UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

ANALIZA ZAGOTAVLJANJA VARNOSTI PODATKOV V IZBRANEM ORGANU DRŽAVNE UPRAVE

Andrej Zemljak

Ljubljana, april 2014

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

ANALIZA ZAGOTAVLJANJA VARNOSTI PODATKOV V IZBRANEM ORGANU DRŽAVNE UPRAVE

Kandidat: Andrej Zemljak
Vpisna številka: 04039459
Študijski program: univerzitetni študijski program Uprava prva stopnja

Mentor: izr. prof. dr. Ljupčo Todorovski

Ljubljana, april 2014

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Andrej Zemljak, študent univerzitetnega študijskega programa Uprava prva stopnja, z vpisno številko 04039459, sem avtor diplomskega dela z naslovom: Analiza zagotavljanja varnosti podatkov v izbranem organu državne uprave.
S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbel, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo, in sem to tudi jasno zapisal v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Ur. list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Tanja Slapar.

Vrhnika, 13. 2. 2014

Podpis avtorja:

POVZETEK

Varnost osebnih, tajnih in drugih podatkov, v fizični in elektronski obliki, je dandanes zelo pomembna za posameznika in organizacije. Skrb za varovanje teh podatkov je predpogoj za nemoteno delovanje organizacij, zato to področje pokrivajo številni normativni akti, od mednarodnih konvencij in direktiv do nacionalnih zakonov, podzakonskih predpisov in internih aktov. Povečana skrb za varnost podatkov je posledica vse večje razširjenosti elektronske oblike podatkov, ki izpodriva fizične oblike zapisov, a jo je težje varovati. Možen je namreč oddaljen dostop do elektronskih podatkov brez fizične navzočnosti in ob vsakem času. Za zagotavljanje varnosti elektronskih podatkov, še posebej osebnih in tajnih, je treba na ravni organizacije sistemsko poskrbeti za varnost računalniških sistemov pred zunanjimi vdori in okužbami sistema.

V diplomskem delu raziskujem, ali je v izbranem državnem organu zagotovljena zadostna varnost podatkov, ki jih upravljajo vsak dan. Organ se namreč srečuje z veliko količino različnih podatkov, med katerimi so tudi osebni in tajni podatki, ki so še posebej občutljivi. Za te mora imeti dobro fizično in tehnično varnost in zagotavljati varno okolje za delo z njimi in njihovo hranjenje. S pomočjo intervjuja ugotovim, da imajo dobro poskrbljeno za fizično in tehnično varnost, ta ustreza tudi stopnji varnosti za hranjenje tajnih podatkov najvišje stopnje – strogo tajno. Njihovo delo je omejeno s pravnimi podlagami s področja varovanja podatkov, ki se ponekod prepletajo, in tem morajo vestno slediti.

Ključne besede: varnost podatkov, podatki v fizični in elektronski obliki, osebni podatki, zasebni podatki, tajni podatki.

SUMMARY

ANALYSIS OF DATA SECURITY PROTECTION IN A GOVERNMENTAL BODY

Security of personal, secret or other data in physical or electronic form is very important for individuals and organizations. Since data security protection is a necessary precondition for functioning of any organization, especially governmental body, a number of laws and normative acts at national and international laws address the issue of data security. This is also due to the continuous growth of data available in electronic form, which requires new ways of data protection when compared to data stored in physical form; electronic data can be accessed from anywhere at any given time. To provide efficient data security protection, particularly for personal and secret data, organization must have a solid computer security in place on all systems.

In the thesis, I am trying to determine whether a selected governmental body in Slovenia adequately protects all the data security, especially for data being used on daily basis. I selected the particular body, that wanted to remain anonymous, so they work with a lot of sensitive data, such as personal and top-secret data. To protect them, they have to establish physical and electronic security and therefore provide safe work environment and storage for these data. I conduct an interview with a contact person at the selected organization to validate my hypothesis that the electronic and physical security is efficient and meets the standards necessary for storing and working with secret data classified as "top secret". One of the problems for employees represents a large number of overlapping laws and normative acts of different areas, which complicates the data-security protocols.

Key words: data security, data in physical and electronic form, personal data, private data, secret data.

KAZALO

KAZALO PONAZORITEV

KAZALO TABEL

1 UVOD

Vsak dan ustvarjamo in pridobivamo vse več različnih podatkov, o sebi in o drugih fizičnih ter pravnih osebah, novih patentih, o dogodkih doma in po svetu, z željo, da so vsi ti podatki varno shranjeni. Tehnološki napredek nas oddaljuje od uporabe papirne dokumentacije in hranjenja podatkov na papirju ter v fizični obliki. Moderna informacijska tehnologija je že tako zelo olajšala delo s podatki v elektronski obliki, da si življenja brez nje ne moremo več predstavljati.

Elektronsko upravljanje podatkov je prineslo veliko prednosti pri delu, saj je njihova obdelava sedaj hitrejša, enostavnejša in izboljšal se je njihov dostop. Hranjenje elektronskih podatkov je lažje, preglednejše in hitrejše kot hranjenje podatkov v fizični obliki, ki jih je treba shranjevati v določenih prostorih, v pravih razmerah. Tudi iskanje in vnašanje popravkov oziroma sprememb v dokumente je zaradi informatizacije preprostejše in hitrejše.

Z vsako novostjo pridejo prednosti in slabosti. Razvoj informatizacije je poenostavil in pospešil obdelavo podatkov, dostopanje do njih in njihovo shranjevanje, s čimer se je povečala učinkovitost dela in nekoliko razbremenilo delo s papirji, hkrati pa povzroča težavnost pri varnem shranjevanju elektronskih podatkov. Dostop do podatkov je mogoč od kjer koli in kadar koli, zato je potrebno dobro tehnično varstvo za podatke, saj fizična prisotnost ni več nujna za dostop in spreminjanje le-teh. Operacijske in informacijske sisteme je zato treba varovati pred zlonamernimi programi, ki lahko omogočijo nepooblaščene dostope v sistem tretjim osebam ali povzročijo okužbo sistema.

Vse več je posegov v zasebnost, osebni podatki so lažje dostopni in razvrednoteni v elektronski obliki, bolj kot so bili v fizični obliki. Najbolj so v uporabi in izpostavljeni javnosti na področju zdravstva, policije, pravosodja in socialnega varstva, zato mora biti za njihovo varstvo dobro poskrbljeno. Podobno velja za tajne podatke, s katerimi je treba ravnati še posebej previdno in zagotavljati njihovo maksimalno varnost za ohranitev avtentičnosti in stran od oči nepooblaščenega osebja.

Namen diplomskega dela je predstaviti, kako na državni ravni zagotavljajo varnost podatkov, tako elektronskih kot v papirni obliki. Zato sem izbral državni organ, ki mora zagotavljati visoko stopnjo tehnične in fizične varnosti, saj se vsakodnevno srečuje z obdelavo osebnih in tajnih podatkov pri svojem delu. Pri delu uporabljajo večinoma elektronske podatke in vse manj fizične zapise. Preveril sem, katere podatke hranijo, kako dolgo jih smejo hraniti, kje jih morajo shraniti in kako jih varujejo. Za natančen pregled kakovosti varnosti sem se osredotočil na varnost fizičnih in elektronskih podatkov osebne in tajne narave.

Cilj diplomskega dela je preveriti, ali je v izbranem državnem organu dobro poskrbljeno za tehnično in fizično varstvo podatkov in ali njihova stopnja varnosti zagotavlja ustrezno varnost tudi za najpomembnejše podatke, kot so tajni in osebni podatki.

Pri raziskovanju sem uporabljal in sintetiziral informacije iz verodostojnih virov, knjig, učbenikov, diplomskih nalog in s spletnih strani s področja varstva in hranjenja osebnih podatkov. Za zbiranje informacij o državnem organu sem intervjuval osebo, ki je zaposlena v informacijskem sektorju državnega organa. Zaradi ohranjanja anonimnosti kontaktne osebe so informacije v diplomskem delu bolj splošne, vendar dovolj natančne, da dosežejo zastavljeni namen in cilj.

Vsebino diplomskega dela sem razdelil na šest poglavij. Prvo poglavje je uvod v diplomsko delo z opisom teme in namena, čemu sem se odločil za to temo. V drugem poglavju so opredeljeni pojmi, ki sem jih pogosto uporabljal v nadaljevanju in jih je dobro poznati ter vedeti, v kakšnem pomenu so uporabljeni. Definirani so pojmi podatek, osebni podatek, tajni podatek, informacija javnega značaja in še drugi pojmi s področja obdelave podatkov. Sledi poglavje s pravno podlago, ki ureja področje varnosti podatkov na nacionalni in mednarodni ravni. Pravna podlaga izhaja iz mednarodne Konvencije o varstvu posameznika glede na avtomatsko obdelovo osebnih podatkov. Poleg Konvencije obstaja še Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov. Konvencija in Direktiva določata, kako naj se zagotavljajo varnost pri obdelavi podatkov in sankcije ob kršitvi le-teh. Četrto poglavje zajema splošno predstavitev področja varnosti podatkov; način hranjenja podatkov je razdeljen med fizične zapise in elektronske podatke, kjer so predstavljene tudi prednosti in slabosti obojih. Temu sledi glavno poglavje, ki opisuje varnost podatkov v izbranem državnem organu. Podatki so bili pridobljeni s pomočjo intervjuja na njihovem oddelku za informatiko. V tem poglavju sem opisal tehnološko in fizično varstvo, ki ga zagotavlja organ, ter predstavil, kako je poskrbljeno za njihovo notranje varovanje pri obdelovanju in hranjenju tajnih in osebnih podatkov. Na koncu so navedeni literatura in viri ter priložen opravljen intervju.

2 OPREDELITEV OSNOVNIH POJMOV

Zaradi različnih interpretacij pomena podatkov bom v tem poglavju razložil, kaj določen pojem pomeni, in naštel vrste podatkov, s katerimi se srečujemo in jih bom uporabljal v diplomskem delu. Opredelil bom tudi nekatere druge pojme, ki jih je treba poznati s področja varnosti podatkov in s tem povezanih zakonskih podlag.

Splošni pomen pojma podatek:
"Je zapis, opis ali predstavitev nekega dogodka, pojava ali dejstva iz realnega sveta v numerični, besedni ali grafični obliki." (Vintar, 1996, str. 47)

Informacijski pomen podatka:
"Podatek je katerokoli zabeleženo dejstvo. Podatek nima pomena. Podatki predstavljajo surovino, ki jo predeluje informacijski sistem. Obstaja več definicij termina Podatek. Podatek je poljubna predstavitev s pomočjo simbolov ali analognih veličin, ki ji je pripisan, ali se ji lahko pripiše neki pomen." (Fakulteta za računalništvo in informatiko, 2013)

Osebni podatek:
"osebni podatek pomeni katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (posameznik, na katerega se nanašajo osebni podatki); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto". To je telefonska številka, osebno ime, EMŠO, številka osebne izkaznice, naslov bivališča, starost, plača, če ne gre za javni sektor. (Direktiva 95/46/ES, 2. člen)

Zbirka osebnih podatkov:
Vsak strukturiran niz podatkov, ki vsebuje enega ali več osebnih podatkov, dostopnih na podlagi meril, ki omogočijo uporabo in združevanje podatkov v centraliziranem ali decentraliziranem nizu ali če je razpršen na geografski ali funkcionalni podlagi. (Likar, 2009, str. 3)

Zasebni podatek:
"je vsaka informacija, ki jo je možno povezati z osebo. Če se zbirajo, obdelujejo ali shranjujejo zasebni podatki, mora biti jasno zapisan namen zbiranja." (Safe.si, 2013)

Zasebni in osebni podatek sta pravzaprav ista zadeva, vendar bom v diplomskem delu uporabljal zasebni podatek kot podatek, ki je lastnina neke osebe, kot so slike, videi, dnevnik o tej osebi, oziroma je ta oseba avtor tega podatka iz svojega zasebnega življenja. Osebni podatek pa, kot je zgoraj definirano, način za neposredno identifikacijo specifične osebe.

Zasebnost je zmožnost posameznika ali skupine, da nadzoruje pretok informacij o sebi in tako te informacije odkriva selektivno. Zasebnost večkrat povezujejo z anonimnostjo – željo, da v javnosti ostaneš neopažen. (Safe.si, 2013)

Posameznik:
Je določena fizična oseba oziroma določljiva fizična oseba, na katero se nanaša določen osebni podatek. Posameznik je določjiva fizična oseba, ko ga lahko identificiramo posredno ali neposredno s sklicevanjem na identifikacijsko številko ali na vsaj en dejavnik, ki je značilen za njegovo fizično, duševno, fiziološko, kulturno, družbeno ali ekonomsko identiteto. Ta način identifikacije ne sme povzročati prevelikih stroškov, časa ali napora. (Likar, 2009, str. 3)

Tajni podatek:
Gre za podatek s tako pomembno vrednostjo, da bi zaradi razkritja tega podatka nepoklicani osebi lahko nastale škodljive posledice za varnost države, za njene politične ali gospodarske koristi. Vsak, ki pozna tajni podatek, ga je dolžen ohraniti tajnega in skrbeti za njegovo varnost ter ohranitev tajnosti. Nanaša se na (MNZ, 2013):

- javno varnost;
- obrambo;
- zunanje zadeve;
- obveščevalno in varnostno dejavnost državnih organov;
- sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije;
- znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije.

Po definiciji v Zakonu o tajnih podatkih "je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno". (ZTP, 2. člen)

Javno dostopni podatki:
Kot javno dostopne podatke razumemo vse podatke, do katerih dostop ni nikakor omejen. Taki podatki so dostopni javnosti in pravna ali fizična oseba nima zadržkov, da postanejo javno poznani in dostopni. (Šaponja v: Kotnik, 2010, str. 6)

Pri nas je na tem področju prišlo do spremembe leta 2003, ko je Državni zbor Republike Slovenije sprejel Zakon o dostopu do informacij javnega značaja, ki daje vsem ustavno pravico do informacij javnega značaja. Vendar mora za ta dostop imeti upravičen pravni interes, le v nekaterih z zakonom določenih primerih ta ni potreben. K informacijam javnega značaja spadajo informacije, ki nastanejo na delovnem področju organa. To so

dokument, zadeva, dosje, register, evidenca ali dokumentarno gradivo, izdelani v organu ali v sodelovanju z drugimi osebami ali organi. (Upravne enote, 2013)

Med definiranimi vrstami podatkov so tajni podatki tisti z najvišjo stopnjo pomembnosti. Njihovo razkritje lahko povzroči ogromno škode za vse povezane pravne in fizične osebe ter tudi tretje osebe. S temi podatki so seznanjeni le tisti, ki imajo posebna pooblastila in nihče drug. Tajni podatki se navezujejo na javno varnost, državno obrambo, mednarodne zadeve, ki jih je treba varovati po Zakonu o tajnih podatkih, da njihovo razkritje ne pripelje do katastrof. Kot tajni podatek lahko označimo podatke o prevozu denarja. Če kakršna koli informacija o poteku prevoza pride v javnost, je ogrožena varnost denarja, kar povzroči posledice na nacionalni ravni.

Zelo pomembni so tudi osebni podatki, a manj kot tajni podatki. Za obstoj osebnih podatkov vedo praktično vsi, saj obstajajo osebni podatki za vsakogar. Pomembno je, da je njihova vsebina poznana le lastniku in tistim, ki jim lastnik dovoli, oziroma je dovoljeno z Zakonom o osebnih podatkih. Pod osebne podatke štejemo EMŠO, številko osebne izkaznice in številko bančnega računa.

Zasebni podatki so obravnavani kot osebna lastnina. Njihova varnost ni državnega pomena tako kot pri osebnih in tajnih podatkih. Pomembni so za lastnika in on sam poskrbi za njihovo varnost in se odloči, ali jih s kom deli ali ne. Zasebni podatki se običajno hranijo v obliki fotografije, videa, zapiskov, kot sta na primer fotografija prijateljev ali videoposnetek z rojstnodnevne zabave.

Najmanj varnostno pomembni so podatki javnega značaja, saj so splošno znani vsem in jih ni treba varovati pred razkritjem ali krajo. Sem spadajo vse informacije, ki jih dobimo preko medijev ali s strani občin, ministrstev. Na primer informacije o prometni nesreči na avtocesti proti Ljubljani, Ustavno sodišče je razveljavilo novi zakon o davku na nepremičnine ali informacije o spremembah ministrske funkcije.

Ob kršitvi Zakona o tajnih podatkih in Zakona o osebnih podatkih so zakonsko določene sankcije za odgovorne osebe. Te sankcije so visoke globe, ki jih morajo kršitelji plačati zaradi kršenja zakona. Ob kraji zasebnega podatka se ta obravnava kot osebna lastnina in temu sledi primerna kazen, prav tako je to običajno globa, vendar nižja kot za osebne in tajne podatke. Kraja in razkritje tajnih podatkov ogrožata nacionalno varnost, lahko tudi mednarodno, kar lahko privede do slabih odnosov z drugimi državami ali celo vojne. Razlog za krajo osebnih podatkov je lahko javno blatenje imena, razkritje zdravstvenih problemov, kraja denarja ali celo identitete. Vsi razlogi pripeljejo do neprijetnih in neželenih posledic za žrtev. S krajo zasebnih podatkov lahko nekoga osramotimo, kaj več pa s temi podatki težko dosežemo. Najmanj nevšečnosti in ogroženosti povzročajo javni podatki, za katere ni treba skrbeti, ker so znani celemu svetu in z njimi ni možno ogrožati nikogar.

Obdelava osebnih podatkov:
Gre za kakršno koli delovanje v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali del zbirke osebnih podatkov pri ročni obdelavi ali pa so namenjeni za vključitev v zbirko osebnih podatkov. O tem dejanju govorimo, kadar se osebni podatki zbirajo, pridobivajo, vpisujejo, urejajo, shranjujejo, prilagajajo ali spreminjajo, preklicujejo, kadar gre za vpogled, uporabo, razvrstitev, uporabo, povezovanje, anonimiziranje, izbris, blokiranje, uničenje. (Likar, 2009, str. 3)

Anonimiziranje:
Anonimiziranje je postopek, pri katerem se oblika osebnih podatkov spremeni do te mere, da jih ni več mogoče povezati s posameznikom, oziroma je za to potrebno veliko napora, časa in stroškov. (Likar, 2009, str. 3)

Avtomatizirana obdelava:
To je obdelava osebnih podatkov s pomočjo informacijske tehnologije.

Upravljavec osebnih podatkov:
Fizična, pravna ali katera druga oseba javnega ali zasebnega sektorja, ki določa namene in sredstva obdelave osebnih podatkov. Te osebe in nameni ter sredstva so določeni z zakonom. (Likar, 2009, str. 3)

3 PRAVNA PODLAGA ZA VARSTVO OSEBNIH IN TAJNIH PODATKOV V SLOVENIJI

V nadaljevanju bom naštel in predstavil pravne podlage, ki pokrivajo področje varstva osebnih in tajnih podatkov. Opisal bom tudi kratek razvoj le-te.

Leta 1890 je bil v ZDA napisan prvi članek, ki je obravnaval področje pravice do zasebnosti in z njim je ta pravica pridobila pravno prepoznavnost. Avtorja članka z naslovom Pravica do zasebnosti sta dva sodnika ameriškega vrhnovnega sodišča, Warren in Brandeis. Ta pravica je bila kodificirana šele v letu 1960 s člankom Zasebnost, čigar avtor je Prosser. In Prosser je kodifikacijo pravice do zasebnosti ponovno opredelil leta 1977 z izdajo civilnih deliktov[1]. (Likar, 2009, str. 6)

Na področju varstva informacijske zasebnosti in osebnih podatkov so velik del prispevale mednarodne organizacije. Generalna skupščina Združenih narodov je leta 1948 sprejela Splošno deklaracijo človekovih pravic, ki v 12. členu določa, da se s samovoljnim vmešavanjem ne sme nadlegovati nikogar v njegovem zasebnem življenju, stanovanju, z dopisovanjem in napadi na njegov ugled in čast. Deklaracija določa pravico do pravnega varstva pred takimi napadi za vsakogar.

Leta 1974 je bilo spisano pomembno poročilo z naslovom Človekove pravice in znanstveni in tehnološki razvoj – Uporaba elektronike, ki lahko vpliva na pravice oseb, in omejitve, ki bi morale biti podane v demokratični družbi. Pripravil ga je generalni sekretar Organizacije združenih narodov (OZN) za Ekonomski in socialni svet Združenih narodov in je pomembno iz dveh razlogov:

- državam priporoča, naj čim prej sprejmejo zakonske ureditve varstva informacijske zasebnosti posameznika, če tega še niso storile;
- vsebuje temeljne zahteve za zakonsko urejanje varstva informacijske zasebnosti, ki naj bi jih države upoštevale.

OZN je sprejela še en dokument – Smernice o avtomatiziranih zbirkah osebnih podatkov, ki se prav tako nanaša na varstvo informacijske zasebnosti. Zgleduje se po načelih, izoblikovanih v okviru drugih mednarodnih integracijskih oblik, predvsem pa po evropskih integracijskih oblikah.

Poleg OZN so za področje varstva informacijske zasebnosti pomembne še: Organizacija za ekonomsko sodelovanje in razvoj (OECD), v okviru te so leta 1980 sprejeli Smernice OECD, Svet Evrope in Evropska skupnost.

---

1 Civilni delikti so protipravna dejanja ali opustitve, ki povzročajo premoženjsko škodo, zato lahko prizadeti zahteva od povzročitelja odškodnino. Civilni delikt je ena izmed vrst pravnih kršitev.

Svet Evrope je leta 1953 sprejel Evropsko konvencijo o človekovih pravicah. 8. člen konvencije določa vsakemu posamezniku pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja. Javna oblast se v to pravico ne sme vmešavati, razen če je razlog za poseg v to pravico določen z zakonom zaradi državne varnosti, ekonomske blaginje, da se prepreči zločin ali da se zavarujejo zdravje, morala, pravice in svoboščine ljudi. Z 19. členom konvecije je Svet Evrope ustanovil Evropsko sodišče za človekove pravice. (Ur. list RS, št. 33/94, MP, št. 7/94, 2013)

Na podalgi te konvencije je bila leta 1981 izdana še Konvencija o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov. S to konvencijo so želeli poenotiti nacionalno ureditev in enakopravno varstvo posameznikov.

Nekaj let kasneje, leta 1990, je Evropska skupnost sprejela predloge iz treh direktiv (Čebulj, 1992, str. 11–14):

1. Ta predlog se nanaša na varstvo posameznika z vidika obdelave osebniih podatkov in se zgleduje po Svetu Evrope.
2. Ta predlog je usmerjen na bolj specifično področje varnosti podatkov. Vsebuje točno določene zahteve za varstvo zasebnosti v okviru javniih digitalnih komunikacijskih omrežij, posebno v povezavi z digitalizirano mrežo integriranih storitev in javnimi digitalnimi prenosnimi omrežji.
3. Zadnji predlog direktive je namenjen zagotovitvi globalne strategije zaščite posameznikov pred naključnimi in namernimi vdori in zlorabami njihovih podatkov, ki so jih elektronsko shranili, procesirali in prenesli in s tem povezanih informacijskih sistemov.

Pravno varstvo informacijske zasebnosti je v evropskih državah podobno urejeno za vse. Glavne značilnosti vseh normativnih ureditev s tega področja v teh državah so naslednje:

- varstvo osebnih podatkov je urejeno z zakonom;
- zakonodaja je usmerjena v varstvo zasebnosti subjektov zasebnega prava;
- enako varstvo za lastne in tuje državljane;
- zakonodaja obravnava računalniške in ročno vodene zbirke podatkov;
- zakonsko varstvo obravnava zbiranja podatkov, njihovo obdelovanje, shranjevanje, prenos in brisanje;
- natančno definiranje vseh pojmov zakona, da ne pride do napačnih razlag zakona;
- oblikovanje posebnih neodvisnih teles, ki spremljajo vse dogodke na področju varstva informacijske zasebnosti;
- strogost glede izjem;
- določene formalnosti glede vzpostavitve zbirk osebnih podatkov, njihov namen in vsebino;
- svoboden prenos podatkov prek državnih meja;
- posameznikom daje ustrezno pravno sredstvo.

Varstvo osebnih podatkov je tisto, kar nas oziroma bi nas moralo najbolj skrbeti v današnjih časih. Zasebni in tajni podatki niso v tako obširni in pogosti uporabi v vsakdanjem življenju in jih je zato lažje varovati in ohraniti skrite pred svetom. Osebni podatki pa so potrebni že skoraj za vsako stvar v naših življenjih. Služijo kot identifikacija, ko kupujemo s plačilno kartico, prevzamemo pošto, pošiljamo življenjepise za službo, razni e-računi, spletno kupovanje in podobni opravki izpostavljajo osebne podatke posameznikov. Zato je njihovo pravno varstvo vse bolj pomembno.

Normativna ureditev področja varstva osebnih podatkov v Sloveniji je urejena z lastnimi pravnimi akti in z določbami iz mednarodnih konvencij, pogodb, direktiv in drugih pravnih aktov s tega področja, saj je Slovenija članica Evropske unije, OZN in nekaterih drugih mednarodnih organizacij ter forumov. Tako mora Slovenija pri sprejemanju novih nacionalnih zakonov ali pri spremembah že veljavnih upoštevati vse te mednarodne akte, ki služijo kot obvezujoča in neobvezujoča podlaga za njih. Pravna praksa Slovenije se je s tem približala mednarodni pravni praksi, ki ureja to področje, predvsem evropski.

3.1 KONVENCIJA O VARSTVU POSAMEZNIKOV GLEDE NA AVTOMATSKO OBDELAVO OSEBNIH PODATKOV

Konvencija predpisuje minimalne, temeljne in nujno potrebne ukrepe za varstvo osebnih podatkov pri obdelavi, ki jih morajo upoštevati vse države članice Sveta Evrope in podpisnice te Konvencije. Na tej pravni podlagi temeljijo nadaljnje direktive s tega področja in nacionalni zakoni.

Tako je Slovenija leta 1985 začela uveljavljati, leta 1994 pa je tudi ratificirala določbe iz Konvencije o varstvu posameznikov glede na avtomatsko obdelavo podatkov, ki jo je leta 1981 sprejel Svet Evrope. Državi podpisnici Konvencije je omogočena možnost, da lahko ali ob podpisu ali kasneje poda izjavo generalnemu sekretarju Sveta Evrope, da se bo ta konvencija uporabljala tudi za druge zbirke osebnih podatkov, ki niso vodene avtomatsko.

Glavni namen uveljavljanja Konvencije je zagotovitev spoštovanja pravic posameznika, njegovih temeljnih svoboščin, pravice do zasebnosti avtomatsko obdelanih podatkov za vsakogar, ne glede na njegovo državljanstvo in prebivališče.

Konvencija vsebuje preambulo in sedem poglavij, drugo poglavlje bom razložil bolj podrobno, saj je najpomembnejši del z načeli.

Kratek pregled sedmih poglavij Konvencije:

1. V prvem poglavju so opredeljeni predmet in namen, obseg ter definicije izrazov.
2. Drugo poglavje vsebuje, kot že omenjeno, načela.

3. Tretje poglavje se posveča načelu prostega pretoka podatkov, prenosu podatkov čez državne meje. S tem je onemogočeno, da bi ena podpisnica Konvencije onemogočila ali prepovedala prenos osebnih podatkov drugi na njeno nacionalno ozemlje zgolj zaradi zaščite zasebnosti.
4. Četrto poglavje predpisuje medsebojno sodelovanje držav pogodbenic Konvencije. Predpisuje pomoč dajalcem podatkov, ki so v tujini, zaščitne ukrepe v okviru te pomoči, nastali stroški ne morejo biti večji od stroškov porabljenih za izvedence in tolmače in pokrije jih pogodbenica, ne posameznik.
5. Peto poglavje določa ustanovitev posvetovalnega odbora. Vsaka pogodbenica imenuje po enega člana in enega namestnika v odbor, ostale članice Sveta Evrope, nepogodbenice, imajo lahko v odboru opazovalce. Namen odbora je predlagati načine za boljšo in hitrejšo uporabo Konvencije, predlagati izboljšave in dodajati svoje mnenje o vprašanjih v povezavi z uporabo Konvencije.
6. Šesto poglavje določa, kakšen je postopek za dopolnitev Konvencije.
7. Sedmo poglavje opredeljuje veljavnost v okviru končnih določb.

Drugo poglavje vsebuje temeljna načela zaščite podatkov in to poglavje zagotavlja posameznikom spoštovanje njihove zasebnosti tudi v mednarodnem pretoku podatkov. Eno od teh načel je načelo kakovosti podatka, ki postavlja pet zahtev pri avtomatičnem obdelovanju osebnih podatkov:

- pridobitev in obdelava podatkov na zakonit način;
- shranjevanje in uporaba podatkov z jasnim namenom;
- glede na namen zbiranja ne smejo biti preobsežni podatki;
- točnost podatkov;
- določena oblika shranjevanja podatkov.

Načelo prepovedi obdelovanja določenih vrst podatkov prepoveduje obdelavo osebnih podatkov, če ti razkrivajo raso, versko prepričanje, verovanja, zdravstveno stanje, seksualno življenje, kazenske obsodbe, če v nacionalni zakonodaji ni primernega varstva.

Načelo zavarovanja podatkov predpisuje, da morajo imeti podpisnice Konvencije ustrezne organizacijske in tehnične ukrepe za zaščito osebnih podatkov, hranjeniih v avtomatskih zbirkah podatkov. S temi ukrepi naj bi preprečevali nenamerno in nepooblaščeno uničenje podatkov, izgubo podatkov, nepooblaščene vpoglede, obdelave, spremembe in širjenje osebnih podatkov.

Vsaki osebi je z načeloma odprtosti in udeležbe ljudi omogočeno:

- da izve za obstoj posamezne zbirke podatkov, ki vsebuje osebne podatke, za njen namen obstoja in sedež upravljavca te zbirke;
- da v razumnem času, brez večjih zamud in stroškov pridobi potrdilo o tem, kateri podatki v povezavi z njim se hranijo v določeni zbirki podatkov;
- če so bili osebni podatki obdelani v nasprotju s pravili iz nacionalne zakonodaje, lahko zahteva njihov izbris ali popravek;

- če njegovi zahtevi po prej naštetih informacijah, dejanjih ni ustreženo, ima možnost uporabe določenih pravnih sredstev, kot so zahteva, pritožba, ugovor.

Posebno načelo Konvencije je načelo izjeme uporabe prikazanih načel, s tem povezanih omejitev pravic posameznikov s področja varstva osebnih podatkov. To načelo se uporablja v točno določenih primerih, ki so zapisani v Konvenciji, na primer za zaščito državne ali javne varnosti, denarnih interesov države, zatiranje kriminala, za zaščito dajalcev podatkov ali za zaščito pravic in svoboščin drugih ljudi.

Načelo odgovornosti obvezuje podpisnice, da v nacionalni zakonodaji določijo pravice in obveznosti upravljavcev in uporabnikov podatkov in ob kršitvah obveznosti ustrezne sankcije.

Z načelom o široki razlagi odločb Konvencije je določeno, da nobenega načela ni mogoče razlagati kot omejujoče, da bi oviralo podpisnice pri zagotovitvi širše zaščite osebnih podatkov posameznikov kot je minimalno določena v Konvenciji. (Čebulj, 1990, str. 5–14)

3.2 DIREKTIVA O VARSTVU POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV IN O PROSTEM PRETOKU PODATKOV

(Direktiva 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem toku takih podatkov, UL Evropskih skupnosti, št. L281)

Direktiva številka 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov določa, da morajo vse države podpisnice slediti določbam Direktive in pravne predpise, sprejete na podlagi Direktive, morajo poslati Komisiji Evropske unije. Vsi potrebni ukrepi za usklajevanje notranje zakonodaje z Direktivo morajo biti sprejeti v treh letih od sprejema Direktive.

Direktivo sestavljata dva glavna dela, to sta uvodni oziroma pojasnjevalni in normativni del. Prvi del ima tri vsebinske sklope, to so preambula, opredelitev temeljnih ciljev in pojasnjevalni napotki. Drugi del Direktive, normativni del, je razdeljen na sedem poglavij in jih bom na kratko predstavil, saj pokrivajo področje varnosti osebnih podatkov.

Prvo poglavje, Splošne določbe, opredeljuje cilje Direktive, njene glavne definicije in področje, kjer naj bi se uporabljalo Direktivo ter nacionalno pravo. Vsebina Direktive se nanaša na avtomatsko in ročno procesiranje podatkov, določa pa tudi izjeme in situacije, kjer se Direktive ne uporablja.

Najobsežnejše je drugo poglavje, ki vsebuje načela in se navezuje na opredelovanje pojmov za zakonitost obdelovanja osebnih podatkov. Poleg načel se v tem poglavju določajo še izjeme in omejitve, pravica posameznika do ugovora in obveznost po uradnem obveščanju nadzornega organa.

- Načelo zakonitosti – obdelava osebnih podatkov je zakonita le, če posameznik nedvoumno v to privoli in v določenih situacijah, kot so:
    - upravljavec zbirke podatkov ima zakonsko pooblastilo za obdelavo teh osebnih podatkov, obdelava je nujna za izpolnitev nalog upravljavca zbirke ali pa je obdelava nujna za varnost javne koristi;
    - obdelava osebnih podatkov lastnika je nujna zaradi njegove varnosti;
    - kadar je obdelava potrebna za izvršitev pravnih poslov, katerih udeleženec je posameznik.
- Načelo predhodne določitve namena: za obdelavo podatkov mora bit vnaprej točno določen namen.
- Načelo relavantnosti pomeni, naj se zbirajo le nujno potrebni podatki, preprečuje prevelike količine zbiranja osebnih podatkov, zahteva sorazmerje med količino zbiranja in namenom obdelave osebnih podatkov.
- Načelo kvalitete podatkov stremi k točnosti podatkov, ki se zbirajo, in če je treba tudi njihovo popolno ažurnost.
- Načelo časovne omejitve: osebne podatke se shranjuje le toliko časa, kolikor je potrebno za identifikacijo posameznika, v času, ki je potreben za doseganje namena zbiranja podatkov.
- Načelo zavarovanja opredeljuje tehnične in druge ukrepe za varstvo zbirke osebnih podatkov in preprečitve nepooblaščenega dostopa do njih.
- Načelo svobodnega pretoka prek državnih mej je potrebno zaradi skupnega evropskega trga s svobodnim pretokom blaga, storitev, oseb in kapitala in tukaj pride v poštev tudi skupni evropski informacijski trg.
- Načelo notifikacije: države članice morajo poskrbeti, da nacionalna zakonodaja upravljavcu zbirke osebnih podatkov nalaga obveznost obvestiti določen državni organ o začetku obdelovanja specifične vrste podatkov z določenim namenom.
- Načelo seznanjenosti zavezuje posameznika, da upravljavcu zbirke podatkov predpiše obveznost, da ga ta seznani z zbiranjem in obdelavo njegovih podatkov. (Čebulj, 1996, str. 237–239)

Tretje poglavje govori o določitvah pravnih sredstev, odgovornostih ter sankcijah v nacionalnih zakonodajah. Države članice so s podpisom te Direktive zavezane k določitvi ustreznih pravnih sankcij ob kršitvah informacijske zasebnosti posameznika. Vsakomur morata biti zagotovljeni pravica sodnega varstva, če so kršene določbe predpisov varstva osebnih podatkov, in pravica do odškodnine, če nastane škoda ob kršitvi informacijske zasebnosti posameznika.

Tema četrtega poglavja je prenos osebnih podatkov v tretje države. Po določilih Direktive mora nacionalna zakonodaja predpisovati, da je prenos osebnih podatkov v druge države možen le, če je v tej državi zagotovljena primerna raven varnosti osebnih podatkov. Komisija Evropske unije in države članice se morajo obveščati o zadevah in primerih tega področja, če katera od njih meni, da določena država nima ustrezno zagotovljene zaščite

osebnih podatkov. Če do tega pride in Komisija v posebnem postopku potrdi to mnenje, se prepreči vsakršen iznos osebnih podatkov v to dotično državo.

Peto poglavje spodbuja pripravo kodeksov ravnanja pri obdelavi osebnih podatkov. Namen kodeksov je pravilno izvajanje nacionalnih predpisov, ki jih države podpisnice Direktive s tem sprejmejo.

V šestem poglavju se določa obveznost za ustanovitev dveh posebnih organov, ki skrbita za varnost informacijske zasebnosti posameznika. Na nacionalni ravni je to nadzorni organ in delovno telo za varstvo posameznika z vidika obdelave osebnih podatkov na ravni Evropske unije.

Sedmo poglavje predvideva ustanovitev posebnega odbora, ki naj pomaga Komisiji Evropske unije pri sprejetju operativnih ukrepov izvajanja vsebine Direktive.

Komisija je dolžna poročati o problemih implementacije Direktive Svetu Evropske unije in Evropskemu parlamentu, pripravljati nove predloge in amandmaje za Direktivo.

3.3 USTAVA REPUBLIKE SLOVENIJE

Ustava RS je temeljni nacionalni zakon, ki je podlaga vsem ostalim zakonom in podzakonom države ter drugim pravnim aktom. Ustava RS ureja vsa možna področja v državi, med katerimi je tudi varstvo podatkov, ki sledi smernicam Konvencije in Direktive. Poleg tega mora biti skladno z mednarodniimi akti, saj je Slovenija članica več mednarodnih organizacij.

Varnost osebnih podatkov spada med ustavno zagotovljene človekove pravice in temeljne svoboščine, zato Ustava RS služi kot neposredna podlaga pri zakonski ureditvi varstva osebnih podatkov. Varstvo osebnih podatkov štejemo med pravice na področju zasebnosti, med katerimi najdemo še: pravico do osebnega dostojanstva (Ustava RS, 34. člen), varstvo pravic zasebnosti in osebnostnih pravic (Ustava RS, 35. člen), nedotakljivost stanovanja (Ustava RS, 36. člen), varnost tajnosti pisem in drugih občil (Ustava RS, 37. člen), svobodo izražanja (Ustava RS, 39. člen) in svobodo vesti (Ustava RS, 41. člen).

V 38. členu Ustave RS je vsakomur zagotovljeno varstvo osebnih podatkov z zahtevo po zakonitem zbiranju, obdelavi in uporabi osebnih podatkov in za to mora biti vnaprej določen namen. Posamezniku je dana pravica seznanjenosti s tem, kateri podatki o njem se zbirajo, in pravica do sodnega varstva, ki ob zlorabi osebnih podatkov posamezniku omogoča sodne ukrepe proti kršitelju. V tem členu so razvidna načela, obravnavana v prej omenjenih Konvenciji in Direktivi, to so načelo zakonitosti, namenskosti, seznanjenosti in načelo sodnega varstva. Načelo zakonitosti obravnava tudi možnost soglasja osebe za zbiranje, obdelavo in uporabo njegovih osebnih podatkov. Primeri in pogoji tega dejanja

morajo poleg soglasja biti skladni z zakonom in soglasje mora vidno nakazati, za katere podatke in kakšen namen je izdano.

3.4 ZAKONI

- Zakon o varstvu osebnih podatkov, ZVOP-1

Zakon bolj točno določa pravice in varstvo podatkov. Zajema Zakon o varstvu podatkov (2004), Zakon o informacijskem pooblaščencu (2005), Zakon o spremembah in dopolnitvah Zakona o ustavnem sodišču (2007) in Zakon o spremembah in dopolnitvah Zakona o varstvu podatkov (2007). Služi preprečitvi neustavnih, nezakonitih, neupravičenih posegov v zasebnost in dostojanstvo posamemznika pri obdelavi osebnih podatkov.

Zakon o varstvu osebnih podatkov, prva verzija, je začel veljati leta 1990 z namenom ureditve varstva osebnih podatkov, preprečiti nezakonite in čezmerne posege v integriteto posameznikove osebnosti, ki bi lahko bili posledica zbiranja, obdelovanja, hranjenja, uporabe in posredovanja osebnih podatkov brez zakonskega varstva tega področja. Leta 1999 je RS sprejela nov Zakon o varstvu osebnih podatkov, ker se je začela bližati vstopu v Evropsko unijo in je morala točneje upoštevati določila in zahteve Direktive Evropskega parlamenta in Sveta o zaščiti posameznika na področju varovanja osebnih podatkov pri obdelavi. Leta 2001 se je izkazalo, da je zakon še vedno pomanjkljiv, zato so morali sprejeti Zakon o spremembah in dopolnitvah k Zakonu o varstvu osebnih podatkov. Leta 2003 je sodna praksa Sodišča Evropskih skupnosti odločila, da so nekatere vsebinske določbe v Direktivi tako podrobne, da jih morajo države članice sprejeti točno tako, kot je zapisano v Direktivi. Zato je leta 2005 začel veljati današnji Zakon o varstvu osebnih podatkov, ki je imel po tem še nekaj dodatkov in sprememb, zadnja je bila leta 2007.

ZVOP-1 (v nadaljevanju) sestavlja 117 členov, ki so razdeljeni na osem delov, nekateri deli imajo tudi svoja poglavja. (Zakonodaja, november 2013)

Prvi del se imenuje Splošne določbe in je sestavljen iz sedmih členov. Prvi člen opredeljuje vsebino in namen zakona, preostali členi pa opredeljujejo načela, ki so bistvo zakona: načelo zakonitosti in poštenosti, sorazmernosti, prepoved diskriminacije itd.

Drugi del se imenuje Obdelava osebnih podatkov, razdeljen je na štiri poglavja in zajema člene od 8 do 28 Prvo poglavje je osredotočeno na ureditev pravne podlage za obdelavo osebnih podatkov. Pravna podlaga je razdeljena na obdelavo osebnih podatkov v javnem in zasebnem sektorju, prav tako določa tudi izjeme. Drugo poglavje opredeljuje varstvo posameznika pri obdelavi osebnih podatkov, zagotavlja pravno varstvo pri namenu, zbiranju, hranjenju in obdelavi osebnih podatkov in skrbi, da se ne kršijo pravice posameznika pri tem opravilu. Tretje poglavje določa vsebinsko varovanje osebnih podatkov in dolžnosti zavarovanja zbranih podatkov. V četrtem poglavju je urejeno vodenje evidenc in registra osebnih podatkov in potreba po vzpostavitvi kataloga zbirke

osebnih podatkov. Določa tudi postopke, ki jih mora upravljavec osebnih podatkov upoštevati pri obveščanju nadzornega organa.

Tretji del se imenuje Pravice posameznika, sestavlja ga osem členov. Določa postopke in pravice posameznika do seznanitve, popravkov, brisanja, dopolnitve, blokiranja, izbrisa in ugovora do osebnih podatkov, zbranih v njegovem imenu. Zagotavlja sodno varstvo posameznika ob možni zlorabi osebnihi podatkov.

Četrti del, Institucionalno varstvo osebnih pravic, se deli na štiri poglavja. Prvo in drugo poglavje določata nadzorni organ za varstvo osebnih podatkov, opredeljujeta njegove naloge, dolžnosti, položaj, določata njegove pristojnosti in možnosti sodelovanja z drugimi organi. V tretjem poglavju so opredeljeni inšpekcijski nadzor, njegov obseg nadzora in pristojnosti. Četrto poglavje se opredeli še do nalog varuha človekovih pravic na področju obdelave osebnih podatkov.

Peti del, Iznos osebnih podatkov, določa zakonsko podlago za prost pretok podatkov, če se ti iznašajo v državo članico EU ali v državo, ki je v Evropskem gospodarskem prostoru. Iznos podatkov v tretjo državo je možen, če to dovoli državni nadzorni organ, ki mora izdati odločbo, s katero zagotavlja, da je za varnost osebnih podatkov v tej tretji državi dobro poskrbljeno.

V šestem delu so urejene področne ureditve, kot so pravice in dolžnosti upravljavca osebnih podatkov ter pravice posameznika. Ureja pa tudi področja videonadzora, biometrije, evidence vstopov in izstopov iz prostora, javne knjige in varstva osebnih podatkov, povezovanja zbirk osebnih podatkov, strokovnega nadzora.

V sedmem delu so opredeljene kazenske določbe. Določa sankcije za vse, ki kršijo zakon oziroma nepravilno ravnajo z osebnimi podatki. Določene so tudi visoke globe.

Zadnji, osmi del, določa prehodne in končne določbe. Določa nekatere pristojnosti, predvsem pa roke pri izdaji zakonskih predpisov, kdaj začne določba veljati, in določa spremembe v drugih zakonih. (Zakonodaja, november 2013)

- Zakon o tajnih podatkih

Zakon o tajnih podatkih je bil sprejet leta 2001. Ureja področja varovanja zasebnosti države, poleg tega še določevanje, označevanje ter dostop do tajnih podatkov. Zakon uvaja nove termine oziroma oznake za tajnost podatkov: interno, zaupno, tajno in strogo tajno. Ti so prikazani v spodnji tabeli.

Tabela 1: Oznake tajnosti

OZNAKA	KRITERIJ – možne škodljive posledice
STROGO TAJNO	razkritje bi ogrozilo vitalne interese RS
TAJNO	razkritje bi lahko hudo škodovalo varnosti ali interesom RS
ZAUPNO	razkritje bi lahko škodovalo varnosti ali interesom RS
INTERNO	razkritje bi lahko škodovalo delovanju organa

Vir: Urad vlade RS za varovanje tajnih podatkov (2013)

Zavedati se je treba, da je kakršno koli razkritje tajnih podatkov nelegalno in nosi hude posledice. Še posebej se kriterij varnosti in sankcije zaostrijo za oznake zaupno in višje.

Leta 2003 so bile potrebne spremembe zakona, predvsem na področju preverjanja, zato so uvedli tri varnostna preverjanja: osnovno, dodatno in varnostno s poizvedovanjem. Uporaba teh preverjanj je odvisna od stopnje tajnosti podatkov, do katerih bo določena oseba imela dostop pri delu. Leta 2006 so sledile še nekatere spremembe, ki so izboljšale nacionalni sistem obravnavanja in varovanja tajnih podatkov, s tem se je povečala učinkovitost sistema in izboljšala varnost tajnih podatkov.

ZTP opredeljuje tudi vlogo informacijskega pooblaščenca in njegov postopek pri ugotavljanju javnega interesa za razkritje tajnih podatkov.

Določa inšpekcijski nadzor, ki ga na obrambnem področju zagotavlja in izvaja Inšpektorat RS za obrambo, z njim pa je zagotovljena večja enotnost izvajanja predpisov, ki se navezujejo na tajne podatke.

Zakon o tajnih podatkih določa skupne osnove enotnega sistema o odločanju, varovanju in dostopu do tajnih podatkov na delovnem področju državnih organov RS. Velja za delovna področja, ki se nanašajo na javno varnost, obrambo, prenehanje tajnosti podatka, zunanje zadeve, obveščevalno in varnostno dejavnost države. Zakon velja za vse državne organe, lokalne skupnosti, nosilce javnih pooblastil, gospodarske družbe in vse druge organizacije, ki razpolagajo s prej omenjenimi podatki. Če se tak podatek posreduje dobaviteljem, izvajalcem gradnje ali storitve, se morajo ti prav tako ravnati po tem zakonu. Vsak, ki je seznanjen z vsebino tajnega podatka, je odgovoren za varovanje in ohranitev tajnosti tajnega podatka.

3.5 NOTRANJI AKTI, PREDPISI DRŽAVNEGA ORGANA

- Zakon o varstvu pred naravnimi in drugimi nesrečami, katerega nadzor vsako leto opravi Inšpektorat Republike Slovenije. Do sedaj na tem področju niso imeli težav in je bilo za varnost dobro poskrbljeno.
- Notranji predpisi in pravila, ki jih morajo upoštevati pri obdelavi, hranjenju in posredovanju podatkov. Predvsem so podatki osebne, tajne narave, zato so natančno določeni protokoli dela z njimi.
- Predpisi, ki omejujejo prost vstop v poslopje. Potrebna je identifikacijska kartica in najava dan prej. Po vpisu v register obiskovalcev sledi varnostni pregled za kovinske izdelke, po stavbi pa so videonadzori in alarmi.
- Pravilnik o pogojih in načinu računalniškega dostopa do podatkov iz evidenc in zbirk geodetskih podatkov. Pravilnik ureja elektronsko varne pogoje in načine dostopa do geodetskih podatkov in pogoje, ki jih morajo geodetska uprava in pravne osebe, sodelujoče pri delu, upoštevati za zagotovitev varstva podatkov. Ureja tudi elektronske storitve, ki jih lahko uporabnik izvaja, in potrebno tehnično varstvo pri uporabi. Podobne pravilnike uporabljajo ostali državni organi, ki opravljajo elektronske storitve.

4 VARNOST PODATKOV

Zaradi razvoja tehnologije in vse večjega zbiranja različnih vrst podatkov v računalniških bazah so ti podatki v vse večji nevarnosti za nedovoljene, nepooblaščene dostope, spremembe in za izkoriščanje za nelegalne posle.

Potreba po zaščiti zasebnosti ljudi se je pojavila predvsem zaradi zlorabe zasebnih podatkov, napadov, žalitev in blatenja imena. Pred razvojem tehnologije so bili naši osebni podatki veliko bolj varni in naša zasebnost ni bila odprta in dostopna svetu, tako kot je sedaj v prisotnosti elektronskega poslovanja, nakupov preko spleta, telekomunikacij, e-pošte in e-bančništva.

Z novo tehnologijo lahko že vsak prisluškuje vsakemu, videonadzori so na skoraj vsakem našem koraku, računalniški vdori so vedno bolj pogosti in s tem kraja identitete, kraja denarja in elektronskih računov, kraja gesel za dostop na pomembne spletne strani, kot so e-poslovalnice, Klik, spletne trgovine ipd.

Primeri tega se velikokrat začnejo v naši e-pošti, kjer dobimo zanimive in vabljive ponudbe, ki v resnici niso resnične in želijo od naslovnika le osebne podatke, vpis na lažno stran, nakazilo denarja za začetek transkacij in podobne goljufije. Te goljufije so na primer "nigerijska prevara", "phishing", kraja identitete, goljufije pri spletnih nakupih in prodaji.

Za varnost na spletu moramo bolj ali manj poskrbeti sami. Dejstvo, da imamo na svojem računalniku antivirusni program in požarni zid, še ne pomeni, da smo varni. To je le osnovna zaščita, ki naj bi jo imel vsak računalnik, da sistem ni povsem odprt in dostopen vsakemu neznancu, ki želi videti podatke na trdem disku. Mislim, da bi si moral vsak, predvsem otroci (ti so že v zelo mladih letih dejavni na spletu), prebrati dejstva iz priročnika na spletu s tega področja. Ta priročnik se imenuje Hitri vodnik abc varnosti na spletu, ki seznani bralce s pomembnimi dejstvi in nasveti za ohranjanje varnosti med brskanjem po spletnih vsebinah. (SI-CERT, 2013)

Pred razvojem tehnologije so bili današnji elektronski podatki o nas shranjeni na papirjih in njihov dostop možen le s fizično prisotnostjo v arhivu oziroma prostoru, kjer so bili ti dokumenti hranjeni. Danes se dostopa do teh podatkov kar od doma, z nekaj kliki na računalniku. V večini primerov je za dostop do podatkov preko spleta potrebno digitalno potrdilo, geslo ali kakšna druga oblika identifikacije, vendar taka varnost ni vedno omogočena ali pa ni dovolj temeljita.

Varnost podatkov je pomembna za individualne osebe in za skupine oseb, pridobitne in nepridobitne organizacije, javna in zasebna podjetja. Vsakdo ima takšen ali drugačen podatek o sebi, o nekom drugem, o podjetju, poslovnem načrtu, novem izdelku, inovaciji, ki ga želi obdržati zase in ne deliti s svojo konkurenco in zunanjim svetom. Za preprečitev

neželenih dostopov do naših podatkov je pomembno, da dobro poskrbimo za varnost leteh. Odvisno od prostora, kjer se ti podatki hranijo, se tudi vrste varnosti razlikujejo.

Če so ti podatki shranjeni v fizični obliki, na papirju, v elektronskih medijih (diskete, zgoščenke, kasete, USB-ključki), je za njih potrebna fizična varnost. Če pa so ti podatki shranjeni na računalniških trdih diskih, na spletnem omrežju ali strežnikih, sta za njih potrebni elektronska varnost in fizična varnost, ki omejuje dostop do računalnika le na pooblaščeno osebje.

4.1 FIZIČNA VARNOST PODATKOV

Varnost podatkov je vsem vsak dan bolj pomembna, saj so zlorabe nekaterih naših podatkov vse bolj pogoste in preproste in povzročijo hude posledice žrtvam zlorabe. Prav zaradi teh nevšečnosti ZVOP-1 vsebuje sedmi del, ki se izključno nanaša na kazenske določbe. Za kazniva dejanja v povezavi s tajnimi podatki pa Zakon o tajnih podatkih predpisuje visoke globe za kršitelje.

Fizična varnost je en od elementov v celotnem sistemu varovanja podatkov. Bolj je pomembna pri organih države, institucijah, podjetjih, kjer so shranjene velike količine podatkov, predvsem osebnih, zaupnih, tajnih podatkov, ki so dostopni le pooblaščenim osebam. Varovanje osebnih podatkov je določeno z Zakonom o osebnih podatkih, podrobneje v 24. in 25. členu. Določata, kaj vse se mora varovati in na kakšen način. Zakon o tajnih podatkih določa, kdo, kdaj, kje in kako ima dostop do tajnih podatkov in do katerih tajnih podatkov glede na njihovo oznako. Dovoljenja za dostop in varovanje ter nadzor teh podatkov so podrobneje opredeljena v tretjem, četrtem in petem poglavju Zakona o tajnih podatkih.

Glavni cilj fizične varnosti je preprečiti nepooblaščen vstop v poslopje in nepoooblaščen dostop do podatkov ter odvrniti pozornost od teh podatkov. Sestava fizične varnosti je sklop povezanih postopkov in ukrepov, kot so organizacijski, varnostno-tehnični, mehanski ter postopki in ukrepi fizičnega varovanja. Za učinkovito varstvo podatkov je potrebna tesna povezanost vseh teh elementov in učinkovitost in kakovost vsakega posameznega elementa.

Na stopnjo varnosti vplivajo stopnja tajnosti varovanih podatkov, vrsta in oblika podatkov, njihova količina, način in mesto hranjenja, ocena ogroženosti teh podatkov in varnostna kultura zaposlenih. (Urad Vlade RS za varovanje tajnih podatkov, 2013)

Za fizično varstvo podatkov je pomembna organizacija varovanja podatkov, fizično varovanje, varstvo fizičnega dostopa osebja do nosilcev podatkov in varovanje nosilcev podatkov pred okvarami in uničenjem (naravne nesreče, namerno uničenje). Ob nesreči je dobro, če imamo na drugi lokaciji kopije podatkov. To pomeni, da moramo varovati še eno lokacijo, kar je lahko finančno zelo obremenilno za večino.

Za učinkovito fizično varovanje objekta oziroma prostora, kjer fizično hranimo podatke, je treba imeti zaupanja vredne zaposlene, usposobljeno varnostno osebje, ki poskrbi, da brez dovoljenja vstop v objekt ni možen. Pri tem delu pomaga videonadzor (ZVOP-1, 74. člen) poslopja zunaj in znotraj, da je celotno območje ves čas pod nadzorom. Redni varnostni pregledi okolice in notranjosti nikoli ne škodijo. Detektorji dima, tihi alarmi, detektorji gibanja, alarm za nepooblaščeno vstopanje v prostore in konstantna povezava s policijo so še dodatne možnosti, ki krepijo varnost objekta.

Naslednji primer prikazuje izreden primer fizične varnosti, ki se zdi že skoraj pretiran in paranoičen, vendar je cilj, varnost hranjenih podatkov, zagotovo dosežen.

Primer dobre fizične varnosti:
International Business Machines Corporation (IBM) ima odlično poskrbljeno za fizično varnost svojega celotnega objekta in je lahko zgled marsikateremu podjetju. Njihov fizično varen objekt vsebuje večkratne kontrole oskrbe z energijo, kontrole okolja in ukrepe za preprečitev nepooblaščenega dostopa. Celoten prostor pa varuje posebej usposobljeno osebje, ki ima zagotovljeno še dodatno podporo. Celotni varnostni sistem pokriva in varuje vse možnosti vdorov in prekinitve normalnega delovnega okolja.

Njihovi strežniki in oprema so pod stalnim varnostnim nadzorom, varnostniki identificirajo in beležijo vsak obisk, vsak dan, cele dneve, celo leto. Poleg stalne fizične prisotnosti varnostnikov so vhodi varovani še s sistemi človeške pasti, po celi stavbi so detektorji gibanja, dima in tihi alarmi, ki opozarjajo varnostnike in organe pregona o vdorih. Dostop do vrat in kletk je varovan z biometričnimi napravami, varnostne kamere pa pokrivajo vsak centimeter poslopja. Poskrbljeno je za neprekinjen dovod energije, imajo kar dva lokalna distributerja energije. Za povrh vsega pa imajo še akumulatorje in neprekinjeno napajanje (UPS), ki se atvomatsko vključi v nujnih primerih. Poskrbeli so tudi za nadzor okolja, ogrevanje, zračenje, klimatske naprave, ki zagotavljajo stalno temperaturo, vlažnost in pretok zraka v stavbi. Tudi ti sistemi za nadzor okolja so pod stalnim varstvom. Prostori so opremljeni z detektorji dima in ognja in ustreznim avtomatskim gašenjem – cevnimi sistemi in podtalnimi sistemi kontrole tesnosti. Stavba ima zagotovljeno lastno zalogo vode, kadar mestni vodovod ne dela.

Varnost je velikega pomena za IBM in svoj objekt so zavarovali do potankosti in onemogočili nepooblaščene vstope ali namerno motenje sistemov delovanja in poslovanja. Veliko varnostnih ukrepov, ki jih IBM uporablja, se zdi nepotrebnih in pretiranih, vendar je pri njih veliko pomembnih podatkov, ki opravičijo vse te ravni varnosti in so potrebni za zagotovitev zaupnosti in dolgotrajno varstvo hranjenih podatkov. (Dejavniki uspeha, 2013)

Ta raven varnosti v Sloveniji ni možna, saj nimamo toliko ponudnikov energije, vode, in mislim, da niti ni potrebe po takšni ekstremni varnosti. Finančna zmožnost podjetij pri nas ni primerljiva z IBM. Dobili smo predstavo, kaj vse je treba v današnjih časih varovati, da

se počutimo popolnoma varne in se ne obremenjujemo z možnostjo kraje hranjenih podatkov.

4.2 ELEKTRONSKA VARNOST PODATKOV

Veliko podatkov še vedno hranimo na papirju in v fizični obliki. Vendar se trudimo to opustiti in vse več podatkov shranjujemo na različne medije, kot so zgoščenke, diskete (te se ne uporabljajo več pogosto), USB-ključi, trdi diski, zunanji diski, strežniki ipd. Stare zapise na papirju se danes prenaša in zapisuje v elektronske, ker so tako lažje in hitreje dostopni. Elektronski način je poskrbel za hitrejše delovanje organizacij, vladnih institucij, dostop do javnih podatkov in informacij z nekaj kliki na spletni strani, ki hrani te podatke. Ni več treba brskati po kupih papirjev in arhivih, da najdemo določen podatek za nas ali stranko, saj do njega pridemo hitro in brez napora, samo vtipkamo v iskalnik, kaj želimo, in nam računalnik sam najde želeni podatek iz baze podatkov, ki ga nato uporabimo za svoje delo oziroma elektronsko posredujemo stranki ali natisnemo na papir. Kadar pride do prenašanja občutljivih osebnih podatkov preko omrežja, je treba uporabiti kriptografske metode in elektronski podpis, kar zagotovi nečitljivost in neprepoznavnost teh med prenosi. Šele v tem primeru lahko rečemo, da so podatki zavarovani, tako kot to določa Zvop-1 v 2. odstavku 14. člena.

Odprtost, dostopnost in razvoj tehnologije prinašajo tudi slabe strani podatkov v elektronski obliki. Skoraj vsak računalnik je povezan s spletom in je zato dostopen za vdore, okužbe, nedovoljene uporabe podatkov na našem računalniku. Če naši računalniki niso dovolj dobro in ustrezno zavarovani, obstaja možnost za okužbo sistema z virusi, s črvi, trojanskim konjem, neželeno pošto ipd. Zato se mora na tem področju upoštevati 24. člen ZVOP-1, ki ureja varnost podatkov. Hekerji2 so sposobni nedovoljeno vstopati v naše sisteme in si znajo pridobiti dostop do osebnih, tajnih podatkov ali česar koli drugega, kar želimo ohraniti zase, oziroma ne želimo deliti z drugimi. Da se obranimo vdorov, so potrebni dobri antivirusni programi, ki blokirajo neželeno pošto, skenirajo trdi disk za možne viruse, črve in trojanske konje. Če je tak škodljiv program najden, ga je treba popolnoma izbrisati iz sistema. Za to moramo biti tudi uporabniki previdni, katere spletne strani obiskujemo, katere povezave kliknemo, kaj vse snamemo s spleta, še posebej pa, čigavo e-pošto odpiramo, saj ravno preko e-pošte dobimo veliko okuženih datotek.

Pomembne vire hranimo na računalnikih, boljšo zaščito potrebujemo, da jih zavarujemo, saj so nekateri viri bolj privlačni za krajo ali nepooblaščeno spreminjanje kot drugi. Pod

---

2 Heker (angleško hacker) je oseba, vešča računalnikov, ki uživa v raziskovanju in pisanju programov in spoštuje svoja etična pravila. Meni, da nam računalniki izboljšujejo življenje, oblasti ne zaupa, računalniki in informacije pa naj bodo po njenem mnenju dostopne vsem. Kot intelektualni izziv ali pa namensko zlonamerno vdira v informacijske sisteme in omrežja, kjer lahko povzroči veliko škode in sitnosti žrtvam. (TikTak, 2013)

vire spadajo poslovni načrti in skrivnosti, številka socialnega zavarovanja, številke kreditnih kartic, zdravstvene kartoteke ipd. Paziti se moramo lažnih spletnih strani (npr. Klik NLB), kjer nevedoč vpišemo svoje podatke, ki jih prejme druga oseba, kot ji je bilo namenjeno, in s tem ji omogočimo dostop do svojega računa. Če veliko poslujemo in se dogovarjamo preko spleta, je dobro uporabljati digitalne podpise in kriptografske mehanizme. Za dodatno varnost lahko poskrbimo z dodatnimi gesli, s požarnim zidom, z odpravo pomanjkljivosti programske opreme in z redno posodobitvijo sistemov ter programske opreme. (Arzenšek, 2009, str. 15–18)

Poleg različnih varnostnih programov je dobro, da svoje podatke hranimo še na pomožni lokaciji kot "backup". Za vse izgube in nevarnosti podatkov na elektronskih medijih niso krivi le hekerji, virusi ipd., ampak tudi človeške napake in strojna oprema. USB-ključki so danes hitra in enostavna rešitev tega problema, saj lahko datoteke hitro prenesemo s trdega diska na USB in do teh datotek dostopamo iz katerega koli računalnika, če vključimo USB-ključek vanj. Druga rešitev je spletno hranjenje podatkov, kot ga ponujata Google Cloud Storage in iCloud. Varnost naših podatkov v tem primeru zna biti pod vprašajem, ker sta za dostop do njih potrebni le geslo in uporabniško ime, ki ju v nekaterih primerih ni težko pridobiti. (Arrow ECS, 2013)

Ljudje, kot so hekerji, zelo otežujejo varstvo elektronskih podatkov, zato je težko trditi, da so naši podatki varni. Mislim, da so še najbolj varni na USB-ključku, za katerega vemo le mi sami, in če se nam zdi potrebno, lahko datoteke na njem še dodatno zavarujemo z gesli. Do uničenja in spreminjanja podatkov v tem primeru pride le, če nam ga nekdo ukrade ali ga fizično uničimo.

Primer dobre elektronske varnosti:
International Business Machines Corporation (IBM) ima poleg dobre fizične varnosti tudi dobro poskrbljeno za elektronsko varnost svojega poslopja in podatkov, shranjenih v elektronski obliki. Previdni so že pri zagotovitvi internetne povezave celotnemu poslopju. Povezani so preko dodatnih IBM-povezav z več ponudniki spletnih storitev. Vse to podpira močna in odporna arhitektura za usmerjanje in uravnavanje bremenitev pri distribuciji. S pomočjo dveh aktivnih širokopasovnih ponudnikov internetnega omrežja je zagotovljena zanesljiva pasovna širina, optimalen promet pa je omogočen na podlagi tehtnega usmerjanja na osnovi BGP4 (Border Gateway Protocol). Njihovi sistemi so varovani s požarnimi zidovi Cisco PIX in z dodatnimi Cisco stikali. Obremenitev je uravnotežena z redundatnimi napravami Alteon, dovoljujejo pa le SSL (Secure Sockets Layer – kriptografski protokol) promet preko vrat 443 (internetna vrata, ko omogočajo odpiranje terminal.exe aplikacij) ter tako omogočajo najvišjo možno varnost. (Dejavniki uspeha, 2013)

4.3 MESTO HRANJENJA PODATKOV

Podatke vsak posameznik hrani na drugačen način, na mestih, kjer sam misli, da bodo najbolj varni in dostopni zanj. Imamo različne predstave o tem, kateri podatek nam osebno pomeni več in kateri manj. Glede na to jih bomo drugače varovali in hranili. Elektronsko hranjenje podatkov zveni najbolj varno in enostavno, vendar je včasih tudi fizično hranjenje dobra rešitev. Obe strani imata dobre in slabe strani, pri obeh lahko pride do težav, ki bi uničile naše podatke.

4.3.1 HRANJENJE FIZIČNIH PODATKOV

Kjub tehnološkemu razvoju se še marsikje hranijo podatki v fizični obliki. Javna uprava, sodišča, pravne službe, zasebna podjetja, posamezniki in drugi imajo še vedno vsaj nekaj podatkov, dokumentov, projektov na papirju in posebej shranjene nekje v svojem prostoru, kjer so vedno na dosegu, če se kaj zgodi. Vsakršna oblika hranjenja podatkov mora biti v skladu s 24. členom ZVOP-1, tudi dostopanje in zavarovanje.

Večina nas ima doma te spravljene v predalu, morda v sefu doma ali v banki, če so podatki bolj osebne, zaupne narave. Med drugim so to osebni dokumenti, potni list, rojstni list, spričevala, podatki o dohodnini, pogodbe ipd.

Podjetja, ustanove in pravne osebe imajo tega več kot mi doma, zato so potrebni posebni prostori za njihovo hranjenje. Ti prostori se imenujejo arhiv, ki morajo biti zavarovani pred nedovoljenimi vstopi, da zagotovijo kredibilnost podatkov v arhivu, varovani ob naravnih nesrečah, pred uničenjem datotek zaradi vlage in razpadom papirja.

Papir je na dolgi rok lahko uničen, če ni ustrezne vlage, temperature, svetlobe; ne sme biti preveč vlažno in svetlo v arhivu in temperatura naj bi bila sobna ter stalna. Prostor mora biti zavarovan pred naravnimi nesrečami in blizu izhoda, da se ob nesreči lahko reši podatke. Zaradi vseh teh dejavnikov so ponavadi arhivi v kletnih prostorih.

Med fizično hranjenje bi lahko šteli tudi podatke, shranjene na CD-jih, DVD-jih, zunanjih diskih, USB-napravah, saj so običajno na teh zaradi želje po dolgoročnem hranjenju elektronskih zapisov, ki jih ne potrebujemo vsakodnevno, in so fizično prenosljivi z ene lokacije na drugo.

Slabosti fizičnega hranjenja podatkov:
- Nedovoljen dostop do podatkov in fizično spreminjanje, kraja ali uničenje.
- Hranjenje na CD-jih, DVD-jih zavaruje podatke pred okužbo in hekerji, vendar je kakovost teh zgoščenk vprašljiva; moramo vedeti, da imajo omejen rok trajanja, še posebej, če so v pogosti uporabi, saj se površina popraska ali kako drugače poškoduje in s tem onemogoči branje zapisanih podatkov.

- Hranjenje na USB-ključkih je danes še najbolj priročno in hitro; tudi njihova kakovost in velikost je že tolikšna, da skoraj ni potrebe po drugih medijih, vendar se tudi ti dokaj hitro uničijo, če nismo pazljivi.
- Za večje datoteke, kot so filmi, serije, slike ali drugi podatki, pride v poštev hranjenje na zunanjih trdih diskih, kjer je ponovno pod vprašanjem kakovost in možnost okvare ali nezdružljivosti z računalnikom.
- Uničenje zaradi naravnih nesreč, vlage, neustrezne temperature ipd.
- Izguba papirjev, ne najdemo podatkov, ko jih potrebujemo.
- Lahko se zamaže napis in so podatki neberljivi.
- Za večje količine podatkov je potrebno veliko prostora, ki mora imeti ustrezne razmere za dolgotrajno hranjenje podatkov.
- Podatke je treba še fizično varovati.

Podatki, še posebej v veliki količini, so lažje dostopni, če so v elektronski obliki, saj je iskanje hitro in enostavno. Papirji se lahko izgubijo, založijo ali uničijo in tako izgubimo podatke. Je pa res, da se do fizične oblike podatkov dostopa le fizično, medtem ko so elektronski podatki dostopni ljudem z vsega sveta, če smo povezani s spletom in imamo slabo zaščiten sistem.

4.3.2 HRANJENJE ELEKTRONSKIH PODATKOV

Elektronske podatke smo včasih hranili na disketah, ki so nudile za današnje pojme "nič" prostora, le nekaj megabajtov (MB). Danes njihovo funkcijo opravljajo trdi diski, na katerih hranimo podatke in so veliki tudi po več terabajtov (TB). Diskete so zamenjali CD-ji z velikostjo 700 MB in DVD-ji z velikostjo nekaj gigabajtov (GB). Nato so tukaj še USB-ključki, ki so imeli sprva majhno zmogljivost, danes pa krepko presegajo DVD-je, saj imajo lahko do 128 GB prostora. USB-ključki so zelo priljubljeni, saj so majhni, lahko se pospravijo v žep in kljub temu vsebujejo ogromne količine elektronksih podatkov. Da razbremenimo naše trde diske v računalnikih za boljše delovanje sistema, so nam na voljo zunanji diski, ki nudijo prav tako kot trdi diski zmogljivost v terabajtih.

V večjih organizacijah, kjer delo poteka računalniško in iste podatke uporablja več zaposlenih na različnih delovnih področjih, je koristno imeti strežnik, ki povezuje vse računalnike in omogoča dostop do podatkov med njimi, brez da motijo drug drugega. Za večjo varnost ta strežnik ni nujno povezan z zunanjim svetom s spletno povezavo, tako da so podatki dosegljivi le znotraj organizacije.
Na ta način imajo urejene podatke tudi v izbranem državnem organu, kjer je interno delo povezano preko strežnika brez zunanjih povezav. Soba s strežnikom je pod videonadzorom, vodi se register vstopov in potrebna sta ustrezna izkaznica ter geslo za vstop. (Intervjuvanec, 2013)

Poleg vseh možnosti, ki nam jih ponujajo različni mediji za shranjevanje podatkov, je tukaj še splet. Na spletu si lahko najamemo svoj prostor, kamor naložimo podatke, ki so nato na voljo vsem (osebne ali poslovne spletne strani). Lahko pa zakupimo prostor na

spletu, ki služi kot neke vrste spletno skladišče, kamor naložimo in shranimo podatke in jih imamo pod geslom (iCloud). Ta drugi način nam tako kot pošta omogoča dostop do teh podatkov od kjer koli in kadar koli, dokler imamo internetno povezavo in vstopno geslo ter uporabniško ime.

Slabosti elektonskega hranjenja podatkov:

- Okužba računalniškega sistema z virusi, trojanskim konjem ali črvi, ki omogočijo nedovljen dostop do našega sistema ali druge oblike škode zbirki podatkov.
- Hekerski vdor v sistem, s katerim posameznik pridobi možnost vpogleda v naš sistem in spreminjanje vsebine, nastavitev ipd.
- Sesutje sistema lahko povzroči izgubo vseh podatkov, oziroma onemogoči dostop do njih, dokler se sistem ne vzpostavi nazaj.
- Odpoved strojne opreme, kot je trdi disk, ki hrani naše podatke; s tem izgubimo vse, kar smo imeli shranjeno na njem.
- Nenamerno izbrišemo podatke (te se v večini primerov da povrniti, če imamo znanje in program za to).
- Veliko ljudi, posebej poslovnežev, mora imeti stalen dostop do svojih podatkov od kjer koli in kadar koli, za take primere so primerni spletna skladišča podatkov kot sta iCloud, Google Cloud Storage in "dropbox" program; a tudi tu obstaja možnost hekerskih vdorov ali pa ponagaja slaba internetna povezava.

4.4 DOSTOP DO PODATKOV

Javni podatki so podatki, do katerih ima dostop vsak posameznik z zakonom zagotovljeno pravico. Problem dostopa do podatkov se pojavi pri zasebnih in osebnih podatkih, ki jih ne želimo deliti z javnostjo.

Za podatke in njihovo varnost skrbimo glede na njihov pomen za nas. Nekatere podatke imamo spravljene le v predalu ali kar na mizi, na vidnem mestu, druge pa v sefu doma ali v banki. Dostopanje do podatkov doma je za družinske člane lahko in ponavadi brez večjih ovir, razen če je za to posebej poskrbljeno in so zaklenjeni ali skriti. Tujec bo do teh podatkov težje prišel, ker bi moral vlomiti v stanovanje in preiskati stanovanje. Če doma hranimo podatke, za katere so ljudje pripravljeni kršiti zakon, je dobro, da imamo vgrajen alarm proti vlomilcem in nadzorne kamere. Možna rešitev so sefi v banki, kjer je za varnost in omejen dostop že zagotovljeno, sami pa dobimo še svoj unikaten ključ, s katerim dostopamo do zakupljenega sefa pri njih. Banka nadzira in beleži vse vstope v trezor oziroma prostor s sefi.

Podatki na računalnikih bi bili najbolj varni, če ta nima spletne povezave. Nenavadna gesla, ki se ne navezujejo na lastnikove lastnosti, so dobra zaščita, ki onemogočajo neposreden dostop do zasebnih podatkov. Tajni podatki pa so za večino ljudi lahko neberljivi in nevredni, saj so zavarovani z enkripcijo, ki se je ne da razbrati brez enkripcijskega ključa.

5 VARNOST PODATKOV V IZBRANEM ORGANU DRŽAVNE UPRAVE

5.1 PREDSTAVITEV ORGANA

Zaradi varnosti želi organ ostati neimenovan, zato bodo podatki predstavljeni splošno in brez podrobnosti, da se ohrani anonimnost. Ta organ se ukvarja s področjem dela, ki potrebuje pomembne podatke in dobro zaščito za njih.

Organ je imel leta 2013 vsega skupaj 8619 zaposlenih. Iz meseca v mesec se število zaposlenih ljudi pri njih ne spreminja za več kot deset. Skupno število zaposlenih jih uvršča med javne organe z večjim deležem zaposlenih v javni upravi.

Tako kot ostali državni organi tudi ta sledi piramidnemu sistemu, z ministrom na vrhu in državnim sekretarjem. Sledijo jima notranje organizacijske enote, kot so:
- različni direktorati;
- službe, ki pokrivajo razna notranja in zunanja področja;
- generalni sekretariat;
- organi v sestavi, ki jih ne morem bolj točno imenovati ali opisati, mednje spadajo inšpektorati, uprave ipd.

Organ opravlja še funkcije, ki izvirajo s področja informacij javnega značaja. Te so:
- demokratična funkcija, ki se izvaja zaradi deliberativnih modelov demokracije3;
- nadzorna funkcija, s katero se izpostavi pravica državljanov Republike Slovenija do neposrednega nadzora javnega sektorja;
- ekonomska funkcija, ta se ukvarja z ekonomsko vrednostjo informacij javnega značaja in potencialno dodatno vrednostjo kombiniranih informacij javnega značaja;
- funkcija posodabljanja javnega sektorja, ta se nanaša na informatizacijo dostopa do javnih informacij preko iniciativ za razvoj državnih portalov e-uprave.

5.2 VARNOST PODATKOV V ORGANU

Za pridobitev informacij o varstvu podatkov v izbranem državnem organu sem opravil intervju pri njih. Za kontaktno osebo sem izbral vodjo oddelka za informatiko, odgovori

---

3 Deliberativni model demokracije ali diskurzivna demokracija je neke vrste neposredna demokracija, kjer politične odločitve sprejema in oblikuje ljudsvto v procesu razprave oziroma deliberacije, vse skupaj pa poteka javno. Ta tip demokracije ni usmerjen v volitve, glasovne mehanizme, referendume. V ospredju so komunikacijski mehanizmi in deliberacija. Namen razvoja deliberativne demokracije je v odpravljanju pomankljivosti predstavniške demokracije, glasovnih mehanizmov, preprečitev izkrivljanja in zanemarjanja volje ljudstva. (Wikipedija, 2013)

niso povsem podrobni, saj želi organ ostati anonimen in ne sme razkriti informacij o njihovem načinu zaščite podatkov in dela. Informacije v nadaljevanju so pridobljene z intervjujem, ta pa je priložen diplomskemu delu.

5.2.1 KATERE VRSTE PODATKOV HRANIJO IN KJE?

Vsakodnevno se v organu obdelujejo velike količine podatkov osebne in tajne narave, ki morajo zaradi varnosti ostati skrbno varovani. Tajnost teh podatkov je pomembna za ohranitev ugleda organa in neovirano delo zaposlenih.

Zaradi širokega področja, ki ga ta organ pokriva, se zaposleni tukaj ukvarjajo z vsemi možnimi vrstami podatkov; od osebnih, ekonomskih do tajnih. Ogromno podatkov nastaja z delovnega področja državnega organa, kar nekaj pa jih je z nacionalnega področja in iz tujine, saj so vsi ti potrebni za delo, s katerim se ukvarjajo. Dokumenti so v fizični in elektronski obliki, zaradi tehnologije pa elektronska oblika dokumentov že nekaj let prevladuje nad fizično. Vse vrste podatkov so še posebej označene s stopnjo tajnosti in imajo temu primerno urejeno varnost.

Podatki so shranjeni v prostorih organa oziroma na njihovi informacijski opremi (mediji, trdi diski, zunanji diski, USB-ključki, strežniki) v prostorih državnega organa; informacije javnega značaja pa najdemo na njihovi spletni strani. Prostori in informacijska oprema so zasnovani tako, da zagotavljajo čim večjo trajnost in varnost podatkov. Fizično so podatki hranjeni v protivlomnih omarah, pomembnejši podatki, kot so tajni podatki, pa v trezorjih in ustreznih blagajnah. Varnostna stopnja teh omar in trezorjev mora ustrezati potrebni varnostni stopnji tistega dokumenta z najvišjo varnostno stopnjo.

Rok hranjenja posameznih podatkov je različen in odvisen od potrebe po podatkih, ki izhajajo iz delovnega procesa, dodatno pa morajo za rok upoštevati še zakonska določila, ki urejajo hranjenje podatkov, njihovo obdelavo in arhiviranje.

5.2.2 KAKO JE POSKRBLJENO ZA VARNOST PODATKOV?

Varnost podatkov določata Zakon o osebnih podatkih in Zakon o tajnih podatkih, kar organ upošteva pri obdelavi, prenosu in hranjenju podatkov. Zaradi velike količine in raznovrstnosti podatkov je treba pri delu poznati in upoštevati več zakonskih predpisov in področij, ki urejajo njihovo varnost, pri tem sta pomembna tip podatka in oznaka tajnosti. S pomočjo teh parametrov se določijo ustrezna varnost, tehnična rešitev in organizacijski postopki za varovanje.

Predvsem za podatke v fizični obliki je pomembna regulacija in nadzor dostopa do podatkov, s katerima se zagotovi sledljivost dostopa. Fizično varovanje je poskrbljeno že pri vhodu, saj so tam varnostniki in za vstop mimo recepcije vsi potrebujejo dovoljenje in potreben je prehod skozi napravo, ki skenira kovinske izdelke. Hodniki so pod nadzorom

kamer, pisarne imajo protipožarne alarme, vstop v določene prostore je še dodatno varovan z gesli in s karticami. Sam dostop v uradne poslovne prostore ureja ZVOP-1 v 75. členu.

Dokumenti v fizični obliki so hranjeni v posebnem prostoru, arhivu, z omejenim dostopom in vsakemu dostopu do teh se sledi z evidenco, tako da ne pride do nepooblaščenih vstopov in razvrednotenja dokumentov. Ti prostori so zasnovani tako, da dokumentov ne uničijo vlaga, temperatura, poplava ali druge naravne nesreče. Za varnost prostora skrbi kombinacija fizičnih, tehničnih in organizacijskih oblik varovanja. Kombinacija vseh teh oblik varovanja zagotavlja zahtevano varnost fizičnih in elektronskih podatkov. Za varnost takih predelov poskrbijo protivlomna vrata, ključavnice, varnostne verižice in zapahi. Oprema in material, ki zahtevata za svojo ohranitev in delovanje ustrezne klimatske razmere, sta nameščena v posebej urejenih prostorih. Taki prostori so velik finančni zalogaj, posebej pri veliki količini takega materiala, zato se skuša takšne vrste prostorov združevati in priti do minimalne potrebne količine takšnihi prostorov, vendar združevanje ni vedno mogoče.

Več ali manj vse delo poteka računalniško in v elektronski obliki. Še vedno pa se hodi po podpise in štemplje odgovorne osebe na dokumentih v papirni obliki in se nato ta dokument upodobi (skenira) nazaj v elektronsko obliko. Delo, ki se opravlja v organu in poteka računalniško, je zavarovano z antivirusnimi programi, ki jim organ zaupa in so redno posodobljeni. Poleg tega so računalniki opremljeni s požarnimi zidovi in z rednimi pregledi računalnikov, da ne bi prišlo do hekerskih vdorov ali drugih nepooblaščenih dejanj. Pri delu so vsi zaposleni povezani le z Intranetom in ne z globalnim internetom, kar zagotavlja dodatno varnost pri njihovem delu z elektronskimi podatki. Organ uporablja notranji strežnik, ki ni povezan z zunanjim svetom, in na njem se hranijo elektronski podatki, ki so tako na voljo vsem pooblaščenim delavcem hitro in brez težav. Hranijo tudi kopije podatkov, podatki, namenjeni le enemu oddelku ali za nevsakdanjo rabo, so hranjeni na medijih, kot so CD-ji, DVD-ji, USB-ključki in prenosni diski. Slednji so v varnosti zaposlenih, ki z njimi ravnajo. Ker so prostori informatikov dostopni le preko gesla ter predhodnih varnostnih ukrepov, so mediji, kot so USB-ključki, zgoščenke in podobno, varne v njihovih prostorih. Ob koncu delovnega dneva se ti mediji pospravijo v predale oziroma omare, ki se zaklenejo. USB-ključki, ki vsebujejo bolj občutljive podatke, so zavarovani z geslom.

Organ ima svoje informatike, ki skrbijo za posodobitve programske opreme in popravilo okvare strojne opreme. Poskrbljeno je za dodatne izobraževalne programe na področju nove tehnologije, novih programov, ki jih uvajajo v delo, tako so informatiki seznanjeni z novostmi na trgu informacijske tehnologije. S tem je poskrbljeno za njihovo ustrezno usposobljenost pri delu in pomoč drugim zaposlenim, vsak namreč ne sledi posodobitvam pisarniške opreme, kot so Microsoftovi programi, ki hitro dobivajo nove verzije in uvajajo spremembe. V takih primerih je treba imeti izobražen kader, ki zna pomagati.

5.2.3 ELEMENTI FIZIČNE VARNOSTI

Varnostnik je en od glavnih elementov fizične varnosti. Njegovo delo obsega obhode, naloge čuvajev in varnostno-receptorkso službo. Njihova osnovna naloga je zagotavljanje varnosti objekta pred škodo, vlomi, ropi, odtujitvijo in uničenjem lastnine. Varnostne ocene, ocene tveganja in sama zahtevnost objekta določajo obliko in stopnjo potrebne varnosti. Na podlagi tega se določi, ali so varnostniki stalno prisotni ali le občasno. Pravice in dolžnosti varnostnika veljajo le za območje, ki ga varuje, izven njega varnostnik nima pooblastil.

Za bolj učinkovito in lažje delo varnostnikov je potrebna urejena okolica objekta, ki omogoča preglednost. Prav tako je pomembna osvetlitev območja, kjer poteka delo, saj je dobra vidljivost pomemben del varnosti. Pregledna okolica varovanega objekta omogoča boljši videonadzor, omogočen mora biti dostop interventnim silam. Če so v bližini strelovodi, morajo biti redno vzdrževani in ob možnosti nalivov mora biti poskrbljeno za odvajanje meteorne vode, da ne pride do nepotrebnih naravnih nesreč v objektu.

Meje varovanega objekta označuje varnostna ograja. Ta ograja mora služiti kot fizična ovira pred nepooblaščenim vstopom, onemogočati plezanje preko nje in preskakovanje. Mora biti dovolj močna, da je ni mogoče raztegniti ali prerezati. Celotno mejno območje, ki ga označuje ograja, je pod videonadzorom.

Okna so varovana z rešetkami, odpornimi proti udarcem, rezanju ali raztezanju. V pritličnih in kletnih prostorih se uporablja protivlomna folija, ki prepreči razsutje stekla, če se ta razbije.

5.2.4 KAKO JE POSKRBLJENO ZA PODATKE OB NARAVNI NESREČI?

Ob naravni nesreči, ki bi ogrozila varnost podatkov, hranjenih v prostorih organa, se uporabijo primeri dobre prakse oziroma priporočila in standardi, ki urejajo to področje in določajo postopke, ki se uporabljajo za varovanje podatkov. Za ključne sisteme so izdelani ustrezni načrti. Vse to se stalno ažurira in občasno preverja njihova učinkovitost in uporabnost.

5.2.5 ALI JE OBMOČJE ORGANA UREJENO S SEKTORJI VAROVANJA?

Območje je deljeno na cone oziroma na varnostna območja. Stopnja območja in temu ustrezna varnost se razlikuje glede na pomembnost prostora. Na primer recepcija ima manjšo varnostno stopnjo kot prostor s tajnimi podatki in zato so tudi varnostni predpisi za prostor za tajne podatke veliko bolj podrobni in natančni. Že uporaba mobilnih telefonov je odvisna od varnostnega območja, v katerem se nahajamo. V 1. varnostnem območju se mobilnih telefonov ne sme uporabljati, v 2. varnostnem območju pa le pogojno.

5.2.6 KAKO LAHKO NEZAPOSLENI VSTOPI V PROSTORE ORGANA?

Ni važno, katera oseba je to, se mora najaviti vsaj en dan prej, da se zanjo uredi izkaznica. Če je to prijatelj zaposlenega ali sorodnik, lahko to uredi zaposleni sam ob vhodu pri varnostniku. Osebo preverijo skladno z Zakonom o obrambi in Zakonom o tajnih podatkih in vpišejo v register ter zanjo pripravijo izkaznico obiskovalca.

Za obiskovalce, zunanje izvajalce in posebne goste velja hišni red državnega organa. Hišni red določa obveznosti gostitelja in dolžnosti gosta. Ob prihodu se ta oseba identificira z osebnim dokumentom, prevzame izkaznico, ki jo mora ves čas nositi na vidnem mestu, in biti v spremstvu zaposlenega. Pred vstopom osebo preverijo z detektorjem kovine. Gost ima dostop le do prostorov, za katere je bil namen obiska predviden.

Pri poslovnih obiskih in sestankih se prav tako osebo najavi prej in uredi njen dostop v prostore. Oseba se identificira z osebnim dokumentom in preverijo jo z detektorjem in nato lahko dostopa do zaposlenega, s katerim je dogovorjena. Ob odhodu teh oseb mora gostitelj pospremiti gosta do recepcije, kjer gost preda izkaznico in izstopi iz poslopja.

5.2.7 ALI ZAKONSKI PREDPISI OVIRAJO, ZAVIRAJO DELO S PODATKI?

Praviloma vsak predpis ovira izvajanje nalog, nenazadnje tudi omejitev hitrosti omejuje pretočnost vozil na cestah. Zakonodajalec (nosilec posameznega predpisa) s predpisom želi določeno področje/postopek/okolje urediti na sistematičen in urejen način. Vsak predpis vsebuje podatke o namenu predpisa, obseg in ostale elemente, ki so nujni za izvedbo naloge. Obstaja velika verjetnost, da so področja prenormirana, da so predpisi med seboj neusklajeni. Posledica je, da se veliko časa porabi za medsebojno preverjanje predpisov in manj za samo delo.

Dolžnost javnih uslužbencev in državljanov je opozarjati na neusklajenost predpisov, dolžnost državnih organov pa ažuriranje teh anomalij.

5.2.8 ALI OBSTAJAJO POTREBE PO IZBOLJŠANJU VARNOSTI?

Zaradi sprememb v zakonodaji, ki ureja področje varovanja podatkov, je velika pozornost namenjena stalnemu nadgrajevanju sistemov. Reorganizacija in kadrovske fluktuacije povzročijo potrebo po spremembi notranjih aktov, ki urejajo organizacijo varovanja podatkov. Poleg tega je tehnološki razvoj tako hiter, da informacijska oprema in tehnologija, ki ju organ uporablja, hitro zastarata in je zato potrebno stalno nadgrajevati sisteme, se učiti o novostih in upoštevati implementacijo novih tehnoloških standardov.

Za fizično varnost in nadzor je dobro poskrbljeno in niso imeli še nobenih zapletov, ki bi škodovali organu ali delu, ki ga opravljajo. Varnost se začne že pri vstopu na parkirišče, kjer varnostno osebje preverja izkaznice. Pri varnosti sledijo zakonskim predpisom in jih izpolnjujejo, prav tako niso imeli nobenih hekerskih vdorov. Varnost njihovih operacijskih sistemov je zagotovljena in ker vse delo poteka na notranjem strežniku, brez zunanje povezave, je vdor možen le od znotraj. Če ne pride do kakšnih drastičnih sprememb in novih groženj, je za varnost pri njih ustrezno poskrbljeno.

5.3 TAJNI PODATKI

Tajni podatki so pogosti pri delu v izbranem državnem organu, zato organ vsako leto organizira predavanja in preverjanja na tem področju za svoje zaposlene. Tudi Pravilnik o varovanju tajnih podatkov sledi spremembam in se spreminja, zadnje spremembe so bile dodane letos.

V nadaljevanju so podani primeri, ki jih morajo poznati zaposleni, ki imajo dostop do tajnih podatkov. (Test, 2013)

Tabela 2: Primerjava poimenovanja oznak tajnosti

SLOVENSKE	NATO	EU
STROGO TAJNO	COSMIC TOP SECRET	TRES SECRET UE/EU TOP SECRET
TAJNO	NATO SECRET	SECRET UE/EU SECRET
ZAUPNO	NATO CONFIDENTIAL	CONFIDENTIEL UE/EU CONFIDENTIAL
INTERNO	NATO RESTRICTED	RESTREINT UE/EU RESTRICTED

Vir: Urad Vlade RS za varovanje tajnih podatkov (2013)

Poimenovanje tajnosti je predvsem pomembno, če je delo na mednarodni ravni, saj je treba vedeti, katero stopnjo tajnosti podatka obravnava njihovo delo.

V nadaljevanju je naštetih nekaj zadev s testa, ki jih morajo poznati vsi zaposleni z dostopom do tajnih podatkov:

- Če se najde dokument z oznako strogo tajno in se ga ne potrebuje več, se tak dokument uniči, vendar je o tem treba pisno obvestiti izdajatelja tega dokumenta.

- Postopek določitve stopnje tajnosti dokumenta se začne z oceno možnih škodljivih posledic, nato se dokument označi s stopnjo, evidentira in podpiše ga poooblaščena oseba.
- Čeprav ima zaposleni nacionalno dovoljenje stopnje tajnosti tajno, še ne pomeni, da lahko dostopa do podatkov EU z oznako tajno. Za te podatke mora zaprositi za izdajo dovoljenja EU tajno.
- tajnem dokumentu lahko govorimo šele, ko vsebuje stopnjo tajnosti in se ve, kdo ga je izdal, tako kot to določa ZTP.
- Vsak, ki je v stiku s tajnimi podatki, tudi kurir, mora biti ustrezno preverjen in imeti dovoljenje oziroma pooblastilo za prenos. Rok varovanja tajnih podatkov ne poteče tudi po prenehanju delovnega razmerja.
- Če zaposleni želi oziroma mu je treba dodeliti dostop do dokumentov z oznako nacionalno tajno, ga je treba najprej varnostno preveriti. To je mogoče le, če obravnavana oseba s tem pisno soglaša.
- Dokumentov z oznako EU strogo tajno ne sme kopirati nihče, niti direktor za obrambno politiko, in pod nobenimi pogoji.
- ZTP omogoča dostop do tajnih podatkov brez varnostnega preverjanja naslednjim osebam: predsedniku Vlade RS, poslancem, članom Komisije za nadzor nad delom varnostnih obveščevalnih služb, informacijskemu pooblaščencu in županu.
- Kopiranje tajnih podatkov je dovoljeno le do stopnje tajno in le na podlagi pisarniške odredbe.
- Tajnih podatkov z oznako zaupno se ne pošilja po informacijskem sistemu.
- Če se izda naročilo zaupne narave zunanjemu izvajalcu, mora ta pridobiti varnostno dovoljenje za stopnjo, ki je v pogodbi.
- Dokumenta z oznako nato secret se ne sme hraniti v pisarni zaposlenega po izteku delovnega časa.
- Zaposleni z dovoljenjem tajno to dovoljenje obdrži tudi po odhodu v pokoj in se mu ga ne sme odvzeti.
- Podatke s stopnjo zaupno je treba preveriti, če izponjujejo vse pogoje za oznako vsaka tri leta.
- Član Državne revizijske komisije lahko dostopa do tajnih podatkov tudi brez dovoljenja za dostop.

Za tajne podatke je tudi poskrbljeno varovanje v primernih varnostnih območjih glede na njihovo stopnjo. To prikazuje naslednje preglednica.

Tabela 3: Varnostna območja

Stopnje tajnosti tajnega podatka	Obravnavanje tajnega podatka	Osebje	Hranjenje tajnega podatka	Prenašanje tajnega podatka
Strogo tajno	Varnostno območje I. ali II. stopnje	Dovoljenje za dostop do tajnih podatkov stopnje STROGO TAJNO	Blagajna najmanj protivlomne stopnje III	Lastna prenosna mreža
Tajno	Varnostno območje I. ali II. stopnje	Dovoljenje za dostop do tajnih podatkov TAJNO	Blagajna najmanj protivlomne stopnje II	Lastna prenosna mreža
Zaupno	Varnostno območje I. ali II. stopnje	Dovoljenje za dostop do tajnih podatkov ZAUPNO	Blagajna najmanj protivlomne stopnje II	Lastna prenosna mreža
Interno	Upravno območje oziroma varnostno območje III. stopnje	Osnovno usposabljanje in podpisana izjava o seznanjenosti s predpisi	Pisarniška ali kovinska omara	Najmanj priporočeno s povratnico

Vir: Urad vlade RS za varovanje tajnih podatkov (2013)

Iz preglednice je razvidno, da sta za tajne podatke stopnje interno potrebni le osnovna varnost in seznanjenost oseb. Upravno območje dovoljuje le dostop do internih tajnih podatkov, prostor je nadzorovan, preverja se vstop in izstop.

Varnostno območje I. stopnje ima prav tako nadzor nad vstopi in izstopi ter dogajanjem v samem prostoru. Vsak vstop in izstop se evidentira, vodi se tudi evidenca tajnih podatkov, do katerih posamezna oseba dostopa. Oseba, ki želi dostopati do tega območja, potrebuje posebno dovoljenje predstojnika. Prepovedan je vstop s kakršnimi koli napravami, ki bi omogočale presnemavanje ali odtujitev dokumentov. Ves čas je prisotno fizično varovanje prostora in podatkov v njem.

6 ZAKLJUČEK

Varnost podatkov postaja vse bolj pomembno področje in potrebuje čedalje več pozornosti s pravnega, fizičnega in tehničnega vidika. Zato se zakonodaja v zadnjem času bolj posveča področju varnosti podatkov, elektronskemu poslovanju in uveljavlja spremembe za boljšo varnost.

Z diplomskim delom sem skušal prikazati prednosti in slabosti uporabe elektronskih podatkov, ki vse pogosteje nadomeščajo papirno obliko. Na podlagi izbranega državnega organa sem predstavil potrebno fizično in tehnično varovanje, ki omogočata varno obdelovanje podatkov, med katerimi se najdejo številni občutljivi podatki, kot so osebni in tajni. Ob tem morajo zaposleni v organu upoštevati še vrsto zakonov, ki urejajo varnost osebnih in tajnih podatkov, obdelavo podatkov ter njihovo hranjenje. Zaradi varnosti je organ ostal anonimen, vendar sem skušal pridobiti čim več konkretnih in uporabnih informacij o njihovi varnosti podatkov.

Okolica objekta je pod konstantnim videonadzorom, območje obkroža mreža, ki preprečuje prehod na njihovo ozemlje. Varnostniki opravljajo redne obhode, pri vstopu v objekt pa vodijo evidenco prihodov in odhodov. Vsak se mora identificirati pred vstopom in stopiti skozi napravo za odkrivanje kovinskih predmetov. Elektronski vdori od zunaj so onemogočeni, saj zaposleni uporabljajo Intranet, računalniški sistemi so na najvišji stopnji varnosti, z antivirusnimi in protivohunskimi programi. Poleg tega redno izvajajo tehnične preglede.

Na podlagi vseh varnostnih ukrepov, ki jih uporabljajo, lahko sklepam, da je dostop do elektronskih podatkov dobro varovan in zelo otežen. Poskrbljeno je tudi za omejitev osebnih pristopov k fizičnim podatkom in vsak dovoljen pristop je evidentiran in nadzorovan.

Kljub zadržanosti organa za več konkretnih podatkov sem dosegel namen diplomskega dela. Iz podatkov iz intervjuja s kontaktno osebo, zaposleno na oddleku za informatiko v izbranem državnem organu, je razvidno, da je za varnost pri njih dobro poskrbljeno. Glede na to, da gre za državni organ, ki nima opravka le z osebnimi podatki, ampak tudi s tajnimi podatki najvišje stopnje, sklepam, da je pri nas tudi drugje na državni ravni enako dobro poskrbljeno za tehnično in fizično varnost, kot je v tem organu.

S pridobljenimi podatki sem dokazal, da je organ varnostno sposoben upravljanja vseh vrst podatkov, tudi tajnih podatkov stopnje strogo tajno. Dostop do podatkov imajo le osebe s posebnimi dovoljenji, le te jih lahko obdelujejo in le v svojih delovnih prostorih. Ob koncu uporabe se ti hranijo v trezorjih ali varnostnih omarah, če so ti v fizični obliki. Elektronske podatke hranijo pod gesli in enkripcijami v varnem sistemu. Ko podatkov ne potrebujejo več za delo in jim poteče zakonski rok hranjenja, te podatke uničijo, blokirajo ali anonimizirajo.

Kljub napredku informatizacije, razvoju e-poslovanja in e-uprave bodo v organu še nekaj časa uporabljali oba načina shranjevanja podatkov in zato potrebovali dobro organiziranost in varnost, da se kakšen podatek ne izgubi, zameša ali razvrednoti.

S povečanjem obsega elektronskih podatkov se bo olajšalo delo v arhivu, ne bo več potrebnih toliko varnih prostorov za shranjevanje fizičnih dokumentov. Potrebna bo večja varnost na tehničnem področju, zagotoviti bo treba varno elektronsko okolje za dolgoročno in kratkoročno shranjevanje podatkov in še naprej uspešno nadzorovati in preprečevati nepooblaščene in zlonamerne vdore do hranjenih podatkov.

Pri pregledu sem opazil, da so sankcije za kršitev zakonov o varnosti podatkov le globe. Te so sicer visoke, vendar mislim, da zgolj globa ni zadostna sankcija, predvsem za kršitev zakonov o osebnih podatkih in tajnih podatkih, ker so posledice lahko katastrofalne za organizacijo, državo in posameznika.

Glede na stanje varnosti pri njih verjamem, da je tudi pri drugih državnih organih za varnost podatkov dobro poskrbljeno in na podoben način. Dokler bodo sledili novostim in zagotavljali sedanjo raven varnosti, bodo vsi podatki pri njih varni.

LITERATURA IN VIRI

LITERATURA

- Arzenšek, Milica (2009). Tehnično varovanje v e-poslovanju. Diplomsko delo, Ekonomsko-poslovna fakulteta Maribor, Maribor.
- Čebulj, Janez (1990). Varstvo osebnih podatkov z zakonskimi pooblastili. Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, Ljubljana.
- Čebulj, Janez, Žurej, Jurij (2005). Varstvo osebnih podatkov in informacije javnega značaja. Nebra, Ljubljana.
- Kotnik, Mateja (2010). Obveščevalne službe in varstvo podatkov. Diplomsko delo, Fakulteta za varnostne vede, Maribor.
- Likar, Simon (2009). Varstvo osebnih podatkov v policiji. Diplomsko delo, Fakulteta za upravo Ljubljana, Ljubljana.
- Test s področja tajnih podatkov (2013). Anonimen državni organ.
- Verdonik, Ivan, Bratuša, Tomaž (2005). Hekerski vdori in zaščita. Pasadena, Lubljana.
- Vintar, Mirko (1996). Informatika. Paco, Ljubljana.
- Šaponja, Vladimir (1999). Taktika dela obveščevalno varnostnih služb. Visoka policijsko-varnostna šola, Ljubljana.

SPLETNI VIRI

- An SAP Company (2013). Fizična varnost in povezljivost. Dejavniki uspeha. Privzeto 22. 6. 2013 iz: http://www.dejavnikiuspeha.si/sl/fizicna-varnost.
- Arrow ECS (2013). Zagotovitve varnosti podatkov. Privzeto 5. 8. 2013 iz: http://www.arrowecs.si/novice/zagotovite-varnost-podatkov.
- Blažič Jerman, A. (2004). Informacijska varnost. Monitor. Privzeto 5. 8. 2013 iz: http://www.monitor.si/clanek/informacijska-varnost/122021/?xURL=301.
- Ministrstvo za notranje zadeve (2013). Osebni in tajni podatki. Privzeto 3. 7. 2013 iz: http://www.mnz.gov.si/si/mnz_za_vas/osebni_in_tajni_podatki.
- Safe.si (2013). Center za varnejši internet. Privzeto 1. 7. 2013 iz: http://www.safe.si.
- Slovenski center za posredovanje pri omrežnih incidentih (2013). Varni na internetu. Privzeto 8. 7. 2013 iz: https://www.varninainternetu.si.
- TikTak Wikipedia (2013). Heker. Privzeto 1. 7. 2013 iz: http://www.tiktak.si/geslo/Heker.
- Trend Micro (2013). Data Security. Privzeto 5. 8. 2013 iz: http://www.trendmicro.com/us/enterprise/data-protection/index.html.
- Upravne enote RS (2013). Informacije javnega značaja. Privzeto 22. 6. 2013 iz: http://www.upravneenote.gov.si/informacije_javnega_znacaja.
- Urad RS za varovanje tajnih podatkov (2013). Privzeto 23. 6. 2013 iz: http://www.uvtp.gov.si.

- Urad vlade RS za varovanje tajnih podatkov (2013). Fizična varnost. Privzeto 7. 8. 2013 iz: http://www.uvtp.gov.si/si/delovna_podrocja/fizicna_varnost/.
- Wikipedija (2013). Deliberativna demokracija. Privzeto 7. 8. 2013 iz: http://sl.wikipedia.org/wiki/Deliberativna_demokracija.
- Zakonodaja.com (2013). Zakon o osebnih podatkih. Privzeto 1. 7. 2013 iz: https://zakonodaja.com/zakon/zvop-1.

ZAKONI

- (1991). Ustava Republike Slovenija (Ustava RS). Ur. list RS, št. 33/1991-I, 42/1997, 66/2000, 24/2003 in 69/2004, 68/2006, 47/2013.
- (1994). Evropska konvencija o človekovih pravicah (EKČP). Ur. list RS – Mednarodne pogodbe, št. 7–41/1994, UL RS št. 33/1994.
- (1995). Direktiva 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov. Informacijski pooblaščenec.
- (1995). Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov 1981 (Konvencija, št. 108). Ur. list RS, št. 11/1994 – Mednarodne pogodbe, št. 3/1994.
- (2004). Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). Ur. list RS, št. 94/2007.
- (2001). Zakon o tajnih podatkih (ZTP-UPB2). Uradni list RS, št. 50/2006, 60/2011.
- (2008). Pravilnik o pogojih in načinu računalniškega dostopa do podatkov iz evidenc in zbirk geodetskih podatkov. Ur. list RS, št. 25/2008, 10/2011.

PRILOGA

Intervjuval sem kontaktno osebo s področja informatike v izbranem državnem organu.

1. Katere vrste podatkov hranite pri vas?

Državni organ obdeluje in hrani lastne podatke z delovnega področja državnega organa ter tiste nacionalne in tuje podatke, ki jih potrebuje za izvajanje nalog državnega orgnana. Ti podatki so v fizični obliki (dokumenti) in v elektronski obliki. Že nekaj let je obseg podatkov v elektronski obliki precej obsežnejši kot obseg podatkov v fizični obliki. Podatki, ki jih državni organ hrani, so tudi označeni z različnimi stopnjami tajnosti.

2. Kje se hranijo podatki v fizični in elektronski obliki?

Državni organ hrani podatke v svojih prostorih oziroma v informacijski opremi, ki je last državnega organa in je v prostorih državnega organa. Prostori so zgrajeni tako, da se zagotavlja čim večja trajnost in varnsot hranjenih podatkov.

3. Koliko časa se hranijo podatki?

Podatke se hrani skladno s potrebami, ki izhajajo iz delovnega procesa ter z obveznim upoštevanjem zakonskih določil, ki urejajo obdelavo, hranjenje in arhiviranje podatkov.

4. Kako je poskrbljeno za varnost podatkov pri vas?

Pri obdelavi, prenosu in hranjenju se upoštevajo zakonska določila, ki urejajo varnost podatkov. Varnost podatkov ureja več zakonov, kar pomeni, da je treba glede na tip podatka ter oznako tajnosti samega podatka izbrati ustrezno tehnično rešitev ter organizacijske postopke. Pri tem je eden od ključnih elementov regulacija dostopa do podatkov, na osnovi katere je zagotovljena sledljivost dostopa do podatkov.

5. Zakaj je potrebna varnsot vaših podatkov? Kakšne so možne posledice slabega varstva?

Nepooblaščeno razkritje podatkov ima različne posledice. Skupni imenovalec vseh posledic je zmanjšanje ugleda državnega organa oziroma škodovanje delu. Glede na vrsto podatka so posledice tudi: posledice zaradi nepooblaščenega razkrivanja osebnih podatkov javnih uslužbencev, zaposlenih v organu, finančno-komercialne posledice zaradi nepooblaščenega razkrivanja tehničnih podatkov, ki so predmet izvajanja pogodb oziroma raziskovalnih projektov, kjer je v pogodbah posebej označeno, da se morajo ti podatki varovati, in posledice zaradi nepooblaščenega razkrivanja tajnih podatkov, kjer je treba upoštevati, da je varovanje tajniih podatkov urejeno z mednarodnimi pogodbami, katerih podpisnica je RS.

6. Ali imate interne akte, ki določajo varnost podatkov?

Imamo lastne pravilnike, navodila in druge interne akte, s katerimi so predpisani tehnični in organizacijski ukrepi za varovanje podatkov.

7. Ali je potreba po izboljšavi varnostnih sistemov pri vas?

Zaradi spreminjanja zakonodaje, ki ureja to področje, je posebna pozornost namenjena nadgradnji sistemov. Zaradi reorganizacije ter kadrovske funkcije so potrebne spremembe notranjih aktov, ki urejajo organizacijo varovanja podatkov. Nenazadnje pa je zaradi hitre tehnološke zastarelosti informacijske tehnologije treba te sisteme stalno nadgrajevati, pri tem pa je vključena implementacija novih tehnoloških standardov. Varnostni sistemi se nadgrajujejo in preverjajo dovolj pogosto, da ne zastarajo, prav tako se nudi izobraževanje našim zaposlenim, predvsem informatikom, za novosti na področju informacijske tehnologije.

8. Ali zakonski predpisi ovirajo delo s podatki? Je zaradi predpisov o postopku obdelave podatkov čas, porabljen za obdelavo podatkov, nekoristno porabljen?

Praviloma vsak predpis ovira izvajanje nalog, nenazadnje tudi omejitev hitrosti omejuje pretočnost vozil na cestah. Zakonodajalec (nosilec posameznega predpisa) s predpisom želi določeno področje/postopek/okolje urediti na sistematičen in urejen način. Vsak predpis vsebuje podatke o namenu predpisa, obseg predpisa in vse ostale elemente, za katere zakonodajalc meni, da so nujni za izvedbo naloge. Obstaja velika verjetnost, da so določena področja prenormirana in da so predpisi med seboj neusklajeni in zato obstaja tudi verjetnost, da je veliko časa lahko nekoristno porabljenega za medsebojno preverjanje predpisov. Dolžnost javnih uslužbencev in državljanov je ob neusklajenosti predpisov opozarjati na takšne anomalije, dolžnost državnega organa (skrbnika predpisa) pa je redno ažuriranje teh predpisov.

9. Kako je poskrbljeno za fizično varnost podatkov in kako za elektronsko?

Za varnost je poskrbljeno s kombinacijami tehničnih, fizičnih in organizacijskih oblik varovanja. Le kombinacija naštetih zagotavlja zahtevano varnost podatkov v fizični obliki. Oprema, ki za svoje delovanje zahteva ustrezne klimatske razmere, oziroma material, ki za trajnejše hranjenje zahteva predpisane klimatske razmere, sta v ustrezno urejenih prostorih. Zaradi visokih stroškov ureditve takšnih prostorov se poskuša z združevanjem število takšnih prostorov zmanjšati na nujno potreben minimum, vendar združevanje ni vedno možno.

10. Kako je poskrbljeno za varnost podatkov v primeru naravne nesreče?

Vsaj za ključne podatke oziroma ključne sisteme so izdelani ustrezni načrti. Pri tem se v največji možni meri uporabljajo dobre prakse oziroma priporočila in standardi, ki urejajo to področje. Načrti se stalno ažurirajo in občasno tudi preverjajo.

11. Ali je območje organa deljeno po sektorjih varovanja?

Da. Za vsako območje so določena pravila, ki obravnavajo možnost dostopa, kaj se lahko počne in česa se ne sme početi.

12. Ali se lahko mobilni telefoni uporabljajo kjer koli v organu?

Ne. Skladno z Zakonom o tajnih podatkih se v I. VO mobilnega telefona ne sme uporabljati, v II. VO pa le pogojno.

13. Se varnostno preveri vse zaposlene in obiskovalce? Kako je urejen vstop na območje organa obiskovalcem?

Varnostno preverjanje se izvaja skladno z Zakonom o obrambi in Zakonom o tajnih podatkih. Za obiskovalce, zunanje izvajalce in posebne goste velja hišni red državnega organa. Hišni red predpisuje postopke najave takšnega dogodka, obveznosti gostitelja ter dolžnosti gosta.

Hvala za sodelovanje