MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

SPECIJALISTIČKI DIPLOMSKI STRUČNI STUDIJ

MENADŽMENT TURIZMA I SPORTA

MARTINA PINTARIĆ

ULOGA I VAŽNOST KORPORATIVNE SIGURNOSTI U POSLOVANJU PODUZEĆA

ZAVRŠNI RAD

ČAKOVEC, 2015.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

SPECIJALISTIČKI DIPLOMSKI STRUČNI STUDIJ

MENADŽMENT TURIZMA I SPORTA

MARTINA PINTARIĆ

ULOGA I VAŽNOST KORPORATIVNE SIGURNOSTI U POSLOVANJU PODUZEĆA

The Role and Importance of Corporative Security in Business of Companies

ZAVRŠNI RAD

Mentor: mr. sc. Vrbanec Miljenko, pred.

ČAKOVEC, 2015.

SAŽETAK

Rad prikazuje ulogu i važnost korporativne sigurnosti u poslovanju poduzeća, s obzirom na promjenjive i nestabilne uvjete današnjice. U radu je predstavljena poslovna strategija, koja je kako navode stručnjaci ključ svakog poslovnog uspjeha. Detaljno je objašnjen pojam poslovnog procesa i samo upravljanje poslovnim procesima. Navodi se i kako je potrebno kontinuirano provoditi proces kontrole, zaštite i sigurnosti u poslovanju, da bi se na taj način zaštitili podaci i informacije od gubitka ili zlouporabe. Postavlja se pitanje na koji način spriječiti dolazak ugroze poslovnih procesa i koju sigurnosnu politiku odabrati? Da bismo dobili najtočniji odgovor potrebno je dobro poznavati normativni okvir korporativne sigurnosti. Prikazana su različita stajališta procesa korporativne sigurnosti. Obrazložen je i normativni okvir korporativne sigurnosti, u kojem su identificirane, sistematizirane, analizirane i detaljno opisane sve dimenzije korporativne sigurnosti: informacijska sigurnost, privatna zaštita, zaštita intelektualnog vlasništva, zaštita podataka, business intelligence, sprječavanje pranja novca i financiranja terorizma, zaštita na radu, zaštita od požara i zaštita okoliša. Vrhunac radnje je područje zaštite podataka, gdje su detaljno objašnjeni osnovni pojmovi, način pristupa klasificiranim i neklasificiranim podacima, te mjere i standardi koje je potrebno ispuniti da bi bili zadovoljeni minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka. Ukratko je navedena i zakonska regulativa, te kaznenopravna odgovornost za one koji se ne pridržavaju zakona. Spomenut je i model „business intelligence“, koji u suvremenim uvjetima predstavlja strateški menadžerski resurs i pojam industrijske špijunaže, odnosno ilegalnog dolaska do podataka i informacija u cilju postizanja konkurentske prednosti. Rad završava metodama zaštite korporativne sigurnosti u poslovanju poduzeća. U suvremenim uvjetima i okolnostima dolazi do porasta svijesti o važnosti osiguravanja rada na siguran način za poslodavca i zaposlenika, te sve veći broj poduzeća shvaća i primjenjuje mjere i radnje iz područja zaštite na radu, zaštite od požara i zaštite okoliša. No, za uspješno poslovanje nije dovoljno zaštititi samo materijalne i ljudske resurse, već je potrebna i zaštita financijskih sredstava, koja je objašnjena putem metode sprječavanja pranja novca i financiranja terorizma.

Ključne riječi:

korporativna sigurnost, poslovanje, poduzeće, strategija, proces, zaštita, menadžment

SUMMARY

This thesis explains the role and importance of corporate security in business enterprises with regard to changeable and unstable conditions today. It presents a business strategy, which is, according to experts, the key to any business success. The concept of business process itself and business process management is explained in details. It also mentions the necessity of continuous process control as well as safety and security in business in order to protect the data and information from loss or misuse. The question is how to prevent the arrival of compromising business processes and which security policy to choose? To get the most accurate answer, it is crucial to know the normative framework of corporate security really well. Different views of the process of corporate security are also presented in this thesis. The normative framework of corporate security is well explained, together with all the dimensions of corporate security identified, systemized, analyzed and precisely described: information security, private security, intellectual property protection, data protection, business intelligence, prevention of money laundering and terrorist financing, workplace safety, fire protection and environmental protection. The highlight of this thesis is on the area of data protection, which contains the detailed explanations of the basic terms, method of access to classified and unclassified information as well as measures and standards which must be fulfilled in order to meet the minimum criteria for the protection of classified and unclassified information. The legislation and criminal liability for those who do not obey the law is also briefly described in this thesis. The model of "business intelligence", which in modern conditions represents a strategic management resource and the concept of industrial espionage or illegal arrival to the data and information in order to achieve competitive advantage, is also mentioned. The thesis concludes with methods of protection of corporate

security in business enterprises. In modern conditions and circumstances, awareness of the importance of protecting work in a safe manner for both the employer and employee increases; therefore more and more companies understand and apply measures and actions for workplace safety, fire protection and environmental protection. However, for a successful business it is not enough to only protect material and human resources. The protection of financial resources, which is explained by the methods of preventing money laundering and terrorist financing, is also significant and necessary.

Key words:
corporate security, business, company, strategy, process, protection, management

SADRŽAJ

1. Uvod

Tema ovog diplomskog rada odabrana je nastavno na tematiku, koja se obrađivala na specijalističkom diplomskom studiju u sklopu kolegija Menadžment poslovne sigurnosti.

Osnove obrađene na predavanju bile su temelj za pisanje diplomskog rada, te su iste nadopunjene uz pomoć stručne literature.

Tematika kolegija bila je zanimljiva i na temelju nje potaknut je dodatni interes za detaljniju obradu. Zbog uvjeta današnjice, teških poslovnih okolnosti, koje mnoge poduzetnike potiču na neetično postupanje u odnosu na konkurente, došlo je do želje za upoznavanjem zakonskih osnova i propisa, te kaznenih sankcija koje slijede ukoliko se ne poštuju zakoni i propisi.

Na početku rada obrađena je poslovna strategija, koja je ključ poslovnog uspjeha. Prikazana je u funkciji upravljanja ostalim poslovnim procesima. Kako korporativna sigurnost ima važnu ulogu u ostvarenju ciljeva poduzeća, dolazi do potrebe za ustrojem organizacijske jedinice koja će se baviti integralnom sigurnošću poduzeća i ostalim poslovima zaštite i sigurnosti u poslovanju.

Rad se nastavlja obradom normativnog okvira korporativne sigurnosti koji uključuje informacijsku sigurnost, privatnu zaštitu, zaštitu intelektualnog vlasništva, zaštitu podataka, business intelligence, sprječavanje pranja novca i financiranja terorizma, zaštitu na radu, zaštitu od požara i zaštitu okoliša. To su dimenzije korporativne sigurnosti koje se smatraju važnima za sprječavanje ugroze poslovnih procesa ili smanjenje ugroze na što je moguće manju razinu i pronalazak najbolje sigurnosne politike za poduzeće.

2. Poslovna strategija poduzeća u funkciji upravljanja poslovnim procesima

Proces globalizacije, tehnološke inovacije, jaka konkurencija i brze društvene promijene neke su od glavnih značajki današnjice. Zbog njih se mnogi poduzetnici odlučuju na neetično ponašanje prema konkurentima. Kako bi se spriječilo takvo ponašanje svako poduzeće trebalo bi jasno definirati viziju svog razvoja, ciljeve (SMART), ali prije svega i strategiju[1]. Kao što i mnogi autori navode: "Poslovna strategija poduzeća – ključ poslovne uspješnosti".

2.1. Poslovna strategija poduzeća

Činjenično stanje je da se poslovanje današnjice odvija u promjenjivim i nestabilnim okolnostima, stoga je potrebno formulirati i implementirati strategiju poduzeća s takvom okolinom i prilagoditi joj se. Pod pojmom strateškog upravljanja podrazumijeva se uspostavljanje dugoročnih ciljeva, određivanje pristupa za njihovo ostvarivanje, te implementacija, kontrola i vrednovanje ciljeva.

Strategiju možemo definirati i sagledati na tri razine:

- korporativna
- poslovna
- funkcionalna[2]

Unutar strateškog upravljanja odvijaju se tri poslovna procesa: strateško planiranje, implementacija strategije, kontrola i vrednovanje strategije. Pojam strateško planiranje obuhvaća analizu okruženja poduzeća u kojem se trenutno nalazi i definiranje detaljnog strateškog plana s jasno definiranim ciljevima. Implementacija strategije najvažniji je segment strateškog upravljanja. Većina poduzeća ne uspijeva provesti svoju strategiju što dovodi do ograničenog mjerenja poslovne uspješnosti. Često se mjeri financijski učinak poduzeća ili

[1] „Određivanje osnovnih dugoročnih ciljeva poduzeća, te usvajanje smjera akcije i alokacije resursa potrebnih za ostvarivanje tih ciljeva." Alfred Chandler – stručnjak za strateški menadžment

[2] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost", Zagreb, UHMS, str. 25.

pak se pažnja posvećuje samo njemu dok se ostala mjerila zanemaruju. To dovodi do nemogućnosti detektiranja kritičnih dijelova poslovnih procesa i tada poduzeća ne mogu reagirati u smislu inovacija ili ukidanja pojedinih neefikasnih procesa. S druge strane ako poslovni sustavi primjenjuju procesni pristup, mjerenje uspješnosti na procesnoj razini nije zastupljeno u dovoljnoj mjeri i zbog toga je nužno implementirati sustav mjerenja na svim komponentama poslovne strategije, koji omogućava poslovnom sustavu da se bori protiv nepovoljnih okolnosti kod provedbe strategije. Kao najvažniji uzrok provedbe neuspješne strategije navodi se neznanje zaposlenih i parcijalno promatranje poslovnog sustava, te skupi metodologijski okviri praćenja uspješnosti, koje je u praksi teško implementirati zbog njihove neodrživosti, cijene i kompleksnosti. Kontrola i vrednovanje strategije posljednja je faza procesa strateškog upravljanja. Ona daje povratnu informaciju o kvaliteti aktivnosti provedenih kroz cijeli proces strateškog upravljanja. Kontrola je kontinuirani proces koji omogućava da se pojedinačni zadaci u poduzeću izvrše efikasno i da se sve odvija po planu. Ako se kontrolom utvrdi potreba za značajnijom promjenom definiranih strateških projekata pristupa se reviziji. Ona se u pravilu provodi jednom do dva put godišnje. Ostvarenje sigurnosti poslovnog uspjeha kompanije je osnovni cilj korporativne sigurnosti u poduzeću. Tu se javlja nepoznanica - kako i na koji način ostvariti taj cilj? Sigurnosna strategija u poduzeću kreira se istovremeno s korporativnom strategijom i kad je ona definirana za jednu organizaciju ne može se primijeniti na neku drugu, jer različite organizacije imaju različite poslovne potrebe i ciljeve. Ona je dugoročna obveza i mora biti održiva uz jasno definirane ciljeve. Pozicioniranje sigurnosti je najvažniji dio sigurnosne strategije i kao takav mora biti u skladu s ciljevima organizacije i poslovnom strategijom. Pozicioniranje sigurnosti je faza utvrđivanja prioritetnih resursa i imovine poduzeća. Sigurnost mora biti u skladu s upravljanjem rizicima u organizaciji. Upravljanje rizicima je kompleksno područje i u većini hrvatskih poduzeća trenutno se nalazi u fazi implementacije. Proces upravljanja rizicima utvrđen je međunarodnim standardom ISO 31000:2009. Standard ISO 31000 nije certifikacijski, već predstavlja smjernice za uspostavu i poboljšanje procesa za upravljanje rizicima u organizaciji. U organizacijama njegova primjena nije

obvezujuća. Procjena rizika je proces identifikacije i sprječavanja ili svođenja na najnižu razinu svih čimbenika koji predstavljaju prijetnju za ispunjenje osnovnog cilja sigurnosne strategije.

Postoje četiri koraka procjene rizika:

1. identifikacija

2. analiza

3. vrednovanje

4. obrada rizika

Kod faze identifikacije rizika zahtijeva se identifikacija sigurnosnih rizika koji proizlaze iz svih aspekata analize okoline i pozicioniranje sigurnosti u poduzeću. Identifikacija mora uključivati sve prijetnje (rizike), bez obzira jesu li ili nisu pod kontrolom poduzeća.

Glavni cilj kod analize rizika je odvajanje manje prihvatljive rizike od glavnih rizika i postupanje s njima.

Vrednovanje rizika uključuje usporedbu stupnja rizika određenog tijekom procesa analize prema prethodno utvrđenim kriterijima rizika.

Faza obrade rizika uključuje identificiranje opcija za postupke, procjenu tih rizika, pripremu planova za tretiranje rizika i njihovu implementaciju. [3]

2.2. Upravljanje poslovnim procesima

Temeljni cilj svakog poduzeća je stvaranje vrijednosti. Korporativnu sigurnost prema Ivandić-Vidović (2011.) svrstavamo u potporne procese.[4] Poslovni sustavi današnjice moraju identificirati, kategorizirati, modelirati, pratiti i mjeriti poslovne procese prema kritičnim čimbenicima uspješnosti. Zbog toga svaka organizacija razvija sustav upravljanja poslovnim procesima, koji omogućuje kontinuirano upravljanje i nadzor poslovnih procesa. Dobivene

[3] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 40.
[4] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 43.

rezultate menadžment koristi za usporedbu s konkurencijom i praćenje uspješnosti provedbe strategije. Proces se definira kao skup aktivnosti koji koriste jedan ili više inputa i kreiraju rezultat vrijednosti za kupca.[5]

Opća podjela procesa prema vrsti posla koje obavlja neko poduzeće je na:

- upravljačke
- temeljne
- potporne poslovne procese[6]

S sigurnosnog stajališta tek neznatne štete koje bi prouzročili nezadovoljni pojedinci, dok je situacija danas mnogo gora. U današnjici se susrećemo s napadima organiziranih skupina čiji je cilj ugrožavanje poslovanja poduzeća ili uništavanje cijele organizacije. Kako bi se ovakav događaj spriječio organizacije moraju zaštititi svoje upravljačke, temeljne i potporne poslovne procese. Kako bi se to postiglo važno je da je sigurnosna strategija usklađena s poslovnom strategijom poduzeća i ostalim funkcijskim strategijama.

Faze upravljanja polovnim procesima korporativne sigurnosti su:

- dizajn
- implementacija
- kontrola procesa korporativne sigurnosti[7]

Korporativna sigurnosti u poduzeću ima važnu ulogu u ostvarivanju postavljenih strateških ciljeva. Iz tog razloga potrebno je ustrojiti organizacijsku jedinicu korporativne sigurnosti s jasnim odgovornostima i ovlaštenjima u ispunjavanju svojih temeljnih zadataka. Kod poduzeća s manjim brojem djelatnika potrebno je ustrojiti odbor za sigurnost ili imenovati menadžera sigurnosti koji će izravno odgovarati vrhovnom menadžmentu. U velikim

[5] Hammer M., Champy J. (2004.) „Reinženjering tvrtke“, Zagreb, MATE str. 37.
[6] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 47.
[7] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 67.

poduzećima za to se koristi organizacijska jedinica integralne sigurnosti, koja se dalje raščlanjuje na poslove sigurnosti i zaštite.

Menadžer sigurnosti je izravno odgovoran za upravljanje poslovnim procesima korporativne sigurnosti. U današnje vrijeme postoji sve veća potreba za kompetentnim osobama za upravljanje sigurnosnim procesima u poduzeću. Kompetencije koje mora posjedovati i znati demonstrirati su znanja, vještine, sposobnosti i osobne karakteristike. Uz sve navedeno važno je i da posjeduje menadžerske vještine (motivacija, karizma, emocionalna inteligencija, upornost, poštenje, razvijene komunikacijske vještine, visoka razina odgovornosti, prepoznavanje i rješavanje problema, profesionalno znanje, inovativnost u radu, praćenje i komunikacija s okolinom poduzeća (vanjskom i unutarnjom), organiziran i ambiciozan).

Voditelj informacijske sigurnosti zadužen je da premosti poteškoće između informatike, sigurnosti, poslovnih jedinica i vrhovnog menadžmenta. Naime, dokazano je da u praksi postoje poteškoće između informatičke tehnologije i poslovnih jedinica, te između informatičke tehnologije i vrhovnog menadžmenta. Informacijska sigurnost često je izolirana od poslovnih jedinica, informatičke tehnologije i vrhovnog menadžmenta.[8]

3. Normativni okvir korporativne sigurnosti

3.1. Informacijska sigurnost

Jedan od temelja za djelovanje i funkcioniranje ljudskog društva su informacije. Važno je napomenuti da podatak i informacija nisu sinonimi. Podatak je činjenica za koju se zna da se dogodila, da postoji ili da je istinita odnosno činjenica koja se navodi da se njome što dokaže[9] dok je informacija obavijest o činjenicama, izvještaj o čemu, odnosno podaci u bilo kojem stupnju obrade podataka.[10] Znači, informacija je obrađeni podatak.

[8] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 74.
[9] Anić V. (2003.) „Veliki rječnik hrvatskog jezika“, Zagreb, Novi Liber, str. 1060.
[10] Anić V., Goldstein I. (2002.) „Rječnik stranih riječi“, Zagreb, Novi Liber, str. 597.

Poslovnu informaciju predstavlja svaka informacija potrebna za obavljanje poslovnih aktivnosti te za ostvarivanje poslovnih interesa i ciljeva poslovnog subjekta.[11]

Poslovne informacije temeljni su resurs svakog poslovnog sustava, te mu posjedovanje informacija daje prednost u odnosu na konkurente. Informacije omogućuju prepoznavanje i iskorištavanje poslovnih prilika, donošenje kvalitetnih odluka, poboljšanje produktivnosti te uočavanje tržišnih trendova i prilagođavanje na njih, što u konačnici dovodi do ostvarenja poslovnog uspjeha i boljeg pozicioniranja u odnosu na konkurente. Iz tog razloga svako poduzeće stvara i razvija vlastito područje poslovnih podataka i informacija.

Informacijska sigurnost je 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.

Povjerljivost informacija znači da je informacija dostupna samo osobama koje imaju ovlaštenje za njezino korištenje. Integritet je zaštita podataka od namjernog ili slučajnog neovlaštenog mijenjanja, a dostupnost je jamstvo ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku.[12] Informacijska i informatička sigurnost su dva različita pojma. Informacijska sigurnost obuhvaća zaštitu svih informacija, bez obzira u kakvom obliku one bile.

Zakon o informacijskoj sigurnosti utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područje informacijske sigurnosti te tijela nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.[13] Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i regionalne samouprave te na sve pravne i fizičke osobe koje u svom djelovanju koriste ili imaju pristup klasificiranim i neklasificiranim podacima.

11 Javorović B., Bilandžić M. (2007.) „Poslovne informacije i business intelligence, Zagreb, Golden marketing-Tehnička knjiga, str. 116.
12 Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 94.
13 Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 95.

Zakon o zaštiti osobnih podataka odnosi se na područje informacijske sigurnosti i utvrđuje zaštitu osobnih podataka o fizičkim osobama, a primjenjuje se na obradu osobnih podataka od strane državnih tijela, tijela jedinica lokalne i regionalne samouprave te na sve pravne i fizičke osobe i predstavništva koja obrađuju osobne podatke.[14]

Zakon o zaštiti i tajnosti podataka propisuje mjere i postupke za utvrđivanje, upotrebu i zaštitu podataka, koji predstavljaju profesionalnu i poslovnu tajnu.[15]

Zakon o elektroničkoj ispravi uređuje pravo fizičkih i pravnih osoba na upotrebu elektroničke isprave u poslovnim djelatnostima. On sadrži odredbe koje se odnose na informacijsku sigurnost, a propisuje mjere koje se moraju primijeniti u odnosu na elektroničku arhivu s ciljem ostvarenja sigurnosti elektroničkih isprava i podataka pohranjenih u njima.[16]

Zakon o sigurnosno - obavještajnom sustavu Republike Hrvatske[17] uključuje sustavno prikupljanje, analize, obrade i ocijene podataka značajnih za državnu sigurnost koji su nužni za donošenje odluka značajnih za ostvarivanje državnih interesa u području državne sigurnosti. Tim zakonom se osniva Sigurnosno – obavještajna agencija i Vojno sigurnosna obavještajna agencija, te Ured Vijeća za nacionalnu sigurnost.

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo odgovorno za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u Republici Hrvatskoj, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.[18]

[14] NN broj: 103/03, 118/06 i 41/08
[15] NN broj: 108/96 i 79/07
[16] NN broj: 150/05
[17] NN broj: 79/06 i 105/06
[18] Ivandić Vidović D.,Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 96.

Zakon o sigurnosnim provjerama[19] utvrđuje sustav sigurnosne provjere osoba koje ostvaruju pristup klasificiranim podacima.

Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite poslovnih kategorija osobnih podataka[20] propisuje mjere održavanja i provjere ispravnosti rada računalne, telekomunikacijske i programske opreme, te sustava za vođenje zbirki posebnih kategorija osobnih podataka i osiguranje radnih prostorija u kojima je smještena oprema.

Uredba o mjerama informacijske sigurnosti[21] propisuje mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima.

Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima[22] propisuje osobe za koje se provodi sigurnosna provjera, vrste i postupci sigurnosne provjere.

Pravilnikom o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost[23] su utvrđeni kriteriji za ustrojavanje radnih mjesta i imenovanje savjetnika za informacijsku sigurnost.

Odluka o primjerenom upravljanju informacijskim sustavom[24] propisuje obveze kreditnih institucija koje se odnose na upravljanje informacijskim sustavom.

Odluka o upravljanju rizicima[25] utvrđuje obvezu kreditnih institucija na primjereno upravljanje informacijskim sustavom i njegovim rizikom.

Svaki poslovni subjekt prikuplja i obrađuje određenu vrstu podataka. Za neke od tih podataka postoji zakonska obveza njihove zaštite, dok će za druge podatke biti u interesu poslovnog subjekta da oni ostanu povjerljivi, cjeloviti i raspoloživi. U današnjici informacijski sustavi izloženi su različitim sigurnosnim

[19] NN broj: 85/08
[20] NN broj: 139/04
[21] NN broj: 46/08
[22] NN broj: 72/07
[23] NN broj: 100/08
[24] NN broj: 37/10
[25] NN broj: 1/09, 41/09, 75/09 i 2/10

prijetnjama koje ugrožavaju cjelokupno poslovanje. Prijetnje mogu dolaziti izvana i iznutra.

Predmet ugroženosti može biti svaka vrijednost u informacijskom sustavu, kao npr.

- Informacijsko – komunikacijski sustav kao cjelina
- Računala i podaci koji se u njima nalaze
- Podaci o poslovnim suradnicima
- Osobni podaci zaposlenika
- Evidencije i baze podataka
- Informacijsko – komunikacijska tehnologija, uključujući računala i mobilne telefone
- Poslovni i proizvodni procesi
- Tehnologija
- Zaposlenici zaposleni u informacijsko – komunikacijskim sustavima
- Tehničko - sigurnosni sustavi
- Intelektualno vlasništvo
- Poslovne organizacije i korisnici informacijsko – komunikacijskih sustava[26]

Uspješna primjena informacijske sigurnosti zahtijeva sustavno upravljanje različitim aspektima informacijske sigurnosti u skladu s odgovarajućim standardima i normama.

Vodeća međunarodna norma za upravljanje informacijskom sigurnošću je norma ISO/IEC 27001:2005. Ona je 2006. godine prihvaćena kao hrvatska

[26] Javorović B. i Bilandžić M. (2007.) „Poslovne informacije i business intelligence“, Zagreb, Golden marketing – Tehnička knjiga, str. 296.

norma, koja definira zahtjeve za uspostavu, održavanje i kontinuirano poboljšavanje sustava upravljanja informacijskom sigurnošću.[27]

Certifikat ISO 27001 ishođen je primjenom norme ISO 27001, njime se potvrđuje da je informacijska sigurnost u poduzeću provedena na najbolji mogući način. Višestruke su prednosti certificiranja, što u konačnici dovodi do poboljšanja poslovnih odnosa.

Norma ISO/IEC 27002:2005 detaljnije opisuje način provedbe pojedinih mjera utvrđenih normom ISO 27001.[28]

Norma ISO/IEC 27005:2008 detaljnije opisuje proces procjene rizika u području informacijske sigurnosti.[29]

3.2. Privatna zaštita

Privatna zaštita je dopuna zaštiti koju predstavlja država putem redarstvenih vlasti. Država nema mogućnosti osigurati nazočnost redarstvenih službenika u svakom trenutku i na svakom mjestu gdje može doći do povrede dobara. Iz tog razloga svaki pojedinac i organizacija dužni su preuzeti odgovornost za vlastitu sigurnost. U današnjici postoji sve više vlasnika poduzeća koji se trude što bolje i potpunije zaštititi svoju imovinu. Temelj sustava privatne zaštite je pravo svakog pojedinca na samozaštitu, dok je samozaštita temelj svake sigurnosti i ona podrazumijeva samo zaštitno djelovanje i ponašanje kako pojedinca, tako i organizacije. „U Republici Hrvatskoj privatna zaštita je prvi put uređena tek 1996. godine, donošenjem Zakona o zaštiti osoba i imovine. Taj Zakon vrijedio je do 2003. godine, nakon čega je stupio na snagu trenutno važeći Zakon o privatnoj zaštiti.“[30] Zakon uređuje način obavljanja djelatnosti privatne zaštite i propisuje uvjete i način rada za obavljanje privatne zaštite. U djelatnost privatne zaštite pripadaju poslovi zaštite osoba i imovine koju ne osigurava država jer su izvan njezinog opsega.

[27] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 98.
[28] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 101.
[29] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 101.
[30] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 103.

Poslovi koji se najčešće pojavljuju u djelatnosti privatne zaštite su:

- osiguranje mirnih prosvjeda i javnih okupljanja
- osiguranje stambenih i poslovnih prostora
- poslovi tjelohranitelja
- zaštita prirodnih dobara i okoliša
- osiguranje u pratnja novca, vrijednosnih papira i dragocjenosti.[31]

Zakon obvezuje na sklapanje ugovora o pružanju usluga privatne zaštite s ciljem pružanja pravne sigurnosti objema ugovorenim stranama. Nesklapanje ugovora u pisanom obliku predstavlja prekršaj.

Pojam tjelesna zaštita obuhvaća zaštitu osoba i imovine koja se obavlja osobnom prisutnošću osobe zadužene za poslove zaštite i njezine zaštitne aktivnosti.

Tehnička zaštita je skup radnji za posrednu ili neposrednu zaštitu ljudi i imovine. Provodi se tehničkim sredstvima i sustavima tehničke zaštite s osnovnom namjerom sprječavanja protuprovalnih radnji usmjerenim prema štićenim osobama i imovini.

3.3. Zaštita intelektualnog vlasništva

Pojam intelektualno vlasništvo obuhvaća skup prava na proizvodima ljudskog uma kao nematerijalnim dobrima. S stajališta poslovnog subjekta intelektualno vlasništvo je nematerijalna imovina tvrtke kojoj se pridaje knjigovodstvena vrijednost i u koju se ulaže s ciljem ostvarenja što veće dobiti.[32] Činjenica je da je intelektualno vlasništvo danas postalo jedna od najvrednijih stavki u imovini poslovnog subjekta, potrebno ga je zaštititi od zlouporabe i njime planski upravljati.

[31] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 104.
[32] Korper D., „Pravo intelektualnog vlasništva“ u Mintas Hodak Lj., (2010) „Pravno okruženje poslovanja“, Zagreb, MATE, str. 172. – 173.

Podjela prava intelektualnog vlasništva:

- pravo industrijskog vlasništva
- autorsko pravo
- autorskom pravu srodna prava[33]

Prava iz intelektualnog vlasništva mogu se prenositi te biti predmet nasljeđivanja, zaloga i ovrhe. Autorsko pravo može se prenijeti putem autorsko-pravnih ugovora, dok se za prenošenje pojedinih oblika industrijskog vlasništva koristi ugovor o licenciji. Njime se obvezuje da će davatelj licencije ustupiti stjecatelju licencije pravo iskorištavanja izuma, znanja, iskustva, žiga i uzorka, a stjecatelj licencije se obvezuje da će mu za to platiti određenu naknadu. Za intelektualno vlasništvo u Republici Hrvatskoj nadležan je Državni zavod za intelektualno vlasništvo, gdje se vrši i sama registracija intelektualnog vlasništva. Osim toga Državni zavod za intelektualno vlasništvo provodi propisane postupke za priznavanje svih oblika intelektualnog vlasništva, pruža usluge pretraživanja informacija iz područja intelektualnog vlasništva te promiče zaštitu i poštivanje prava intelektualnog vlasništva.

Pravo industrijskog vlasništva označava sva prava kojima proizvođač štiti od konkurenata svoje poslovne interese, položaj na tržištu te sredstva uložena u istraživanje, razvoj i promociju. Ovaj oblik intelektualnog vlasništva obuhvaća:

- patente
- žigove
- industrijski dizajn
- oznake zemljopisnog podrijetla
- oznake izvornosti
- topografija poluvodičkih proizvoda[34]

[33] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 151.

Autorsko pravo štiti književna, znanstvena i umjetnička djela, dok se autorskom pravu srodna prava odnose na zaštitu umjetničkog izražaja i zaštitu organizacijskih, poslovnih i financijskih ulaganja u izvođenje, proizvodnju i distribuciju autorskih djela.[35]

Autorsko pravo obuhvaća:

- moralna prava autora
- imovinska prava autora
- druga prava autora[36]

Autorsko pravo i srodna prava u Republici Hrvatskoj uređeni su Zakonom o autorskom pravu i srodnim pravima[37], te nizom podzakonskih akata. Autorsko pravo traje za života autora i sedamdeset godina nakon njegove smrti, bez obzira kada je autorsko djelo zakonito objavljeno.

Srodna prava su:

- prava umjetnika izvođača na njihovim izvedbama
- prava proizvođača fonograma na njihovim fonogramima
- prava filmskih producenata na njihovim videogramima
- prava organizacija na radiodifuziju na njihovim emitiranjima
- prava nakladnika na njihovim izdanjima
- prava proizvođača baza podataka na njihovim bazama podataka[38]

Žig je isključivo pravo priznato za znak koji služi za razlikovanje proizvoda ili usluga jednog poduzetnika od proizvoda i usluga ostalih sudionika u gospodarskom prometu. Nositelj žiga posjeduje pravo korištenja tog znaka za

[34] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 152.
[35] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 152.
[36] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 156.
[37] NN broj: 167/03 i 79/07
[38] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 156.

označavanje svojih proizvoda ili usluga, te time on ne predstavlja samo simbol proizvoda i usluga već i simbol reputacije koju poduzetnik ima od potrošača.[39] Iz toga proizlazi da je registracija žiga efikasan način da proizvođači, tj. pružatelji usluga zaštite sredstva uložena u marketing svojih proizvoda i usluga. Postoje različiti žigovi, a osnovna podjela je na individualne i zajedničke. Individualni je kao što i samo ime govori onaj koji se odnosi na pojedinačnu pravnu ili fizičku osobu, a zajednički se odnosi na udruženje proizvođača, pružatelja usluga. Jamstveni žig označava kakvoću, podrijetlo, način proizvodnje ili druga zajednička obilježja proizvoda ili usluga. Postupak stjecanja prava na žig i njegova pravna zaštita utvrđena je Zakonom o žigu[40] i Pravilnikom o žigu.[41] Zakon o žigu propisuje da se kao žig može zaštititi svaki znak koji se može grafički prikazati, te riječi, crteži slova, osobna imena i kombinacije svih navedenih znakova, pod uvjetom da su prikladni za razlikovanje proizvoda ili usluga jednog poduzetnika od ostalih. U Republici Hrvatskoj stječe se registracijom, tj. upisom žiga u registar žigova. Nositelj registriranog žiga može biti svaka fizička i pravna osoba. Zaštita registriranog žiga traje u razdoblju od deset godina računajući od dana podnošenja prijave za registraciju žiga. Registracija se može produljivati neograničeno, a provodi se za razdoblja po deset godina.

Industrijski dizajn podrazumijeva vanjski izgled proizvoda u cijelosti ili djela proizvoda, koji proizlazi iz njegovih obilježja crta, obrisa, boja, oblika,teksture, te kombinacije navedenih obilježja. Upravo dizajn čini proizvod privlačnim, dopadljivim ili poželjnim i kao takav bitno pridonosi prodaji proizvoda ili povećanju njegove komercijalne vrijednosti. Registrirani industrijski dizajn daje nositelju industrijskog dizajna isključivo pravo korištenja, odnosno isključivo pravo sprječavanja drugih da dizajn neovlašteno kopiraju ili oponašaju. Ukoliko dođe do kopiranja ili oponašanja industrijskog dizajna ovlašteni nositelj može spriječiti korištenje dizajna i ishoditi naknadu za štetu koju je eventualno pretrpio zbog neovlaštene uporabe zaštićenog dizajna. Dizajn zaštićen industrijskim

[39] Zlatović D. (2010.) „Intelektualno vlasništvo i marketing“, Zagreb, INMAG, str.50.
[40] NN broj: 173/03, 54/05, 76/07, i 30/09
[41] NN broj: 117/07

dizajnom, može biti i autorsko djelo, ako ispunjava uvjete za zaštitu autorskih djela. U tom slučaju ima autorsko pravnu zaštitu od trenutka stvaranja u bilo kojem obliku, bez obzira hoće li naknadno biti pokrenut i proveden postupak za registraciju industrijskog dizajna. Postupak stjecanja prava za zaštitu industrijskog dizajna i uvjeti propisani su Zakonom o industrijskom dizajnu[42] i Pravilnikom o industrijskom dizajnu.[43] Osnovni uvjeti koji dizajn mora zadovoljiti za priznavanje zaštite su novost i individualni karakter dizajna. Dizajn se smatra novim ako nijedan istovjetni dizajn nije bio učinjen dostupan javnosti prije datuma prijave za registraciju industrijskog dizajna ili ako je zatraženo pravo prvenstva. Dizajni se smatraju istovjetnima ako se njihova obilježja razlikuju u nebitnim pojedinostima. Dizajn ima individualni karakter ako se ukupni dojam koji ostavlja na upućenog korisnika razlikuje od ukupnog dojma koji je na korisnika ostavio bilo koji drugi dizajn. Fizička osoba koja je stvorila dizajn je dizajner i njegovo moralno pravo je da kao takav bude naveden u svim dokumentima, te prilikom javnog izlaganja njegov dizajna. To pravo dizajnera je neprenosivo. Ukoliko je u stvaranju dizajna sudjelovalo više dizajnera, navedeno moralno pravo pripada svim dizajnerima. Dizajner je ovlašteni za pokretanje postupka i stjecanje industrijskog dizajna. Ukoliko je dizajn stvorio dizajner zaposlenik prema uputama poslodavca, za pokretanje postupka i stjecanje industrijskog dizajna ovlašten je poslodavac. Državni zavod za intelektualno vlasništvo nositelju industrijskog dizajna na zahtjev izdaje ispravu o industrijskom dizajnu, pod uvjetom da je plaćena propisana naknada troškova za izdavanje isprave. Zaštita industrijskog dizajna traje pet godina računajući od datuma podnošenja prijave i može se produljivati za razdoblja po pet godina, ali najdulje do dvadeset i pet godina od datuma podnošenja prijave.

Patent je pravo priznato nositelju patenta za određeni izum koji daje novo rješenje nekog tehničkog problema, a može se odnositi na određeni postupak, primjenu ili određeni proizvod.[44] Zaštita izuma patentom u Republici Hrvatskoj

[42] NN broj: 173/03, 54/05,76/07 i 30/09
[43] NN broj: 72/04 i 117/07
[44] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 173.

utvrđena je Zakonom o patentu[45] i Pravilnikom o patentu.[46] Zakon o patentu utvrđuje da je patent isključivo pravo koje štiti nositelja patenta u pogledu gospodarskog iskorištavanja izuma. Da bi neki izum mogao biti zaštićen patentom mora zadovoljavati tri uvjeta: mora biti nov, mora imati inventivnu razinu i mora biti industrijski primjenjiv. Pravo na stjecanje patenta ima izumitelj ili njegov pravni sljedbenik. Izumitelj je osoba koja je svojim stvaralačkim radom stvorila izum. Njegovo je moralno pravo da je naveden u svojstvu izumitelja u prijavi patenta i svim ispravama koje se izdaju za priznavanje patenta, te u registru prijava i registru patenta. Ovo moralno pravo je neprenosivo, ako je izum stvoren zajedničkim radom dvaju ili više izumitelja tada je pravo na patent zajedničko i pripada izumiteljima. Patent traje dvadeset godina računajući od dana podnošenja prijave patenta. U Zakonu o patentu navodi se konsenzualni patent kao posebni oblik patentne zaštite. On se priznaje bez potpunog ispitivanja, na temelju sporazuma *(konsenzusa)* javnosti, ukoliko protiv njega ne postoje prigovori. Zaštita konsenzusnim patentom može trajati najviše deset godina a postupak je brži, jednostavniji i jeftiniji od postupka za dobivanje klasičnog patenta. Važno je napomenuti da konsenzualni patent pruža zaštitu samo u vremenu dok mu se nitko ne protivi.

Oznake izvornosti su nazivi područja, određenog mjesta ili zemlje koja se koristi za označavanje proizvoda ili usluga koji odatle potječu i čija kvaliteta nastaje pod utjecajem posebnih prirodnih i ljudskih čimbenika određene zemljopisne sredine. Oznaka zemljopisnog podrijetla je naziv regije, određenog mjesta ili zemlje koja se koristi za označavanje proizvoda i usluga koji odatle potječu i imaju određenu kakvoću. One se štite kroz sustav intelektualnog vlasništva, jer pridonose povećanju komercijalne vrijednosti proizvoda i usluga određenog područja. Zaštita oznake izvornosti i zemljopisnog podrijetla u Republici Hrvatskoj regulirana je Zakonom o oznakama zemljopisnog podrijetla i oznakama izvornosti proizvoda i usluga[47], te Pravilnikom o oznakama

[45] NN broj: 173/03, 54/05, 87/05, 76/07, 30/09 i 128,10
[46] NN broj: 117/07 i 03/11
[47] NN broj: 173/03, 186/03, 54/05 i 76/07

zemljopisnoga podrijetla i oznakama izvornosti proizvoda i usluga[48]. Postupak za registraciju oznaka izvornosti i oznaka zemljopisnog podrijetla proizvoda ili usluga i postupak za njihovo proglašenje nevažećim provodi Državni zavod za intelektualno vlasništvo. Njihova zaštita ostvaruje se upisom u registar oznaka zemljopisnog podrijetla te upisom u registar oznaka izvornosti, ovisno o kojoj kategoriji je riječ. Trajanje oznake zemljopisnog podrijetla i oznake izvornosti proizvoda i usluga nije ograničeno, dok pravo korištenja oznake zemljopisnog podrijetla i oznake izvornosti traje deset godina od dana upisa ovlaštenog korisnika u registar. To pravo se na zahtjev ovlaštenog korisnika može produžavati neograničeno, ali pritom treba poštivati propisane uvjete.

Zaštita topografije poluvodičkih proizvoda je prikaz trodimenzionalnog uzorka, tj. rasporeda slojeva vidljivog, izolacijskog u poluvodičkog materijala u poluvodičkim proizvodima namijenjenima izvođenju određene elektroničke funkcije.[49] Ona je nužna jer razvoj novih poluvodičkih proizvoda zahtjeva intelektualne napore i znatna materijalna ulaganja, dok je s druge strane kopiranje postojećih industrijskih rješenja vrlo jednostavno i jeftino. Nositelju prava ona daje isključivo pravo davanja odobrenja ili zabrane umnožavanja topografija, uvoza i prodaje topografije ili poluvodičkog proizvoda proizvedenog korištenjem zaštićene topografije. Njihova zaštita uređena je Zakonom o zaštiti topografija poluvodičkih proizvoda[50], te Pravilnikom o zaštiti topografija poluvodičkih proizvoda[51]. Topografija se štiti isključivim pravima ako je ista rezultat nečijeg intelektualnog napora i ako nije uobičajena u industriji poluvodiča. Njezina zaštita provodi se u opsegu u kojem kombinacija elemenata u cjelini ispunjava uvijete izvornosti i noviteta u industriji poluvodiča. Pravo na zaštitu topografije imaju fizičke osobe pod uvjetom da su njezini stvaratelji, a ako je topografiju stvorilo više osoba zajedno, također je zajedničko i njihovo pravo na zaštitu. Ako je topografija stvorena u radnom odnosu, pravo na zaštitu ima poslodavac stvaratelja topografije. Postupak za registraciju topografije pokreće se prijavom koja se podnosi Državnom zavodu za intelektualno

[48] NN broj: 72/04 i 117/07
[49] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 185.
[50] NN broj: 173/03, 76/07 i 30/09
[51] NN broj: 72/04 i 117/07

vlasništvo, koji zatim izdaje podnositelju prijave rješenje o registraciji topografije, koja se tada upisuje u registar topografija, a podaci iz registra objavljuju se u službenom glasilu Državnog zavoda za intelektualno vlasništvo. Isključiva prava prestaju važiti istekom roka deset godina, osim u slučaju da topografija nije bila komercijalno iskorištena u svijetu, u tom slučaju istječu nakon petnaest godina.

4. Zaštita podataka

4.1. Zaštita osobnih podataka

Zaštita privatnosti pojedinca ne smije biti zanemarena, posebno ne u uvjetima današnjice kada je vrlo razvijeno informacijsko društvo i kada postoje brojne mogućnosti zlouporabe osobnih podataka s jedne strane, dok druge strane postoje propisi koji zahtijevaju posebnu zaštitu ovakve vrste podataka. Činjenica je da se svaki poslovni subjekt u svojem poslovanju susreće s nekom vrstom osobnih podataka (najčešće to budu podaci o zaposlenicima). Nužno je da osobe zadužene za poslove korporativne sigurnosti raspolažu sa znanjima o temeljnim pravima i obvezama u vezi sa zaštitom osobnih podataka. Pod pojmom osobni podatak podrazumijeva se svaka informacija koja se odnosi na identificiranu fizičku osobu.

4.1.1. Pravo na zaštitu osobnih podataka

Temeljno pravo svakog čovjeka je pravo na zaštitu osobnih podataka, te je zaštita osobnih podataka u Republici Hrvatskoj osigurana svakoj fizičkoj osobi bez obzira na njezino državljanstvo i prebivalište, te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju i drugim osobinama.[52]

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

[52] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 188.-189.

Zakon o zaštiti podataka[53] temeljni je propis u Republici Hrvatskoj, koji uređuje zaštitu osobnih podataka, a primjenjuje se na obradu osobnih podataka od strane državnih tijela, tijela lokalne i regionalne samouprave, te pravnih i fizičkih osoba koje obrađuju osobne podatke. Iznimka je da se zakon ne primjenjuje na obradu osobnih podataka koju provode fizičke osobe isključivo za osobnu primjenu ili potrebe kućanstva.

4.1.2. Obrada osobnih podataka

Obrada osobnih podataka obuhvaća svaku radnju ili skup radnji izvršen na osobnim podacima. Prilikom prikupljanja osobnih podataka ispitanik mora biti upoznat sa svrhom prikupljanja podataka, koja je u skladu sa zakonom. Osobni podaci trebaju biti točni, potpuni i ažurni, te trebaju biti bitni za postizanje utvrđene svrhe i ne smiju se prikupljati u većem opsegu nego što je to nužno, da bi se postigla utvrđena svrha. Čuvanje osobnih podataka odvija se u obliku koji dopušta identifikaciju ispitanika i ne dulje nego je to potrebno za svrhu u koju se podaci prikupljaju i dalje obrađuju. Kada ispitanik dozvoli prikupljanje i obradu osobnih podataka, on ima pravo u svako doba odustati od dane privole i zatražiti prestanak daljnje obrade njegovih podataka.

4.1.3. Obrada posebnih kategorija podataka

Zakonom je zabranjeno prikupljanje i daljnja obrada takozvanih posebnih kategorija podataka. U posebne kategorije podataka ubrajaju se podaci o rasnom ili etičkom podrijetlu, političkom stajalištu, vjerskim uvjerenjima, zdravlju i spolnom životu i slično. Prikupljanje i obrada takvih podataka dopušteni su samo u iznimnim slučajevima uz poduzete posebne mjere zaštite. Mjere, sredstva i uvjeti pohranjivanja, osiguranja i zaštite posebnih kategorija osobnih podataka propisani su Uredbom o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka.[54]

[53] NN broj: 103/03, 118/06 i 41/08
[54] NN broj: 139/04

4.1.4. Voditelj zbirke osobnih podataka i njegovo djelovanje

Voditelj zbirke osobnih podataka je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka. Zbirka osobnih podataka je skup osobnih podataka koji je dostupan prema posebnim kriterijima i neovisno o tome je li sadržan u računalnim bazama osobnih podataka ili se vodi primjenom drugih tehničkih pomagala ili ručno. Voditelj zbirke osobnih podataka ima ovlasti povjeriti drugoj fizičkoj ili pravnoj osobi poslove u svezi s obradom osobnih podataka, ta osoba naziva se izvršitelj obrade osobnih podataka. Izvršitelj obrade mora biti registriran za obavljanje takve djelatnosti i mora imati jamstva u pogledu ostvarivanja odgovarajućih mjera zaštite osobnih podataka. Poslovi obrade podataka između voditelja zbirke i izvršitelja obrade utvrđuju se ugovorom.

4.1.5. Informiranje ispitanika i davanje podataka korisnicima

Prije prikupljanja bilo kojih osobnih podataka voditelj zbirke ili izvršitelj obrade dužni su informirati ispitanika čije podatke prikupljaju. Voditelj zbirke također je dužan informirati ispitanika i o davanju osobnih podataka na korištenje drugim korisnicima. Voditelj zbirke osobnih podataka ovlašten je osobne podatke dati na korištenje drugim korisnicima na temelju pisanog zahtjeva korisnika, ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene djelatnosti korisnika.

4.1.6. Iznošenje osobnih podataka iz Republike Hrvatske

Zbirke osobnih podataka smiju se iznositi iz Republike Hrvatske u svrhu daljnje obrade samo ako država ili međunarodna organizacija u koju se osobni podaci iznose ima osiguranu adekvatnu razinu zaštite. Ako postoji sumnja o odgovarajuće uređenoj zaštiti osobnih podataka u zemlji u koju se podaci trebaju iznijeti, voditelj zbirke osobnih podataka je dužan prije iznošenja podataka iz Republike Hrvatske pribaviti mišljenje Agencije za zaštitu osobnih podataka.

4.1.7. Zbirke i evidencije osobnih podataka

Voditelj zbirke osobnih podataka za svaku zbirku osobnih podataka koju vodi, dužan je uspostaviti i voditi evidenciju koja sadrži temeljne informacije o zbirci osobnih podataka. Evidencije se dostavljaju Agenciji za zaštitu osobnih podataka, gdje se onda objedinjuju u Središnjem registru. Prije uspostave zbirke osobnih podataka, voditelji zbirke dužni su o namjeravanoj uspostavi zbirke osobnih podataka obavijestiti Agenciju za zaštitu podataka. Agenciju za zaštitu podataka dužni su obavijestiti i o svakoj daljnjoj namjeravanoj obradi tih podataka i to prije poduzimanja bilo kakvih aktivnosti obrade.

Evidencije osobnih podataka sadrže temeljne podatke o zbirci osobnih podataka. Upisivanje podataka u evidenciju zbirke osobnih podataka i druge poslove vezane uz evidenciju zbirke provodi osoba odgovorna za vođenje pojedine zbirke osobnih podataka. Evidencije se mogu voditi ručno ili sredstvima za automatsku obradu podataka. Način vođenja evidencije osobnih podataka detaljno je propisan Uredbom o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka.[55]

4.1.8. Mjere zaštite osobnih podataka

Osobni podaci u zbirkama osobnih podataka moraju biti pod odgovarajućom zaštitom, radi sprječavanja slučajne ili namjerne zlouporabe, uništenja, gubitka, te neovlaštenih promjena ili dostupnosti. Voditelj zbirke osobnih podataka i korisnik dužni su poduzeti tehničke i kadrovske, te organizacijske mjere zaštite osobnih podataka koje su potrebne da bi se osobni podaci zaštitili.

4.1.9. Nadzor nad obradom osobnih podataka

Nadzor nad obradom osobnih podataka provodi Agencija za zaštitu osobnih podataka na zahtjev ispitanika ili po službenoj dužnosti. Zakon obvezuje Agenciju na razmatranje svih zahtjeva koji se odnose na utvrđivanje povrede prava u obradi osobnih podataka i izvješćivanje podnositelja zahtjeva o mjerama koje su poduzete u vezi s utvrđenim činjeničnim stanjem. Agencija ima

[55] NN broj: 105/04

pravo pristupa svim osobnim podacima, bez obzira da li su evidencije o tim podacima objedinjene u središnji registar ili ne. Agencija također ima pravo pristupa svim spisima i dokumentaciji koja se odnosi na obradu osobnih podataka, kao i sredstvima elektronske obrade bez obzira na stupanj njihove tajnosti.

4.2. Zaštita podataka od državnog značaja

Tajnost podataka od državnog značaja regulirana je Zakonom o tajnosti podataka.[56] Navedenim zakonom uveden je jedinstveni sustav utvrđivanja, imenovanja, i zaštite klasificiranih i neklasificiranih podataka, te je propisan postupak utvrđivanja stupnjeva tajnosti i postupak pristupa tajnim podacima te nadzor nad primjenom Zakona.

4.2.1. Određenje temeljnih pojmova

4.2.1.1. Podatak

Podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, usmeno priopćenje ili informacija koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika, pri čemu je vlasnik podatka nadležno tijelo u okviru čijeg djelovanja je podatak nastao.[57]

4.2.1.2. Klasificirani podatak

Klasificirani podaci su oni podaci koje je nadležno tijelo, u propisanom postupku takvima označilo i za koje je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.[58]

[56] NN broj: 79/07
[57] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 198.
[58] Mišević P., materijali s predavanja, kolegij Menadžment poslovne sigurnosti, ppt: Zakonski i podzakonski propisi u radu s klasificiranim podacima

4.2.1.3. Neklasificirani podatak

Neklasificirani podaci su podaci bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.[59]

4.2.1.4. Stupnjevi tajnosti

Zakon o tajnosti podataka predviđa četiri stupnja tajnosti podataka:

1. „vrlo tajno“
2. „tajno“
3. „povjerljivo“
4. „ograničeno“[60]

Stupnjevi tajnosti „vrlo tajno“, „tajno“ i „povjerljivo“ međusobno se razgraničavaju na temelju stupnja štete koja bi nastala za nacionalnu sigurnost i vitalne interese Republike Hrvatske, ako bi ti podaci bili neovlašteno otkriveni. Tako je stupanj tajnosti „vrlo tajno“ predviđen za podatke čijim bi neovlaštenim otkrivanjem nastala nepopravljiva šteta, stupanj tajnosti „tajno“ utvrđen je za podatke čijim bi neovlaštenim otkrivanjem nastala teška šteta, dok je stupanj tajnosti „povjerljivo“ utvrđen za podatke čijim bi neovlaštenim otkrivanjem nastala šteta za nacionalnu sigurnost i vitalne interese Republike Hrvatske. Stupanj tajnosti „ograničeno“ predviđen je za podatke čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u području obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ako su podaci od sigurnosnog interesa za Republiku Hrvatsku.[61]

[59] Mišević P., materijali s predavanja, kolegij Menadžment poslovne sigurnosti, ppt: Zakonski i podzakonski propisi u radu s klasificiranim podacima
[60] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 199.
[61] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 199.-200.

4.2.1.5. Klasifikacija i deklasifikacija podataka

Postupak utvrđivanja jednog od stupnjeva tajnosti podataka tajnosti, s obzirom na stupanj ugroze i područje zaštićenih vrijednosti, naziva se klasifikacija podataka. Nasuprot tome, postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran odgovarajućim stupnjem tajnosti naziva se deklasifikacija podataka.

Klasificiranje podataka stupnjevima tajnosti „vrlo tajno“ i „tajno“ mogu provoditi samo:

- predsjednik Republike Hrvatske
- predsjednik Hrvatskog sabora
- predsjednik Vlade Republike Hrvatske
- ministri
- Glavni državni odvjetnik
- Načelnik Glavnog stožera Oružanih snaga Republike Hrvatske
- čelnici tijela sigurnosno-obavještajnog sustava Republike Hrvatske, te
- osobe koje oni za tu svrhu ovlaste [62]

Klasificiranje podataka stupnjevima tajnosti „povjerljivo“ i „ograničeno“ mogu provoditi uz gore navedene i čelnici ostalih državnih tijela.

4.2.1.6. Pristup klasificiranim i neklasificiranim podacima

4.2.1.6.1. Certifikat

S klasificiranim podacima mogu raditi samo osobe kojima je to nužno za obavljanje poslova iz njihovog djelokruga i koje imaju uvjerenje o sigurnosnoj provjeri, koje se naziva sigurnosni certifikat. Zahtjev za izdavanje certifikata podnosi se Uredu Vijeća za nacionalnu sigurnost. Certifikat se izdaje za

[62] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 200.

stupnjeve tajnosti „vrlo tajno“, „tajno“ i „povjerljivo“ na rok od pet godina. Certifikat predstavlja neklasificirani podatak. Ured Vijeća za nacionalnu sigurnost izdaje certifikat ako utvrdi da ne postoje sigurnosne zapreke za pristup klasificiranim podacima. Postojanje sigurnosnih zapreka utvrđuje se na temelju sigurnosne provjere koju obavlja nadležna sigurnosno-obavještajna agencija.[63]

4.2.1.6.2. Pristup podacima bez izdanog certifikata

Prema Zakonu utvrđene su određene kategorije osoba koje imaju pravo na pristup klasificiranim podacima bez prethodno izdanog certifikata, pri čemu je pristup navedenim osobama ograničen samo na podatke iz njihovog djelokruga.

Za pristup klasificiranim podacima certifikat ne moraju imati:

- Saborski zastupnik
- Ministar
- Državni tajnik središnjega državnog ureda
- Sudac
- Glavni državni odvjetnik[64]

Sve navedene osobe dužne su prije pristupanja klasificiranim podacima potpisati izjavu kojom potvrđuju da su upoznate s odredbama Zakona i drugih propisa, kojima se uređuje zaštita klasificiranih podataka te se obvezuju raspolagati klasificiranim podacima u skladu s propisima.

4.2.1.7. Pristup neklasificiranim podacima

Pravo pristupa neklasificiranim podacima imaju osobe kojima je to nužno u službene svrhe radi obavljanja poslova iz njihovog djelokruga.

[63] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 202.
[64] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 202.

4.2.1.8. Dužnost čuvanja tajnosti podataka

Sve osobe koje imaju pristup ili postupaju s klasificiranim i neklasificiranim podacima, dužni su čuvati tajnost klasificiranog podatka za vrijeme i nakon prestanka obavljanja dužnosti, sve dok je podatak utvrđen jednim od stupnjeva tajnosti ili dok odlukom vlasnika podatka ne budu oslobođeni obveze čuvanja tajnosti podataka.

4.2.2. Označavanje klasificiranih i neklasificiranih podataka

Način označavanja klasificiranih i neklasificiranih podataka propisan je Uredbom o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima.[65]

4.2.2.1. Označavanje klasificiranih podataka

Označavanje klasificiranih podataka stupnjevima tajnosti provodi se pri nastanku klasificiranih dokumenata ili prilikom periodične procjene stupnja tajnosti podataka. Oznaka stupnja tajnosti klasificiranog podatka označava se na svakoj stranici dokumenta u gornjem desnom kutu, velikim tiskanim slovima. Jednakim stupnjem tajnosti kakvim je označen klasificirani podatak, označava se i omotnica u kojoj se klasificirani podatak prenosi ili pohranjuje. Klasificirani dokument i njegovi pojedini dijelovi ili prilozi mogu biti označeni različitim stupnjevima tajnosti, u tom slučaju cjelina takvog dokumenta označava se najvišim stupnjem tajnosti klasificiranog dokumenta, njegovog pojedinog djela ili priloga.

4.2.2.2. Označavanje neklasificiranih podataka

Neklasificirani podaci označavaju se oznakom „neklasificirano“ pri nastanku dokumenta. Prva stranica dokumenta označava se oznakom „neklasificirano“ velikim tiskanim slovima, u gornjem desnom kutu stranice. Označavanje neklasificiranog podatka provodi se prilikom njegove izrade ili naknadnom obradom.

[65] NN broj: 102/07

4.2.3. Zaštita klasificiranih i neklasificiranih podataka

Način i provedba zaštite klasificiranih i neklasificiranih podataka propisani su Zakonom o informacijskoj sigurnosti.[66] Navedeni zakon utvrđuje mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti te tijela nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. Zakon o informacijskoj sigurnosti primjenjuje se na sve osobe koje ostvaruju pristup ili postupaju s klasificiranim ili neklasificiranim podacima.

Zakon o informacijskoj sigurnosti definira pojam informacijske sigurnosti propisujući kako informacijska sigurnost podrazumijeva 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.[67]

4.2.4. Mjere i standardi informacijske sigurnosti

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama, koje u svom djelokrugu koriste i ostvaruju pristup klasificiranim i neklasificiranim podacima. Mjere i standardi informacijske sigurnosti utvrđuju se sukladno stupnju tajnosti klasificiranih i neklasificiranih podataka.

Mjere informacijske sigurnosti opća su pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjeni sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.[68]

Mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima propisane su Uredbom o mjerama informacijske sigurnosti.[69]

[66] NN broj: 79/07
[67] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 205.
[68] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 205.
[69] NN broj: 46/08

4.2.5. Područja informacijske sigurnosti

Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet cjelina s ciljem sustavne i učinkovite realizacije, donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti. Podjela područja informacijske sigurnosti su:

1. sigurnosna provjera
2. fizička sigurnost
3. sigurnost podataka
4. sigurnost informacijskog sustava
5. sigurnost poslovne suradnje[70]

Standardi područja informacijske sigurnosti propisani su pravilnicima koje je donio Ured Vijeća za nacionalnu sigurnost. Ured Vijeća za nacionalnu sigurnost trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima informacijske sigurnosti, te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

4.2.5.1. Sigurnosna provjera

Sigurnosna provjera je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti, koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima.

4.2.5.2. Fizička sigurnost

Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekata, prostora i uređaja u kojem se nalaze klasificirani podaci.

[70] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 206.

4.2.5.3. Sigurnost podataka

Sigurnost podataka obuhvaća područje informacijske 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 podataka.

4.2.5.4. Sigurnost informacijskog sustava

Sigurnost informacijskog sustava podrazumijeva područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu, te zaštitu cjelovitosti i raspoloživosti informacijskog sustava.

4.2.5.5. Sigurnost poslovne suradnje

Sigurnost poslovne suradnje je područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom, koji obvezuju pravne i fizičke osobe koje ostvaruju pristup klasificiranim i neklasificiranim podacima ili postupaju s njima.

4.2.6. Središnja državna tijela nadležna za informacijsku sigurnost

Središnja državna tijela nadležna za informacijsku sigurnost u Republici Hrvatskoj su:

1. Ured Vijeća za nacionalnu sigurnost

2. Zavod za sigurnost informacijskih sustava

3. CERT[71]

Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost, koje koordinira i trajno usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj, te u razmjeni

[71] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 207.-208.

klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. [72]

Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskog sustava u državnim i ostalim tijelima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.[73]

CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Ustrojava se u Hrvatskoj akademskoj i istraživačkoj mreži CARNet, a usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama kad su povezani s Republikom Hrvatskom. CERT uz sve navedeno usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava, te određuje pravila i načine zajedničkog rada.[74]

4.2.7. Upravljanje rizikom informacijske sigurnosti

Prilikom postupanja s klasificiranim podacima, državna tijela i pravne osobe s javnim ovlastima dužne su upravljati rizikom informacijske sigurnosti. Upravljanje rizikom sastoji se od trajnog procjenjivanja i obrade rizika, radi sprječavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa klasificiranim podacima. Rezultati dobiveni procesom procjenjivanja rizika temelj su za odabir odgovarajućih mjera zaštite od rizika u skladu s prioritetima upravljanja rizicima.

Tijela i pravne osobe prilikom postupanja s klasificiranim podacima imaju dužnost vođenja dnevnika procijene rizika, koji sadrži datum procjene, opis rizika, procjenu i vrijednost utjecaja pojedinog rizika, primijenjene sigurnosne mjere i izjavu o potrebnim sigurnosnim mjerama s određenim nositeljem i rokom provedbe.[75]

[72] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 207. – 208.
[73] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 208.
[74] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 208.
[75] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 220.

4.3. Zaštita poslovne tajne

4.3.1. Pojam poslovne tajne

Poslovna tajna je skup podataka i informacija koje se koriste u poslovanju i koje poslovnom subjektu kojemu ti podaci i informacije pripadaju donose gospodarsku korist i osiguravaju određenu prednost pred konkurencijom. Predmet poslovne tajne pritom mogu biti proizvodni postupci, tehnologije, izumi, poslovne metode, sastojci nekog proizvoda, sadržaj ugovora i drugi. Pojam poslovne tajne te mjere i postupci za utvrđivanje, uporabu i zaštitu poslovne tajne u našem pravnom sustavu propisane su Zakonom o zaštiti tajnosti podataka. [76] Uvjet koji je prema navedenom zakonu potreban za proglašavanje nekog podatka poslovnom tajnom je da se radi o podatku koji je tako važan za pravnu osobu da bi njegovo neovlašteno odavanje moglo naštetiti njezinim gospodarskim interesima.

4.3.2. Dužnost čuvanja tajnosti podataka

Podaci koji se smatraju poslovnom tajnom ne smiju se priopćavati niti činiti dostupnim neovlaštenim osobama, osim ako posebnim zakonom nije drugačije određeno. Svi zaposlenici dužni su čuvati poslovnu tajnu, ako na bilo koji način saznaju za podatak koji se smatra poslovnom tajnom. Pravne osobe također imaju dužnost čuvanja tajne i podataka. U praksi se često pojavljuju slučajevi kada je, radi obavljanja poslova pravne osobe nužno drugim osobama priopćiti neke od navedenih kategorija tajnih podataka. Navedene podatke drugoj osobi može priopćiti samo osoba koja je na to ovlaštena općim aktom pravne osobe i obavezno uz prethodnu pisanu suglasnost pravne osobe o čijoj se poslovnoj tajni radi.

4.3.3. Opći akt o poslovnoj tajni

Opći akt o poslovnoj tajni pobliže određuje način upotrebe i čuvanja podataka koji se smatraju poslovnom tajnom te mjere, postupci i druge okolnosti za čuvanje poslovne tajne.

[76] NN broj: 108/96 i 78/07

Opći akt o poslovnoj tajni treba biti primjeren poslovnom subjektu i njegovom poslovanju, jer će ponegdje možda biti potrebno zaštititi samo nekoliko poslovnih podataka a drugdje će ovakvu zaštitu trebati osigurati u odnosu na značajan dio djelatnosti poslovnog subjekta. [77]

4.3.4. Ugovor o povjerljivosti poslovne tajne

Ugovor o povjerljivosti („*Non-Disclosure Agreement-NDA*“) pored ostalog ugovara vrlo visoke novčane kazne za slučaj otkrivanja podataka koji predstavljaju poslovnu tajnu. U mnogim zemljama uobičajeno je sklapanje tog ugovora, a sve češće se takvi ugovori sklapaju i u Hrvatskoj i to ne samo u fazi zaključenja nekog posla već i prije početka pregovora oko zaključenja nekog posla kako bi se osigurala zaštita važnih poslovnih podataka u slučaju da ne dođe do sporazuma.

4.3.5. Kaznenopravna zaštita poslovne tajne

Poslovna tajna u hrvatskom pravnom sustavu štiti se Kaznenim zakonom, što pokazuje značaj koji zakonodavac pridaje ovoj problematici. Kazneno djelo neizdavanja i neovlaštenog odavanja poslovne tajne čini osoba koja neovlašteno drugome priopći, preda ili na drugi način učini pristupačnim podatke koji su poslovna tajna, kao i osoba koja pribavlja takve podatke s ciljem da ih preda nepozvanoj osobi. [78]

5. Business intelligence

Informacije pružaju potporu u donošenju kvalitetnih odluka u skladu s osnovnom politikom i okruženjem u području djelovanja poduzeća, zbog toga je nemoguće zamisliti bilo kakav poslovni proces bez upravljanja poslovnim informacijama. *„Business intelligence“* i poslovne informacije u uvjetima današnjice predstavljaju strateški menadžerski resurs, bez kojeg je gotovo nemoguće poslovanje današnjice.

[77] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 222.-223.
[78] Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 224.

Činjenica je da korporativna sigurnost podrazumijeva ukupnu sigurnost tvrtke s ciljem postizanja sigurnosti poslovnog uspjeha poduzeća. Iz toga proizlazi da je *„business intelligence“* sastavni dio korporativne sigurnosti.

„U suvremenim uvjetima otvorene tržišne utakmice svaki poslovni subjekt ima priliku za poslovni uspjeh. S druge strane, svaki poslovni subjekt istovremeno je izložen najrazličitijim ugrozama i prijetnjama u poslovanju. Stoga je posve razumljivo da danas menadžeri moraju predvidjeti buduće događaje i prijetnje u poslovanju te pripremiti adekvatne mjere i odgovore na buduće poslovne izazove. Poslovanje u nemirnoj i složenoj poslovnoj okolini nametnulo je potrebu traženja primjerenih instrumenata koji će strateškom menadžmentu pomoći da adekvatno odgovori na buduće poslovne izazove i prijetnje. Upravo se sustav *„business intelligence“* pokazuje kao prikladan instrument za ostvarenje tog cilja.“ [79]

5.1. Pojam „business intelligence“

Pojam „*business intelligence*“ prvi put pojavio se 1989. godine kao pojam koji označava proces prikupljanja informacija, odnosno poslovno obavještajnu djelatnost u poslovnom svijetu. [80] „*Business intelligence*“ je poslovno-obavještajna aktivnost u poslovnom svijetu koja je usmjerena na prikupljanje podataka i informacija potrebnih za donošenje što kvalitetnijih poslovnih odluka u cilju očuvanja pozicije u poslovnom okruženju i postizanja poslovnog uspjeha. [81]

Važno je napomenuti da su „*business intelligence*“ i poslovna špijunaža dva različita pojma. „*Business intelligence*“ je legalna i javna aktivnost poslovnih subjekata koja obuhvaća legalna i dopuštena sredstva i metode u prikupljanju javnih i svima dostupnih informacija i podataka s ciljem postizanja poslovnog uspjeha, dok je poslovna špijunaža nelegalna aktivnost koja obuhvaća

[79] Javorović B. i Bilandžić M.: Poslovne informacije i business intelligence, Golden marketing – Tehnička knjiga, Zagreb, 2007, str. 233-234
[80] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 236.
[81] Bilandžić M.: Poslovno-obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb, 2008., str. 71.

korištenje nezakonitih, prijevarnih i neetičnih metoda i aktivnosti s ciljem dolaska do osjetljivih i zaštićenih informacija.

5.2. Model „business intelligence“

„*Business intelligence*“ je kružna aktivnost koja ima nekoliko temeljnih faza, pri čemu svaka faza zahtijeva pažljivo planiranje i sustavnu provedbu.

„Business intelligence“ je planska i sustavno provođena aktivnost čiji su rezultat poslovno-obavještajna izvješća koja predstavljaju poslovno znanje i služe menadžmentu kao podrška u procesu planiranja i donošenja odluka, na strateškoj i operativnoj razini. Ovom poslovno-obavještajnom djelatnošću postoji mogućnost pribavljanja informacija koje menadžmentu omogućuju da stekne jasnu i detaljnu sliku o uvjetima i okolini djelovanja poslovnog subjekta. Model obuhvaća pravne, sigurnosne, gospodarske, socijalne, političke i druge uvjete, strategiju i aktivnosti konkurencije, navike i sklonosti potrošača i ukupne trendove na tržištu. Rezultati poslovno-obavještajnog djelovanja omogućuju menadžmentu jasno određivanje pozicije poslovnog subjekta na tržištu i pravovremeno prepoznavanje i iskorištavanje poslovnih prilika (prije drugih) te pravovremeno uočavanje i prilagođavanje tržišnim trendovima.

Dijelovi ciklusa „*business intelligence*“ su:

1. planiranje i upravljanje,

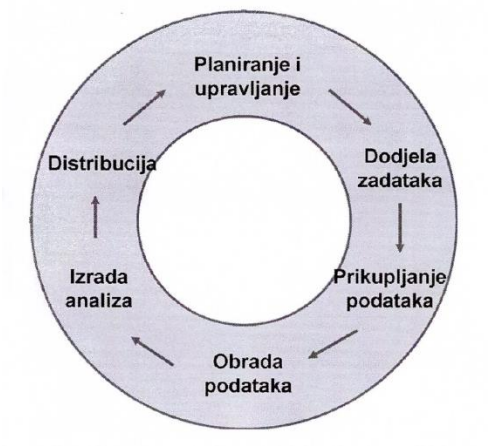
2. prikupljanje podataka,

3. obrada i analiza podataka,

4. distribucija analiza i njihova uporaba [82]

[82] Javorović B., Bilandžić M. (2007.), Poslovne informacije i business intelligence, Zagreb, Golden marketing-Tehnička knjiga, str. 207.

Slika 1. Model „Business intelligence“



Izvor: Mišević P., materijali s predavanja, kolegij Menadžment poslovne sigurnosti, ppt „Business intelligence“

5.2.1. Faza planiranja i upravljanja

Faza planiranja i upravljanja podrazumijeva određivanje ciljeva od strane menadžmenta i definiranje konkretnih interesa do kojih se želi stići procesom prikupljanja podataka. Nakon definiranja ciljeva dolazi do izrade planova za ostvarivanje postavljenih ciljeva te utvrđivanje i dodjela konkretnih zadataka i uspostava mehanizma za upravljanje i koordinaciju procesa prikupljenih podataka.

5.2.2. Faza prikupljanja podataka

U ovoj fazi prikupljaju se javni i svima dostupni podaci iz raznih baza podataka, evidencija, časopisa, publikacija, novina. Prikupljanje podataka može se odvijati uz pomoć tehničkih sredstava – Interneta te iz ljudskih izvora. Pod pojmom prikupljanja podataka iz ljudskih izvora podrazumijeva se prikupljanje podataka od osoba unutar ili izvan poslovnog subjekta koje raspolažu informacijama koje su predmet interesa. „U prikupljanju podataka izdvajaju se tri najznačajnije kategorije koje mogu predmet interesa:

- podaci o okruženju u kojem poslovni subjekt djeluje
- podaci koji se odnose na tržište

- podaci koji se odnose na konkurenciju“ [83]

5.2.3. Faza obrade i analize podataka

U fazi analize podataka provodi se raščlamba, kategorizacija, sistematizacija, vrednovanje i interpretacija prikupljenih podataka. Analizom podataka dolazi se do poslovno-obavještajnih izvješća u kojima se iznose odgovarajući zaključci i procjene budućih kretanja te načini za rješavanje detektiranih pitanja ili problema (ukoliko za to postoji mogućnost).

5.2.4. Faza distribucije, analize i upotrebe podataka

U posljednjoj fazi prezentira se poslovno-obavještajno izvješće krajnjim korisnicima te se ta izvješća koriste u procesu planiranja i donošenja poslovnih odluka. Ciklus *„business intelligence*“ ne mora nužno završiti ovdje, jer ukoliko se otkriju neki nedostaci ili proturječnosti dolazi do novog pokretanja ciklusa poslovno-obavještajnog djelovanja.

6. Metode zaštite korporativne sigurnosti u poslovanju poduzeća

6.1. Sprečavanje pranja novca i financiranja terorizma

Zakon o sprječavanju pranja novca i financiranja terorizma[84] propisuje mjere i radnje u bankarskom i nebankarskom financijskom poslovanju, te u novčarskom i drugom poslovanju koje se poduzimaju radi sprječavanja i otkrivanja pranja novca i financiranja terorizma. Odredbe se odnose na sprječavanje pranja novca i odgovarajuće se primjenjuju na sprječavanje financiranja terorizma u cilju sprječavanja i otkrivanja aktivnosti pojedinaca, pravnih osoba, skupina i organizacija u vezi s financiranjem terorizma.

[83] Bilandžić M. (2008.), Poslovno-obavještajno djelovanje: Business intelligence u praksi, Zagreb, AGM, str. 91-95
[84] NN broj 87/08

6.1.1. Pojmovi pranje novca i financiranje terorizma

Pranje novca podrazumijeva izvršavanje radnji kojima se prikriva pravi izvor novca ili druge imovine za koju postoji sumnja da je pribavljena na nezakonit način u zemlji ili inozemstvu.

Financiranje terorizma podrazumijeva osiguravanje ili prikupljanje sredstava, odnosno pokušaj osiguravanja ili prikupljanja sredstava, zakonitih ili nezakonitih, na bilo koji način, izravno ili neizravno, s namjerom da se upotrijebe ili sa znanjem da će biti upotrijebljena za počinjenje terorističkog kaznenog djela, od strane terorista ili terorističke organizacije.

6.1.2. Mjere za sprječavanje i otkrivanje pranja novca i financiranja terorizma

Mjere, radnje i postupci za sprječavanje i otkrivanje pranja novca i financiranja terorizma utvrđeni Zakonom provode se prije i prilikom svake transakcije, kao i pri sklapanju pravnih poslova kojima se stječe ili koristi imovina, te u ostalim oblicima raspolaganja novcem, pravima i drugom imovinom koji mogu poslužiti za pranje novca i financiranje terorizma.

6.1.3. Ured za sprječavanje pranja novca i financiranje terorizma

Upravna organizacija u sustavu Ministarstva financija je ured za sprječavanje pranja novca, koji obavlja zadaće u cilju sprječavanja pranja novca i financiranja terorizma i ostale zadaće utvrđene Zakonom. U cilju sprječavanja pranja novca i financiranja terorizma ured prikuplja, pohranjuje, analizira i dostavlja podatke i dokumente o sumnjivim transakcijama nadležnim državnim tijelima radi daljnjeg postupanja.

6.1.4. Dužnosti obveznika

6.1.4.1. Obveza obavješćivanja ureda o gotovinskim transakcijama

Obveznik je dužan obavijestiti Ured o svakoj transakciji koja se provodi u gotovini u vrijednosti 200.000,00 kuna i većoj. Obavijest Uredu dostavlja se odmah, a najkasnije u roku od tri dana od dana obavljene transakcije.

6.1.4.2. Obveza imenovanja ovlaštene osobe

Obveznik je dužan imenovati jednu osobu i zamjenika te osobe koji su ovlašteni i odgovorni za provođenje mjera i radnji koje se poduzimaju radi sprječavanja i otkrivanja pranja novca i financiranja terorizma. O imenovanju osobe obveznik je također dužan obavijestiti Ured i to odmah, a najkasnije u roku od sedam dana od dana imenovanja.

6.1.4.3. Obveza donošenja internog akta

Obveznik je dužan donijeti interni akt kojim se određuju mjere, radnje i postupanja radi sprječavanja i otkrivanja pranja novca i financiranja terorizma u skladu sa Zakonom o sprječavanju pranja novca i financiranja terorizma i propisima donesenim na temelju njega. U internom aktu potrebno je utvrditi odgovornost ovlaštenih osoba zaduženih za provedbu Zakona za slučaj nepoštivanja odredaba Zakona i propisa donesenih na temelju Zakona o sprječavanju pranja novca i financiranja terorizma, kao i odgovornost svih zaposlenika obveznika koji sudjeluju u provedbi Zakona i propisa donesenih na temelju Zakona.

6.1.4.4. Obveza redovitog stručnog osposobljavanja i izobrazbe

Obveznik također ima dužnost voditi brigu da se redovito stručno osposobljavaju i obrazuju djelatnici koji obavljaju zadaće na području sprječavanja i otkrivanja pranja novca i financiranja terorizma. Stručno osposobljavanje odnosi se na kontinuirano upoznavanje s odredbama Zakona i propisa donesenih na temelju Zakona, s internim aktima obveznika i s međunarodnim standardima koji proizlaze iz međunarodnih konvencija s područja sprječavanja pranja novca i financiranja terorizma.

6.1.4.5. Obveza redovite interne revizije

Najmanje jednom godišnje, obveznik ima dužnost osigurati internu reviziju obavljanja zadaća sprječavanja pranja novca i financiranja terorizma. Svrha revizije je uočavanje i sprječavanje nepravilnosti u provedbi Zakona i poboljšanje internog sustava u otkrivanju sumnjivih transakcija i osoba.

6.1.5. Zaštita i čuvanje podataka

Obveznici i njihovi zaposlenici, uključujući članove upravnih i nadzornih odbora trebaju poštivati načelo tajnosti prikupljenih podataka i postupaka i ne smiju stranci ili trećoj osobi otkriti:

1. da je u uredu bio ili da će biti dostavljen podatak

2. da je ured privremeno zaustavio izvršenje sumnjive transakcije

3. da je ured tražio kontinuirano praćenje financijskog poslovanja stranke

4. da je protiv stranke ili treće osobe započet ili bi mogao biti započet pred istražni postupak zbog postojanja sumnje na pranje novca ili financiranje terorizma[85]

Zabrana otkrivanja navedenih podataka i članaka ne vrijedi ako su podaci, informacije i dokumentacija potrebni za utvrđivanje činjenica u kaznenom postupku, te ako su podaci, informacije i dokumentacija potrebni nadležnom nadzornom tijelu radi obavljanja nadzora nad obveznikom i pokretanja prekršajnog postupka.

6.1.6. Nadzor nad obveznicima

Nadzor poslovanja obveznika u provedbi Zakona i na temelju njega donesenih propisa obavljaju u okviru svojih nadležnosti:

1. Ured

2. Financijski inspektorat RH

3. Porezna uprava

4. Hrvatska narodna banka

5. Hrvatska agencija za nadzor financijskih usluga[86]

[85] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 254.
[86] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 256.

Ako bilo koje od navedenih nadzornih tijela u obavljanju nadzora utvrdi postojanje osnove sumnje da je počinjen prekršaj propisan Zakonom dužno je putem ovlaštene osobe Financijskom inspektoratu podnijeti optužni prijedlog i poduzeti ostale mjere utvrđene Zakonom. Protiv rješenja Financijskog inspektorata Republike Hrvatske može se podnijeti žalba Visokom prekršajnom sudu Republike Hrvatske.

6.2. Zaštita na radu

Zaštita na radu skup je tehničkih, zdravstvenih, pravnih, socijalnih i drugih mjera i aktivnosti kojima je svrha spriječiti i otkloniti opasnosti i štetnosti koje mogu ugroziti zdravlje i život osoba na radu. Ozljede na radu i profesionalne bolesti nanose štetu radniku, njegovoj obitelji, ali i poslodavcu i cjelokupnoj društvenoj zajednici. Iz tog razloga zaštita na radu provodi se kao organizirana djelatnost sa svrhom osiguranja uvjeta rada u kojima neće postojati opasnosti za zdravlje i život, odnosno uvjete u kojima će te opasnosti biti smanjene na najmanju moguću mjeru.

U današnje vrijeme još uvijek postoje poslodavci koji zaštitu na radu ne percipiraju kao sastavni dio poduzeća i izvođenja procesa rada te dugoročno ulaganje, već to smatraju dodatnim troškom. S druge strane ipak se postupno povećava broj poslodavaca koji su potpuno svjesni važnosti zaštite sigurnosti i zdravlja na radu, unatoč troškovima koji nastaju zbog poboljšanja radnog okruženja.

Zaštita na radu sastavni je dio organizacije rada i izvođenja radnog procesa, koja se ostvaruje obavljanjem poslova zaštite na radu i primjenom propisanih, ugovorenih i priznatih pravila zaštite na radu, te naređenih mjera i uputa poslodavca.

6.2.1. Zakon o zaštiti na radu

Zakon o zaštiti na radu je temeljni propis koji u hrvatskom zakonodavstvu uređuje prava, obveze i odgovornosti u vezi zaštite na radu. Njegova svrha je uvođenje mjera za poticanje unaprjeđivanja sigurnosti i zdravlja radnika na

radu, sprječavanje ozljeda na radu, profesionalnih i drugih bolesti u vezi s radom, te zaštita radnog okoliša. Zakon o zaštiti na radu utvrđuje subjekte, njihova prava, obveze i odgovornosti glede provedbe zaštite na radu, kao i sustav pravila zaštite na radu čijom se pravilnom primjenom u najvećoj mogućoj mjeri postiže svrha Zakona o zaštiti na radu.

Prava, obveze i odgovornosti u vezi zaštite na radu uređuju se izravno i neizravno propisima radnog zakonodavstva, propisima mirovinskog osiguranja, propisima zdravstvenog osiguranja i zdravstvene zaštite te tehničkim i drugim propisima kojima se štite sigurnost i zdravlje osoba na radu.

6.2.2. Odgovornost poslodavca za provedbu zaštite na radu

Poslodavac je odgovoran za organizaciju i provedbu zaštite na radu u svim radnim procesima i dijelovima poduzeća. Odgovornost poslodavca ne može se umanjiti niti isključiti neovisno o tome da li je organiziranje provedbu zaštite na radu ustrojio na način da je odredio radnika za obavljanje aktivnosti zaštite na radu, ili je ugovorio suradnju s pravnom osobom ovlaštenom za obavljanje poslova zaštite na radu. Primjena pravila zaštite na radu i mjera zdravstvene zaštite ne smije predstavljati nikakve troškove za zaposlenike, a svako traženje poslodavca da radnik sudjeluje u troškovima provođenja zaštite na radu je prekršaj. Poslodavac odgovara radniku za štetu uzrokovanu ozljedom na radu, profesionalnom bolešću ili bolešću vezanom uz rad po načelu objektivne odgovornosti, na koju utječu propisane obveze zaposlenika u području sigurnosti i zdravlja na radu. Uz iznimku poslodavac se može osloboditi odgovornosti prema općim propisima obveznog prava, ako je riječ o događajima nastalih zbog nepredvidivih okolnosti na koje poslodavac nije mogao utjecati.

6.2.3. Osposobljavanje za rad na siguran način

Poslodavci moraju biti osposobljeni iz područja zaštite na radu ako se radi o tehnologijama gdje postoji opasnost od ozljeda na radu i profesionalnih bolesti koje bi mogle ugroziti sigurnost radnika. Obvezi osposobljavanja podliježu poslodavci u svim djelatnostima u kojima postoji opasnost od ozljeda na radu i profesionalnih bolesti koje bi mogle ugroziti sigurnost radnika. Način

osposobljavanja poslodavca propisan je Pravilnikom o programu, sadržaju i načinu provjere znanja poslodavca iz područja zaštite na radu[87].

Poslodavac je dužan zaposlenika prije početka rada obavijestiti o svim činjenicama i okolnostima koje utječu ili bi mogle utjecati na sigurnost i zdravlje radnika, a vezane su uz obavljanje poslova. Zaposlenicima koji nisu osposobljeni za rad na siguran način poslodavac ne smije dopustiti samostalno obavljanje poslova. Ako zaposlenik nije osposobljen za rad na siguran način poslodavac je dužan osposobiti ga na rad za siguran način i osigurati da radnik radi pod nadzorom radnika koji je osposobljen za rad na siguran način, ali ne dulje od 30 dana. Poslodavac je dužan osposobiti zaposlenika za rad na siguran način i dati mu upute vezane uz njegovo mjesto rada prije početka rada, kod promjena u procesu rada, kod uvođenja nove radne opreme i tehnologije te kod upućivanja radnika na novi posao. Osposobljavanje se mora provesti uzimajući u obzir nove ili promijenjene opasnosti i štetnosti kojima bi zaposlenik mogao biti izložen. Po potrebi dužnost poslodavca je periodički ponavljati osposobljavanje. Osposobljavanje zaposlenika za rad na siguran način poslodavac je dužan provesti tijekom radnog vremena o svojem trošku. Program osposobljavanja za rad na siguran način poslodavac može izvoditi sam ili ih za njega mogu izvoditi ovlaštene ustanove.

Poslovi s posebnim uvjetima rada su poslovi koje mogu obavljati samo djelatnici koji osim općih uvjeta za zasnivanje radnog odnosa ispunjavaju i posebne uvjete kao što su životna dob, spol, stručne sposobnosti, te zdravstveno, tjelesno i psihičko stanje. Sposobnost zaposlenika za obavljanje poslova s posebnim uvjetima rada utvrđuje se prije njegovog rasporeda na takve poslove i ponovno se provjerava u rokovima određenim propisom o zaštiti na radu i kada to procijeni specijalist medicine rada. Ako zaposlenik ne ispunjava potrebne uvjete poslodavac ga ne smije rasporediti na poslove s posebnim uvjetima rada. Ispunjenje propisanih uvjeta dokazuje se odgovarajućim potvrdama i svjedodžbama koje moraju biti u skladu s odgovarajućim propisima.

[87] NN broj: 69/05

6.2.4. Zaštita posebnih kategorija zaposlenika

Poslodavac je dužan voditi brigu o zaštiti na radu posebnih kategorija zaposlenika. Tu pripadaju malodobni zaposlenici, žene i zaposlenici smanjenih radnih sposobnosti. U skupinu zaposlenika smanjenih radnih sposobnosti ubrajaju se zaposlenici čija je radna sposobnost smanjena zbog starosti, invaliditeta, ozljede na radu te profesionalnih ili ostalih bolesti i drugih razloga utvrđenim kolektivnim ugovorom poslodavca.

6.2.5. Pružanje prve pomoći i medicinska pomoć

Dužnost poslodavca je da organizira i osigura pružanje prve pomoći zaposlenicima u slučaju ozljede na radu ili iznenadne bolesti, sve do njihovog upućivanja na liječenje zdravstvenoj ustanovi. U svakom radnom prostoru u kojem istovremeno radi do dvadeset zaposlenika, najmanje jedan zaposlenik mora biti osposobljen i određen za pružanje prve pomoći, taj se broj povećava za jedan na svakih daljnjih pedeset zaposlenika. Osobama određenim za pružanje prve pomoći potrebno je osigurati i staviti na raspolaganje svu potrebnu opremu.

6.2.6. Dužnosti poslodavca prema tijelima nadzora te isprave i evidencije iz područja zaštite na radu

Poslodavac je obvezan inspektoru rada na njegov zahtjev dati obavijest i podatke koji su mu potrebni u obavljanju nadzora. Za vrijeme obavljanja nadzora poslodavac je dužan inspektoru rada dati na uvid potrebne isprave i omogućiti utvrđivanje činjenica, koje su mu potrebne radi donošenja ocijene da li je postupano u skladu s propisima o zaštiti na radu. Poslodavac ima obvezu izvijestiti inspekciju rada o svakoj smrtnoj, težoj ili skupnoj ozljedi i to odmah po nastanku događaja, a u roku od 48 sati od nastanka događaja dužan je inspekciji rada dostaviti propisano pisano izvješće.

Zakon o zaštiti na radu obvezuje poslodavca na čuvanje određene dokumentacije, vođenje odgovarajućih evidencija, vođenje knjiga nadzora i podnošenje odgovarajućih izvješća. Te obveze odnose se na sva mjesta rada

poslodavca. Način vođenja evidencija iz područja zaštite na radu, sadržaj i način vođenja knjige nadzora i način podnošenja izvješća propisani su Pravilnikom o evidenciji, ispravama, izvještajima i knjizi nadzora iz područja zaštite na radu.[88]

6.2.7. Obveze i prava zaposlenika

Zaposlenik je dužan osposobiti se za rad na siguran način kada ga na osposobljavanje uputi poslodavac, te je dužan pristupiti liječničkom pregledu za utvrđivanje radne sposobnosti kada ga poslodavac uputi na taj pregled. Sve poslove radnik je dužan obavljati s dužnom pozornošću i pri tome voditi računa o svojoj sigurnosti i zdravlju, kao i sigurnosti i zdravlju drugih zaposlenika. Zaposlenik radi s dužnom pozornošću kada poslove obavlja sukladno znanjima koja je stekao tijekom osposobljavanja za rad na siguran način i u skladu s uputama poslodavca. Zaposlenik je dužan surađivati s poslodavcem u rješavanju svih pitanja zaštite na radu. Poslodavac mora obavijestiti zaposlenika o svim promjenama u radnom procesu koje utječu na njegovu sigurnost i zdravlje, a zaposlenik tada ima pravo odbiti rad ako mu neposredno prijeti opasnost za život i zdravlje zbog toga što nisu primijenjena propisana pravila zaštite na radu. Zaposlenik koji zbog navedenih razloga odbije rad ne smije biti doveden u nepovoljniji položaj i mora biti zaštićen od bilo kakvih štetnih i neopravdanih posljedica.

6.2.8. Nadzor nad provedbom propisa o zaštiti na radu

Inspekcijski nadzor nad provedbom Zakona o zaštiti na radu i propisa donesenih na temelju zakona obavljaju inspektori rada Državnog inspektorata. Inspektori nadziru provedbu propisa kojima su uređeni sigurnost i zaštita zdravlja osoba koje obavljaju poslove za poslodavca, ali i drugih osoba koje se po bilo kojoj osnovi rada nalaze u prostorima poslodavca.

U provedbi inspekcijskog nadzora u području zaštite na radu inspektor rada ovlašten je u skladu s utvrđenim činjeničnim stanjem donijeti slijedeća rješenja:

[88] NN broj: 52/84

- rješenje o privremenoj zabrani korištenja sredstava rada, prostora ili instalacija
- rješenje o zabrani određenog načina postupanja
- rješenje kojim naređuje poslodavcu da zaposlenika privremeno udalji s obavljanja poslova, u slučajevima kada utvrdi da su izravno ugroženi život ili zdravlje zaposlenika ili drugih osoba[89]

U slučaju da inspektor utvrdi da postoje nedostaci u primjeni propisa zaštite na radu, ali da oni kao takvi ne utječu štetno na život i zdravlje zaposlenika i drugih osoba u prostoru, te da se oni mogu otkloniti u roku od trideset dana, izdat će rješenje o otklanjanju nedostataka.

Do inspekcijskog nadzora može doći na temelju prijave pravnih ili fizičkih osoba, na temelju naloga rukovodeće strukture unutar Državnog inspektorata ili postupanjem inspektora prema planu rada.[90] Inspektor nakon obavljenog inspekcijskog nadzora sastavlja zapisnik o obavljenom inspekcijskom nadzoru.

6.3. Zaštita od požara

Svaka tvrtka koja želi preventivnu zaštitu od požara će posvetiti veliku važnost organizacijskim i tehničkim mjerama i radnjama usmjerenim na uklanjanje opasnosti od nastanka požara, rano otkrivanje požara i njegovo učinkovito gašenje. Sustav zaštite od požara obuhvaća planiranje zaštite od požara, provođenje mjera zaštite od požara, financiranje zaštite te osposobljavanje za obavljanje poslova zaštite od požara. Glavni cilj je zaštititi život, zdravlje i sigurnost ljudi, te sigurnost materijalnih dobara, okoliša i prirode od požara, uz prihvatljiv požarni rizik. Sustav zaštite od požara u Republici Hrvatskoj uređen je Zakonom o zaštiti od požara[91], a zaštita od požara zakonom je utvrđena kao djelatnost od posebnog interesa za Republiku Hrvatsku. Zaštitu od požara provode fizičke i pravne osobe utvrđene zakonom o zaštiti od požara i pravne osobe i udruge koje obavljaju vatrogasnu djelatnost.

[89] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 300.
[90] Puljić N. (2009.) „Sigurnost i zaštita zdravlja na radu“, Zagreb, Poslovni zbornik, str. 203.
[91] NN broj: 92/10

Svaka fizička i pravna osoba mora djelovati na način kojim se požar ne može izazvati i mora provoditi mjere zaštite od požara utvrđene Zakonom o zaštiti od požara i propisima donesenim na temelju tog zakona. Također je svaka osoba odgovorna za neprovođenje mjera zaštite od požara, izazivanje požara i sve posljedice koje bi iz toga mogle nastati. Svatko ima pravo, ali i obvezu biti upoznat s opasnostima od požara na mjestu gdje radi ili boravi. Odluku o planu i programu te načinu upoznavanja s opasnostima od požara donose pravne osobe na svom vlasništvu. Kako bi se pravovremeno i učinkovito osigurala zaštita od požara pravne osobe organiziraju osposobljavanje zaposlenika za provedbu preventivnih mjera zaštite od požara, gašenje požara i spašavanje ljudi i imovine ugroženih požarom. Djelatnici službe za zaštitu od požara moraju imati odgovarajuće obrazovanje, ovisno o poslovima koje obavljaju i položen stručni ispit u području zaštite od požara. Program, uvjeti i način polaganja propisani su Pravilnikom i stručnim ispitima u području zaštite od požara[92]. Fizičke i pravne osobe osiguravaju financijska sredstva za provedbu zaštite od požara prema vlastitim planovima.

6.4. Zaštita okoliša

U današnjici svaka ljudska djelatnost u većoj ili manjoj mjeri utječe na okoliš, pri čemu zagađivači nisu samo velike multinacionalne kompanije, već i srednja i mala poduzeća različitim aktivnostima znatno utječu na štetno djelovanje okoliša. Svako poduzeće može smanjiti svoj negativan utjecaj na okoliš na način da smanji ispuštanje štetnih tvari, smanjenje količine proizvedenog otpada i racionalnije korištenje skupih i neobnovljivih resursa. S obzirom na porast svijesti o važnosti smanjenja i kontroliranja utjecaja na okoliš, kao i činjenicu da uspostavljanje sustava upravljanja zaštitom okoliša postalo sastavni dio društveno odgovornog poslovanja, nužno je upoznati se s važećom zakonskom regulativom ovog područja.

[92] NN broj 40/94, 55/94 i 89/01

6.4.1. Zakon o zaštiti okoliša

Zakon o zaštiti okoliša[93] uređuje između ostalog načela zaštite okoliša i održivog razvoja, zaštitu sastavnica okoliša i zaštitu okoliša od utjecaja opterećenja, subjekte zaštite okoliša, dokumente održivog razvoja i zaštite okoliša, instrumente zaštite okoliša, odgovornost za štetu i druga pitanja od značaja za zaštitu okoliša.

Cjelovito upravljanje zaštitom okoliša provodi se na način da se ostvari održivi razvoj u skladu sa Zakonom o zaštiti okoliša i posebnim propisima.

6.4.2. Subjekti zaštite okoliša

Subjekti zaštite okoliša održavaju razvoj i zaštitu okoliša, u Republici Hrvatskoj to su:

- Hrvatski sabor
- Vlada Republike Hrvatske
- Ministarstva i druga nadležna tijela državne uprave
- Županije i Grad Zagreb, te ostali gradovi i općine
- Agencija za zaštitu okoliša
- Fond za zaštitu okoliša i energetsku učinkovitost
- Pravne osobe s javnim ovlastima
- Pravne i fizičke osobe odgovorne za onečišćavanje okoliša
- Druge pravne i fizičke osobe koje obavljaju gospodarsku djelatnost
- Udruge civilnog društva koje djeluju na području zaštite okoliša
- Građani kao pojedinci, njihove skupine, udruge i organizacije[94]

[93] NN broj: 110/07
[94] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 324.

Agencija za zaštitu okoliša je nezavisna javna ustanova osnovana za prikupljanje, objedinjavanje i obradu podataka o okolišu.

Fond za zaštitu okoliša je pravna osoba koja ima javne ovlasti, a osnovana je radi obavljanja poslova financiranja pripreme, provedbe i razvoja programa, projekata i sličnih aktivnosti u području zaštite okoliša te u području energetske učinkovitosti i korištenja obnovljivih izvora energije, promidžbe ciljeva i načela zaštite okoliša, očuvanja prirodnih zajednica i racionalnog korištenja prirodnih dobara i energije, kao i osnovnih uvjeta održivog razvoja i ostvarivanja prava građana na zdrav okoliš.[95]

Pravna osoba koja je ovlaštena za stručne poslove zaštite okoliša mora ispunjavati posebne uvjete utvrđene posebnim propisom i mora imati suglasnost za obavljanje tih poslova.

6.4.3. Informacijski sustav zaštite okoliša i informiranje javnosti o okolišu

Informacijski sustav zaštite okoliša uspostavljen je sa svrhom cjelovitog upravljanja zaštitom okoliša, te u svrhu izrade i praćenja provedbe dokumenata održivog razvoja i zaštite okoliša. On sadrži podatke i informacije o stanju okoliša, opterećenjima i utjecajima na okoliš, te odgovorima društva. Nadležno upravno tijelo u županiji vodi registar onečišćavanja okoliša. Registar je skup podataka o izvorima, vrsti, količini, načinu i mjestu ispuštanja, prijenosa i odlaganja onečišćujućih tvari i otpada u okoliš. Tijelo javne vlasti dužno je osigurati pristup informacijama o okolišu koje posjeduje u skladu sa Zakonom o zaštiti okoliša, uz odgovarajuću primjenu posebnih propisa kojima se uređuje pravo javnosti na pristup informacijama.

6.4.4. Odgovornost za štetu u okolišu

Poduzeće koje obavlja djelatnost koja predstavlja rizik za okoliš i za ljudsko zdravlje odgovara za štetu u okolišu i prijeteću opasnost od štete, osim ako dokaže da opasna djelatnost nije bila uzrok štete u okolišu. Poduzeće za prouzročenu štetu odgovara po načelu objektivne odgovornosti (uzročnosti).

[95] Ivandić Vidović D., Karlović L., Ostojić A. (2011.) „Korporativna sigurnost“, Zagreb, UHMS, str. 325.

Djelatnosti opasne za okoliš i ljudsko zdravlje utvrđene su posebnim propisima. Poduzeće odgovara za štetu u okolišu ili prijeteću opasnost od štete i u slučaju kada ne obavlja opasnu djelatnost, ali u obavljanju te djelatnosti ne otklanja opasnosti i ne sprječava nanošenje štete biljnim i životinjskim vrstama ili prirodnim staništima zaštićenim prema posebnom propisu. Za prouzročenu štetu ili prijeteću opasnost poduzeće odgovara po načelu dokazane krivnje ili dokazanog nemarnog djelovanja. Poduzeće je dužno u utvrđenom roku izraditi sanacijski program za uklanjanje štete u okolišu koja je nastala zbog prekoračenja graničnih vrijednosti emisija u skladu s posebnim propisom. Operater tvrtke obvezan je osiguranjem kod osiguravatelja u skladu sa zakonom osigurati raspoloživa sredstva za naknadu štete koja bi mogla biti nanesena okolišu, odnosno za otklanjanje prijeteće opasnosti od štete.

6.4.5. Elementi opće politike zaštite okoliša

Neki od elemenata opće politike zaštite okoliša su znak zaštite okoliša, priznanja i nagrade za dostignuća na području zaštite okoliša, te propisivanje obveze proizvođača vezano za označavanje proizvoda i ambalaže. Znak zaštite okoliša dodjeljuje se pravnim i fizičkim osobama koje proizvode ili distribuiraju proizvode koji se s drugim istovrsnim proizvodima odlikuju manje negativnim utjecajima na okoliš i time pridonose visokom stupnju zaštite okoliša. Priznanja i nagrade za dostignuća na području zaštite okoliša dodjeljuju se fizičkim i pravnim osobama koje su postigle mjerljive rezultate u zaštiti okoliša i zadovoljavanju uvjeta održivog razvoja. U okviru opće politike zaštite okoliša utvrđuje se i obveza proizvođača da prije stavljanja proizvoda na tržište, na ambalažu proizvoda i na prateću tehničku dokumentaciju uz proizvod trebaju staviti uputu kojom se potrošač obavješćuje o utjecaju proizvoda i ambalaže na okoliš u način postupanja s proizvodom i ambalažom nakon njegove upotrebe.

6.4.6. Inspekcijski nadzor u zaštiti okoliša

Inspekcijski nadzor nad primjenom Zakona o zaštiti okoliša i propisa donesenih na temelju zakona provode državni službenici ministarstva nadležnog za zaštitu okoliša. Inspekcijski nadzor u području okoliša provode i

druge inspekcije nadležne prema posebnim propisima za nadzor pojedinih sastavnica okoliša i zaštite od utjecaja opterećenja na okoliš.

Inspektor svoj službeni identitet dokazuje službenom iskaznicom ili značkom. Početak provedbe inspekcijskog nadzora inspektor nije dužan najaviti nadziranoj osobi, osim ako procijeni da je takva obavijest potrebna u svrhu obavljanja nadzora.

Nadzirane osobe imaju dužnost inspektoru omogućiti provedbu inspekcijskog nadzora i osigurati mu uvjete za neometan rad, te mu dati na uvid svu potrebnu dokumentaciju.

U inspekcijskom nadzoru inspektor nadzire osobe koje su obavezne provoditi mjere i aktivnosti zaštite okoliša, te ispunjavanje i način rada nadziranih osoba, obavlja izravan uvid u opće i pojedinačne akte, te poduzima mjere određene Zakonom i propisima donesenim na temelju Zakona o zaštiti okoliša.

Stranka u inspekcijskom postupku može biti svaki onečišćivač, nositelj zahvata, poduzeće, operater, ovlaštenik, županija, grad ili općina. Ako je onečišćivač nepoznatog boravišta, stranka u inspekcijskom nadzoru je grad ili općina na čijem području je došlo do onečišćenja.

U provedbi inspekcijskog nadzora inspektor može na licu mjesta zatvoriti prostorije i pristup u prostor u kojima nadzirana osoba obavlja određenu djelatnost i onemogućiti joj korištenje postrojenja i opreme pečaćenjem.

Protiv rješenja o obustavi postupka izvršenja i zaključka o troškovima izvršenja koje je donio inspektor može se izjaviti žalba u roku od petnaest dana. Žalba se podnosi ministarstvu nadležnom za zaštitu okoliša.

7. Zaključak

U radu je prikazana uloga i važnost korporativne sigurnosti u poslovanju poduzeća, te na koji način zaštititi podatke i informacije od gubitka i zlouporabe. S obzirom na promjenjive i nestabilne okolnosti današnjice potrebno je kontinuirano provoditi proces kontrole, zaštite i sigurnosti u poslovanju.

Na početku rada kratko je predstavljena poslovna strategija, kao ključ poslovnog uspjeha poduzeća. Zatim slijedi objašnjenje pojma poslovnog procesa i upravljanja poslovnim procesima. Prikazuju se različiti aspekti procesa korporativne sigurnosti, a to su ustroj organizacijske jedinice za korporativnu sigurnost, te obilježja i profil menadžera sigurnosti.

U trećem poglavlju rada prikazan je i obrazložen normativni okvir u kojem djeluje korporativna sigurnost. Tu su identificirane, sistematizirane, detaljno opisane i analizirane sve dimenzije korporativne sigurnosti: informacijska sigurnost, privatna zaštita, zaštita intelektualnog vlasništva.

Četvrto poglavlje je glavna tema ovog rada, u kojem su detaljno objašnjeni osnovni pojmovi i način na koji se pristupa podacima, zatim mjere i standardi koje je potrebno ispuniti, kako bi se zadovoljili minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka. Ovdje je navedena i zakonska regulativa zaštite podataka, te kaznenopravna odgovornost za fizičke i pravne osobe koje se ne pridržavaju zakona.

U petom poglavlju spominje se model „business intelligence“ koji u uvjetima današnjice uz poslovne informacije predstavlja strateški menadžerski resurs. Riječ je zapravo o procesu prikupljanja informacija potrebnih za donošenje što kvalitetnijih poslovnih odluka. Ovdje je važno napomenuti da je ovo legalan način prikupljanja informacija, za razliku od poslovne špijunaže kojom se na ilegalan način korištenjem prijevarnih i neetičnih aktivnosti pokušava doći do osjetljivih i zaštićenih informacija, te na taj način steći konkurentsku prednost.

U posljednjem poglavlju rada navedene su metode zaštite korporativne sigurnosti u poslovanju poduzeća. U današnje vrijeme povećava se broj

poduzeća koja su potpuno svjesna važnosti osiguravanja rada na siguran način za zaposlenika i poslodavca, a to postižu primjenom mjera i radnji iz područja zaštite na radu, zaštite od požara, zaštite okoliša. U ove metode svrstava se i sprječavanje pranja novca i financiranje terorizma.

Popis literature

Bibliografija

1. Anić V., (2003.), Veliki rječnik hrvatskog jezika, Zagreb, Novi Liber

2. Anić V., Goldstein I., (2002.), Rječnik stranih riječi, Zagreb, Novi Liber

3. Bilandžić M. (2008.), Poslovno-obavještajno djelovanje: Business intelligence u praksi, Zagreb, AGM

4. Hammer M., Champy J., (2004.), Reinžinjering tvrtke, Zagreb, MATE

5. Ivandić Vidović D., Karlović L., Ostojić A., (2011.), Korporativna sigurnost, Zagreb, UHMS

6. Javorović B., Bilandžić M., (2007.), Poslovne informacije i business intelligence, Zagreb, Golden marketing -Tehnička knjiga

7. Mintas Hodak Lj., (2010.), Pravno okruženje poslovanja, Zagreb, MATE

8. Mišević P., materijali s predavanja, kolegij Menadžment poslovne sigurnosti, PPT. Zakonski i podzakonski propisi u radu s klasificiranim podacima

9. Puljić N., (2009.), Sigurnost i zaštita zdravlja na radu, Zagreb, Poslovni zbornik

10. Zlatović D., (2010.), Intelektualno vlasništvo i marketing, Zagreb, INMAG

Elektronički zapis na prijenosnom mediju

CD s urednički pročišćenim tekstovima svih zakona koji normativno uređuju područje korporativne sigurnosti, prilog uz knjigu Ivandić Vidović D., Karlović L., Ostojić A. (2011.), Korporativna sigurnost, Zagreb, UHMS

NN broj: 103/03, 118/06, 41/08, 108/96, 79/07, 150/05, 79/06, 105/06, 85/08, 139/04, 46/08, 72/07, 100/08, 37/10, 1/09, 41/09, 75/09, 2/10, 167/03, 79/07, 173/03, 54/05, 76/07, 30/09, 117/07,173/03, 54/05,76/07, 30/09, 72/04, 117/07, 173/03, 54/05, 87/05, 76/07, 30/09, 128,10, 117/07, 03/11, 173/03, 186/03, 54/05, 76/07, 72/04, 117/07, 173/03, 76/07, 30/09, 72/04, 117/07, 103/03, 118/06, 41/08, 139/04, 105/04, 79/07, 102/07, 79/07, 46/08, 108/96, 78/07, 87/08, 69/05, 52/84, 92/10, 40/94, 55/94, 89/01 i 110/07.