. Međutim, kako se broj korisnika povećavao i kako korisnici interneta više nisu bili samo pouzdani građani, pojavila se potreba za implementacijom sigurnosnih standarda poput antivirusnih programa.[16] Tako su razvoj interneta i implementacija sigurnosnih standarda doveli do pojave i razvoja informacijske sigurnosti.[17]

Prema svemu sudeći, mogu se uočiti dvije suprotstavljene teze. Prva teza govori o tome kako je razvoj informacijske sigurnosti počeo davno u prošlosti. Ljudi su uvijek imali određene informacije koje su smatrali važnijima od drugih. Znali su ih prepoznati i na adekvatan način zaštititi. Druga teza zastupa mišljenje da je razvoj informacijske sigurnosti počeo tek sredinom 20. stoljeća pojavom prvih računala, a zatim i njihovim umrežavanjem. Prvotno se štitio sam fizički pristup računalu, dok se kasnije razvijala svijest da se mora štititi i programski sloj računala jer je postalo moguće pristupiti informacijama na računalu a da se fizički ne pristupi računalu.

Međutim, ni jedna teza nije pogrešna. Iako su mjere koje su ljudi poduzimali u prošlosti u svojoj naravi rudimentarne, na tragu su onoga što informacijska sigurnost danas u svojoj biti jest, a to je zaštita informacija. Kada je riječ o razvoju discipline informacijske sigurnosti i onoga što ona danas predstavlja, misli se na drugu polovicu 20. stoljeća te pojavu računala i mreža. Tada se, osim fizičke zaštite računala (informacija), počeo štititi i programski dio računala. Oko tog problema razvila se cijela disciplina informacijske sigurnosti sa svim svojim pravilima i mjerama kako bi se osigurala cjelovitost, povjerljivost i dostupnost informacija.

2.2. Informacijska sigurnost danas

Da bi se moglo raspravljati o informacijskoj sigurnosti danas, potrebno je prije svega definirati taj pojam. Prema CNSS-u informacijska sigurnost definira se kao zaštita informacije i njezinih kritičnih elemenata, što uključuje i zaštitu softvera i hardvera koji koriste informaciju, pohranjuju je i prenose.[18] Nadalje, prema Whitmanu i Mattordu informacijska sigurnost definira

[16] Ibid.
[17] Ibid.
[18] CNSS (*Committe of National Security Systems*) tijelo je u SAD-u zaduženo za sva pitanja vezna za kibernetičku sigurnost. Definicija je preuzeta u knjizi iz bilješke broj 3 str. 8.

se kao zaštita povjerljivosti, cjelovitosti i dostupnosti informacije, bez obzira bila ona pohranjena, u obradi ili u prijenosu, primjenom politika, obrazovanja, obuke i tehnologije.[19]
Prema Direktivi EU 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, informacijska sigurnost definira se kao sposobnost mrežnih i informacijskih sustava da odolijevaju na određenoj razini pouzdanosti bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup.[20]
Naposljetku, Zakon o informacijskoj sigurnosti u članku 2. definira informacijsku sigurnost kao stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.[21]
Promatrajući definicije možemo uočiti nekoliko činjenica. Prvo, informacijska sigurnost ima za cilj zaštitu informacija i informacijskih sustava. Drugo, da bi se postigla informacijska sigurnost potrebno je primijeniti određene mjere. Treće, pravila i mjere informacijske sigurnosti tehnološki su neutralna.

Dakle, informacijska sigurnost ima cilj zaštititi informacije, odnosno osigurati njihovu povjerljivost, cjelovitost i dostupnost (raspoloživost). Povjerljivost, cjelovitost i dostupnost informacija još se naziva i C.I.A trokut. Predstavlja standard onoga što svaka organizacija želi zaštititi u informaciji.[22]

Povjerljivost označava karakteristiku prema kojoj samo ovlašteni korisnici ili korisnici s potrebom da pristupe informaciji zaista njoj i pristupaju. Dakle, osigurava se da ne dođe do neovlaštenog pristupa informaciji.[23] Cjelovitost označava karakteristiku prema kojoj je informacija cjelovita, potpuna i neiskvarena. Informacija je u predviđenom svojstvu u kojem joj se može povjeriti.[24] U konačnici dostupnost (raspoloživost) označava atribut prema kojem ovlašteni korisnici mogu pristupiti informaciji bez smetnji ili prepreka.[25] Premda C.I.A., standard danas predstavlja minimum onoga što se želi zaštititi u informaciji. Uglavnom je

[19] Op.cit. (bilješka 3.) str. 8.
[20] Direktiva EU 2016/1148 Europskog parlamenta i vijeća od 6. srpnja 2016. o mjerama za visoku razinu sigurnosti i mrežnih i informacijskih sustava širom Unije, Službeni list Europske unije br. 194/1. Dalje u tekstu NIS direktiva.
[21] Zakon o informacijskoj sigurnosti, Narodne novine br. 79/2007; dalje u tekstu ZIS.
[22] Op.cit. (bilješka 3.) str. 8. C.I.A. je akronim za pojmove *confidentiality*, *integrity*, *availability*.
[23] Ibid. str. 11.
[24] Ibid. str. 12.
[25] Ibid. str. 13.

napušten. Pored povjerljivosti, dostupnosti i cjelovitosti razvilo se još niz atributa koje se žele zaštititi.[26] Tako se pored C.I.A trokuta razvio i manje poznati *parkerian hexade* koji pored atributa cjelovitosti, povjerljivosti, dostupnosti sadrži još tri atributa, a to su kontrola, izvornost i korisnost.[27]

Prema Whitmanu i Mattordu, informacijski sustav sastoji se od softvera, hardvera, podataka, ljudi, propisanih postupaka postupanja i mreže.[28] Važno je napomenuti da svaka komponenta ima svoje posebne sigurnosne zahtjeve koji se moraju implementirati kako bi sustav u konačnici bio siguran.[29]

Softver je komponenta informacijskog sustava koju je možda najteže osigurati, gdje se iskorištavaju rupe u kodu kako bi se neovlašteno pristupilo informacijama koje su u njemu sadržane. [30]

Hardver su fizičke komponente sustava u kojima se nalazi softver. To je mjesto na koje se spremaju podatci i koje ih prenosi, a osigurava sučelje za unos i izvoz informacija iz sustava.[31] Budući da je hardver fizička komponenta sustava, štiti se tako da se osiguraju određene fizičke mjere poput zaključavanja prostorija u kojem se nalazi kako bi se osiguralo da ne dođe do neovlaštenog pristupa ili krađe.[32] Fizička zaštita hardvera bila je glavna premisa u početku razvoja koncepta informacijske sigurnosti jer se vjerovalo da se dobrom fizičkom zaštitom može osigurati cijeli sustav, odnosno nije se obraćala pažnja na softversku komponentu sustava.

Sljedeća komponenta informacijskog sustava su podatci. Definicija podatka jest da je to *činjenica za koju se zna da se dogodila, da postoji ili da je istinita.*[33] Podatak se, kao i svaka druga komponenta sustava, mora adekvatno zaštititi jer je podatak jedna od najčešćih meta napada.[34]

Ljudi kao dio informacijskog sustava predstavljaju možda i najslabiju kariku u lancu. Ističe se da iz nehaja ili iz namjere predstavljaju najveću prijetnju informacijskoj sigurnosti organizacije u kojoj djeluju.[35] Zbog toga se razvio pojam koji se naziva kultura informacijske sigurnosti, a

[26] Ibid. Str. 8.
[27] Andress, Jason, *The Basics of Information Security*, Syngress, Amsterdam, 2011., str. 7.
[28] Op.cit. (bilješka 3.) str. 15.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid. str 16.
[33] Hrvatski jezični portal, https://hjp.znanje.hr/index.php?show=search, pristupljeno 1. lipnja 2024. godine.
[34] Op.cit. (bilješka 3.) str. 16.
[35] Arbanas, Krunoslav, *Ključni čimbenici kulture informacijske sigurnosti*; Policija i sigurnost, br. 4/2020, str. 376-388, str. 378.

koji se definira kao *proces integracije vjerovanja, percepcije, stavova, vrijednosti, pretpostavki i znanja koja vode, usmjeravaju, i upravljaju percepcijama i stavovima zaposlenika čime se utječe na njihovo sigurno ponašanje.*[36] Ističe se da, iako zaposlenici predstavljaju najslabiju kariku u lancu informacijske sigurnosti, oni isto tako s kvalitetnom obukom i povećanjem svijesti o važnosti informacijske sigurnosti mogu postati najjača karika u tome lancu. Dakle, iz problema mogu postati rješenje.[37]

Nadalje, propisani postupci postupanja su pisane instrukcije o tome kako ispuniti određeni zadatak, kao što sam naziv sugerira. Samim time kada neovlašteni korisnik ima pristup postupcima postupanja, to predstavlja prijetnju na cjelovitost informacije.[38] Problem kod postupka javlja se kada organizacije upute svoje zaposlenike u postupak. Međutim, propuste zaposlenike obučiti o važnosti sigurnog korištenja propisanih postupaka, što dovodi do narušavanja informacijske sigurnosti.[39]

Posljednja komponenta informacijskog sustava jest mreža čija je uloga razmjena podataka i informacija između ostalih komponenti informacijskog sustava.[40] Pojavom mreža, posebice interneta, još je više do izražaja došla svijest da same fizičke mjere zaštite informacijskog sustava nisu dovoljne kako bi se osigurala informacijska sigurnost, nego se pritom moraju implementirati mjere za zaštitu mreže poput vatrozida ili sustava koji prepoznaje zlonamjerni program i o tome obavještava korisnika.[41]

Kako bi se zaštitila svaka pojedina komponenata informacijskoga sustava, potrebno je implementirati određene sigurnosne mjere kako bi se smanjili rizici i otklonile određene prijetnje. Već je rečeno da se svaka komponenta štiti na poseban način. Njihova ukupnost dovodi nas do stanja informacijske sigurnosti. Andress te mjere naziva kontrole i dijeli ih u tri grupe (kategorije).[42]

Prvu grupu naziva fizička kontrola. Svrha te kategorije jest da štiti prostor u kojem se nalazi sustav i podatci.[43] Mjere koje se provode su fizičke, kako i sam naziv kategorije govori.[44] Poput ograda, zaštitara, sigurnosnih kamera i zaključanih vrata, te mjere služe tome da održe određeno

[36] Ibid.
[37] Ibid. str. 383.
[38] Op.cit. (bilješka 3.) str. 16.
[39] Ibid. str. 17.
[40] Ibid.
[41] Ibid.
[42] Op.cit. (bilješka 27.) str. 11.
[43] Ibid.
[44] Ibid.

stanje prostorije u kojoj se sustav nalazi. Mjere u biti nalažu postavljanje razne opreme poput rezervnih agregata, protupožarnog sustava, sustava grijanja i hlađenja.[45] Fizičke mjere zaštite zapravo predstavljaju prvu crtu zaštite informacijskog sustava jer je bez dobre fizičke zaštite sustav izrazito izložen napadima.

Sljedeća kategorija odnosi se na logične ili tehničke kontrole. To su mjere koje štite mreže, sustav, okolinu koja obrađuje, prenosi i sprema podatke samo kako bi se spriječile neovlaštene aktivnosti na sustavu.[46] Mjere koje se implementiraju su lozinke, vatrozidi, enkripcija i sl.[47]

Posljednja grupa mjera naziva se administrativna kontrola. Mjere se oslanjanju na pravila, zakone, politiku, postupke, smjernice i predstavljaju pravila o tome kako želimo da se korisnici sustava ponašaju.[48] Vrlo važno kod administrativnih mjera jest mogućnost rukovodećeg kadra da osigura poštovanje propisanih mjera jer se u slučaju nepoštovanja mjera stvara lažna sigurnost gdje mislimo da je nešto savršeno u redu, no zbog korisničke neimplementacije mjera sustav je pun rupa i otvoren za napad.[49]

Prilikom implementacije sigurnosnih mjera u bilo koji sustav nameće se problem i pitanje balansa između toga da se implementiraju sve moguće mjere (to stajalište obično zauzimaju ljudi u organizaciji zaduženi za informacijsku sigurnost) ili da se implementira što manje mjera (to stajalište najčešće zauzimaju rukovodeći želeći pritom što manje ograničenja u radu).[50] Rješenje je balans gdje se moraju implementirati mjere koje osiguravaju informacijsku sigurnost, a da se pritom ne ometa previše redovno poslovanje organizacije.[51] Rješenje, iako jednostavno, zapravo je jako teško postići. Međutim, ključan faktor za uspjeh i postizanje informacijske sigurnosti jest podrška rukovodstva za implementaciju mjera informacijske sigurnosti.[52]

Govoreći o implementaciji mjera informacijske sigurnosti u organizaciji, načelno se može govoriti o dva pristupa kako to postići. To je pristup *bottom-up* i pristup *top-down*.[53] Kod *bottom-up* pristupa sami administratori sustava, radeći zajedno, pokušavaju implementirati

[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Arbanas, Krunoslav; Nikolina Žajdela Hrustek. *Key Success Factors of Information Systems Security*, Journal of Information and Organizational Sciences 43, br. 2, 2019, str.131-144, str. 132.
[51] Ibid.
[52] Ibid. str. 136.
[53] Op.cit. (bilješka 3.) str. 18.

mjere informacijske sigurnosti.[54] Prednost takvog pristupa jest u tome što administratori najbolje poznaju sustav u kojem rade, stoga mogu primijeniti točno one mjere koje su sustavu potrebne.[55] Najveća je mana pristupa u tome što administratori imaju malo utjecaja na ostatak organizacije pa mjere teško zažive.[56] *Top-down* pristup djeluje tako da se informacijska sigurnost postavi kao prioritet u rukovodstvu organizacije.[57] Rukovodstvo propisanim postupcima, politike upravljanja postavlja ciljeve i određuje kako će se ciljevi odraditi.[58] Kod takvog pristupa projekt ima punu potporu rukovodstva organizacije, zacrtane ciljeve i osigurana sredstva čime se pokušava osigurati i podrška ostalih zaposlenika u organizaciji.[59] Nadalje, kod takvog pristupa imenuje se voditelj projekta koji ima zadatak osigurati da projekt, odnosno mjere informacijske sigurnosti što više zažive u organizaciji.[60] Na mjestu voditelja projekta obično se nalazi *chief information officer (*CIO), no nema prepreke, ako je organizacija tako strukturirana, da se na mjestu voditelja projekta nalazi i *chief information security officer* (CISO).[61]

Potrebno je napraviti distinkciju između informacijske sigurnosti i kibernetičke sigurnosti. Iako se ta dva pojma često poistovjećuju, informacijska sigurnost širi je pojam od kibernetičke sigurnosti zato što informacijska sigurnost obuhvaća pravila za zaštitu podataka, informacija i sustava koji ih obrađuju, prenose i pohranjuju u bilo kojem obliku bilo fizičkom bilo digitalnom. Suprotno tome kibernetička sigurnost odnosi se samo na digitalni oblik. Dakle, kibernetička sigurnost sastavnica je informacijske sigurnosti.

Promatrajući ono što danas predstavlja informacijska sigurnost, može se reći da je to izrazito kompleksan sustav koji se od svojih rudimentarnih začetaka u prvoj polovici 20. stoljeća razvijao jednako brzo kao i tehnologija. Današnja stvarnost jest da se većina informacija obrađuje, pohranjuje i prenosi računalom, stoga se cjelovita znanost informacijske sigurnosti temelji upravo na računalu i njegovoj zaštiti od raznih zlonamjernih napada. Međutim, ni najbolji softver s najboljim vatrozidom i ostalim mjerama zaštite ne može biti siguran ako nema ljudi koji mogu njime rukovati i ako se ti ljudi ne pridržavaju ostalih mjera informacijske sigurnosti. Kao što je već istaknuto, ljudi su najveći problem u postizanju informacijske

[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid. CIO se u organizaciji nalazi odmah ispod Izvršnog direktora, dok CISO u hijerarhiji organizacije dolazi odmah ispod CIO-a. Više o CIO i CISO bit će riječi dalje u tekstu.

sigurnosti, no uz pravilnu obuku i podizanje svijesti o značaju informacijske sigurnosti mogu postati i jesu rješenje problema.

3. Zakonodavni okvir informacijske sigurnosti u Republici Hrvatskoj

3.1. Međunarodno pravni izvori

Najznačajniji međunarodno pravni izvor za područje informacijske sigurnosti jest Konvencija o kibernetičkom kriminalu Vijeća Europe iz 2001. godine (Budimpeštanka konvencija). Konvenciju je do sada ratificiralo 68 država, dok su je još 23 države potpisale ili su pozvane da joj pristupe.[62] Posebno je značajno što su je ratificirale i mnoge druge države izvan Europe poput SAD-a i Brazila.

Pored same Konvencije na snazi su i dva dodatna protokola. Prvi protokol sastavljen je i otvoren za potpisivanje 2003. godine, a odnosi se na inkriminiranje djela rasističke i ksenofobne naravi počinjenih s pomoću računalnih sustava. Drugi protokol sastavljen je i otvoren za potpisivanje 2021. godine, a njime su predviđeni postupci za poboljšanje prekograničnog pristupa elektroničkim dokazima i visoka razina zaštitnih mjera. Time će se olakšati suradnja država potpisnica u pogledu kibernetičkog kriminala. Također su predviđene zaštitne mjere za međunarodni prijenos osobnih podataka koje su u skladu sa zakonodavstvom EU-a čime će se značajno olakšati prijenos osobnih podataka između zemalja potpisnica.[63]

Hrvatska je konvenciju potpisala 23. studenoga 2001. godine dok ju je ratificirala 8. srpnja 2002. godine Zakonom o potvrđivanju konvencije o kibernetičkom kriminalu.[64]

Konvencija propisuje četiri grupe kaznenih djela ovisno o objektu zaštite ili sredstvu počinjenja. Nadalje, sankcioniranje kaznenih djela ograničeno je samo na kaznena djela počinjena s namjerom. Također se sankcionira namjerno pomaganje ili poticanje na činjenje kaznenih djela propisanih konvencijom.[65]

Kaznena djela propisana Konvencijom implementirana su u kazneno zakonodavstvo Republike Hrvatske prvi puta 2004. godine i od tada su sastavni dio Kaznenog zakona.[66] U Kaznenom

[62] Council of Europe, The Budapest convention (ETS No.185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention; pristupljeno 18. studenoga 2023.
[63] Ministar Malenica u Strasbourgu potpisao Drugi dodatni protokol Konvencije o kibernetičkom kriminalu, https://mpu.gov.hr/vijesti/ministar-malenica-u-strasbourgu-potpisao-drugi-dodatni-protokol-konvencije-o-kibernetickom-kriminalu/26599; prestupljeno 18. studenoga 2023.
[64] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, Narone novine br. 9/2002.
[65] Dragičević, Dražen; Lisičar, Hrvoje; Gumzej, Nina; Jurić, Marko; Katulić, Tihomir. *Pravna informatika i pravo informacijskih tehnologija*, Narodne novine Zagreb, 2015., str. 198.
[66] Ibid. str. 200.

zakonu iz 2011. godine kaznena djela propisana su u glavi 25. nazvanoj Kaznena djela protiv računalnih sustava, programa i podataka.[67]

Naš zakon preuzeo je sve temeljne pojmove kako su definirani u Konvenciji. Jedini pojam koji je drugačiji u odnosu na Konvenciju jest pojam računalnog sustava gdje se izjednačava s informacijskom sustavom ostavljajući pritom mogućnost da se pojam primijeni na razne tehnologije, a ne striktno na računalo.[68]

3.2. Zakonodavstvo Europske unije

Kada se govori o pravu Europske unije u području informacijske sigurnosti, tada se ponajprije misli o sekundarnim pravnim izvorima, odnosno direktivama i u manjoj mjeri uredbama.

Najznačajnija uredba iz područja informacijske sigurnosti jest svakako Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Međutim, njezin primarni cilj jest zaštita prava pojedinca u vezi s obradom osobnih podataka te će o njoj biti riječ dalje u tekstu.[69]

Pored Uredbe važna je i Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) kojom se nastoji postići visoka razina kibersigurnosti, kiberotpornosti i povjerenja u Europskoj uniji.[70]

Prva direktiva koja se bavila područjem informacijske sigurnosti i kibernetičkom sigurnosti jest Direktiva o kibersigurnosti poznatija pod nazivom NIS direktiva.[71] Donošenje direktive bilo je predviđeno Strategijom kibernetičke sigurnosti EU-a, dok je sama direktiva donesena 2016. godine. Međutim, NIS direktiva u potpunosti je zaživjela u državama članicama tek 2020.

[67] Kazneni zakon, Narodne novine br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21.
[68] Op.cit. (bilješka 65.) str. 199.
[69] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), dalje u tekstu Uredba
[70] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), Službeni list Europske unije L 151/15
[71] Op.cit. (bilješka 20.)

godine, što je izrazito dugo razdoblje, posebno uzimajući u obzir da je *vacatio legis* za Uredbu bio dvije godine.[72]

Direktiva predlaže niz mjera koje imaju za cilj podizanje mjere sigurnosti mrežnih i informacijskih sustava kako bi se osigurale usluge koje su od ključne važnosti za društvo i gospodarstvo cjelokupne Europske unije. Nadalje, direktivom se pokušava osigurati da države članice budu pripravne na rješavanje kibernetičkih napada. To se nastoji postići određivanjem nadležnih tijela, uspostavljanjem mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-ova)[73] te donošenjem nacionalnih strategija za kibersigurnost. Izrazito je važna mreža CSIRT-ova koju uvodi direktiva. Imaju važnu ulogu u praćenju incidenata, pružanju pravodobnog upozorenja o napadu subjektima kojima prijeti napad. U slučaju napada zaduženi su za ublažavanje i otklanjanje posljedica napada.[74] Također, uspostavlja se i suradnja u okviru EU-a na strateškoj i tehničkoj razini te se, najvažnije, uvodi obveza za pružatelje ključnih i digitalnih usluga (bankarstvo, energetika, prijevoz, financije, zdravstvo i digitalna infrastruktura kojima bi kibernetički napad poremetio ključnu uslugu) da provedu odgovarajuće sigurnosne mjere u cilju smanjivanja rizika i da obavijeste nadležna nacionalna tijela o ozbiljnim slučajevima.

Republika Hrvatska transponirala je direktivu donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.[75]

Prepoznavši sve veću važnost koju tehnologija ima na život i poslovanje, Europska unija odlučila je ažurirati NIS direktivu te je 2022. godine donesena NIS 2 direktiva.[76] Direktiva ima cilj utvrditi zajednički regulatorni okvir kibersigurnosti čiji je cilj povećati razinu kibersigurnosti u Europskoj uniji (EU), tražiti od država članica EU-a da jačaju sveukupne kapacitete u području kibersigurnosti te uvesti mjere upravljanja kibersigurnosnim rizicima i izvješćivanja u kritičnim sektorima, uz pravila o suradnji, razmjeni informacija, nadzoru i izvršavanju. Umjesto operatora ključnih usluga i davatelja digitalnih usluga, direktiva uvodi

[72] Katulić, Tihomir. *Towards the Trustworthy AI: Insights from the Regulation on Data Protection and Information Security,* Medijska istraživanja, vol. 26, br. 2, 2020., str. 9-28, str. 15.
[73] CSIRT je skraćenica za Computer Security Incident Response Team
[74] Katulić, Tihomir. *Transposition of EU Network and Information Security Directive into National Law*, 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Hrvatska, 2018., str. 1143-1148, str. 1146.
[75] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine broj 64/18.
[76] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), Službeni list Europske unije 333/80. Dalje u tekstu NIS 2 direktiva.

drugačiju kategorizaciju, odnosno ključne i važne subjekte.[77] Sukladno tome NIS 2 direktiva značajno je povećala broj sektora, podsektora i subjekata koji su obveznici primjene mjera kibersigurnosti.
Hrvatska je transponirala NIS 2 direktivu u svoje zakonodavstvo donošenjem Zakona o kibernetičkoj sigurnosti.[78]

Od važnijih direktiva valja spomenuti Direktivu 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP koja za cilj ima borbu protiv računalnog zločina i pružanje informacijske sigurnosti snažnijim nacionalnim zakonima, većim kaznama i boljom suradnjom između relevantnih tijela.[79]

Polazna točka za direktivu bila je okvirna odluka donesena 2005. godine koja je donošenjem direktive stavljena izvan snage, dok je polazna točka za odluku bila Konvencija Vijeća Europe o kibernetičkom kriminalu.[80]

3.3. Zakonodavstvo Republike Hrvatske

Prateći razvoj tehnologije i uvidjevši kako je sve više važno osigurati određenu razinu povjerljivosti, raspoloživosti i cjelovitosti informacija, hrvatski zakonodavac donio je niz zakona i podzakonskih propisa kako bi se postiglo i osiguralo stanje informacijske sigurnosti.

Zakon o informacijskoj sigurnosti utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, određuje područja informacijske sigurnosti, nadležna tijela za donošenje, provođenje i nadzor mjera te standarda informacijske sigurnosti.[81] Izričito navodi tko su obveznici primjene pa se tako zakon primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima koje u svojem djelokrugu koriste klasificirane i neklasificirane podatke. Također, primjenjuje se i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podatcima. Pored adresata pravnih normi zakon određuje koja su to područja informacijske sigurnosti. Tako se navodi da su područja informacijske sigurnosti sigurnosna provjera, fizička sigurnost,

[77] Zajedno za kibernetičku otpornost Europske unije, https://www.cert.hr/zajedno-za-kiberneticku-otpornost-europske-unije/; pristupljeno 22. studenoga 2023.
[78] Zakon o kibernetičkoj sigurnosti, Narodne novine 14/2024.
[79] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, Službeni list Europske unije 218/8.
[80] Op.cit. (bilješka 65.) str. 351.
[81] Op.cit. (bilješka 21.)

sigurnost podataka, sigurnost informacijskog sustava i sigurnost poslovne suradnje. Nadalje, zakon određuje i središnja državna tijela zadužena za informacijsku sigurnost.
Tako je Ured Vijeća za nacionalnu sigurnost[82] središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i razmjenu klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. Također, UVNS donosi pravilnike za područje informacijske sigurnosti te pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost.

Sljedeće središnje državno tijelo koje se navodi u ZIS-u jest Zavod za sigurnost informacijskih sustava zadužen za tehničko područje informacijskih sustava koje se sastoji od standarda sigurnosti informacijskih sustava, sigurnosne akreditacije informacijskih sustava, upravljanja kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka, koordinacije prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. Također, ima zadatak obrađivati računalno-sigurnosne incidente koji se pojave u tijelima za koje je nadležan prema ZSI-u, odnosno ustrojen je i kao CERT-ZSIS.

Pored središnjih državnih tijela, ZSI je u sustav informacijske sigurnosti u Hrvatskoj ustanovio još jedno tijelo koje kao samostalno tijelo do tada nije postojalo u Hrvatskoj. Riječ je o nacionalnom CERT-u koji je prije nego što je ustanovljen kao nacionalno tijelo djelovao kao CARNet CERT sa zadatkom praćenja računalnih incidenata i rješavanja istih. Donošenjem ZIS-a ustanovljen je nacionalni CERT kao zasebna ustrojstvena jedinica u CARNet-u. Njegov je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke, a potom i informacijske sigurnosti u Republici Hrvatskoj. Pored praćenja i rješavanja incidenata nacionalni CERT provodi razne edukacije kako bi se incidenti sveli na najmanju moguću razinu.[83] Ujedno se nalazi u mreži CSIRT-ova koja je ustanovljena spomenutom NIS direktivom i koja pored nacionalnih CSIRT-ova sadrži i CERT-EU i ENIS-u.[84] Osim nacionalnog CERT-a, u Hrvatskoj još djeluje unutar Zavoda za sigurnost informacijskih sustava i CERT-ZSIS koji pruža svojim korisnicima sve usluge koje karakteriziraju CERT tim.[85] Pored toga postoji još i CERT MO i OSRH.

[82] Ured vijeća za nacionalnu sigurnost, dalje u tekstu UVNS.
[83] O nacionalnom CERT-u, https://www.cert.hr/onama/, pristupljeno 23. studenoga 2023.
[84] CERT-EU je zadužen za sigurnost i računalne incidente za tijela EU. ENISA je agencija Europske unije za kibersigurnost, a njezin cilj je postizanje visoke zajedničke kibersigurnosti u EU.
[85] CERT, https://www.zsis.hr/default.aspx?id=16, pristupljeno 23. studenoga 2023.

Kako bi se osiguralo provođenje ZIS-a i mjera koje on uvodi, predviđen je i nadzor informacijske sigurnosti. Između ostalih zadaća, nadzor nad informacijskom sigurnosti unutar tijela koje su dužne primjenjivati zakon provodi savjetnik za informacijsku sigurnost.[86]

Sljedeći zakon koji je relevantan za područje informacijske sigurnosti jest Zakon o tajnosti podataka[87] kojim se utvrđuje pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podatcima, zaštita podatka i, naposljetku, sami nadzor nad provedbom zakona. Adresati zakona državna su tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podatcima. Dakle, adresati pravnih normi identični su kao i kod ZIS-a. Klasificirani podatak jest onaj podatak koji je nadležno tijelo u propisanom postupku takvim označilo i za koji je utvrđen stupanj tajnosti. Stupnjevi tajnosti podataka prema ZTP-u su ograničeno, povjerljivo, tajno i vrlo tajno, a pod takvu klasifikaciju mogu se podvući samo podatci iz djelokruga državnih tijela iz područja obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva, ako su takvi podatci od interesa za Republiku Hrvatsku.

Nadalje, od važnosti za informacijsku sigurnost jest Zakon o kibernetičkoj sigurnosti. Kao što je navedeno, zakonom se u hrvatski pravni poredak transponira NIS 2 direktiva i uspostavlja sustav upravljanja kibernetičkom sigurnošću kako bi se osigurala djelotvorna provedba postupka i mjera za postizanje visoke razine kibernetičke sigurnosti u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta. Kako bi se postigao cilj, zakon uređuje postupke i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti, kriterije za kategorizaciju ključnih i važnih subjekata, zahtjeve kibernetičke sigurnosti za ključne i važne subjekte, posebne zahtjeve za upravljanje podatcima o registraciji naziva domena i kontrole njihove provedbe, dobrovoljne mehanizme kibernetičke zaštite, nadležna tijela u području kibernetičke sigurnosti, kao i njihove zadaće i ovlasti. Nadalje, zakon uređuje i stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti, prekršajne odredbe, praćenje provedbe zakona te druga pitanja važna za kibernetičku sigurnost. Posebno zakon uspostavlja okvir strateškog planiranja i odlučivanja u području kibernetičke sigurnosti te utvrđuje nacionalni okvir upravljanja kibernetičkim incidentima velikih razmjera i kibernetičkim krizama. Novim se zakonom u odnosu na prijašnje

[86] O savjetniku za informacijsku sigurnost i njegovim zadaćama bit će riječ više kasnije u radu.
[87] Zakon o tajnosti podataka, Narodne novine broj 79/2007, 86/2012. Dalje u tekstu ZTP.

uređenje značajno proširuje krug organizacija koje moraju provoditi mjere kibernetičke sigurnosti.

Novim zakonom o kibernetičkoj sigurnosti stavlja se izvan snage dosadašnji Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, a posredno i NIS direktiva. Ako uzmemo za primjer pravo zaštite osobnih podataka, gdje je Unija prvotno to područje uređivala direktivom, pa zatim uvidjevši da direktiva nije dostatna te je donesena Uredba, tada možemo s pravom očekivati da će se tijekom nekoliko godina i na području kibernetičke sigurnosti posegnuti za većim ujednačenjem te da će se donositi uredba tim više što se digitalne tehnologije sve više koriste u svakodnevnom životu i poslovanju, pa i umjetna inteligencija, što sve dovodi do povećanog rizika od raznih napada.

Od zakona važnih za informacijsku sigurnost još valja spomenuti Zakon o kritičkim infrastrukturama, Zakon o pravu na pristup informacijama, Zakon o državnoj informacijskoj infrastrukturi, Zakon o sigurnosnim provjerama i Zakon o provedbi Opće uredbe o zaštiti podataka.

Promatrajući cjelokupno zakonodavstvo Republike Hrvatske, može se uočiti da se velika većina zakona odnosi na postizanje informacijske sigurnosti u državnim tijelima, tijelima jedinica lokalne (regionalne) i područne samouprave te u pravnim osobama s javnim ovlastima, kao i kod pravnih i fizičkih osoba koje ostvaruju kontakt s navedenim subjektima. Nadalje, naše zakonodavstvo u području informacijske sigurnosti jest pod utjecajem zakonodavstva EU-a. Unija je ta koja svojim uredbama i direktivama pokušava postići stanje informacijske sigurnosti ne samo kod subjekata javnog prava nego i kod pravnih osoba koje imaju određenu važnost u društvu i gospodarstvu te na to potiče države članice. Na državama članicama samo je da tu politiku slijede. U prilog tome govori i donošenje direktive NIS 2 koja značajno proširuje obveznike implementacije sigurnosnih mjera.

4. Savjetnik za informacijsku sigurnost

Jedna od novosti koja se uvodi u hrvatski pravni poredak, a i u sustav informacijske sigurnosti jest pozicija savjetnika za informacijsku sigurnost. ZIS u sedmom poglavlju uvodi poziciju savjetnika za informacijsku sigurnost, dok je ostavljeno Uredu vijeća za nacionalnu sigurnost da detaljnije pravilnikom propiše kriterije za ustroj radnih mjesta savjetnika za informacijsku sigurnost.

Važno je spomenuti poziciju CISO (*Chief Information Security Officer)* koja je slična poziciji savjetnika za informacijsku sigurnost. Predviđena je kako bi svojom stručnošću i iskustvom pomogla organizaciji prepoznati potencijalne ugroze za informacijsku sigurnost te ih u slučaju povrede spriječiti i otkloniti.[88] Stoga mora široko poznavati koje su to najveće prijetnje i ugroze za informacijsku sigurnost. Također, mora imati široku paletu znanja i vještina kako bi mogao implementirati mjere informacijske sigurnosti u organizaciji u kojoj djeluje.[89] Kako bi što uspješnije proveo svoj zadatak u većim organizacijama, CISO ujedno provodi obuku zaposlenika, uspostavlja svoj tim stručnjaka, nadgleda sigurnosne incidente, nadzire provedbu mjera informacijske sigurnosti i surađuje s nadzornim tijelima.[90] Dobar CISO mora razmišljati izvan okvira, dobro poznavati područje informacijske sigurnosti, znati kako prenijeti svoju viziju informacijske sigurnosti prema višem rukovodstvu da ga zatim podrže, biti dobar poslovni partner i vođa kako bi svoje znanje mogao prenijeti na cjelokupnu organizaciju.[91]

4.1. Obveznici imenovanja savjetnika za informacijsku sigurnost

Sukladno ZIS-u nisu svi obveznici primjene ZIS-a ujedno i obveznici imenovanja savjetnika za informacijsku sigurnost, što znači da je obveza imenovanja savjetnika sužena na samo određene adresate.

Tako su obveznici imenovanja savjetnika za informacijsku sigurnost državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave i pravne osobe koje u svojem djelokrugu

[88] Katulić, Tihomir. *CISO, DPO, AIHO? Navigating the EU's AI regulatory efforts in pursuit of dana protection and information security compliance*, u knjizi: *Artificial Intelligence for human-centric society: The future is here*, European Liberal Forum, Bruxelles, 2024., str. 56-81, str. 70.
[89] Ibid.
[90] Ibid.
[91] Alexander, Aileen; Cummings, Jamey, *The Rise of the Chief Information Security Officer*, People and Strategy, vol. 39, br.1, 2016., str. 10-13, str. 11.

koriste klasificirane i neklasificirane podatke.[92] Dakle, od obveze imenovanja savjetnika isključene su pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podatcima.

Obveza imenovanja savjetnika odnosi se na ona tijela i pravne osobe koje u svojem djelokrugu svakodnevno postupaju s klasificiranim i neklasificiranim podatcima pa je samim time potrebna određena veća razina sigurnosti i nadzora nad postupanjem, stoga je zakonodavac procijenio da je imenovanje savjetnika nužno. S druge strane, zakonodavac je procijenio da imenovanje savjetnika nije potrebno kod subjekata prava koji tek povremeno ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podatcima.

Međutim, prema Pravilniku o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, članku 2., navodi se kako su radno mjesto savjetnika dužna ustrojiti tijela i pravne osobe koje u svojem djelokrugu stvaraju ili koriste klasificirane podatke.[93] Dakle, kao kriterij za ustrojavanje radnih mjesta savjetnika ne spominje se stvaranje ili korištenje neklasificiranih podataka. Neklasificirani je podatak prema ZTP-u podatak bez utvrđenog stupnja tajnosti koji se koristi u službene svrhe.

Na ovome mjestu došlo je do antinomije između dvije pravne norme, dva pravna propisa različite hijerarhije i specijalnosti. Prema Periću, u takvoj se situaciji za rješavanje antinomije mora primijeniti načelo zakonitosti, odnosno hijerarhijski viši propis.[94] Stoga se u ovome incidentu mora primijeniti ZIS i smatrati da su obveznici imenovanja savjetnika i tijela i pravne osobe koje u svojem djelokrugu koriste i neklasificirane podatke.

4.2. Kriteriji za ustrojavanje radnog mjesta savjetnika za informacijsku sigurnost

Iako postoje obveznici imenovanja savjetnika za informacijsku sigurnost, Pravilnik postavlja određene kriterije o tome koje tijelo ili pravna osoba mora ustrojiti novo radno mjesto savjetnika za informacijsku sigurnost, a koje tijelo ili pravna osoba može poslove savjetnika dodijeliti u opis poslova postojećeg radnog mjesta.

Tako su kriteriji za ustrojavanje radnog mjesta savjetnika za informacijsku sigurnost u tijelu ili pravnoj osobi broj, vrsta i stupanj tajnosti klasificiranih podataka koje to tijelo ili pravna osoba

[92] Dalje u tekstu tijela i pravne osobe.
[93] Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, Narodne novine broj 30/2011. Dalje u tekstu Pravilnik.
[94] Perić, Berislav, *Država i pravni sustav*, Informator, Zagreb, 2009., str. 193.

stvara ili koristi. Pravilnik razlikuje kvantitativnu (broj podataka) i kvalitativnu (vrsta i stupanja tajnosti) kategoriju kao kriterij za ustrojavanje radnog mjesta savjetnika.[95]

Prva kategorija tijela i pravnih osoba ona je kategorija koja nije dužna ustrojiti novo radno mjesto savjetnika za informacijsku sigurnost, nego je dužna poslove savjetnika dodati u opis poslova nekog od postojećih radnih mjesta. U tu kategoriju spadaju tijela i pravne osobe koje u svojem djelokrugu stvaraju ili koriste manju količinu klasificiranih podataka, kao i ona tijela i pravne osobe koje u svojem djelokrugu stvaraju ili koriste veću količinu klasificiranih podataka, ali su ti podatci pretežno označeni stupnjem tajnosti ograničeno.[96]

Nadalje, u drugoj kategoriji nalaze se tijela i pravne osobe koje mogu ustrojiti posebno radno mjesto savjetnika za informacijsku sigurnost. U toj kategoriji nalaze se tijela i pravne osobe koje u obavljanju poslova iz svojeg djelokruga stvaraju ili koriste veću količinu klasificiranih podataka označenih pretežno stupnjem tajnosti povjerljivo, tajno i vrlo tajno.[97]

Pored ustrojavanja posebnog radnog mjesta savjetnika za informacijsku sigurnost i dodavanja poslova savjetnika u opis poslova postojećeg radnog mjesta, Pravilnikom je predviđena još jedna mogućnost kako tijela i pravne osobe mogu riješiti pitanje savjetnika i njegovih poslova. Naime, Pravilnikom je ostavljena mogućnost da tijelo ili pravna osoba poslove savjetnika doda u opis poslova već ustrojene jedinice ili službe; ili da ustroji novu ustrojstvenu jedinicu ili službu čiji bi jedini zadatak tada bio da obavlja poslove koje mora obavljati savjetnik za informacijsku sigurnost. Dakle, prema Pravilniku ni jedno tijelo ili pravna osoba, neovisno o stupnju tajnosti, količini i vrsti podataka koje stvaraju ili obrađuju, nije dužna ustrojiti posebno radno mjesto savjetnika za informacijsku sigurnost. Ostavljeno je na raspolaganje čelnicima tijela i pravnih osoba da, ovisno o tome koliku količinu klasificiranih i neklasificiranih podataka

[95] Vojković, Goran. *Novi pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, Informator*, broj 5965, 2011., str. 5-6, str 5.

[96] Prema ZTP-u stupnjem tajnosti ograničeno označavaju se oni podatci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova iz područja obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te poslovi iz područja znanosti, tehnologije, javnih financija i gospodarstva ako su ti podatci od sigurnosnog interesa za Republiku Hrvatsku.

[97] Prema ZTP-u stupnjem tajnosti vrlo tajno klasificiraju se podatci čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i interesima Republike Hrvatske, a osobito vrijednostima kao što su temelji Ustavom utvrđenog ustrojstva Republike Hrvatske, neovisnost, cjelovitost i sigurnost Republike Hrvatske, međunarodni odnosi Republike Hrvatske, obrambena sposobnost i sigurnosno-obavještajni sustava, sigurnost građana, osnove gospodarskog i financijskog sustava Republike Hrvatske, znanstvena otkrića, pronalasci i tehnologije od važnosti za nacionalnu sigurnost Republike Hrvatske. Nadalje, stupnjem tajno klasificiraju se podatci čije bi neovlašteno otkrivanje teško naštetilo navedenim vrijednostima dok se stupnjem povjerljivo klasificiraju podatci čije bi neovlašteno otkrivanje naštetilo navedenim vrijednostima.

stvaraju ili obrađuju, sami odluče kako će riješiti pitanje radnog mjesta savjetnika i njegovih poslova.

4.3. Uvjeti za raspored na radno mjesto savjetnika za informacijsku sigurnost

Pored kriterija, koje moraju zadovoljiti tijela i pravne osobe da bi mogle imenovati savjetnika za informacijsku sigurnost, i kandidati za radno mjesto savjetnika moraju ispunjavati određene kriterije, uvjete kako bi mogli biti imenovani na nadasve odgovornu poziciju.

Pravilnikom su propisani minimalni uvjeti koje kandidati za savjetnika moraju zadovoljiti kako bi mogli biti primljeni u službu i s određenom kvalitetom obavljati svoj posao. Kao što je spomenuto, Pravilnikom su propisani minimalni uvjeti, što znači da je ostavljena mogućnost tijelima i pravnim osobama da, ovisno o prirodi posla koji obavljaju, propišu i dodatne uvjete.
Od uvjeta koji su propisani Pravilnikom od kandidata se traži da ima visoku stručnu spremu, odnosno preddiplomski i diplomski sveučilišni studiji, integrirani preddiplomski i diplomski sveučilišni studij ili specijalistički diplomski stručni studij. Vezano za ovaj uvjet, s obzirom na prirodu posla koji savjetnik obavlja, razuman zahtjev bio bi da kandidat ima završeni studij iz tehničkog ili društvenog područja.
Sljedeći je uvjet da kandidat mora imati najmanje tri godine radnog iskustva u tijelima ili pravnim osobama. Kod ovog uvjeta nejasno je na što Pravilnik misli kada govori da je potrebno radno iskustvo u tijelima ili pravnim osobama, odnosno znači li to da budući savjetnici za informacijsku sigurnost moraju imati najmanje trogodišnje radno iskustvo samo u državnim tijelima, tijelima jedinica lokalne (područne) regionalne samouprave te u pravnim osobama s javnim ovlastima. Znači li to da su ostali potencijalni kandidati, koji su svoju karijeru gradili izvan nabrojenih subjekata prava, uskraćeni za mogućnost postati savjetnikom za informacijsku sigurnost?

Također, uvjet je i poznavanje engleskoga jezika ako tijelo ili pravna osoba postupa s međunarodnim klasificiranim podatcima.

U konačnici uvjet za kandidate jest i da posjeduju odgovarajući certifikat o obavljenoj sigurnosnoj provjeri koju izdaje UVNS. Sami postupak sigurnosne provjere provodi Sigurnosno-obavještajna agencija na zahtjev UVNS-a.[98]

[98] Zakon o sigurnosnim provjerama, Narodne novine broj 85/08, 86/12.

O svim rasporedima na radno mjesto savjetnika za informacijsku sigurnost, kao i o dodavanju poslova savjetnika u opis poslova postojećeg radnog mjesta čelnik tijela ili pravne osobe dužan je pismeno obavijestit UVNS. Također, takva obveza postoji i ako su poslovi savjetnika dodani u opis poslova postojeće ustrojstvene jedinice ili službe te ako se za obavljanje poslova savjetnika za informacijsku sigurnost ustroji nova ustrojstvena jedinica ili služba.

4.4. Poslovi savjetnika za informacijsku sigurnost

Nadležnost i poslovi savjetnika za informacijsku sigurnost utvrđeni su ponajprije Pravilnikom. Jedan dio poslova, onaj koji se tiče nadzora, propisan je i ZIS-om. Međutim, Pravilnikom je detaljnije propisano na koji način obavlja taj dio posla. Ostali dio poslova, koje obavlja savjetnik, utvrđeni su i detaljnije propisani pravilnicima koji uređuju područja informacijske sigurnosti koja su propisana ZIS-om.

Člankom 9. Pravilnika propisano je da je savjetnik za informacijsku sigurnost odgovoran za usklađivanje, nadzor, edukaciju i koordinaciju provedbe mjera i standarda informacijske sigurnosti. Pravilnik općenito u ovome članku nabraja koje su to dužnosti savjetnika. Detaljnije su poslovi savjetnika, kako to stoji u članku 11., utvrđeni zakonima i podzakonskim aktima koji uređuju područja informacijske sigurnosti.

Područja informacijske sigurnosti utvrđena su ZIS-om, kako je to napomenuto.[99] UVNS je za svako pojedino područje donio poseban pravilnik.

Tako je Pravilnikom o standardima sigurnosne provjere uređeno područje informacijske sigurnosti koje se odnosi na sigurnosnu provjeru. Sigurnosna provjera jest područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podatcima.

Nadalje je Pravilnikom o standardima fizičke sigurnosti uređeno područje informacijske sigurnosti koje se odnosi na fizičku sigurnost. Fizička sigurnost područje je informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podatci.

Zatim je Pravilnikom o standardima sigurnosti podataka uređeno područje informacijske sigurnosti koje se odnosi na sigurnost podataka. Sigurnost podataka područje je informacijske

[99] Vidi *supra* str. 14.

sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.

Potom je Pravilnikom o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava uređeno područje informacijske sigurnosti koje se odnosi na sigurnost informacijskih sustava. Sigurnost informacijskih sustava područje je informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, prenosi ili pohranjuje u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.
Naposljetku je Pravilnikom o standardima sigurnosti poslovne suradnje uređeno područje informacijske sigurnosti koje se odnosi na sigurnost poslovne suradnje. Sigurnost poslovne suradnje područje je informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranim dokumentima koji obvezuju pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

4.4.1. Nadzor informacijske sigurnosti

Nadzor informacijske sigurnosti posao je savjetnika koji je detaljnije propisan samim ZIS-om i Pravilnikom. Nadzor je posao koji je izvorno predviđen ZIS-om kao posao savjetnika. Svi ostali poslovi koje savjetnik obavlja utvrđeni su pravilnicima.

Poslovi nadzora informacijske sigurnosti poslovi su nadzora organizacije, provedbe i učinkovitosti propisanih mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama. Savjetnik je dužan propisani nadzor obaviti najmanje dva puta godišnje. Pravilnikom je ostavljena mogućnost da savjetnik u tijelima i pravnim osobama, koje obrađuju i stvaraju veću količinu klasificiranih i neklasificiranih podataka većeg stupnja tajnosti, nadzor obavlja više puta godišnje. Koliko puta godišnje savjetnik obavlja nadzor, ponajprije će ovisiti, kao što je rečeno, o količini, vrsti i stupnju tajnosti podataka koje tijelo ili pravna osoba stvara ili obrađuje. Također, ulogu o tome koliko će puta savjetnik obaviti nadzor svakako ima i politika tijela ili pravne osobe prema informacijskoj sigurnosti, kao i podrška savjetniku u provođenju njegovih zadataka od rukovodećih osoba tijela i pravne osobe premda se i ovdje postavlja pitanje ravnoteže između postizanja što boljeg stanja informacijske sigurnosti (što bi se postiglo

sve češćim provođenjem nadzora) i omogućavanja poslovanja tijela ili pravne osobe bez previše opstrukcije (što se pak postiže sa što rjeđim provođenjem nadzora, odnosno pridržavanja minimuma propisanog Pravilnikom).

Po završetku nadzora savjetnik za informacijsku sigurnost dužan je sastaviti izvješće o provedenom nadzoru koje mora sadržavati procjenu provedenih mjera i standarda informacijske sigurnosti te opis uočenih i eventualnih nedostataka. Nadalje, ako postoje nedostatci, mora predložiti mjere za uklanjanje nedostataka i kopije popunjenih nadzornih lista. Savjetnik mora predati izvješće čelniku tijela ili pravne osobe te Uredu vijeća za nacionalnu sigurnost kao središnjem državnom tijelu zaduženom za informacijsku sigurnost.

Čelnik tijela po primitku izvješća može postupiti u okviru svoje nadležnosti te, ako to smatra nužnim, implementirati nove mjere informacijske sigurnosti koje je u svojem izvješću predložio savjetnik.

Nadalje, UVNS po primitku izvješća ima određene ovlasti u nadziranom tijelu i pravnoj osobi. Tako prema ZIS-u može prvo dati upute u svrhu otklanjanja utvrđenih nedostataka i nepravilnosti. Te su upute obvezne za tijela i pravne osobe kojih su se dužni pridržavati te u određenom roku otkloniti nedostatke i nepravilnosti koje su u prvome redu uočili savjetnik UVNS-a. Zatim UVNS može provesti postupak preispitivanja daljnje valjanosti sigurnosne akreditacije informacijskog sustava. Također, može pokrenuti postupak utvrđivanja odgovornosti. U konačnici ostavljena je otvorena klauzula gdje je UVNS-u dana mogućnost da poduzme sve druge mjere i radnje na koje je ovlašteno po posebnim propisima.

Dakle, UVNS-u su kao središnjem državnom tijelu zaduženom za informacijsku sigurnost ostavljene široke ovlasti kako bi se osigurala što usklađenija primjena mjera i standarda informacijske sigurnosti s ciljem postizanja što boljeg stanja informacijske sigurnosti u tijelima i pravnim osobama. Međutim, kako bi UVNS mogao svoje ovlasti iskoristiti, ključan je rad savjetnika i njegov kvalitetno proveden nadzor i sastavljeno izvješće.

Kako bi se osigurao što bolji rad savjetnika u pogledu nadzora ZIS-om, predviđeno je da je čelnik tijela i pravne osobe dužan poduzeti mjere za otklanjanje nedostataka koji su utvrđeni u samoj provedbi nadzora.

4.5. Odgovornost savjetnika za informacijsku sigurnost

Kada se govori o odgovornosti savjetnika za informacijsku sigurnost unutar tijela ili pravne osobe, odmah se dobije i slika o njegovoj poziciji unutar tijela ili pravne osobe.

Prema Pravilniku, savjetnik za informacijsku sigurnost izravno je odgovoran za svoj rad čelniku tijela ili pravnoj osobi. Takva odredba Pravilnika ponajprije je odraz standarda i smjernica informacijske sigurnosti koje govore kako osoba zadužena za informacijsku sigurnost mora imati otvoren izravan kanal komunikacije prema čelniku tijela ili pravnoj osobi.[100] Također, ako su poslovi savjetnika za informacijsku sigurnost dodani u opis poslova drugog radnog mjesta i kada to radno mjesto ima druge nadređene, zaposlenik u pogledu informacijske sigurnosti odgovara izravno čelniku tijela ili pravnoj osobi.[101]

Govoreći o odgovornosti savjetnika, može se spomenuti ovlast UVNS-a prema kojem ono može, na temelju izvješća savjetnika, pokrenuti pitanje odgovornosti u nadziranom tijelu ili pravnoj osobi. Tumačeći tu normu, ekstenzivno se može zaključiti da ni sam savjetnik nije zaštićen od toga da, ako UVNS uoči određene nepravilnosti u njegovu radu, pokrene pitanje njegove odgovornosti. Pokretanje pitanja odgovornosti UVNS-a zapravo je jedini element prisile koji je moguć u tijelima i pravnim osobama ako se na zadovoljavajući način ne provode mjere i standardi informacijske sigurnosti.

Promatrajući opis poslova savjetnika za informacijsku sigurnost, njegovu odgovornost, poziciju u tijelu ili pravnoj osobi, pa i cjelokupni sustav informacijske sigurnosti u tijelima i pravnim osobama, može se uočiti da se hrvatski zakonodavac odlučio za takozvani *top down* model implementacije informacijske sigurnosti. To se može uočiti na tome da su rukovodeći ljudi tijela i pravnih osoba dužni imenovati savjetnika za informacijsku sigurnost koji je, kao stručna osoba koja direktno odgovara čelnicima tijela, odgovoran za implementaciju mjera i standarda informacijske sigurnosti do najnižih razina organizacije u kojoj djeluje. S druge strane, podrška savjetniku za informacijsku sigurnost i podrška za implementaciju mjera i standarda informacijske sigurnosti čelnika tijela i pravnih osoba pokušava se osigurati nadzorom savjetnika i UVNS-a. UVNS na temelju izvješća može pokrenuti pitanje odgovornosti u nadziranom tijelu i pravnoj osobi.

[100] Op.cit. (bilješka 95.) str. 6.
[101] Ibid.

5. Službenik za zaštitu podataka u suvremenom zakonodavstvu

5.1. Povijesni pregled razvoja prava zaštite podataka

Pravo zaštite podataka relativno je suvremen pojam u odnosu na ostala temeljna prava Europske unije. Prve bojazni da postoji ugroza za osobne podatke pojavile su se 60-ih godina 20. stoljeća u Vijeću Europe.[102] Naime, tada su se računala sve više počela koristiti za obradu podataka u raznim ustanovama, što je dovelo do buđenja svijesti da bi informacijske tehnologije mogle promijeniti odnos države prema pojedincu, odnosno da bi upotreba informacijskih tehnologija mogla predstavljati ugrozu za prava i slobode pojedinca.[103] Kao rezultat takvog razmišljanja, cilj prvih zakonodavnih instrumenata bio je zaštititi pojedinca od posljedica automatizirane obrade koju provode subjekti javnog prava. Ubrzo nakon toga zakonodavstvo se počelo baviti i obradom podataka koju provode subjekti privatnog prava.[104] Prvi zakon koji se bavio problematikom zaštite podataka donesen je 1970. godine u njemačkoj pokrajini Hessen. Zakon o zaštiti podataka od 7. listopada 1970. (*Hessen Datenshutzgesetz*), iako prvi zakon na području zaštite podatka, nije prvi nacionalni zakon jer se primjenjivao samo na području spomenute njemačke pokrajine. Zanimljivo je kod ovog zakona što je predvidio povjerenika za zaštitu podataka koji je imao zadatak osigurati sukladnost primjene zakona.[105] Stoga je prvi zakon koji se bavio problematikom zaštite podatka, a koji se primjenjivao nacionalno, švedski zakon o podatcima (*Datalagen*) od 11. svibnja 1973. godine.[106] Nakon Švedske, zakone na području zaštite podataka počele su donositi i druge države. Tako je SAD donio zakon 1974. godine, zatim Njemačka, Austrija, Danska, Kanada, Norveška, Francuska, Luksemburg itd.[107] Tako su se od početka 70-ih godina 20. stoljeća, pa tijekom 80-ih i 90-ih godina, na nacionalnoj razini donosili zakoni na području zaštite podataka. Te su odredbe o privatnosti našle svoje mjesto u ustavima većine zemalja.[108]

---

[102] Evans, A. C. *European Data Protection Law*, The American Journal of Comparative Law, vol. 29, no. 4, 1981., str. 571–582, str. 573.
[103] Van Alsenoy, Brendan. *Data Protection Law in the EU: Roles, Responsibilities and Liability*. Vol 6. KU Leuven Centre for IT & IP Law Series. Intersentia, Cambridge, 2019., str. 155.
[104] Ibid. str. 156.
[105] Vidi više ibid. str. 168.
[106] Ibid. str. 163.
[107] Vidi više Bennett, Colin J, *Regulating privacy Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca 1992., str. 56.
[108] Holvast, Jan, *History of Privacy*, The Future of Identity in the Information Society, 2009., vol. 298, str. 13-42, str. 28.

Tijekom 70-ih godina 20. stoljeća obrada osobnih podataka postajala je sve opsežnija. Nacionalna zakonodavstva prepoznala su donošenjem posebnih zakona važnost zaštite osobnih podatka. Stoga se počelo razmišljati o prekograničnom protoku osobnih podataka i ugrozi koju protok može imati na prava i slobode pojedinca.[109] Kako bi se spriječile ugroze, a dok bi se s druge strane omogućio neometani prekogranični protok osobnih podatka, međunarodne organizacije počele su razmišljati i stvarati radne skupine kako bi se donijelo rješenje za takav problem.[110]

OECD je na temelju istraživanja i rada radne skupine 23. rujna 1980. godine donio Smjernice za zaštitu privatnosti i međunarodni protok osobnih podataka (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*) koje su uređivale postupanje s osobnim podatcima za subjekte javnog i privatnog prava s time da je ostavljeno prostora za iznimke.[111] Također, pružale su samo minimum standarda koji bi se trebali poštivati dok je ostavljena mogućnost državama da povećaju zaštitu s ciljem zaštite sloboda i prava pojedinca.[112]

U isto vrijeme, Vijeće Europe završilo je svoj dugogodišnji rad na međunarodnom ugovoru koji se bavio zaštitom osobnih podataka, stoga je 17. rujna 1980. usvojena Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*) kolokvijalno nazvane Konvencija 108. Otvorena je za potpisivanje tek 28. siječnja 1981. godine, a stupila je na snagu 1. listopada 1985. godine.[113] Kao i smjernice OECD-a, Konvencija se primjenjuje na subjekte javnog i privatnog prava, uz moguće iznimke i na automatiziranu obradu osobnih podataka.[114] Suprotno smjernicama OECD-a, Konvencija je predvidjela posebnu kategoriju osobnih podataka za koje se smatra da su posebno osjetljivi za pojedinca i kao takvi zaslužuju dodatnu zaštitu.[115] Konvencija 108 nije predviđala izravnu primjenu, nego je svaka država potpisnica morala osigurati instrumente u svojem zakonodavstvu koji su u skladu s njome kako bi se

[109] Op.cit. (bilješka 103.) str. 207.
[110] Ibid.
[111] Ibid. str. 209.
[112] Ibid. str. 210.
[113] Ibid. str. 222.
[114] Ibid.
[115] Ibid. str. 224.

osigurala njezina provedba.[116] Republika Hrvatska ratificirala je Konvenciju i s protokolima implementirala u svoje zakonodavstvo.[117]

Povijesni pregled razvoja prava zaštite osobnih podataka završit će se propisom koji je donedavno bio temelj prava zaštite podataka u Europskoj uniji. Riječ je Direktivi 95/46/EZ o zaštiti pojedinca u pogledu obrade osobnih podataka i slobodnog protoka takvih podataka.[118] O donošenju direktive na području zaštite podataka počelo se razmišljati već sredinom 70-ih godina kada je Europski parlament donio rezoluciju o potrebi donošenja direktive na području osobnih sloboda i obrade podataka.[119] Usprkos ranoj inicijativi Direktiva je donesena tek 1995. godine. Bila je na snazi u EU-u sve do 25. svibnja 2018. godine kada se počela primjenjivati Opća uredba o zaštiti podataka. Svrha donošenja Direktive bila je ujednačiti razinu zaštite prava i sloboda pojedinaca u državama članicama u pogledu njihova prava na privatnost u vezi s obradom njihovih osobnih podataka. Također, svrha Direktive bila je uklanjanje prepreka slobodnom protoku osobnih podatka, što je povezano sa slobodnim razvojem unutarnjeg tržišta EU-a.[120]

Pobliže govoreći o prostoru Europske unije, prema Van Alsenoyu, mogu se razlikovati četiri razdoblja razvoja prava zaštite podataka.[121] Prvo razdoblje je razdoblje pojave nacionalnih zakona o zaštiti podataka. Trajalo je od 1970. do 1980. godine. Slijedi razdoblje internacionalizacije kojeg su obilježile smjernice OECD-a i Konvencija 108, a trajalo je od 1980. do 1981. godine. Treće razdoblje naziva se razdobljem nacionalne implementacije koja se odnosi na smjernice i Konvenciju 108, a trajalo je od 1982. do 1994. godine. Donošenjem Direktive 95/46 započinje posljednje, četvrto razdoblje koje se naziva razdobljem europske harmonizacije. Traje od 1995. godine pa sve do donošenja Opće uredbe o zaštiti podataka 2016. godine.[122]

[116] Ibid.
[117] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, Narodne novine broj 4/25.
[118] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995 . o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, Službeni list Europske unije L 281/31. Dalje u tekstu Direktiva.
[119] Op.cit. (bilješka 102.) str. 576.
[120] Op.cit. (bilješka 65.) str. 119.
[121] Op.cit. (bilješka 103.) str. 151.
[122] Ibid.

5.2. Suvremeno uređenje

Pravo na zaštitu osobnih podataka dovodilo se i dovodi u usku vezu s pravom na privatnost, stoga se pravo na zaštitu osobnih podatka naziva pravom blizanaca (*twin-right*) prava na privatnost.[123] Takvo je bilo razmišljanje u propisima Europske unije sve do početka 21. stoljeća kada se mijenja narativ i postavlja razlika između prava na privatnost i prava na zaštitu osobnih podataka.[124] Pritom se govori kako je distinkcija u tome da se pravom na privatnost nastoji očuvati netransparentnost nečijeg privatnog života, dok se pravom zaštite osobnih podataka nastoji postići transparentnost drugih podataka koji nisu privatni.[125] Nastavak takvog razmišljanja bilo je i donošenje Povelje Europske unije o temeljnim pravima gdje se pravo na zaštitu osobnih podataka u članku 8. navodi kao temeljno pravo svakog čovjeka.[126] Sukladno Povelji Uredba, također, priznaje neovisnost prava na zaštitu osobnih podataka jer je cjelovita Uredba sa svim svojim odredbama posvećena zaštiti osobnih podataka.[127] Veliki doprinos u tumačenju i razgraničenju prava na zaštitu osobnih podataka i prava na privatnost dala je i sudska praksa Europskog suda za ljudska prava i sudska praksa suda Europske unije. Razvoj sudske prakse doveo je do zaključka da su dva prava usko povezana, no da nisu identična, odnosno da se sadržaj dvaju prava značajno preklapa. No, isto tako postoje područja gdje je njihov sadržaj opet različit.[128]

Povezanost prava na privatnost i prava na zaštitu osobnih podataka najbolje dolazi do izražaja kada se promatra odštetno pravo. Iako se pravo na zaštitu osobnih podataka do određene mjere osamostalilo, ono s gledišta odštetnog prava nije samo sebi svrha, nego se osobni podatci štite kako bi se spriječila šteta koju zbog njihove povrede može pretrpjeti pojedinac.[129] Ovdje dolazi do izražaja povezanost prava na zaštitu podataka i prava na privatnost zato što je narušena privatnost prvo što se manifestira kao šteta prilikom povrede prava na zaštitu osobnih podataka.[130]

---

[123] Bukovac Puvača, Maja; Demark, Armando. *Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 2019., vol. 40, br.1, str. 287-315, str. 291.
[124] Ibid.
[125] Ibid.
[126] Ibid. str. 292.
[127] Ibid. str. 293.
[128] Kokott, Juliane; Sobotta, Christoph, *The distincion between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, Internationl Data Privacy Law, 2013., vol. 3, No. 4, str 222-228; str. 228.
[129] Op.cit. (bilješka 123.) str. 303.
[130] Ibid.

Osim odštetnim pravom, pravo na privatnost i pravo na zaštitu osobnih podataka štiti se i kaznenim zakonodavstvom. Tako je Hrvatska donošenjem novog Kaznenog zakona 2011. godine u sami zakon uvrstila i glavu 14. koja je nazvana Kaznena djela protiv privatnosti.[131] U sedam kaznenih djela sadržanih u glavi ponajprije se štiti privatnost, posebno tjelesni i duševni interesi pojedinca, spolni život, spol i spolna orijentacija, osobni podatci, ugled, fotografija i tajnost pisma. Između ostalog, u glavi se nalazi kazneno djelo nedopuštene uporabe osobnih podataka (čl. 146 KZ/11) koje je od svih kaznenih djela prema statistici Državnog zavoda za statistiku najzastupljenije kazneno djelo protiv privatnosti.[132]

Hrvatsko pravo zaštite osobnih podataka još je i prije pristupanja Europskoj uniji značajno bilo pod utjecajem europskog prava. Iako zaštita osobnih podataka u Republici Hrvatskoj uživa status temeljnog ljudskog prava još od donošenja božićnog Ustava 1990. godine, ono nije bilo cjelovito zakonski uređeno sve do donošenja Zakona o zaštiti osobnih podataka 2003. godine.[133] Utjecaj prilikom donošenja zakona svakako je imala i već spomenuta Direktiva 95/46 EZ.[134] Zakon o zaštiti osobnih podataka bio je temeljni propis koji je uređivao područje zaštite osobnih podataka sve do stupanja na snagu Opće uredbe o zaštiti podataka 25. svibnja 2018. godine.

Rad na Uredbi započeo je još 2012. godine kada je Europska unija shvatila da dotadašnji model zaštite osobnih podataka nije dostatan odgovor na izazove koji se javljaju u vidu novih tehnologija. Nakon nekoliko godina rada Uredba je konačno donesena 27. travnja 2016. godine te je stupila na snagu nakon čak dvogodišnjeg *vacatio legisa* 2018. godine. Uredba u pravni poredak država članica uvodi nova tehnološki neutralna pravila u pogledu obrade osobnih podataka i njihova slobodna protoka.[135] Nadalje, Uredbom se u europskom pravnom području nastoji u što većoj mjeri ujednačiti pravni okvir, kao i osigurati što veća pravna sigurnost i zaštita potrošača prilikom obrade i protoka osobnih podataka koju provode subjekti privatnog i javnog prava.[136] Ostvarenje navedenih ciljeva nastoji se postići strožom odgovornosti onih koji obrađuju osobne podatke, zatim dodjeljivanjem snažnijih ovlasti nadzornim tijelima, jačanjem njihove međusobne suradnje i propisivanjem strožih upravnih kazni za prekršitelja odredba Uredbe.[137] Također, u ostvarenju ciljeva Uredbe doprinosi i Europski odbor za zaštitu

[131] Dragičević Prtenjača, Marta; Zagorec, Marina. *Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo nedozvoljene uporabe osobnih podataka*, Godišnjak akademije pravnih znanosti, 2023., str .57-85, str 69.
[132] Ibid.
[133] Op.cit. (bilješka 65.) novo 5. poglavlje str. 16.
[134] Ibid.
[135] Ibid. str. 17.
[136] Ibid.
[137] Ibid.

podataka (EOZP) koji je zamijenio prijašnju radnu skupinu članka 29., a koji svojim tumačenjem Uredbe smjernicama i preporukama pridonosi njezinoj dosljednoj primjeni u državama članicama.[138]

Sa stupanjem na snagu Uredbe u Republici Hrvatskoj stupio je na snagu Zakon o provedbi Opće uredbe o zaštiti podataka čijim je donošenjem ujedno prestao važiti dotadašnji Zakon o zaštiti osobnih podataka.[139] Zakonom se pobliže uređuju poslovi Agencije za zaštitu osobnih podatka (AZOP) koja donošenjem zakona prestaje biti pravna osoba s javnim ovlastima i postaje državno neovisno nadzorno tijelo. Također, zakon u članku 5. utvrđuje Hrvatsku akreditacijsku agenciju kao nadležno tijelo za akreditiranje certifikacijskih tijela u Republici Hrvatskoj. Nadalje, zakon posebno uređuje obradu osobnih podataka u posebnim incidentima, kao što je privola djeteta u odnosu na usluge informacijskog društva, obrada genetskih podataka, obrada biometrijskih podataka, obrada osobnih podataka videonadzorom i obrada osobnih podataka u statističke svrhe.

5.3. Općenito o službeniku za zaštitu podataka

Kao što je rečeno, donošenjem Opće uredbe o zaštiti podataka donesena su nova, tehnološki neutralna pravila koja se odnose na obradu osobnih podataka. Samim donošenjem uredbe, a ne direktive, Europska unija pokazala je da želi što više ujednačiti prava ispitanika u području zaštite osobnih podatka. Unatoč novim pravilima određeni instituti, koji su bili ustanovljeni prijašnjim uređenjem, odnosno Direktivom 95/46 EZ, dorađeni su i ponovno upotrijebljeni u novom zakonskom uređenju. Takvu sudbinu doživjela je i pozicija službenika za zaštitu osobnih podataka.[140] Pozicija službenika za zaštitu podataka pojavila se u nacionalnim zakonodavstvima puno prije nego što je to bilo predviđeno pravom Europske unije.[141] Primjerice, zapadno njemački *Bundesdatenschutzgesetz* iz 1977. godine prvi je zakon koji je predvidio poziciju službenika za zaštitu podataka u nekoj europskoj državi utirući tako put daljnjem razvoju pozicije.[142] Nadalje, pozicija službenika bila je predviđena ranijom Direktivom, no suprotno novom uređenju njegovo imenovanje nije bilo obligatorno, nego je

[138] Ibid. str. 18.
[139] Zakon o provedbi Opće uredbe o zaštiti podatka, Narodne novine broj 42/18.
[140] Dalje u tekstu „službenik"
[141] Katulić, Tihomir; Protrka, Nikola, *Inforamtion Security in Principles and Provisions of the EU Data Protection Law*, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2019., str. 1420-1426, str.1424.
[142] Ibid.

državama članicama ostavljeno na raspolaganje žele li utvrditi funkciju službenika u svojem pravnom poretku.[143] Takvu mogućnost iskoristila je Republika Hrvatska koja je u svojem Zakonu o zaštiti osobnih podataka stipulirala da su svi voditelji obrade koji imaju 20 ili više zaposlenika obvezni imenovati službenika za zaštitu podataka.[144] Hrvatska se tako odlučila za pomalo nespretan kvantitativni kriterij za određivanje tko je obveznik imenovanja službenika za zaštitu podataka, što je pak dovodilo do situacija u praksi gdje voditelji obrade, koji su svakodnevno obrađivali posebno osjetljive osobne podatke i veliku količinu osobnih podataka, nisu bili obveznici imenovanja službenika za zaštitu podataka jer nisu imali 20 zaposlenika.[145]

5.4. Obveznici imenovanja službenika za zaštitu podataka

Novo uređenje zaštite osobnih podataka značajno je proširilo obveznike imenovanja službenika za zaštitu osobnih podataka u odnosu na prijašnje uređenje. Uvidjevši probleme koji su se javljali s prijašnjim uređenjem, Uredba donosi nove kriterije koji se moraju primjenjivati prilikom određivanja tko je obveznik imenovanja službenika za zaštitu podataka pa se tako napušta dotadašnji kvantitativni i uvodi kvalitativni kriterij.[146]

Tako su prema Uredbi obveznici imenovanja službenika za zaštitu podataka svi voditelji obrade i izvršitelji obrade kada obradu provodi tijelo javne vlasti ili javno tijelo (osim sudova kada djeluju o okviru svoje nadležnosti) i kada se osnovna djelatnost voditelja obrade ili izvršitelja obrade sastoji od opsežne obrade koja zbog svoje prirode, opsega i/ili svrhe iziskuje redovito i sustavno praćenje ispitanika u velikoj mjeri. Službenika moraju imenovati svi voditelji i izvršitelji obrade kada se njihova osnovna djelatnost sastoji od opsežne obrade posebne kategorije podataka i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima.

Uredba zahtijeva da službenika za zaštitu osobnih podatka imenuju i subjekti javnog prava i subjekti privatnog prava kada ispunjavaju neki od uvjeta propisanih Uredbom. Uredba, iako detaljna, ipak je ostavila nekoliko praznina za koje je potrebno dodatno tumačenje, primjerice s pojmom *tijelo javne vlasti*. Uredba nije odredila definiciju toga pojma. Međutim, u smjernicama radne skupine iz članka 29. (sadašnji Europski odbor za zaštitu podatka) navedeno

[143] Op.cit. (bilješka 65.) novo 5 poglavlje str. 57.
[144] Ibid.
[145] Katulić, Tihimir; Katulić, Anita. *Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance*, 2019., str. 5.
[146] Ibid.

je da je definiciju pojma potrebno odrediti u nacionalnom pravu.[147] Tako je hrvatski zakonodavac odredio pojam tijela javne vlasti u članku 3. Zakona o provedbi Opće uredbe o zaštiti podataka gdje je rečeno da su tijela javne vlasti tijela državne uprave i druga državna tijela, jedinice lokalne i područne (regionalne) samouprave. Gleda li se pak Zakon o općem upravnom postupku, tada su tijela javne vlasti i pravne osobe koje imaju javne ovlasti kada, u okviru djelokruga utvrđenog na temelju zakona, postupaju i rješavaju u upravnim stvarima.[148] Tako bi sukladno ZUP-u, ali i smjernicama radne skupine kao tijela javne vlasti koja su obvezna imenovati službenika za zaštitu podataka trebalo smatrati i pravne osobe koje imaju javne ovlasti kada, u okviru djelokruga utvrđenog na temelju zakona, postupaju i rješavaju u upravnim stvarima.[149]

Prilikom razmatranja koji subjekti moraju imenovati službenika može se postaviti pitanje kako tumačiti pojam *osnovna djelatnost*. Prema samoj Uredbi u recitalu broj 97. taj se pojam odnosi na primarne djelatnosti voditelja ili izvršitelja obrade, no ne i na obradu osobnih podataka kao dodatne djelatnosti. To su svi oni postupci koji su nužni za ostvarenje ciljeva voditelja obrade ili izvršitelja obrade.[150] Radna skupina taj je pojam tumačila ekstenzivno. Rečeno je da se iz pojma *osnovne djelatnosti* ne bi smjele isključiti djelatnosti u kojima obrada podataka čini neodvojivi dio djelatnosti voditelja obrade ili izvršitelja obrade, a moraju se isključiti djelatnosti poput plaćanja zaposlenika jer to predstavlja pomoćnu funkciju voditelja ili izvršitelja obrade.[151]

Problem s tumačenjima imaju i pojmovi *opsežna obrada* i *redovito i sustavno praćenje*. Uredba u oba incidenta ili daje djelomično određenje pojma u recitalima i člancima ili ga uopće ne daje, stoga je kod oba pojma potrebno dodatno tumačenje koje daje radna skupina.[152] U svakome incidentu voditelji obrade ili izvršitelji obrade, čak i uz smjernice radne skupine, mogu ostati u nedoumici treba li imenovati službenika za zaštitu podataka ili ne. Dakle, moraju izabrati između imenovanja i veće zaštite prava ispitanika, što dolazi uz veće izdatke za plaćanje dodatnog zaposlenika. S druge strane, mogu ne imenovati, ali im tada prijete visoke kazne zbog

[147] Radna skupina za zaštitu podataka iz članka 29., *Smjernice o službenicima za zaštitu podatak*a, WP 243 rev. 01., str. 7.
[148] Zakon o općem upravnom postupku, Narodne novine broj 47/09, 110/21. Dalje u tekstu ZUP.
[149] Popis tijela javne vlasti u Republici Hrvatskoj dostupan je na internetskoj stranici Tijela javne vlasti-povjerenik za informiranje(https://tjv.pristupinfo.hr/, pristupljeno 13. siječnja. 2024.), čiji je autor Povjerenik za informiranje. Povjerenik za informiranje, sukladno Zakonu o pravu na pristup informacijama, ima obvezu objavljivati i ažurirati popis tijela javne vlasti na svojim internatskim stranicama. Na dan 13. siječnja 2024. na popisu se je nalazilo 5814 tijela javne vlasti.
[150] Op.cit. (bilješka 147.) str. 8.
[151] Ibid.
[152] Vidi više smjernice Radne skupine (bilješka 147.) str. 8., 9. i 10.

kršenje odredaba Uredbe, kao što se dogodilo na primjeru jedne njemačke telekomunikacijske tvrtke gdje je njemačko nadzorno tijelo izreklo kaznu zbog opetovanog ignoriranja imenovanja službenika za zaštitu podataka.[153] Stoga je preporuka radne skupine da se u slučaju nedoumice svakako imenuje službenik za zaštitu podataka.

Također, sama Uredba ostavila je mogućnost državama članicama da odrede dodatne situacije kada je imenovanje službenika obligatorno te da sami voditelji i izvršitelji obrade, iako nisu obveznici imenovanje službenika, imenuju službenika kako bi se dodatno zaštitila prava ispitanika u pogledu obrade osobnih podataka. Postoji više razloga zašto bi voditelji ili izvršitelji obrade dobrovoljno imenovali službenika za zaštitu podataka, ponajprije zato što pravo zaštite podataka postaje sve kompleksnije zahvaljujući sve bržem razvoju tehnologija i sve većim društvenim promjenama. Stoga su potrebna nova znanja i vještine kako bi se poslovanje uskladilo s novim uređenjem.[154]
Kao što je spomenuto, novo uređenje značajno je proširilo krug obveznika imenovanja službenika za zaštitu podataka. U prilog tome govore i statistički podatci AZOP-a za 2018. godinu kada se Uredba počela primjenjivati. Naime, tijekom 2018. godine AZOP je zaprimio čak 722 % više obavijesti o imenovanju službenika za zaštitu podataka u odnosu na prethodnu 2017. godinu, dok je ukupni broj novih subjekata, koji su imenovali službenika za zaštitu podataka, oko 45 % (7957 subjekata koji imaju imenovanog službenika u 2018. godini u odnosu na 3653 subjekata u 2017.godini).[155]

5.4.1. Posebnosti kod imenovanja službenika za zaštitu podataka

Pored toga što propisuje tko su obveznici imenovanja službenika za zaštitu podataka, Uredba dodatno razrađuje mogućnosti koje imaju voditelji i izvršitelji obrade kada imenuju službenika. Također, propisuje i određene uvjete u pogledu obrazovanja i stručnosti koje bi morao ispunjavati svaki službenik za zaštitu podataka.

Konkretno, Uredba u članku 37. stavku 2. postavlja mogućnost da grupa poduzetnika imenuje jednog službenika za zaštitu podataka. Međutim, takvo imenovanje uvjetovano je time da službenik bude *lako dostupan*. *Dostupnost* se u ovome slučaju odnosi na mogućnost da

[153] Šidlauskas, Aurimas. The Role and Significance of the Data Protection Officer in the Organization, Socialiniai tyrimai, vol. 44. br. 1, str. 8-28, str. 15.
[154] Op.cit. (bilješka 141.)
[155] Godišnje izvješće o radu Agencije za zaštitu osobnih podataka za razdoblje od 1. siječnja 2018. godine do 31. prosinca 2018. godine, str 51. Dostupno na: https://azop.hr/wp-content/uploads/2020/12/izvjesce_azop_2018.pdf.

učinkovito komunicira i surađuje s ispitanicima i nadzornim tijelom.[156] Dakle, osiguravanje dostupnosti službenika ključna je stavka kako bi se ispitanicima omogućilo stupanje u kontakt sa službenikom te kako bi ispitanici mogli ostvarivati svoja prava koja su im zajamčena Uredbom.

Nadalje, kada su voditelji ili izvršitelji obrade tijela javne vlasti ili javna tijela, tada je dopušteno imenovanje jednog službenika za više tijela. Tada postoji određeni uvjet. Prilikom imenovanja mora se uzeti u obzir veličina i organizacijska struktura tijela, odnosno mora se voditi računa o dostupnosti službenika za zaštitu podataka.

Nadalje, kada se govori o dostupnosti, preporuka radne skupine jest da se službenik, kako bi se osigurala dostupnost, nalazi na prostoru Europske unije, no Uredba to nužno ne nalaže. Službenik se može nalaziti i izvan EU-a ako voditelj ili izvršitelj obrade nemaju poslovni adresu u EU-u.[157]

Kako bi se osiguralo da službenik bude dostupan, Uredba propisuje kako su voditelji ili izvršitelji obrade dužni objaviti kontaktne podatke službenika za zaštitu podataka i da su ih isto tako dužni priopćiti nadzornom tijelu. Prilikom objavljivanja kontaktnih podataka službenika za ispitanike, voditelji ili izvršitelji obrade nisu dužni navesti ime službenika, nego samo informacije, poput telefonskog broja, adrese elektroničke pošte, poštanske adrese, koje omogućuju ispitanicima, ali posredno i nadzornom tijelu da u slučaju potrebe lako stupe u kontakt sa službenikom.[158] S druge strane, voditelji ili izvršitelji obrade dužni su ime službenika obznaniti nadzornom tijelu kako bi službenik mogao ostvariti jednu od svojih funkcija, odnosno poslužiti kao kontaktna točka između nadzornog tijela i organizacije u kojoj djeluje.

Nadalje, Uredba je ostavila mogućnost voditeljima ili izvršiteljima obrade da službenik bude zaposlen u njihovoj organizaciji ili da svoje zadaće obavlja na temelju ugovora o djelu. Uredbom nije striktno naloženo voditeljima ili izvršiteljima obrade da službenik mora biti zaposlenik njihove organizacije, nego je dopušteno *outsourcanje* poslova službenika. S time se otvara mogućnost pojave specijaliziranih organizacija koje se bave isključivo pružanjem usluga obavljanja zadaća službenika za zaštitu podataka. S obzirom na opseg pravnih subjekata koji moraju imati imenovanog službenika, ovo je rješenje osobito prigodno za manje organizacije s malim brojem zaposlenih i malim poslovnim prostorom. Međutim, Uredba ne radi razliku između službenika koji je zaposlen u organizaciji i službenika koji svoje zadaće obavlja na

[156] Op.cit. (bilješka 147.) str. 12.
[157] Ibid.
[158] Ibid. str. 15.

temelju ugovora o djelu. Službeniku koji svoju zadaću obavlja na temelju ugovora o djelu, voditelj ili izvršitelj obrade dužan je osigurati jednaku razinu neovisnosti i zaštite od nepoštenog raskidanja ugovora, kao i službeniku koji je zaposlen u organizaciji.[159]

Naposljetku, Uredba određuje koje kvalifikacije i stručna znanja mora imati službenik kako bi mogao obavljati zadatke koje pred njega postavlja Uredba. Uredba navodi u članku 37. stavka 5. kako se službenici imenuju na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama na području zaštite podataka. Smjernice radne skupine dodatno razrađuju ovo područje te navode kako stručnost službenika mora bit razmjerna osjetljivosti, složenosti i količini podataka koje organizacija obrađuje.[160] Nadalje, govoreći o znanju koje službenik mora posjedovati, smjernice navode kako bi službenik morao posjedovati znanje o nacionalnom pravu i pravu Europske unije, kao i da bi temeljno morao poznavati Opću uredbu o zaštiti podataka.[161] Također, navode kako je korisno da službenik poznaje poslovni sektor i organizaciju voditelja obrade.[162] Kada se govori o poznavanju organizacije voditelja obrade, kao i poznavanju informacijskih sustava i potrebi u pogledu sigurnosti i zaštite podataka voditelja obrade, tada je zapravo vrlo korisno da mjesto službenika zauzme osoba koja je već određeno vrijeme bila zaposlena u organizaciji voditelja obrade, ali na drugom radnom mjestu zato što svakako takva osoba najbolje poznaje način poslovanja voditelja i može pružiti najbolji savjet voditelju obrade kako bi obrada podataka bila sukladna Uredbi.

Kada su u pitanju kvalifikacije i stručna znanja, javlja se veliki problem sa širokim krugom pravnih subjekata koji moraju imenovati službenika. Naime, većina službenika koji su sudjelovali u istraživanju navelo je kako prije stupanja na dužnost službenika za zaštitu podataka nisu imali iskustva u području prava zaštite podataka.[163] Manjak iskustva i nedovoljna stručnost došli su do izražaja u istraživanju kada su službenicima postavljena konkretna pitanja iz područja prava zašite podataka gdje je poprilično velik broj imenovanih službenika krivo odgovorio na neka od jednostavnijih pitanja iz materije.[164] Uzimajući u obzir takve rezultate istraživanja, može se izvući zaključak da je velika većina službenika imenovana samo kako bi

[159] Ibid. str. 14.
[160] Ibid. str. 13.
[161] Ibid.
[162] Ibid.
[163] Koporc, Zvonimir; Mladinić, Anamarija; Puljak, Livia. *Post-GDPR survey on dana protection officers in research and non-research institutions in Croatia: a cross-sectional study*, Biochemia Medica, vol. 31, br. 3, 2021, str. 0-0, str. 4.
[164] Ibid. str. 5.

se ispunila zakonska obveza voditelja ili izvršitelja obrade, a ne kako bi službenik sa svojom stručnošću doprinio usklađenosti obrade podataka s Uredbom.[165]

5.5. Radno mjesto službenika za zaštitu podataka

Uredba pobliže u članku 38. određuje radno mjesto službenika za zaštitu podataka. Detaljnije opisuje koje su dužnosti voditelja ili izvršitelja obrade prema službeniku, što mu se sve mora osigurati kako bi mogao obavljati svoje zadaće određene Uredbom. Osim obveza voditelja ili izvršitelja obrade prema službeniku, Uredba isto tako navodi kako se službenik mora ponašati u okviru svoje pozicije i koje su njegove obveze prema voditelju ili izvršitelju obrade.

Govoreći tako o obvezama koje voditelji ili izvršitelji obrade imaju prema službeniku, prvo što se spominje jest njihova obveza da ga na primjeren način i pravodobno uključe u sva pitanja u pogledu zaštite osobnih podataka. Uključiti službenika u sva pitanja vezana za zaštitu podataka jako je važno kako bi se mogao na odgovarajući način pripremiti i dati savjet voditelju ili izvršitelju obrade, što pridonosi usklađivanju obrade s Uredbom.[166] Također, sama Uredba određuje rano uključivanje službenika kada govori o provedbi procjene učinka na zaštitu podataka. To je postupak koji se provodi prije obrade osobnih podataka u postupcima obrade za koje je vjerojatno da će prouzročiti visoki rizik za prava i slobode pojedinca.[167] Sam postupak procjene učinka na zaštitu podataka osmišljen je kako bi se opisala obrada, procijenila njezina nužnost i proporcionalnost te pružila pomoć u upravljanju rizicima za prava i slobode pojedinca koji nastaju obradom osobnih podataka, njihovom procjenom i određivanjem mjera za uklanjanje.[168] Provedbom procjene voditelj obrade uspostavlja i dokazuje usklađenost obrade s Uredbom.[169] Prilikom provedbe procjene voditelj obrade obligatoran je tražiti savjet od službenika za zaštitu podataka, ako je on imenovan.[170] Kako bi se na neki način olakšao posao voditelja obrade, samom Uredbom je određen, a smjernicama je dodatno pojašnjeno, kako procjena nije potrebna kada je postupak obrade prethodno provjerilo nadzorno tijelo ili službenik za zaštitu podataka.[171] Iako službenik za zaštitu podataka nije ovlašten sam provesti

[165] Ibid. str. 8.
[166] Op.cit. (bilješka 147.) str. 15.
[167] Radna skupina za zaštitu podataka iz članka 29., *Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visoki rizik" u smislu Uredbe 2016/679 WP 248 rev. 01*, str. 5.
[168] Ibid. str. 4.
[169] Ibid.
[170] Op.cit. (bilješka 147.) str. 15.
[171] Op.cit. (bilješka 163.) str. 15.

procjenu, dobra je praksa da sam službenik, uvidjevši da bi određena obrada mogla prouzročiti visoki rizik prava i slobode pojedinca, predloži voditelju obrade provedbu procjene učinka na zaštitu podataka.[172]

Nadalje, sljedeća obveza voditelja ili izvršitelja obrade prema službeniku jest da ga podupiru u izvršavanju njegovih zadaća. To čine osobito pružajući mu potrebna sredstva za rad davanjem pristupa osobnim podatcima i postupcima obrade i održavanjem njegova stručnog znanja. Što je obrada podataka složenija, to više službenik mora biti osposobljen i imati veća sredstva na raspolaganju kako bi mogao izvršiti svoje zadaće.[173]

Prema rezultatima istraživanja većina anketiranih službenika za zaštitu podataka navela je kako se njihov opseg zadataka, koji obavljaju na radnom mjestu, povećao u odnosu na vrijeme kada nisu bili imenovani službenici za zaštitu podataka.[174] Ovdje se ponajprije misli na one službenike koji su i prije stupanja na dužnost bili zaposlenici voditelja ili izvršitelja obrade.[175] U praksi bi tada voditelji obrade morali službeniku za zaštitu podataka dati dovoljno vremena ili ga na određeni način rasteretiti kako bi kvalitetno i profesionalno mogao ispuniti svoju ulogu.[176]

Nadalje, pored osiguranih sredstava ključ izvršavanja zadaća službenika jest njegova neovisnost. Naime, bespotrebno je govoriti kako su neovisnost i određena sigurnost radnog mjesta pretpostavka kvalitetnog obavljanja bilo koje zadaće, posebno kada se radi o odgovornoj zadaći kao što je zadaća službenika koji unutar organizacije mora pratiti poštovanje Uredbe, savjetovati i izvještavati voditelja ili izvršitelja obrade o njihovim obvezama koje proizlaze iz Uredbe, što pak može dovesti do određenog sukoba i netrpeljivosti unutar organizacije. Upravo zato Uredba propisuje kako su voditelj ili izvršitelj obrade dužni osigurati da službenik ne prima nikakve upute u pogledu njegovih zadaća, odnosno dužni su mu osigurati neovisnost.

Kako bi se produbila neovisnost službenika za zaštitu podataka, Uredba određuje da voditelj ili izvršitelj obrade ne smiju razriješiti dužnosti ili kazniti službenika zbog toga što izvršava svoje zadaće. Radna skupina u smjernicama navodi kako kažnjavanje može biti izravno ili neizravno te da se čak i prijetnja kaznom smatra kažnjavanjem. Osim radne skupine, tumačenju pojma neovisnosti službenika doprinio je i Sud Europske unije. Tako je u predmetu Leistritz AG

[172] Ibid. str. 17.
[173] Op.cit. (bilješka 147.) str. 17.
[174] Op.cit. (bilješka 163.) str. 9.
[175] Ibid.
[176] Op.cit. (bilješka 145.) str. 6.

Europski sud naveo kako države članice mogu nacionalnim zakonodavstvom povećati zaštitu od kažnjavanja službenika za zaštitu osobnih podataka.[177] Tako je primjerice učinila Njemačka gdje je nacionalnim pravom određeno da službenik može dobiti otkaz samo zbog opravdanog razloga.[178]

Nadalje, autonomija službenika dodatno se povećava odredbom Uredbe kojom se određuje kako službenik za svoj rad mora odgovarati izravno najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade.

Zanimljivo je istaknuti da su, prema istraživanju koje je provedeno između službenika za zaštitu podataka u Hrvatskoj, upravo manjak neovisnosti i suradnje s nadređenima istaknuti kao najveći problemi s kojima se susreću u svakodnevnom radu.[179]

Osim obveza voditelja ili izvršitelja obrade prema službeniku, u okviru svoje pozicije službenik ima određene obveze prema voditelju ili izvršitelju obrade. Uredba propisuje da je službenik dužan čuvati tajnost i povjerljivost podataka koje sazna u okviru obavljanja svojih zadaća.

Konačno, Uredba daje mogućnost službenicima da u organizaciji obavljaju i drugu dužnost, osim one službenika za zaštitu podataka. Međutim, Uredba uvjetuje obavljanje druge dužnosti ili zadaće tako da ne postoji sukob interesa. Iako se u Uredbi ne spominje što bi zapravo predstavljalo sukob interesa, smjernice daju dodatno objašnjenje i primjere radnih mjesta čije su dužnosti nespojive s dužnostima službenika. Primjerice, to bi bila radna mjesta višeg rukovodstva ili radna mjesta niže u strukturi ako je u opisu tih radnih mjesta utvrđivanje svrhe i način obrade osobnih podataka.[180] Preporučuje se voditeljima ili izvršiteljima obrade da utvrde koje su funkcije nespojive s funkcijom službenika ili da se sastave interna pravila za tu svrhu kako bi se izbjegao sukob interesa.[181] Osim smjernica radne skupine, Sud Europske unije također je pridonio tumačenju pojma *sukob interesa* u kontekstu službenika za zaštitu podataka. U predmetu X-FAB Dresden Sud naveo je kako iz Uredbe proizlazi da se službeniku ne mogu povjeriti zadaće ili dužnosti koje bi ga dovele do toga da određuje svrhu i sredstva obrade osobnih podataka kod voditelja obrade ili izvršitelja obrade zato što, sukladno pravu Unije, službenik treba provoditi neovisni nadzor nad tim svrhama i sredstvima obrade.[182] Također, Sud je naveo kako se postojanje sukoba interesa utvrđuje u svakom slučaju pojedinačno uzimajući

[177] Sud Europske unije, C-534/20 od 22. lipnja 2022. godine
[178] Ibid. točka 7.
[179] Op.cit. (bilješka 163.) str. 3.
[180] Op.cit. (bilješka 147.) str.19.
[181] Ibid.
[182] Sud Europske unije, C-453/21 od 9. veljače 2023. godine, točka 44.

u obzir sve relevantne okolnosti poput organizacijske strukture voditelja ili izvršitelja obrade, sve primjenjive propise u što ulaze i unutarnja pravila organizacije.[183]

5.6. Zadaće službenika za zaštitu podataka

Službeniku za zaštitu podataka Uredbom su povjerene određene zadaće koje mora obavljati u organizaciji voditelja ili izvršitelja obrade. Samom Uredbom navedene su zadaće koje službenik najmanje mora obavljati. Lista zadaća nije zatvorena, nego je dopušteno da službenik obavlja još zadaća, ako te zadaće nisu u suprotnosti s ostalim odredbama Uredbe. Kao što je rečeno, službenik svoje zadaće obavlja profesionalno i na što neovisniji način. Također, službenik prilikom obavljanja svojih zadaća mora voditi računa o riziku povezanom s postupcima obrade te uzeti u obzir prirodu, opseg, kontekst i svrhu obrade. Drugim riječima, Uredba od službenika traži da utvrdi prioritetne aktivnosti i da svoj rad usmjere na pitanja koja predstavljaju veći rizik za zaštitu podataka.[184]

Prvi od zadatka koje propisuje Uredba jest da službenik informira i savjetuje voditelja ili izvršitelja obrade te zaposlenike koji provode obradu o njihovim obvezama koje proizlaze iz Uredbe te o obvezama koje proizlaze iz drugih zakonodavnih akata Unije ili države članice, a koje se tiču zaštite podataka.

Nadalje, sljedeća je zadaća službenika praćenje poštovanja Uredbe i drugih odredaba Unije i država članica koje se odnose na zaštitu podataka i politika voditelja ili izvršitelja obrade u odnosu na zaštitu podataka. To ujedno uključuje raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade i revizije. Unatoč tome što službenik prati usklađenost obrade podataka s Uredbom, nije odgovoran u slučaju pojave neusklađenosti.[185] Voditelj ili izvršitelj obrade provode tehničke i organizacijske mjere kako bi mogao osigurati i dokazati da se obrada podataka provodi u skladu s odredbama Uredbe. Dakle, odgovornost za usklađenost u potpunosti je na strani voditelja ili izvršitelja obrade, a ne na službeniku.[186]

Osim pružanja savjeta o zaštiti podataka, Uredbom je posebno određeno da službenik mora, kada je to zatraženo, pružiti savjet voditelju obrade u pogledu procjene učinka na zaštitu

[183] Ibid. točka 45.
[184] Op.cit. (bilješka 147.) str. 21.
[185] Ibid. str. 19.
[186] Ibid.

podataka. Kako je navedeno u radu, sukladno članku 35., voditelj obrade mora provesti procjenu učinka ako je vjerojatno da će neka vrsta obrade prouzročiti visok rizik za prava i slobode pojedinca. U ovome slučaju voditelj obrade ima obvezu tražiti savjet od službenika za zaštitu podataka, a službenik zatim ima obvezu pružiti savjet. Osim pružanja savjeta u samoj procjeni, voditelju obrade preporučuje se da službenika traži savjet i za pitanja o tome treba li provesti ili ne samu procjenu, kojom se metodologijom služiti, treba li procjenu izvršiti samostalno ili je povjeriti vanjskim izvršiteljima, koje zaštitne mjere primijeniti radi ublažavanja rizika i je li sama procjena pravilno provedena.[187] Također, voditelj obrade ne mora uvažiti savjet službenika u pogledu procjene. Međutim, ako nije uvažio savjet, voditelj obrade mora posebno obrazložiti zašto ga nije uvažio.[188] To je svakako još jedan trenutak u kojem Uredba prepoznaje važnost i neovisnost, a zatim i samu stručnost pozicije službenika za zaštitu podataka.

Prema spomenutom istraživanju, zanimljivo je da je velika većina anketiranih službenika za zaštitu podataka navela kako nije provela analizu postupka obrade niti je sudjelovala u provedbi procjene učinka na zaštitu podataka.[189] Takvi rezultati dovode do zaključka kako zapravo ni voditelji obrade, a ni sami službenici nisu upoznati sa svojim obvezama koje proizlaze iz Uredbe, što je u skladu s podatcima koji pokazuju da imenovani službenici nisu dovoljno upoznati s pravom zaštite osobnih podataka, odnosno nisu dovoljno stručni.

Od zadataka službenika koji su navedeni u Uredbi još se spominje njegova obveza suradnje s nadzornim tijelom i obveza djelovanja kao kontaktne točke za nadzorno tijelo o pitanjima u pogledu obrade, posebno u slučaju iz članka 36. Uredbe. Ovakvo rješenje predviđeno je kako bi nadzornom tijelu bilo lakše pristupiti dokumentima i informacijama te kako bi ono moglo ostvarivati svoje zadatke predviđene Uredbom. Drugo, takvo rješenje pomaže službeniku za zaštitu podatka jer može u svakome trenutku tražiti savjet od nadzornog tijela kako bi obrada podataka bila usklađena s Uredbom.[190]

Kako bi službenicima bilo lakše ostvarivati zadatke, radna skupina preporučuje voditeljima obrade da se u ugovoru službenika za zaštitu podataka i u informacijama za zaposlenike navedu točne zadaće službenika i njihov opseg.[191]

[187] Ibid. str. 20.
[188] Ibid.
[189] Op.cit. (bilješka 163.) str. 9.
[190] Op.cit. (bilješka 147.) str. 20.
[191] Ibid.

Osim što je kontaktna točka za nadzorno tijelo, službenik ujedno služi kao kontaktna točka za ispitanike. Naime, člankom 37. stavka 4. Uredbe predviđeno je da ispitanici mogu kontaktirati službenika u pogledu svih pitanja povezanih s obradom svojih podataka i ostvariti svoja prava zajamčena Uredbom.

Prema podatcima koji su dobiveni anketiranjem službenika za zaštitu podataka, ni jedan službenik u dvogodišnjem razdoblju primjenjivanja Uredbe nije primio nikakvu pritužbu od strane ispitanika vezanu za obradu osobnih podataka.[192]

Kao što je spomenuto, zadatci koji su navedeni u Uredbi predstavljaju samo minimum onoga što službenik mora obavljati. Voditelj ili izvršitelj obrade mogu službeniku za zaštitu podatka dodijeliti još zadataka, poput vođenja evidencije postupka obrade, ako ti zadatci ne dovode službenika u sukob interesa i nisu u suprotnosti s odredbama Uredbe.[193]

Promatrajući poziciju službenika za zaštitu podataka, može se uočiti njegova ponajviše posrednička i savjetodavna uloga. U skladu sa svojim neovisnim položajem, zadatak službenika ponajprije je osigurati zaštitu podataka. Iako nema izvršnu ulogu, on svojim savjetima prema voditelju ili izvršitelju obrade, a i svojom ulogom kao kontaktna točka za nadzorno tijelo može značajno utjecati na usklađenost obrade s Uredbom i time povećati zaštitu podataka ispitanika. Pritom mora voditi računa između postizanja što veće zaštite podataka, a da se opet u značajnoj mjeri ne opstruira obavljanje svakodnevnih poslovnih zadataka voditelja ili izvršitelja obrade. Drugim riječima, dobar službenik za zaštitu podataka mora biti fleksibilan i postaviti se kao arbitar između prava i postupaka organizacije unutar koje djeluje.[194]

[192] Op.cit. (bilješka 163.) str. 9.
[193] Op.cit. (bilješka 147.) str. 20.
[194] Op.cit. (bilješka 153.) str. 12.

6. Zaključak

Pozicije savjetnika za informacijsku sigurnost i službenika za zaštitu podataka u mnogočemu se preklapaju. Obje pozicije imaju sličan zadatak, a to je osigurati što bolju primjenu propisa za koje su nadležni unutar organizacije u kojoj djeluju. Iako slični, krug pravnih subjekata koji moraju imenovati službenika za zaštitu podatka znatno je širi od kruga pravnih subjekata koji moraju imenovati savjetnika za informacijsku sigurnost. Stoga je i razina stručnosti koju mora imati savjetnik veća od stručnosti koju mora imati službenik za zaštitu podataka.

Izvor njihove snage i utjecaja koje imaju unutar organizacije leži ponajprije u njihovoj neovisnosti i stručnosti. Naime, obje pozicije odgovaraju izravno najvećoj rukovodećoj poziciji unutar organizacije, dok je pozicija službenika za zaštitu podataka još osnažena presudama Europskog suda gdje je dopušteno državama članicama da nacionalnim zakonodavstvom jamče veću zaštitu službeniku, u pogledu razloga za otpuštanje, od one koja je propisana Uredbom.

Sličnosti se ogledaju i u činjenici da savjetnik i službenik služe kao svojevrsna produžena ruka nadležnog nadzornog tijela u organizaciji u kojoj djeluju, odnosno da su dužni surađivati s nadležnim nadzornim tijelom. Službenik to čini tako što služi kao kontaktna točka za nadzorno tijelo unutar organizacije voditelja ili izvršitelja obrade, dok savjetnik mora dostaviti izvješće o provedenom nadzoru nadležnom nadzornom tijelu.

Najveća je pak razlika između dvije pozicije zadatak koji obavljaju. Savjetnik u svojem djelokrugu, pored usklađivanja, nadzora i edukacije, mora koordinirati provedbu mjere i standarda informacijske sigurnosti kako bi osigurao stanje informacijske sigurnosti za najosjetljivije sustave i podatke koji mogu biti od iznimne važnosti za funkcioniranje same države. S druge strane, službenik za zaštitu podataka tek prati, savjetuje, osposobljava voditelja ili izvršitelja obrade kako bi njihova obrada podataka bila što bolje u skladu s Uredbom.

Kada bi se htjelo od pozicije savjetnika za informacijsku sigurnost i pozicije službenika za zaštitu podataka stvoriti jedna pozicija, tada bi se od pozicije službenika uzela njegova neovisnost i jamstvo od razrješenja, a od pozicije savjetnika njegova razina stručnosti i ovlasti te obveza da dva puta godišnje obavi nadzor i dostavi svoje izvješće nadzornom tijelu. Tako bi se dobila jedna neovisna, stručna i snažna pozicija koja bi sa svojim utjecajem mogla implementirati propise za koje je nadležna unutar organizacije u kojoj djeluje.
Naposljetku, možda će se u skoroj budućnosti vidjeti nova, stručna i neovisna pozicija koja će biti negdje između savjetnika za informacijsku sigurnost i službenika za zaštitu podataka u

europskom zakonodavstvu kada Europska unija odluči podrobnije regulirati područje umjetne inteligencije.[195] Europska unija intenzivno radi na uredbi o umjetnoj inteligenciji čije donošenje ima cilj stvoriti pogodno okruženje za daljnji razvoj područja umjetne inteligencije uz što veću zaštitu temeljnih prava i sloboda građana.[196] Nameće se pitanje je li tržište Hrvatske i Europske unije spremno isporučiti nove stručne ljude koji će obnašati novu dužnost s obzirom na to da je već prilikom implementacije Uredbe došlo do nestanka kvalitetnih stručnjaka za pravo zaštite podatka.[197]

U konačnici je riječ o pozicijama koje u svojim organizacijama obavljaju ulogu svaka na svoj način, sa svojima pravilima, ovlastima, pravima i obvezama. Na zakonodavcu je da na temelju iskustva revidira rad obje pozicije i po potrebi donese novo zakonodavno rješenje. UVNS je u svoj Plan zakonodavnih aktivnosti za 2020. i 2021. godinu uvrstio Izmjenu i dopunu zakona o informacijskoj sigurnosti.[198] Preostaje vidjeti kako će izgledati novo, revidirano rješenje i pozicije savjetnika za informacijsku sigurnost i pozicije službenika za zaštitu podataka.

[195] Op.cit. (bilješka 72.) str. 17.
[196] Op.cit. (bilješka 88.) str. 59.
[197] Op.cit. (bilješka 72.) str. 17.
[198] Ažurirani Prijedlog Plana zakonodavnih aktivnosti Ureda Vijeća za nacionalnu sigurnost, https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=15200, pristupljeno 27. veljače 2024.

7. Popis literature

Monografije:

1. Andress, Jason. The Basics of Information Security. Elsevier, 2011.
2. Bennett, Colin J. Regulating privacy Data Protection and Public Policy in Europe and the United States. Cornell University Press, 1992.
3. De Leeuw, Karl; Bergstra, Jan. The history of information security, a comprehensive handbook. Amsterdam, 2007.
4. Dragičević, Dražen *et. al.* Pravna informatika i pravo informacijskih tehnologija. Zagreb, 2015.
5. Perić, Berislav. Država i pravni sustav. Zagreb, 2009.
6. Van Alsenoy, Brendan. Data Protection Law in the EU: Roles, Responsibilities and Liability. Vol 6. KU Leuven Centre for IT & IP Law Series. Intersentia, Cambridge, 2019.
7. Whitman, Michael E; Mattord, Herbert J. Principles of Information Security. Cengage, Boston, 2021.

Znanstveni i stručni radovi:

1. Alexander, Aileen; Cummings, Jamey. The Rise of the Chief Information Security Officer. People and Strategy, vol. 39, br. 1, 2016., str. 10-13.
2. Arbanas, Krunoslav. Ključni čimbenici kulture informacijske sigurnosti. Policija i sigurnost, 29, br. 4/2020 (2020), str. 376-388.
3. Arbanas, Krunoslav; Nikolina Žajdela Hrustek. Key Success Factors of Information Systems Security. Journal of Information and Organizational Sciences, 43, br. 2, 2019., str. 131-144.
4. Bukovac Puvača, Maja; Demark, Armando. Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede. Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 40 (2019.), 1, str. 287-315.
5. Dragičević Prtenjača, Marta; Zagorec, Marina. Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo nedozvoljene uporabe osobnih podataka. Godišnjak akademije pravnih znanosti, 2023., str. 57-85.

6. Evans, A. C. European Data Protection Law. The American Journal of Comparative Law, 29 (1981.), 4, str. 571-582.
7. Holvast, Jan. History of Privacy. The Future of Identity in the Information Society, 298 (2009.), str. 13-42.
8. Katulić, Tihomir; Protrka, Nikola. Inforamtion Security in Principles and Provisions of the EU Data Protection Law, 42nd International Convention on Information and Communication Technology. Electronics and Microelectronics (MIPRO), Opatija, 2019., str. 1420-1426.
9. Katulić, Tihomir. Transposition of EU Network and Information Security Directive into National Law, 41st International Convention on Information and Communication Technology. Electronics and Microelectronics (MIPRO), Opatija, 2018., str. 1143-1148.
10. Katulić, Tihomir. CISO, DPO, AIHO? Navigating the EU's AI regulatory efforts in pursuit of dana protection and information security compliance, u knjizi: Artificial Intelligence for human-centric society: The future is here, European Liberal Forum, Bruxelles, 2024., str. 56-81.
11. Katulić, Tihomir. Towards the Trustworthy AI: Insights from the Regulation on Data Protection and Information Security. Medijska istraživanja, 26 (2020.), 2, str. 9-28.
12. Katulić, Tihimir; Katulić, Anita. Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance, 2019.
13. Kokott, Juliane; Sobotta, Christoph. The distincion between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, Internationl Data Privacy Law. 3 (2013.), 4, str. 222-228.
14. Koporc, Zvonimir; Mladinić, Anamarija; Puljak, Livia. Post-GDPR survey on dana protection officers in research and non-research institutions in Croatia: a cross-sectional study. Biochemia Medica, 31 (2021.), 3.
15. Radna skupina za zaštitu podataka iz članka 29., Smjernice o službenicima za zaštitu podataka, WP 243 rev. 01.
16. Radna skupina za zaštitu podataka iz članka 29., Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visoki rizik“ u smislu Uredbe 2016/679, WP 248 rev. 01.
17. Šidlauskas, Aurimas. The Role and Significance of the Data Protection Officer in the Organization. Socialiniai tyrimai, vol. 44. br. 1, str. 8-28.
18. Vojković, Goran, Novi pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, Informator, broj 5965, 2011.

Internetski izvori i studije

1. Ažurirani Prijedlog Plana zakonodavnih aktivnosti Ureda Vijeća za nacionalnu sigurnost, https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=15200, pristupljeno 27. veljače 2024.
2. CERT, https://www.zsis.hr/default.aspx?id=16, pristupljeno 23. studenoga 2023. godine.
3. Council of Europe, The Budapest convention(ETS No.185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention; pristupljeno 18. studenoga 2023. godine.
4. Godišnje izvješće o radu Agencije za zaštitu osobnih podataka za razdoblje od 1. siječnja 2018. godine do 31. prosinca 2018. godine, str 51. Dostupno na: https://azop.hr/wp-content/uploads/2020/12/izvjesce_azop_2018.pdf, pristupljeno 1. lipnja 2024. godine.
5. Hrvatski jezični portal, https://hjp.znanje.hr/index.php?show=search, pristupljeno 1. lipnja 2024. godine.
6. Ministar Malenica u Strasbourgu potpisao Drugi dodatni protokol Konvencije o kibernetičkom kriminalu, https://mpu.gov.hr/vijesti/ministar-malenica-u-strasbourgu-potpisao-drugi-dodatni-protokol-konvencije-o-kibernetickom-kriminalu/26599; pristupljeno 18. studenoga 2023. godine.
7. O nacionalnom CERT-u, https://www.cert.hr/onama/, pristupljeno 23. studenoga 2023. godine.
8. Salus, Peter. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. November 19, 1998., www.sane.nl/events/sane98/aftermath/salus.html., pristupljeno 7. studenoga 2023. godine.
9. Tijela javne vlasti-povjerenik za informiranje, https://tjv.pristupinfo.hr/, pristupljeno 13. siječnja 2024. godine.
10. Zajedno za kibernetičku otpornost Europske unije, https://www.cert.hr/zajedno-za-kiberneticku-otpornost-europske-unije/; pristupljeno 22. studenoga 2023. godine.

Zakoni i drugi propisi:

1. Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u

području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), Službeni list Europske unije L 151/15.
2. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), Službeni list Europske unije L 119/56.
3. Direktiva EU 2016/1148 Europskog parlamenta i vijeća od 6. srpnja 2016. o mjerama za visoku razinu sigurnosti i mrežnih i informacijskih sustava širom Unije, Službeni list Europske unije br. 194/1.
4. Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), Službeni list Europske unije 333/80.
5. Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, Službeni list Europske unije 218/8.
6. Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, Službeni list Europske unije L 281/31.
7. Kazneni zakon, Narodne novine br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21.
8. Zakon o informacijskoj sigurnosti, Narodne novine br. 79/07.
9. Zakon o kibernetičkoj sigurnosti, Narodne novine 14//24.
10. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine broj 64/18.
11. Zakon o općem upravnom postupku, Narodne novine broj 47/09, 110/21.
12. Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, Narone novine br. 9/2002
13. Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, Narodne novine broj 4/25.
14. Zakon o provedbi Opće uredbe o zaštiti podatka, Narodne novine broj 42/18.
15. Zakon o sigurnosnim provjerama, Narodne novine broj 85/08, 86/12.
16. Zakon o tajnosti podataka, Narodne novine broj 79/07, 86/12.

17. Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, Narodne novine broj 30/11.

Sudska praksa:

1. Sud Europske unije, C-534/20 od 22. lipnja 2022. godine.
2. Sud Europske unije, C-453/21 od 9. veljače 2023. godine.