UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

VAROVANJE IN ZAŠČITA DOKUMENTOV IN OSEBNIH PODATKOV V ZBIRKAH DOKUMENTOV

Polona Prelogar Pestotnik

Ljubljana, oktober 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

VAROVANJE IN ZAŠČITA DOKUMENTOV IN OSEBNIH PODATKOV V ZBIRKAH DOKUMENTOV

Kandidatka: Polona Prelogar Pestotnik
Vpisna številka 04025770
Študijski program: visokošolski študijski program Javna uprava
Mentor: višji pred. mag. Iztok Sirnik

Ljubljana, oktober 2011

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Polona Prelogar Pestotnik, študentka visokošolskega strokovnega programa Javna uprava, z vpisno številko 04025770, sem avtorica diplomskega dela z naslovom: Varovanje in zaščita dokumentov in osebnih podatkov v zbirkah dokumentov.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbela, 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 pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in se to tudi jasno zapisala v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja v grafični obliki, s katerim so tuje misli oz. Ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu 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 Lidija Jurman, prof. slov. j.

Ljubljana, 4. 10. 2011 Podpis: Polona Prelogar Pestotnik

POVZETEK

Naloga obravnava varovanje in zaščito dokumentov in osebnih podatkov v zbirkah dokumentov. Prvo poglavje je namenjeno varovanju in zaščiti dokumentov, hrambi dokumentarnega gradiva v digitalni obliki in varovanju tajnih podatkov. Ker je to občutljivo področje, je zelo pomembno, da se upoštevajo zakoni in drugi podzakonski akti. Drugo poglavje zajema varstvo in zavarovanje osebnih podatkov. Vsakršno zbiranje, obdelovanje, namen, nadzor in varstvo osebnih podatkov so točno določeni v zakonih in podzakonskih aktih.

Varovanje in zaščita dokumentov in osebnih podatkov v zbirkah dokumentov sta odvisna tudi od posameznika, ki te podatke obdeluje. Vprašanje je, ali bo upošteval vsa pravila in podatkov ne bo zlorabil ali pa se bo pokazala njegova slabost in bo prišlo do zlorabe teh podatkov. Zato je pri občutljivih dokumentih in osebnih podatkih potrebno še dodatno osebno preverjanje.

Ključne besede: varovanje, zaščita, dokument, dokumentarno gradivo, arhivsko gradivo, osebni podatek

SUMMARY

SECURITY AND PROTECTION OF DOCUMENTS AND PERSONAL DATA IN DOCUMENT MANAGEMENTS SYSTEMS

The paper discusses preservation and protection of documents and personal data in document collections. First chapter is intended for presentation of preservation and protection of documents, records in digital form and preservation of classified information. Since this is very delicate subject it is imperative to regard legislation and other regulation acts. Second chapter describes preservation and protection of personal data. Any kind of collecting, processing, purpose, control and preservation of personal data is precisely defined in legislation and other regulation acts.

Preservation and protection of documents and personal data in document collections also depends on the individual that maintains that information. Does he follow all the rules and won't misuse the information or will his weak nature overcome and data will be misused. That is why additional personal verification is necessary at handling delicate documents and personal data.

Keywords: preservation, protection, document, records, archival material, personal data.

KAZALO

KAZALO PONAZORITEV

KAZALO TABEL

KAZALO PRILOG

1 UVOD

Varovanje in zaščita dokumentov in osebnih podatkov v zbirkah dokumentov nista preprosti opravili. Pri delu z dokumenti in osebnimi podatki je treba upoštevati fizično varovanje oziroma dostopnost samo pooblaščenim osebam, informacijsko varnost, tehnično varovanje itd. Ker se obdelujejo tudi občutljivi dokumenti in osebni podatki, je treba upoštevati osebnostne lastnosti posameznika, ki upravlja z njimi.

Fizično varovanje dokumentov preprečuje, da bi nepooblaščene osebe dostopale do določenih prostorov. Z identifikacijsko kartico ali kodo se določi omejitev gibanja po prostorih. Pri vhodih v zavarovane prostore se lahko uvede tudi video nadzor, vendar z ustreznimi opozorili, da je ta prostor pod video nadzorom. Z določenimi gesli se omeji dostop do različnih računalniških programov, z gesli pa se še dodatno zaščitijo računalnik, različni programi, podatkovna baza itd. Delo v sistemu se dodatno evidentira, pri čemer se zapisujejo vse opravljene transakcije iz različnih računalniških postaj.

Delodajalec se pred zlorabo dokumentov zaščiti tako, da bodočega uslužbenca seznani z njegovimi pravicami in obveznostmi do njega. Velikokrat je treba preveriti lojalnost, zanesljivost, preverjanja pa se razlikujejo glede na varnostno območje. Za preprečevanje njihove zlorabe je potreben celovit varnostni sistem, kot so dokumentacijska, fizična, tehnična varnost in sledljivost podatkov skozi celo njihovo življenjsko obdobje.

Dokumentarno gradivo nastaja v vseh organizacijah. Organizacije so dolžne dokumentarno gradivo hraniti, reproducirati, omogočiti dostopnost do gradiva itd. Arhivsko gradivo je pomembno za znanost, kulturo in strokovno javnost. Javno arhivsko gradivo hrani Arhiv Republike Slovenije. Zaradi varnosti in zlorabe gradiva se določijo roki omejitve uporabe gradiva oziroma roke nedostopnosti. Dokumentarno gradivo morajo podjetja hraniti v ustreznih prostorih in pogojih, da jih zaščitijo pred uničenjem, zlorabo ali izgubo.

Glede na obseg dokumentov postaja hramba dokumentarnega gradiva v digitalni obliki čedalje pomembnejša. Ker so dokumenti shranjeni v elektronskem zapisu, se zmanjšajo težave s prostorom, manjša pa je tudi nevarnost propada oziroma zbledelosti zapisa. V Republiki Sloveniji delujejo podjetja, ki nudijo pomoč in storitve pri shranjevanju dokumentov v digitalni obliki. Za hranjenje, zajemanje in upravljanje dokumentarnega in arhivskega gradiva v digitalni obliki je treba spoštovati zakone in predpise. Podjetje, ki želi hraniti izvorne dokumente v digitalni obliki, se z ustreznimi zahtevki obrne na Arhiv Republike Slovenije, ki mu izda dovoljenje za upravljanje dejavnosti.

Ko se je Republika Slovenija pridružila članicam Nata in Evropske unije, je sprejela določene standarde Nata in Evropske unije glede varovanja in rokovanja s tajnimi dokumenti. Slovenska zakonodaja se je na področju dodatnih oznak tajnih podatkov in

razvrščanja tajnih podatkov popolnoma uskladila z evropsko zakonodajo. Osebe, ki bodo imele dostop do tajnih podatkov, morajo biti ustrezno varnostno preverjene. Preverjanje pa se razlikuje glede na stopnjo tajnosti dokumentov.

Varovanje in zaščito osebnih podatkov ureja Zakon o varstvu osebnih podatkov, pomemben pa je tudi 38. člen Ustave Republike Slovenije. V Republiki Sloveniji je vsakemu človeku ne glede na narodnost in prebivališče zagotovljeno varstvo osebnih podatkov. Posamezniku ta pravica ne sme biti kršena. Osebni podatki se lahko zbirajo le za neki določen namen, vsaka nadaljnja uporaba teh podatkov je prepovedana. Obdelava osebnih podatkov je mogoče le, če je to določeno z zakonom. Upravljavec osebnih podatkov pa mora imeti za obdelavo podatkov posameznika njegovo pisno dovoljenje. Vsakdo se ima pravico seznaniti, zakaj so bili njegovi osebni podatki zbrani.

Proti zlorabi osebnih podatkov oziroma za varstvo posameznika, na katerega se podatki nanašajo, je potrebno ustrezno zavarovanje. Ponovno sta pomembni fizično varovanje in zaščita ter hkrati tudi preverjanje uslužbenca, ki bo upravljal z osebnimi podatki drugih oseb. Fizično varovanje je mogoče doseči z omejitvijo dostopa do določenih prostorov z identifikacijsko kartico ali kodo, s tem se prepreči dostop nepooblaščenim osebam. Zagotoviti je treba učinkovit način blokiranja, uničenja in izbrisa osebnih podatkov ter preprečiti nepooblaščen dostop do osebnih podatkov pri prenosu, tudi preko telekomunikacijskih omrežij. Omogočiti je treba poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni, uporabljeni ali kako drugače obdelani v bazi podatkov ter kdo je to storil in v katerem obdobju. Občutljivi osebni podatki pa morajo biti pri obdelavi posebej označeni in zavarovani.

Obdelava osebnih podatkov je mogoča le na podlagi zakona ali pa na podlagi privolitve posameznika, katerega podatki se obdelujejo. Prepovedana je obdelava osebnih podatkov, ki kažejo na rasni ali politični izvor, politična mnenja, verska in filozofska prepričanja, pripadnost sindikatu, ter podatkov v zvezi z zdravjem ali spolnim življenjem.

Enotna matična številka (EMŠO) je v Republiki Sloveniji identifikacija za opredelitev posameznika. Ob rojstvu vsak posameznik dobi enotno matično številko, ki sestoji iz rojstnih podatkov, številke registra, spola in kontrolne številke. Upravljavci zbirk uporabljajo EMŠO le na podlagi zakona. Drugi najpogostejši povezovalni znak oziroma identifikacija pa je davčna številka. Praviloma se davčna številka uporablja, kadar nastane davčno razmerje.

Osebne podatke je treba hraniti toliko časa, dokler je to potrebno za dosego namena. Zakon glede na različne evidence podatkov določa različne roke hrambe podatkov. Po končanju hrambe osebnih podatkov je treba vse osebne podatke izbrisati, uničiti, blokirati, razen podatkov, ki so opredeljeni kot arhivsko gradivo.

Da bi upravljavci osebnih podatkov lažje vodili postopke, vodijo katalog osebnih podatkov. Katalog osebnih podatkov vsebuje 13 točk, pod vsako točko pa se zapišejo zahtevani

podatki, kot so osebni podatki, pravne podlage, namen obdelave itd. Vsak upravljavec osebnih podatkov je dolžan imeti pri sebi en izpisan izvod kataloga osebnih podatkov za posamezno zbirko podatkov Na podlagi zakona je to dolžan pokazati posamezniku, katerega podatki se obdelujejo.

2 VAROVANJE IN ZAŠČITA DOKUMENTOV

Varovanje in zaščita dokumentov sta zelo pomembni dejavnosti, pred tem pa je treba urediti ustrezno varovanje in zaščito programske opreme. Podjetja nameščajo sisteme za preprečevanje vdorov, protivirusno programsko opremo in požarne pregrade, vedno boljša pa je tudi zaščita strežnikov, omrežij in namiznih delovnih postaj. Pri tem pa večina spregleda zaščito pred zlorabo tiskalnikov in fotokopirnih strojev. Na tiskalnikih in fotokopirnih strojih se obdelujejo, shranjujejo in tiskajo podatki različnih poslovnih enot, oddelkov in uporabnikov. Zaradi pomanjkanja njihove ustrezne zaščite to za podjetje lahko prestavlja finančno breme in še nekatere druge grožnje, saj je za napadalca vrednost tega sistema prav tolikšna kot kateregakoli drugega samostojnega sistema v omrežju. Podatki, ki so namenjeni tiskanju, so prepuščeni številnim varnostnim grožnjam. Pet najpogostejših napak, ki ogrožajo varnost poslovanja, so:

- izguba intelektualne lastnine, ker se je konkurenca preko zaposlenih dokopala do zaupnih podatkov;
- zaupni podatki zaidejo v medije, kar povzroči padec tečaja delnic ali škodi ugledu znamke;
- dostop do zaupnih podatkov podjetja na trdem disku tiskalnika ob njegovi prodaji;
- zaposleni po pomoti dobijo v roke osebne podatke nekoga drugega ali na tiskalniku vzamejo zaupne poslovne načrte podjetja;
- dostop do zaupnih podatkov preko omrežja.

2.1 POMEN IZRAZOV

Da bi lažje razumeli pomen posameznih izrazov s področja varstva dokumentarnega in arhivskega gradiva, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih v 2. členu podrobno razloži njihov pomen (ZVDAGA, 2. člen).

DOKUMENTARNO GRADIVO – je izvirno in reproducirano (pisano, risano, tiskano, fotografirano, filmano, fonografirano, magnetno, optično ali kako drugače zapisano) gradivo, ki je bilo prejeto ali je nastalo pri delu pravnih oziroma fizičnih oseb.

DOKUMENTARNO GRADIVO V FIZIČNI OBLIKI – je dokumentarno gradivo na fizičnem nosilcu zapisa, ki omogoča reprodukcijo vsebine brez uporabe informacijsko komunikacijskih ali sorodnih tehnologij (na primer na papirju, filmu itd.).

DOKUMENTARNO GRADIVO V ELEKTRONSKI OBLIKI – je dokumentarno gradivo v digitalni ali analogni obliki.

DOKUMENTARNO GRADIVO V DIGITALNI OBLIKI – je dokumentarno gradivo v digitalni obliki zapisa in shranjeno na elektronskem nosilcu zapisa.

DOKUMENTARNO GRADIVO V ANALOGNI OBLIKI – (npr. analogni avdio/video zapis) je dokumentarno gradivo v analogni obliki zapisa in shranjeno na elektronskem nosilcu zapisa.

DOKUMENTARNO GRADIVO V DIGITALNI OBLIKI ZA DOLGOROČNO HRAMBO – je gradivo, katerega vsebina je zapisana v digitalni obliki in shranjena na elektronskem nosilcu zapisa, pri čemer tako digitalna oblika kot tudi nosilec zapisa zagotavljata učinkovito dolgoročno hrambo in upoštevanje tehnološkega napredka v skladu s tem zakonom.

IZVIRNO DOKUMENTARNO GRADIVO – je dokumentarno gradivo, ki je nastalo, bilo prejeto ali bilo poslano osebi, ki hrani to gradivo.

ZAJETO DOKUMENTARNO GRADIVO – je dokumentarno gradivo, ki je nastalo ob zajemu izvirnega dokumentarnega gradiva v hrambo s pretvorbo izvirnega dokumentarnega gradiva v novo digitalno obliko zapisa ali na mikrofilm.

ARHIVSKO GRADIVO – je dokumentarno gradivo, ki ima trajen pomen za znanost in kulturo ali trajen pomen za pravno varnost oseb v skladu s strokovnimi navodili pristojnih arhivov.

JAVNOPRAVNE OSEBE – so državni organi, organi samoupravnih lokalnih skupnosti ter nosilci javnih pooblastil in izvajalci javnih služb.

PRISTOJNI ARHIVI – so državni arhiv (Arhiv Republike Slovenije), regionalni arhivi in arhivi samoupravnih lokalnih skupnosti.

JAVNO ARHIVSKO GRADIVO – je arhivsko gradivo, ki se odbere iz dokumentarnega gradiva javnopravnih oseb po strokovnih navodilih pristojnega arhiva.

ZASEBNO ARHIVSKO GRADIVO – je dokumentarno gradivo drugih pravnih in fizičnih oseb, ki ima lastnosti arhivskega gradiva in je kot arhivsko gradivo določeno na podlagi tega zakona ali odločbe državnega arhiva.

HRAMBA GRADIVA – je tista hramba izvirnega ali zajetega dokumentarnega gradiva, ki izpolnjuje pogoje po tem zakonu in zagotavlja uporabnost vsebine hranjenega gradiva.

DOLGOROČNA HRAMBA GRADIVA – je hramba gradiva za časovno obdobje, daljše od pet let.

STORITVE HRAMBE GRADIVA V DIGITALNI OBLIKI – so storitve, ki so neločljivo povezane z ohranjanjem vsebine gradiva v digitalni obliki, vendar ne gre za ponudbo opreme za takšno hrambo.

NOTRANJA PRAVILA ZAJEMA IN HRAMBE GRADIVA V DIGITALNI OBLIKI – so pravila, ki jih kot svoj interni pravni akt sprejme oseba glede hrambe svojega gradiva.

OBČUTLJIVI OSEBNI PODATKI – so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v politični stranki in sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence, ki se vodijo na podlagi zakona, ki ureja prekrške, biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

STROJNA OZIROMA PROGRAMSKA OPREMA ZA ZAJEM OZIROMA HRAMBO GRADIVA V DIGITALNI OBLIKI – je vsaka strojna oziroma programska oprema, katere namen je v celoti ali delno omogočiti zajem ali hrambo gradiva v digitalni obliki ter s tem povezana opravila.

PONUDNIK STROJNE IN PROGRAMSKE OPREME ZA HRAMBO GRADIVA V DIGITALNI OBLIKI – je vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči uporabo strojne ali programske opreme za zajem oziroma hrambo gradiva v digitalni obliki.

PONUDNIK STORITVE HRAMBE DOKUMENTARNEGA GRADIVA V DIGITALNI OBLIKI – je vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči hrambo dokumentarnega gradiva v digitalni obliki na svoji infrastrukturi.

SPREMLJEVALNE STORITVE – so storitve, ki so povezane z zajemom ali hrambo gradiva v digitalni obliki, vendar ne predstavljajo ponudbe opreme za zajem ali hrambo in tudi ne storitev hrambe.

PONUDNIK SPREMLJEVALNIH STORITEV GLEDE ZAJEMA ALI HRAMBE GRADIVA V DIGITALNI OBLIKI – je vsaka oseba, ki za druge osebe odplačno ali neodplačno opravlja takšne storitve.

2.2 DOKUMENTARNO GRADIVO

»Dokumentarno gradivo imenujemo vse zapise (dokumente), ki nastajajo pri delu oziroma poslovanju organizacije, ne glede na način zapisa, vrsto, obliko in namen« (Brejc, 2004, str. 139).

Dokumentarno gradivo delimo na:

- dokumentarno gradivo, ki je v reševanju. Strokovni uslužbenci gradivo še obdelujejo in ga imajo pri sebi;

- tekoča zbirka dokumentarnega gradiva. Gradivo je že rešeno, vendar pa se hrani pri posameznih organizacijskih enotah ali pa centralno;
- stalna zbirka dokumentarnega gradiva. Gradivo ki je že rešeno in se hrani v organizaciji za daljši čas ali trajno.

2.2.1 VRSTE DOKUMENTARNEGA GRADIVA

Glede na nastanek oziroma zapis dokumentarnega gradiva poznamo:

- pisano gradivo je glede na način izdelave lahko pisano z roko, računalnikom, pisalnim strojem ali tiskarskim strojem, ki nastaja v obliki dokumentov, knjig in kartotek. V obliki knjig so predvsem evidence, kot so:
  - uradne evidence: rojstne, poročne in mrliške matične knjige, državljanske knjige, volilni imeniki, zemljiške knjige itd.,
  - neuradne (druge) evidence: knjige soglasij, knjige odtisov, knjige pečatov, knjige hotelskih gostov itd.,
  - kartoteke: finančne evidence, evidenca stanja in zalog materiala, spisovne evidence,
  - druge knjige: dnevniki, kronike, spominske knjige itd.;
- risano gradivo so zapisi, narejeni s črtami, včasih pa so uporabljena tudi druga sredstva za zapis, enako kot pri pisanem gradivu. Risano gradivo sestavljajo: načrti gradbenih objektov, strojev, predmetov, filmskih scen itd.;
- tiskano gradivo nastaja pri velikem številu izvodov. To so: plakati, letaki, vabila, vizitke, zapiski sej itd.;
- slikovni zapis nastaja na steklenih ploščah, fotografskih filmih in papirju slike ter predstavlja zapis določene osebe, dogodka ali stvari. Nastajajo v informacijski dejavnosti, kot sta medicina in kriminalistika;
- zvočni zapis so zapisi govorjene besede in glasbe, ki so posneti na gramofonskih ploščah, filmskih trakovih, magnetofonskih trakovih, kasetah in zgoščenkah. To so zvočni zapisi na sestankih, zborovanjih, glasbenih prireditvah itd.;
- računalniški zapis so posnetki podatkov na določenih materialih, nosilcih, ter omogočajo obdelavo podatkov in besedil in pa hrambo le-teh. To so: magnetni trakovi, magnetni diski, magnetni bobni, zgoščenke itd.

2.2.2 TEMELJNA NAČELA DOKUMENTARNEGA GRADIVA

Temeljna načela so vrednostna merila, ki delujejo na podlagi pravnih pravil ter so opredelitev in napotila za delo.

Temeljna načela dokumentarnega gradiva so:

- načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine. Pomeni, da se ohrani izvirno dokumentarno gradivo ali pa uporabnost vsebine, ki je v gradivu. Da je hramba zajetega gradiva enaka hrambi izvirnega gradiva, je treba zagotoviti zajetemu gradivu vse učinke izvirnega gradiva (ZVDAGA, 3. člen);

- načelo trajnosti. Hramba dokumentarnega gradiva mora zagotavljati trajnost gradiva oziroma reprodukcijo njene vsebine (ZVDAGA, 4. člen);
- načelo celovitosti. Hramba dokumentarnega gradiva mora zagotavljati nespremenjenost in neokrnjenost dokumentarnega gradiva oziroma reprodukcije in urejenosti njene vsebine ter dokazljivost izvora dokumentarnega gradiva (ZVDAGA, 5. člen);
- načelo dostopnosti oziroma reprodukcije. Vsebina dokumentarnega gradiva mora biti ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom (ZVDAGA, 6. člen);
- načelo varstva kulturnega spomenika. Arhivsko gradivo je kulturni spomenik in mora biti varovano kot takšno (ZVDAGA, 7. člen).

2.3 ARHIVSKO GRADIVO

Arhivsko gradivo je dokumentarno gradivo, ki ima trajen pomen za znanost in kulturo ali trajen pomen za pravno varnost oseb v skladu s strokovnimi navodili pristojnih arhivov (ZVDAGA, 23. člen). Arhivsko gradivo je kulturni spomenik in mora biti varovano kot takšno.

Arhivsko gradivo določi pristojna arhivska organizacija (Arhiv Republike Slovenije, regionalni arhiv itd.) in ne ustvarjalec gradiva. Glavna lastnost arhivskega gradiva je njegova vsebina in ne njegova zunanja oblika.

Arhiv hrani (MK, Arhiv RS, 2011):

- arhivsko gradivo republiških upravnih in drugih državnih organov ter nekdanjih državnih ali avtonomnih organov na stopnji dežele ali podobni višji stopnji, ki so imeli sedež na ozemlju Slovenije ter so upravno in sodno pokrivali njeno celotno ozemlje (od 15. stoletja dalje);
- arhivsko gradivo organov, organizacij in društev s področja gospodarstva, bančništva, zdravstva in socialnega varstva, šolstva, kulture in znanosti, ki so po svojih pravilih delovali za celotno območje današnje Slovenije ali njenih nekdanjih dežel (od 16. stoletja dalje);
- arhivsko gradivo zemljiških gospostev, rodbin, družin in posameznikov, ki je pomembno za zgodovino (od 13. stoletja dalje);
- arhivsko gradivo v zbirkah: listine (od 12. stoletja dalje), rokopise (od 9. stoletja dalje), zemljiške knjige (od 18. stoletja dalje), katastre (od 18. stoletja dalje), načrte (od 18. stoletja dalje) itd.

Slovenski filmski arhiv hrani slovenske dokumentarne, animirane in igrane filme od najstarejšega slovenskega filma iz leta 1905. Ohranjenih je več kakor 90 odstotkov slovenskih filmov (MK, Arhiv RS, 2011).

Arhiv po stanju ob koncu leta 2004 hrani 1809 arhivskih fondov in zbirk od 9. stoletja do danes v skupnem obsegu več kakor 16.356 tekočih metrov gradiva na papirju, 5.651 naslovov filmov, 909 video naslovov (1214 kosov), 3.745 mikrofilmskih kolutov, 8.311 mikrofišev in 26 kaset mikrofišev, 157.859 fotografij, 591 kosov nosilcev zvoka in 21.903 kosov zapisov na drugih nosilcih ter druge vrste arhivskega gradiva (listine, diplome, katastre, karte, zemljevide, kasete, diskete itd.) Vse arhivsko gradivo je hranjeno na skupaj 24.980 dolžinskih metrih arhivskih polic, v 187 predalnikih, 158 kovinskih omarah, v 148 kartotečnih omarah itd (MK, Arhiv RS, 2011).

2.3.1 UPORABA ARHIVSKEGA GRADIVA

V arhivih se arhivsko gradivo uporablja v znanstvenoraziskovalne, kulturne, izobraževalne in publicistične namene. Kadar pravne in fizične osebe izkažejo pravni interes, lahko arhivsko gradivo uporabljajo tudi v upravne, poslovne in osebne namene. Za raziskovalne, študijske, kulturne, uradne, poslovne, osebne in druge namene je arhivsko gradivo na voljo v izvirnikih ali kopijah v čitalnicah Arhiva RS na Zvezdarski 1 in na Kongresnem trgu 1 v Ljubljani. Arhiv je odprt tudi za skupine, kot so osnovnošolske, srednješolske, študentske in druge skupine ter posameznike.

Na pisno zahtevo strank izdaja Arhiv Republike Slovenije tudi različna potrdila ter overjene in neoverjene kopije dokumentov za uradne, poslovne in osebne namene po pošti, telefaksu, elektronski pošti ali strankam osebno.

V skladu z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), Uredbo o varstvu dokumentarnega in arhivskega gradiva ter v skladu s Čitalniškim redom Arhiva Republike Slovenije in pogoji izročiteljev fondov in zbirk glede vrst in rokov dostopnosti se daje v uporabo javno in zasebno arhivsko gradivo.

Arhivsko gradivo lahko uporabljajo fizične in pravne osebe, mladoletne osebe pa morajo pred uporabo predložiti potrdilo zakonitega zastopnika ali ustrezne ustanove. Tuji državljani so glede uporabe izenačeni z domačimi. Za raziskovalne in študijske namene uporabnikov arhiv iz arhivskega gradiva ne išče podatkov ter zanje ne opravlja transliteracij[1], prevodov in drugega raziskovalnega dela. Vsi uporabniki odgovarjajo za zlorabo vseh vrst tajnosti, zlorabo osebnih podatkov in podatkov, ki se nanašajo na zasebnost posamezne osebe.

2.3.2 DOSTOP DO ARHIVSKEGA GRADIVA

Za uporabo je javno arhivsko gradivo dostopno v javnih arhivih. Izjema je gradivo, ki ima roke nedostopnosti, ki so določeni z omejitvami uporabe. Roke nedostopnosti je mogoče skrajšati, kadar javni ali znanstveni interesi prevladujejo nad interesi, ki jih je treba

[1] Prečrkovanje, kjer eni črki (ali skupini črk) iz prve pisave ustreza vedno ista črka (ali skupina črk) iz druge pisave (Wikipedija).

varovati zlasti zaradi varstva osebnega in družinskega življenja oseb. Roke javnega arhivskega gradiva je na zahtevo javnopravne osebe mogoče podaljšati, vendar ne več kot za deset let.

Javno arhivsko gradivo, ki vsebuje podatke v zvezi z državno in javno varnostjo, zunanjimi zadevami ali obveščevalno in varnostno dejavnostjo države, v zvezi z gospodarskimi interesi ter davčne in poslovne skrivnosti, je dostopno za uporabo najpozneje 40 let po svojem nastanku.

Javno arhivsko gradivo, ki vsebuje občutljive osebne podatke, postane dostopno 75 let po svojem nastanku ali 10 let po smrti osebe, na katero se gradivo nanaša, če je datum smrti znan, če ni z drugimi predpisi določeno drugače.

Dostop do arhivskega gradiva, kjer so zajeti osebni in zasebni podatki, imajo posamezniki, na katere se ti podatki nanašajo. Ravno tako to velja za pooblaščence posameznikov, zakonite zastopnike in dediče, za državne organe, parlamentarne preiskovalne komisije, organe samoupravnih lokalnih skupnosti ali nosilce javnih pooblastil, ki dokumente potrebujejo za nemoteno delo oziroma za uveljavitev svojih pravic.

Arhiv Republike Slovenije je v skladu z zakonodajo in pravnimi akti prevzel zasebno arhivsko gradivo (pogodba o izročitvi in prevzemu), ki se uporablja v skladu z zakonodajo in pravnimi akti. V primeru dostopnosti pod določenimi pogoji za zasebno arhivsko gradivo je uporabnik dolžan izročitelju priskrbeti dovoljenje za uporabo. Če je potrebno, mora urediti še morebitne avtorske obveznosti (moralne in materialne avtorske pravice).

Ob izročitvi arhivskega gradiva arhivu morajo pravne in fizične osebe v pogodbah o izročitvi ali izročitvenih zapisnikih označiti vrste in roke nedostopnosti (MK, Arhiv RS, 2011).

2.4 VARNOST DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA

»Dokumentarno gradivo, ki ga organizacija sprejema, obdeluje in hrani, je treba zavarovati pred izgubo, uničenjem ali zlorabo, saj ima pomen za organizacijo, za znanost in kulturo oziroma ožjo ali širšo družbeno skupnost« (Brejc, 2004, str. 147). Uničiti ga je mogoče le na podlagi predpisa oziroma posebnih predstojnikovih navodil. Dokumentarno gradivo je treba zaščititi pred zlorabo.

Dokumentarno gradivo v tekočih in stalnih zbirkah je treba hraniti v primernih prostorih, da gradivo ne propada zaradi vlage, prahu, sončne svetlobe itd. Zagotoviti je treba ustrezne klimatske razmere ter ga zavarovati pred vlomom, požarom, vodo ter biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi.

Uredba o varstvu dokumentarnega in arhivskega gradiva določa načine izvajanja materialnega varstva arhivskega in dokumentarnega gradiva (v nadaljnjem besedilu: gradivo), da se pri hranjenju, urejanju, popisovanju, uporabi, transportu in razstavljanju ne poškoduje, uniči ali kako drugače izgubi.

Materialno varstvo arhivskega in dokumentarnega gradiva določa (Uredba o varstvu dokumentarnega in arhivskega gradiva, 40. člen):

- pogoje za ustreznost prostorov in opreme za hrambo gradiva;
- potrebne ukrepe za zavarovanje gradiva pred tatvino, vlomom, obrabo, prahom, ognjem, vodo, neustrezno temperaturo in vlago, vdorom ultravijoličnih žarkov ter drugimi škodljivimi biološkimi, kemičnimi in fizikalnimi vplivi.

Veliko podjetij in javnih ustanov ima arhive v kletnih prostorih. Seveda pa je to lahko velika napaka, kajti kletni prostor ni ravno najprimernejši za varovanje dokumentarnega gradiva. Če pride do poplave, je kletni prostor najbolj na udaru. Težave povzroča tudi vlaga, če prostori niso primerno opremljeni, saj vlaga lahko uniči dokumentarno gradivo.

Področji zavarovanja sta:

- varovanje podatkov – pravno;
- fizični dostop do prostorov in do računalnika:
  - logični dostop v računalnik, program, podatkovno bazo,
  - preverjanje identitete med samo uporabo sistema, ki je občasno – zaklep,
  - vse, kar se dogaja na sistemu, se evidentira,
  - kriptiranje oziroma šifriranje podatkov.

Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifrirnih podatkov (kriptoanaliza). Uporabljata pa se še pojma kripcija (šifriranje) in dekripcija (Overitelj digitalnih potrdil na MJU, 2011).

Uporabnik premaguje ovire z gesli, ki jih mora praviloma občasno spremeniti. Gesla vsak uporabnik sestavi sam. Pri tem velja nekaj pravil:

- gesla morajo biti različna za različne vstope;
- gesla si je treba zapomniti in ne zapisovati;
- dolžina gesel mora biti vsaj 5 znakov;
- ne smejo biti sestavljena iz osebnih ali drugih podatkov iz okolja, kjer živimo, ter običajnih besed, ki so v slovarjih, enciklopedijah itd.

Podatke ščitimo pred branjem, spreminjanjem, nadomeščanjem, dodajanjem, brisanjem, uporabo (pred dostopom iz drugih programom) in kopiranjem.

Varstvo arhivskega gradiva določata Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih (Ur. list RS, št. 30/06) ter Uredba o varstvu arhivskega in dokumentarnega gradiva (Ur. list RS, št. 86/06). V javnem in zasebnem sektorju urejata varstvo dokumentarnega in arhivskega gradiva v elektronski obliki in sta pravna podlaga za varstvo arhivskega gradiva kot kulturnega spomenika (MK, Arhiv RS, 2011).

2.5 HRAMBA DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA V DIGITALNI OBLIKI

Hramba dokumentarnega gradiva v digitalni obliki je hramba izvirnega dokumentarnega gradiva ali varna hramba zajetega dokumentarnega gradiva v digitalni obliki (ZVDAGA, 25. člen).

Načela varovanja in ohranjanja dokumentarnega gradiva v digitalni obliki so:

- načelo dostopnosti. Pomeni, da imajo dostop do dokumentarnega gradiva zgolj pooblaščeni uporabniki. V času trajanja hrambe dokumentarnega gradiva sta vključeni varovanje pred izgubo in stalno zagotavljanje dostopa;
- načelo uporabnosti. Pomeni, da sta ves čas trajanja hrambe za uporabo omogočeni zmožnost reprodukcije in primernost reprodukcije;
- načelo avtentičnosti. Pomeni dokazljivost povezanosti izvirnega gradiva oziroma izvora tega gradiva z reproducirano vsebino;
- načelo celovitosti. Pomeni, da so glede na vsebino izvirnega gradiva zagotovljene nespremenljivost, neokrnjenost ter urejenost reprodukcije vsebine.

»Avtentičnost in celovitost zajetega gradiva v digitalni obliki za dolgoročno hrambo se zagotavljata na tehnološki in organizacijski način na ravni posameznih enot, skupine enot ali celotnega zajetega gradiva:

- z dodajanjem varnostnih vsebin gradivu (npr. dodani metapodatki o preverjanju avtentičnosti in celovitosti, elektronski podpis, časovni žig in podobno),
- z drugimi sorodnimi tehnološkimi sredstvi ali
- z zagotavljanjem dodatnih organizacijskih ukrepov« (Kolokvij Arhiva 2006, Žumer, 2006, stran 14).

Prednosti elektronske hrambe dokumentarnega gradiva so v večji dostopnosti, preglednosti in varnosti.

Primerjava med hrambo dokumentarnega gradiva in hrambo dokumentarnega gradiva v digitalni obliki:

Tabela 1: Primerjava med hrambo dokumentarnega gradiva in hrambo dokumentarnega gradiva v digitalni obliki

	DOKUMENTARNO GRADIVO	E-DOKUMENTARNO GRADIVO
DOSTOPNOST	Fizični dostop	Enostavnejši, oddaljen hkraten dostop
PREGLEDNOST	Zamudno iskanje in brskanje	Učinkovito iskanje in brskanje
VARNOST	Vse je na enem mestu	Kopije so na različnih lokacijah

Vir: lasten

Hramba arhivskega gradiva v digitalni obliki je dovoljena samo kot dolgoročna hramba zajetega gradiva v skladu s strokovnimi navodili pristojnega arhiva (ZVDAGA, 36. člen).

Posameznik, ki v digitalni hrambi hrani zasebno arhivsko gradivo ali hrani javno arhivsko gradivo do izročitve pristojnemu arhivu, mora na zahtevo pristojnega arhiva poročati o načinu in postopkih hrambe. Poročilo mora vsebovati predvsem naslednje podatke o (ZVDAGA, 37. člen):

- uporabljeni opremi in storitvah;
- uporabljenih oblikah in nosilcih zapisa;
- zagotavljanju trajne dostopnosti podatkov;
- načrtovanih in izvedenih pretvorbah v drugo obliko zapisa ali prepisih na drug nosilec zapisa;
- ukrepih za zagotavljanje celovitosti, avtentičnosti in uporabnosti gradiva;
- drugih pomembnih dejavnikih hrambe gradiva.

2.5.1 PREDPISI S PODROČJA ARHIVSKE DEJAVNOSTI

Pravne, fizične in javnopravne osebe morajo spoštovati zakone in predpise, ki določajo vrsto zahtev za zajemanje, upravljanje in hrambo dokumentarnega in arhivskega gradiva v digitalni obliki.

Predpisi (MK, Arhiv RS, 2011):

- Zakon o varstvu dokumentarnega gradiva ter arhivih (ZVDAGA),
- Uredba o varstvu dokumentarnega in arhivskega gradiva,
- Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom,
- Pravilnik o spremembah in dopolnitvah Pravilnika o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom,
- Pravilnik o določitvi tarif pri uporabi arhivskega gradiva,
- Pravilnik o spremembah Pravilnika o določitvi tarif pri uporabi arhivskega gradiva,

- Pravilnik o določanju rokov hranjena dokumentarnega gradiva v javni upravi,
- Enotne Tehnološke Zahteve 2.0.,
- Kontrolni seznam za potrjevanje notranjih pravil in preverjanje njihovega izvajanja ter preverjanje izpolnjevanja pogojev za pridobitev akreditacije storitev v skladu z ZVDAGA,
- Kontrolni seznam za preverjanje usklajenosti programske opreme z ZVDAGA,
- Kontrolni seznam za preverjanje skladnosti strojne opreme z ZVDAGA,
- Pravilnik o strokovnih izpitih na področju varstva kulturne dediščine in varstva arhivskega gradiva,
- Pravilnik o pridobivanju nazivov na področju varstva kulturne dediščine in varstva arhivskega gradiva,
- Sklep o ustanovitvi in načinu dela arhivske komisije,

Drugi predpisi:

- Uredba Vlade RS o organih v sestavi ministrstev (Ur. list RS, št. 58/03, 45/04, 86/04, 138/04, 52/05, 82/05, 17/06, 76/06 in 132/06, 41/07),
- Uredba o upravnem poslovanju (Ur. list RS, št. 20/2005, spremembe: Ur. list RS, št. 106/05, 30/206, 86/06, 32/07, 63/07, 31/2008, 35/09),
- Splošni mednarodni standardi za arhivsko popisovanje in Mednarodni standardi za arhivski zapis o ustvarjalcih arhivskega gradiva: pravnih osebah, fizičnih osebah in družinah. Za objavo pripravila in prevedla Olga Pivk, Arhiv Republike Slovenije, Ljubljana 1998,
- Kodeks etike, ICA, Bulletin No 47, (1997-1). Iz angleščine prevedla Marija Vera Erjavec, Arhivi XX, Ljubljana 1997, str. 14–16,
- Kodeks ravnanja javnih uslužbencev (Ur. list RS, št. 8/01),
- Konvencija o varstvu kulturnih dobrin v primeru oboroženih spopadov (Haaška konvencija) s pravilnikom za njeno izvrševanje in protokolom (Ur. list FLRJ, št. 4/1956, Mednarodne pogodbe),
- Drugi protokol konvencije (Ur. list RS, št. 22/03),
- Priporočilo Odbora ministrov sveta Evrope št. R (2000) 13 z dne 13. 7. 2000 državam članicam o evropski politiki dostopa do arhivov (Recommendation No. R (2000) 13 of the Committee of Ministers to member States on a European policy in acces to arhives),
- Priporočilo Odbora ministrov Sveta Evrope št. R (2002) državam članicam o dostopu do javnih informacij, sprejeto 21. februarja 2002 (Recommendation No. R (2002) of the Commitee of Ministers to member States on access to official information of 21 Februar 2002),
- Resolucija Sveta in ministrov kulture o dogovoru, ki zadeva arhive, na srečanju Sveta 14. novembra 1991 (Ur. list Evropskih skupnosti C 314, 5. 12. 1991),
- Sklepi Sveta z dne 17. junija 1994, ki zadevajo večje sodelovanje na arhivskem področju (Ur. list Evropskih skupnosti C 235/3, 23. 8. 1994),
- Resolucija Sveta z dne 25. junija 2002 o zaščiti jutrišnjega spomina – zaščiti digitalnih vsebin za prihodnje generacije (Ur. list Evropskih skupnosti C 162/4, 6. 7. 2002),

- Resolucija Sveta z dne 6. maja 2003 o arhivih držav članic (Ur. list Evropskih skupnosti C 113/2, 13. 5. 2003).

Poleg vseh navedenih predpisov morajo organizacije upoštevati tudi Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), ki vsebuje določila za pravno veljavnost podatkov v elektronski obliki.

2.5.2 PRIDOBITEV DOVOLJENJA ZA E-HRAMBO DOKUMENTARNEGA GRADIVA

Za opravljanje dejavnosti izvajanja storitev ali dobave opreme na področju zajema in hrambe gradiva v digitalni obliki ni potrebno posebno dovoljenje. Pravne ali fizične osebe morajo Arhivu Republike Slovenije na podlagi 83. člena Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih in 29. člena Uredbe o varstvu dokumentarnega in arhivskega gradiva svojo dejavnost prijaviti najmanj osem dni pred začetkom opravljanja dejavnosti (MK, Arhiv RS, 2011). Bodoči ponudnik mora vložiti naslednja obrazca:

- zahtevo za registracijo,
- zahtevo za potrjevanje notranjih pravil in vzorčnih notranjih pravil.

2.5.2.1 Zahteva za registracijo

Bodoči ponudnik strojne in programske opreme za hrambo v digitalni obliki ter storitev hrambe v digitalni obliki in spremljevalnih storitev pri Arhivu Republike Slovenije (pristojni organ, ki ureja registracijo in vpis v register) vloži zahtevek za registracijo na predpisanem obrazcu zahteve za registracijo ponudnika opreme in storitev (priloga 6 k Uredbi o varstvu dokumentarnega in arhivskega gradiva, Ur. list RS, št. 86/06). Zahtevek se vloži po pošti ali pa elektronsko prek spletne aplikacije.

Elektronski obrazec za zahtevo registracije ponudnika opreme in storitev za digitalno hrambo je objavljen na spletni strani Arhiva Republike Slovenije.

Pristojni organ preveri popolnost prijave in z upravno odločbo odredi vpis ponudnika v register ponudnikov, ki je brezplačno dostopen na spletni strani Arhiva Republike Slovenije: http://reh.ars.gov.si/index.php?page=webInterface&idDefinition=1. Za nadzor nad postopki je pristojno Ministrstvo za kulturo Republike Slovenije, ki je tudi pritožbeni organ.

Arhiv Republike Slovenije z elektronskim oddaljenim dostopom do Poslovnega registra Slovenije osvežuje in pridobiva identifikacijske podatke o ponudniku opreme in storitvi hrambe ali spremljevalnih storitev. Za vse bistvene spremembe je treba na predpisanem obrazcu prijaviti Arhivu Republike Slovenije praviloma osem dni pred spremembo oziroma najpozneje v petnajstih dneh po spremembi. Pristojni organ bo preučil, ali je zaradi spremembe treba popraviti navedbo v registru, ter začel ustrezen postopek in obvestil

ponudnika. Po Zakonu o upravnih taksah (ZUT-UPB5 – prečiščeno besedilo, Ur. list RS, št. 106/10) je treba plačati upravno takso v višini 3,88 eur za vlogo ter v višini 15,49 eur za odločbo. V primeru spremembe se podatki avtomatsko ažurirajo.

Vlagatelj ima pravico, da zoper odločitev Arhiva Republike Slovenije poda pritožbo oziroma ugovor zoper odločbo ali sklep na Ministrstvo za kulturo Republike Slovenije v roku petnajstih dni od prejema odločitve.

2.5.2.2 Zahteva za potrditev notranjih pravil

Sprejem notranjih pravil je pomemben predvsem za zagotavljanje pravne veljavnosti elektronsko hranjenih dokumentov, kajti Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih pravno veljavnost notranjih pravil veže na obstoj in izvajanje potrjenih notranjih pravil. Izvajalci storitev lahko svoja notranja pravila pošljejo v potrditev pristojnemu organu, ki preveri skladnost pravil z zakonodajo in enotnimi tehnološkimi zahtevami. Če pristojni organ ugotovi skladnost, ta pravila potrdi, s čimer se gradivu, ki ga oseba hrani, zagotovi pravna veljavnost že na podlagi zakona (MK, Arhiv RS, 2011).

V potrditev Arhivu Republike Slovenije so javnopravne osebe, ki hranijo arhivsko gradivo in drugo dokumentarno gradivo v digitalni obliki, dolžne posredovati notranja pravila.

Pri pristojnem organu Arhivu Republike Slovenije se na predpisanem obrazcu vloži zahteva za potrditev notranjih pravil osebno, po pošti ali pa elektronsko preko spletne aplikacije.

2.5.2.3 Zahteva za potrditev vzorčnih notranjih pravil

Izvajalci storitev, ki bodo svoje dokumentarno gradivo ali dokumentarno gradivo svojih strank hranili v elektronski obliki, lahko prevzamejo že vnaprej pripravljena vzorčna pravila drugih oseb. Taka pravila so pripravljena za širšo uporabo. Če bodo izvajalci ta pravila sprejeli v celoti, jim ni treba pridobivati dodatne potrditve.

Pri pristojnem organu Arhivu Republike Slovenije se na predpisanem obrazcu vloži zahteva za potrditev vzorčnih notranjih pravil osebno, po pošti ali pa elektronsko preko spletne aplikacije.

K zahtevku je treba priložiti tudi vzorčna notranja pravila v elektronski obliki za dolgoročno hrambo.

Ko pristojni organ ugotovi, da so notranja pravila (vzorčna) v skladu z zakonom, uredbo in Enotnimi tehnološkimi zahtevami (ETZ), jih potrdi in vpiše v register potrjenih notranjih pravil, ki so dostopna na spletni strani Arhiva Republike Slovenije: http://reh.ars.gov.si/index.php?page=webInterface&idDefinition=3.

Za potrditev notranjih oziroma vzorčnih pravil je treba plačati upravno takso v skladu z Zakonom o upravnih taksah (ZUT-UPB5 – prečiščeno besedilo, Ur. list RS, št. 106/10) v višini 3,88 eur za vlogo ter v višini 15,49 eur za odločbo. V primeru spremembe se podatki avtomatsko ažurirajo.

Vlagatelj ima enako pravico do pritožbe kot pri zahtevi za registracijo.

2.5.3 AKREDITACIJA STROJNE IN PROGRAMSKE OPREME

Pri Arhivu Republike Slovenije lahko ponudniki, ki so že registrirani in želijo pridobiti še več zaupanja pri potencialnih odjemalcih, dodatno registrirajo storitev in opremo.

Pri pristojnem organu ponudniki vložijo zahtevo na predpisanem obrazcu za akreditacijo strojne in programske opreme ter storitev hrambe v digitalni oblike in spremljevalnih storitev osebno, po pošti ali elektronsko preko spletne strani Arhiva Republike Slovenije.

Upoštevati je treba še dodatna navodila oziroma priporočila glede oblike in vsebine prilog, predvsem pa Kontrolni seznam za preverjanje usklajenosti programske opreme z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih.

Dodatna akreditacija opreme ali storitev pomeni za ponudnike poslovanje z javnim sektorjem, njihovim uporabnikom pa zagotavlja večno varnost pri uporabi opreme in storitev.

2.5.4 PREDSTAVITEV PODJETIJ GAMA SYSTEM D.O.O. IN AINIGMA D.O.O.

Na slovenskem trgu je veliko podjetij, ki skrbijo za nemoteno in varno hrambo dokumentarnega gradiva v elektronski obliki. Za opravljanje dejavnosti morajo podjetja pri Arhivu Republike Slovenije oddati elektronske vloge za registracijo, za potrjevanje notranjih pravil in za akreditacijo opreme in storitev. Priložiti morajo še kontrolni seznam (to je stolpec reference) in vso dokumentacijo, na katero se sklicujejo.

2.5.4.1 Gama System d.o.o.

Gama System d.o.o. je neodvisno podjetje, ustanovljeno leta 1992, ki sledi doseganju visoko zastavljenih ciljev. V podjetju so s preoblikovanjem družbe iz izobraževalno-svetovalne v programersko-svetovalno-izobraževalno družbo dosegli pomemben razvojni cilj, pri čemer svetovanje izvajajo predvsem v obliki uvajanja lastne programske opreme. Z doseganjem uspehov so si zastavili višje cilje, kot je postati pomemben ponudnik na domačem in tujem trgu v ponudbi programske opreme (Gama System d.o.o., 2011).

V podjetju Gama System so uveljavili inovacijo kot način dela in razmišljanja s ciljem, da počnejo prave stvari in na pravi način. Lotevajo se razvoja programske opreme za področja, ki so tudi v svetovnem merilu slabo ali sploh niso pokrita z dobrimi

programskimi paketi (npr. računalniška podpora za ISO 9001[2]/ISO 14001[3]/OHSAS 18001[4], Work Factor – hitri postopek itd.), zato ne morejo, tudi če bi hoteli, posnemati domačih ali tujih rešitev. Že na začetku razvoja so morali razmišljati, kako rešiti težavo, povezano z namestitvijo programske opreme pri naročnikih, ki uporabljajo različne informacijske sisteme. Za podjetje je to inovacija, saj ustvarjajo lastne, visoko integrirane rešitve in obenem programsko opremo, ki dobro deluje z drugimi informacijskimi sistemi, ki jih že uporabljajo njihovi naročniki (Gama System d.o.o., 2011).

Rešitve Gama System d.o.o., ki jih nudijo uporabnikom, so predvsem močna podpora, sprva v obliki spoznavanja njihovih potreb, kjer vidijo priložnost v vsebinskem obvladovanju področij, ki jih podpira programska oprema, in nato v obliki svetovanja, katero orodje je najbolje uporabiti in kako, kot podporo vsakdanjemu delu. Da bi naročnikom zagotovili najvišjo kakovost storitve in da ne prihaja do kritičnih posledic pri naročnikih, so v Gama System d.o.o. predani delu in uveljavljajo pristope za doseganje uspehov (Gama System d.o.o., 2011).

Gama System eDocs je celovit sistem za upravljanje elektronskih dokumentov, ki omogoča različne vstopne točke – dokumentne ponore. Glavni nalogi sta zajemanje dokumentov, ki vstopajo v sistem, in njihovih metapodatkov ter predaja dokumentov klasifikacijskemu podsistemu (Gama System d.o.o., 2011).

Sistem Gama System e-Archive je namenjen pravno veljavnemu shranjevanju elektronskih dokumentov. Sistem arhiviranja elektronskih dokumentov je sposoben shraniti več milijonov dokumentov, izvažati dokumente, jim spreminjati metapodatke in sprejeti neomejeno količino dokumentov v procesiranje – s pravilnim skaliranjem. Rešitev omogoča shranjevanje poljubnih elektronskih dokumentov, ki jih preko programskega vmesnika shrani v arhiv, ki se nahaja pod okriljem ponudnika storitve (Gama System d.o.o., 2011).

2.5.4.2 Ainigma d.o.o.

Ainigma, svetovanje za varno poslovanje, d.o.o., je dinamično in inovativno svetovalno podjetje, ki izvaja storitve s področja informacijske varnosti. Njegove stranke so državni organi in organi lokalnih skupnosti ter gospodarske družbe in druge organizacije v Sloveniji in tujini, ki jim nudijo objektivno in kompetentno svetovanje v okviru njihovih osnovnih dejavnosti (Ainigma d.o.o., 2011).

Cilj Ainigme d.o.o. je pomagati pri upravljanju in obvladovanju varnostnih tveganj, ki so prisotna ob uporabi informacijskih tehnologij. Za uspešno izvajanje dejavnosti so v podjetju osredotočeni na varstvo interesov strank in so neodvisni od prodajalcev informacijske opreme in rešitev (Ainigma d.o.o., 2011).

[2] Standard o sistemu vodenja kakovosti
[3] Standard o sistemu ravnanja z okoljem
[4] Standard o sistemu vodenja varnosti in zdravja pri delu

Organizacija, ki se odloči za upravljanje dokumentov in varno e-hrambo podatkov, se lahko obrne po pomoč k podjetjem, ki izvajajo storitve s področja informacijske varnosti. Podjetja lahko svetujejo in pomagajo pri organiziranju vseh faz za zajem in hrambo dokumentarnega gradiva v digitalni obliki (Ainigma d.o.o., 2011).

Faze priprave so (Ainigma d.o.o., 2011):

- natančna opredelitev poslanstva, poslovnih in pravnih zahtev, notranjih zadev, bistvenih vplivov oziroma področij tveganja za hrambo dokumentarnega in arhivskega gradiva;
- izdelava študije upravičenosti in izvršljivosti elektronske hrambe, ki temelji na analizi poslovnih aktivnosti (popis posameznih poslovnih aktivnosti in potrebnih virov dokumentarnega gradiva);
- določitev zahtev glede ustvarjanja in hrambe dokumentarnega in arhivskega gradiva za potrebe dokumentiranja poslovanja v skladu z veljavnimi predpisi in poslovnimi potrebami;
- presoja skladnosti obstoječih informacijskih sistemov za hrambo ali upravljanje in drugih informacijskih sistemov z ugotovljenimi potrebami in zahtevami za hrambo;
- izdelava načrta in izbira načina hrambe dokumentarnega gradiva;
- izdelava in sprejem notranjih pravil v obliki, ki jo za potrditev notranjih pravil zahteva Arhiv Republike Slovenije.

Podjetja pa lahko organizacijam pomagajo tudi pri izvedbi postopkov registracije in/ali akreditacije strojne in programske opreme za izvedbo hrambe dokumentarnega gradiva v digitalni obliki, storitev hrambe v digitalni obliki ali spremljevalnih storitev.

Podjetje Ainigma pomaga pri določitvi potrebnih aktivnosti za izboljšanje varnosti poslovanja s podatki in informacijami ter pri njihovi izvedbi. Pristop k izvedbi teh dejavnosti praviloma temelji na metodologiji, določeni s standardom ISO/IEC 27002:2005, ter ob upoštevanju drugih standardov, dobrih praks in predpisov, pomembnih za posamično organizacijo. Rezultat skupnega dela je delujoč sistem upravljanja varovanja informacij in varovanja drugih virov, pomembnih za poslovanje organizacije, podprt z ustreznimi normativnimi, organizacijskimi ter tehnološko-tehničnimi postopki in ukrepi. Dokumentiranje aktivnosti poteka tako, da lahko organizacija, če to želi, s postopkom certificiranja, določenim s standardom ISO/IEC 27001:2005, preko zunanje presoje formalno preveri, ali dejansko izpolnjuje zahteve varovanja podatkov in informacij (Ainigma d.o.o., 2011).

2.6 VAROVANJE TAJNIH PODATKOV

Tajni podatek 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 zakonu, zavarovati pred nepoklicanimi osebami in ki je v skladu z zakonom določeno in označeno za tajno (ZTP-UPB, 2. člen).

Tajni podatek tuje države je podatek, ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ali podatek, ki je rezultat sodelovanja Republike Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njunimi organi in za katerega se dogovori, da mora ostati tajen (ZTP-UPB2, 2. člen).

Po Zakonu o tajnih podatkih lahko le pooblaščena osebe določi neki podatek za tajen. Vsak podatek ali dokument, ki vsebuje tajne podatke, mora biti označen s stopnjo tajnosti in s podatki o organu, če to ni že razvidno. Pravico dostopa do tajnih podatkov imajo samo tiste osebe, katerim je bilo izdano dovoljenje.

Varovanje tajnih podatkov je razdeljeno na (UVTP, 2011):

- osebno varnost,
- fizično varnost,
- dokumentacijsko varnost,
- informacijsko varnost,
- industrijsko varnost,
- usposabljanje.

2.6.1 OSEBNA VARNOST

Pri varovanju tajnih podatkov osebna varnost pomeni, da so vse osebe, ki dostopajo do tajnih podatkov zaradi opravljanja nalog ali funkcije na svojem delovnem mestu, ustrezno varnostno preverjene. Glede na preveritev lojalnosti, zanesljivosti in verodostojnosti osebe se izda ali zadrži dovoljenje za dostop do tajnih podatkov. V samem varnostnem postopku se obravnavajo osebnostni značaj in okoliščine, ki bi lahko pomenile potencialni varnostni problem.

2.6.2 FIZIČNA VARNOST

Fizična varnost je pomemben element celotnega sistema varovanja tajnih podatkov, saj gre za odvrnitev, preprečitev in/ali odkrivanje dostopa nepooblaščene osebe do tajnih podatkov. Fizična varnost je sestavljena iz različnih postopkov in ukrepov, ki so med seboj tesno povezani. Postopki in ukrepi so organizacijski, varnostno-tehnični in mehanski ter postopki in ukrepi fizičnega varovanja. Glede na stopnjo in vrsto podatkov, ki se varujejo, njihovo količino obliko in način hranjenja, oceno ogroženosti ter stopnjo varnostne kulture pri zaposlenih se določi, katera stopnja fizične varnosti je potrebna (UVTP, 2011).

2.6.3 DOKUMENTACIJSKA VARNOST

Tajni podatek je lahko označen s stopnjo tajnosti INTERNO, ZAUPNO TAJNO ali STROGO TAJNO. Dokumentacijska varnost opredeljuje enoten sistem določanja in označevanja tajnih podatkov ter njihovega prenosa, razmnoževanja, evidentiranja, uničevanja in arhiviranja ter postopek ob zlorabi tajnega podatka. Celovit sistem varovanja tajnih podatkov tvorijo dokumentacijska varnost ter fizični in tehnični ukrepi varovanja tajnih podatkov, cilja pa sta preprečiti dostop nepooblaščenim osebam in omogočiti sledljivost podatkov skozi njihovo življenjsko dobo (UVTP, 2011).

2.6.3.1 Dokumentacijska varnost EU

Države članice Evropske unije (v nadaljnjem besedilu: EU), Svet EU in Evropska komisija morajo zagotoviti, da se spoštujejo minimalni standardi varovanja tajnosti, tako da je mogoče vsak tajni podatek EU posredovati naprej v prepričanju, da bodo celotna javna uprava, pogodbeni partnerji, institucije EU in agencije EU z njim ravnali dosledno. Minimalni standardi obsegajo postopke za zaščito tajnih podatkov EU.

Generalni sekretar/visoki predstavnik je skladno s Sklepom Sveta EU o varovanju tajnosti (2001/264/ES z dne 19. 3. 2001) odgovoren za dajanje zahtev državam članicam za ustanovitev registrov za sprejem tajnih podatkov s stopnjo tajnosti STROGO TAJNO. Nacionalni varnostni organi[5] držav članic izdajajo dovoljenja za ustanovitev in delovanje registrov (UVTP, 2011).

Sklep Sveta in Komisije (2001/844/EC, ECSC, Euratom z dne 29. 11. 2001) določa stopnje tajnosti, ki pa so usklajene z Zakonom o tajnih podatkih (Ur. list RS, št. 50/06-UPB2 - uradno prečiščeno besedilo, 9/10 in 60/11). V nadaljevanju so prikazane slovenske in evropske stopnje tajnosti:

Stopnja tajnosti v Sloveniji	Stopnja tajnosti v EU
INTERNO	RESTRIENT UE
ZAUPNO	CONFIDENTIEL UE
TAJNO	SECRET UE
STROGO TAJNO	TRES SECRET/TOP SECRET UE

Pri vprašanjih razvrščanja tajnih podatkov po stopnjah tajnosti, uporabi stopenj tajnosti ter spremembi in preklicu stopnje tajnosti se je slovenska zakonodaja popolnoma uskladila z evropskimi predpisi. Ravno tako je slovenska zakonodaja popolnoma usklajena na področju dodatnih oznak tajnih podatkov z Uredbo o varovanju tajnih podatkov (Ur. list RS, št. 74/05, 7/11, 24/11). Možnost dodatnih oznak določa Sklep Sveta EU.

[5] NSA – National Security Authority

Kombinacije blagajn in ključi morajo biti varovani na enak način kot gradivo, do katerega omogočajo dostop, hranijo pa se v zapečateni zaprti neprosojni ovojnici.

Priprava in razpošiljanje tajnih podatkov EU

Strani, ki vsebujejo tajne podatke, morajo biti označene zgoraj in spodaj na sredini strani. Vsaka stran mora vsebovati oznako trenutne strani in celotno število strani dokumenta (npr. 6/11). Na dokumentih s stopnjama tajnosti STROGO TAJNO in TAJNO morajo vse strani vsebovati šifro dokumenta. Kopije dokumenta morajo biti označene, da je to kopija, številka kopije mora biti navedena na prvi strani dokumenta. Za dokumente s stopnjo tajnosti ZAUPNO in višje se zahteva, da so vse priloge in dodatki navedeni na prvi strani dokumenta. Dokumenti s stopnjo tajnosti STROGO TAJNO lahko krožijo samo preko registrskega sistema. Registri EU morajo v evidenco vpisati vse dokumente s stopnjo tajnosti ZAUPNO in višje ob prihodu ali izhodu iz ustanove. Podatki, ki jih je treba vpisati, morajo omogočati prepoznavo dokumentov in biti vpisani v delovodnik ali vneseni v posebno varovan računalniški nosilec (UVTP, 2011).

Prenos tajnih podatkov EU

Prenos dokumentov s stopnjo tajnosti STROGO TAJNO lahko znotraj države prenašajo le pripadniki kurirske službe, izjemoma javni uslužbenci, če izpolnjuje pogoje iz sklepa Sveta EU (2001/264/EC). V državi tajne podatke TAJNO in ZAUPNO lahko prenašajo pooblaščena kurirska služba in pooblaščeni posamezniki, ki so preverjeni in imajo potrdilo za dostop do tajnih podatkov EU (UVTP, 2011).

Tajne podatke, ki vsebujejo stopnjo tajnosti ZAUPNO in višje, je med državami članicami dovoljeno prenašati le po diplomatski pošti ali vojaški kurirski službi. Pri prenosu dokumentov INTERNO je treba zagotoviti, da ne morejo pasti v nepooblaščene roke.

Prenos dokumentov s stopnjo tajnosti ZAUPNO se opravi v odpornih, neprosojnih dvojnih ovojnicah. Na notranji ovojnici se označi primerna stopnja tajnosti EU, in če je mogoče, s polnimi podatki o naslovniku in njegovem uradnem nazivu.

Potrdilo o prejemu se vloži v notranjo ovojnico in ga lahko potrdi samo nadzorni javni uslužbenec registra EU ali njegov namestnik. Če je ovojnica naslovljena na posamezno osebo, se v register EU vpiše sprejem ovojnice, notranjo ovojnico pa sme odpreti in potrditi sprejem dokumentov v njej pa samo oseba, na katero je naslovljena (UVTP, 2011).

Potrdilo mora vsebovati šifro zadeve (ali več zadev), datum dokumenta in številko kopije. Potrdilo ni tajni podatek, vendar pa nikoli ne sme vsebovati vsebine dokumenta. Kurirji pri oddaji dokumentov s stopnjo ZAUPNO dobijo potrdilo, na katerem se morajo podatki ujemati z odpremnimi podatki. Prenos tajnih podatkov s stopnjama ZAUPNO in TAJNO se

lahko izvaja samo preko akreditiranih komunikacijskih centrov in omrežij in/ali terminalov in sistemov (UVTP, 2011).

Kopije, prevodi in izvlečki tajnih podatkov EU

Odobritev za kopiranje in prevajanje dokumentov STROGO TAJNO ima samo ustvarjalec dokumenta. Skladno z nacionalnimi predpisi o rokovanju s tajnimi podatki lahko dokumente, ki vsebujejo podatke TAJNO in nižje, razmnožuje, prevaja ali pripravlja izvlečke naslovnik.

Vsi registri EU opravijo inventurne popise vseh dokumentov STROGO TAJNO. Izvajajo se tudi naključna interna preverjanja o dokumentih. Dovoljeno je tudi arhiviranje tajnih podatkov EU na mikrofilm ali magnetna ter optična sredstva, pod pogojem, da so nosilci podatkov zaščiteni na enak način kot izvirni dokument. Na nosilcih so lahko shranjeni samo podatki ene stopnje tajnosti (UVTP, 2011).

Uničevanje tajnih podatkov

Tajni podatki stopnje STROGO TAJNO se lahko uničujejo samo v Centralnem registru EU. Ti dokumenti se lahko uničujejo samo zapisniško, skladno s pravilom »dveh oseb«. Potrdila o uničenju in dokumentacija o razpošiljanju se hranijo v registru vsaj deset let od dneva uničenja (UVTP, 2011).

Dokumente TAJNO uničijo pristojni registri EU. Potrdila o uničenju in dokumentacija o razpošiljanju se hranijo v registru vsaj tri leta od dneva uničenja. Dokumente ZAUPNO uničijo pristojni registri. Skladno z nacionalnimi predpisi se v registru hranijo potrdila o uničenju in dokumentacija o razpošiljanju. Dokumente INTERNO uničijo pristojni registri ali uporabnik, če to omogočajo nacionalni predpisi (UVTP, 2011).

Registri EU

Organ, ki skrbi za glavno sprejemanje in opravo za dokumente s stopnjo tajnosti EU v državi članici, je centralni register EU. Za zagotovitev pravilnega evidentiranja, arhiviranja, rokovanja, razpošiljanja in uničenja za tajne podatke STROGO TAJNO skrbi registrski sistem. V primeru, da centralni register ne more izpolniti vseh potreb države, lahko države ustanovijo podregistre STROGO TAJNO, ki so odgovorni za upravljanje z dokumenti STROGO TAJNO. Centralni register EU mora odobriti pošiljanje tajnih podatkov s stopnjo STROGO TAJNO neposredno drugim podregistrom EU. Popis vseh tajnih podatkov, za katere so odgovorni v centralnem registru EU in podregistrih EU, se opravi vsakih dvanajst mesecev. Svoje ugotovitve popisa podregistri EU pošljejo centralnemu registru EU, ki pa nato poroča o stanju na področju tajnih podatkov STROGO TAJNO nacionalnemu varnostnemu organu.[6]

[6] NSA – National Security Authority

Ukrepi varovanja tajnosti v času sestankov, ki potekajo zunaj prostorov Sveta EU

Za prinašanje, odnašanje in varovanje tajnih dokumentov na sestankih so odgovorne delegacije same. Za dostavo na kraj sestanka in odnašanje tajnih dokumentov s kraja sestanka lahko delegacije zaprosijo za pomoč državo članico gostiteljico (UVTP, 2011).

Zaščita tajnih podatkov EU v sistemih informacijske tehnologije in komunikacijskih sistemih

Pod tehnične ukrepe varovanja tajnosti spadata tudi nadzor in sledljivost podatkov. Za tajne podatke TAJNO in višje se vodi evidenca dostopa, ki je lahko avtomatska ali ročna. Organ za varnostno akreditacijo[7] določi postopke za nadzor pri pošiljanju izpisov, nastalih v sistemu, ki obdeluje tajne podatke EU, z območja informacijske tehnologije na območje oddaljenega terminala. Vsi izmenljivi računalniški nosilci s stopnjo ZAUPNO in višje morajo biti primerno označeni. Tajni podatki EU morajo biti shranjeni na nosilcih skupaj z ustrezno označeno stopnjo tajnosti in zaščite. Stopnje tajnosti pri računalniških nosilcih, ki se uporabljajo za vnos tajnih podatkov EU, se lahko znižajo, razen za računalniške nosilce tajnih podatkov STROGO TAJNO. Računalniških nosilcev tajnih podatkov STROGO TAJNO tudi ni mogoče ponovno uporabiti. Kadar stopnje tajnosti za računalniški nosilec ni mogoče preklicati ali se ta ne sme ponovno uporabiti, se računalniški nosilec uniči po odobrenem nacionalnem postopku (UVTP, 2011).

2.6.3.2 Dokumentacijska varnost NATO

Za usklajevanje, spremljanje in uresničevanje varnostne politike zveze NATO skrbi Urad zveze NATO za varnost[8]. Direktor NOS-a je glavni svetovalec generalnega sekretarja za varnostna vprašanja in predsednik Natovega Odbora za varnost[9] (UVTP, 2011).

Zakon o ratifikaciji sporazuma med pogodbenicami Severnoatlantske pogodbe o varnosti podatkov (Ur. list RS-MP, št. 22/04) določa, da pogodbenice:

- ščitijo in varujejo:
  - tajne podatke zveze NATO, označene kot take, ali tiste, ki jih zvezi NATO predloži država članica;
  - tajne podatke, označene kot take, ki jih države članice predložijo drugi državi članici v podporo programu, projektu ali pogodbi zveze NATO;
- ohranjajo stopnjo tajnosti podatkov, kot so opredeljeni pod točko 1 tega zakona, in storijo vse potrebno, da jih varujejo primerno stopnji tajnosti;

[7] SAA – Security Accreditation Authorities
[8] NOS – Nato Office of Security
[9] NSC – Nato Security Committee

- ne uporabljajo tajnih podatkov, kot so opredeljeni pod točko 1 tega zakona, v druge namene kot tiste, ki so določeni v Severnoatlantski pogodbi, sklepih in resolucijah, ki se nanašajo na to pogodbo;
- ne razkrivajo v točki 1 tega zakona opredeljenih podatkov stranem, ki niso članice zveze NATO, brez soglasja lastnika podatkov (UVTP, 2011).

Zakon določa, da pogodbenice vzpostavijo in izvajajo varnostne standarde, ki zagotavljajo skupno raven varovanja tajnih podatkov (UVTP, 2011).

Tajni podatki zveze NATO so v tem zakonu opredeljeni tako, da:

- podatki pomenijo vedenje, ki se lahko sporoča v kakršni koli obliki;
- tajni podatki pomenijo podatke ali sredstva, za katere je določeno, da morajo biti zavarovani pred nepooblaščenim razkritjem, in so bili določeni s stopnjo tajnosti;
- izraz sredstvo pomeni dokumente in vsak del strojev, opreme ali orožja, ki je že bil izdelan ali je v postopku izdelave;
- izraz dokument pomeni vsak zapisan podatek, gledano na njegovo obliko ali značilnost, vključno s pisnim ali natisnjenim gradivom, karticami ali trakovi za obdelavo podatkov, zemljevidi, kartami, fotografijami, slikami, risbami, grafikami, skicami, delovnimi zapisi, kopijami in pisalnimi trakovi ali reprodukcijami s sredstvi ali postopki ter zvočnimi, glasovnimi, magnetnimi, elektronskimi, optičnimi ali videoposnetki v kakršni koli obliki ter prenosno opremo za avtomatsko obdelavo podatkov z vgrajenimi računalniškimi sredstvi za shranjevanje podatkov in odstranljivimi računalniškimi sredstvi za shranjevanje podatkov (UVTP, 2011).

V nadaljevanju so prikazane slovenske in NATO stopnje tajnosti:

Stopnja tajnosti v Sloveniji	Stopnja tajnosti v NATO
INTERNO	NATO RESTRICTED
ZAUPNO	NATO CONFIDENTIAL
TAJNO	NATO SECRET
STROGO TAJNO	COSMIC TOP SECRET

2.6.4 INFORMACIJSKA VARNOST

Pri informacijski varnosti gre za uporabo in določanje ukrepov za zaščito tajnih dokumentov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov, pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov (UVTP, 2011).

Informacijska varnost – INFOSEC vsebuje tako ukrepe varovanja tajnosti v računalniških sistemih oziroma računalniško varnost – COMPUSEC (varnost strojne opreme, varnost programske opreme in varnost programsko-strojne opreme) kot ukrepe varovanja tajnosti

v komunikacijskih sistemih oziroma komunikacijsko varnost – COMSEC (varnost prenosnih sistemov – TRANSEC, varnost kriptografskih metod in naprav – CRYPTOSEC, varnost proti elektromagnetnemu sevanju elektronskih naprav – EMSEC). Izvajajo se tudi ukrepi za odkrivanje, dokumentiranje in zoperstavljanje vsem oblikam groženj, ki so usmerjene proti tajnim podatkom in proti sistemom, ki tajne podatke obravnavajo (UVTP, 2011).

2.6.5 INDUSTRIJSKA VARNOST

Kadar naročila in dodeljevanje naročil vsebujejo tajne podatke, morajo biti sprejeti ukrepi za varovanje tajnih podatkov med gospodarskimi družbami in organizacijami. Industrijska varnost je uporaba ukrepov in postopkov za preprečevanje, odkrivanje in povrnitev izgube ali prenehanje ogrožanja tajnih dokumentov, s katerimi razpolaga izvajalec ali podizvajalec med pogajanji pred dodelitvijo tajnega naročila oziroma tajnega podnaročila in med njegovim izvajanjem (UVTP, 2011).

Tajno naročilo je vsako naročilo za dobavo izdelkov, izvedbo del ali opravljanje storitev, katerih izvršitev zahteva ali vključuje dostop do tajnih podatkov ali njihov nastanek. Tajno podnaročilo je naročilo, ki ga izvajalec sklene z drugim izvajalcem – podizvajalcem za dobavo blaga, izvedbo del ali opravljanje storitev, katerih izvršitev zahteva ali vključuje dostop do tajnih podatkov ali njihov nastanek (UVTP, 2011).

2.6.6 USPOSABLJANJE

Na podlagi Zakona o tajnih podatkih ter Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov Urad Vlade RS organizira (v nadaljnjem besedilu: UVTP) in izvaja osnovna usposabljanja s področja obravnavanja in varovanja tajnih podatkov za osebe, ki bodo imele dostop do teh podatkov. Prijave ali zaprosila za usposabljanje se pošljejo na elektronski naslov UVTP.

Vsa zaprosila za izvedbo usposabljanja ali prijave na usposabljanje se posredujejo na uradni elektronski naslov UVTP. UVTP izvaja usposabljanje za osebe, ki svoje znanje s področja obravnavanja tajnih podatkov prenesejo svojim sodelavcem.

Osnovno in dodatno usposabljanje s področja tajnih podatkov lahko za organe in organizacije izvajajo osebe, ki jih določi predstojnik.

Usposabljanje je brezplačno, vendar mora biti na usposabljanju ustrezno število mest dano na voljo državnim organom. Praviloma naj usposabljanje opravljajo osebe, ki imajo ustrezno predznanje s področja varnostnih ved in dejansko izvajajo naloge s področja obravnavanja tajnih podatkov, kar predstavlja neposreden prenos znanja in izkušenj ostalim. Glede na udeležence in njihove potrebe v zvezi z obravnavanjem tajnih podatkov se prilagodi vsebina usposabljanja (UVTP, 2011).

Udeleženci po končanem usposabljanju prejmejo potrdilo oziroma dokazilo o udeležbi, na katerem so navedeni osebno ime, rojstni datum udeleženca ter naziv organizacije oziroma organa, ki je izvedel usposabljanje. Organi in organizacije morajo voditi ustrezno evidenco izvedenih usposabljanj oziroma podatkov o dovoljenjih uslužbencev, ki imajo dostop do tajnih podatkov (UVTP, 2011).

3 VARSTVO IN ZAVAROVANJE OSEBNIH PODATKOV

Zakon o varstvu osebnih podatkov (v nadaljnjem besedilu: ZVOP-1-UPB1) ureja varstvo osebnih podatkov v Republiki Sloveniji in je bil sprejet 15. julija 2004, veljati pa je začel 1. januarja 2005. Zakon izhaja iz 38. člena Ustave RS, ki pravi:

»Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi«.

Z ZVOP-1-UPB1 so določene pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice (v nadaljnjem besedilu: posameznik) pri obdelavi osebnih podatkov (ZVOP-1-UPB1, 1. člen).

Najpomembnejša načela ZVOP-1-UPB1 so:

- načelo zakonitosti in poštenosti;
- načelo sorazmernosti;
- prepoved diskriminacije.

Na spremembo ZVOP-1-UPB1 (objavljeno v Ur. listu RS, št. 94/07, z dne 16. oktobra 2007) so se s svojim mnenjem odzvali tudi posamezniki:

»Spremembe se nanašajo predvsem na zmanjšanje obveznosti delodajalcev pri izdelavi katalogov zbirk osebnih podatkov, pri izdelavi pravilnika o zavarovanju zbirk in pri vpisu v Register zbirk osebnih podatkov, ki ga vodi Informacijski pooblaščenec. Novela tako razbremenjuje samo tiste delodajalce, ki imajo manj kot 50 zaposlenih. Obveznosti pa ostajajo enake za upravljavce občutljivih osebnih podatkov in za določene vrste upravljavcev (upravljavci v javnem sektorju, notarji, odvetniki, detektivi, izvršitelji).

Pomembna novost, ki jo prinaša ZVOP-1A, so tudi spremembe na področju postopka seznanitve z lastnimi osebnimi podatki, zlasti uvedba pravilnika o stroških zaračunavanja vpogleda v lastne osebne podatke, ki ga bo izdal minister, pristojen za pravosodje, na predlog Informacijskega pooblaščenca.

ZVOP-1A vsebuje tudi določbe o uskladitvi zneskov glob v slovenskih tolarjih z zneski glob

v evrih. Poleg tega ZVOP-1A določa novo kategorijo storilca prekrška – posameznika, ki samostojno opravlja dejavnost – in tako Zakon o varstvu osebnih podatkov usklajuje z Zakonom o prekrških.« (IEPRI, 2006).

3.1 POMEN IZRAZOV

V tem poglavju so navedeni pomeni posameznih izrazov s področja varstva osebnih podatkov iz Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, 6. člen).

OSEBNI PODATEK – je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

POSAMEZNIK – je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo 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 družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

OBDELAVA OSEBNIH PODATKOV – pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).

AVTOMATIZIRANA OBDELAVA – je obdelava osebnih podatkov s sredstvi informacijske tehnologije.

ZBIRKA OSEBNIH PODATKOV – je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

UPRAVLJAVEC OSEBNIH PODATKOV – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

UPORABNIK OSEBNIH PODATKOV – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.

POSREDOVANJE OSEBNIH PODATKOV – je posredovanje ali razkritje osebnih podatkov.

KATALOG ZBIRKE OSEBNIH PODATKOV – je opis zbirke osebnih podatkov.

REGISTER ZBIRK OSEBNIH PODATKOV – je register, v katerem so podatki iz katalogov zbirk osebnih podatkov.

OSEBNA PRIVOLITEV POSAMEZNIKA – je prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavec po tem zakonu; osebna privolitev posameznika je lahko pisna, ustna ali druga ustrezna privolitev posameznika.

PISNA PRIVOLITEV POSAMEZNIKA – je podpisana privolitev posameznika, ki ima obliko listine, določila v pogodbi, določila v naročilu, priloge k vlogi ali drugo obliko v skladu z zakonom; podpis je tudi na podlagi zakona s podpisom izenačena oblika, podana s telekomunikacijskim sredstvom, ter na podlagi zakona s podpisom izenačena oblika, ki jo poda posameznik, ki ne zna ali ne more pisati.

USTNA ALI DRUGA USTREZNA PRIVOLITEV POSAMEZNIKA – je ustno ali s telekomunikacijskim ali drugim ustreznim sredstvom ali na drug ustrezen način dana privolitev, iz katere je mogoče nedvomno sklepati na posameznikovo privolitev.

OBČUTLJIVI OSEBNI PODATKI – so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške (v nadaljnjem besedilu: prekrškovne evidence); občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

ISTI POVEZOVALNI ZNAKI – so osebna identifikacijska številka in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbirati oziroma priklicati osebne podatke iz tistih zbirk osebnih podatkov, v katerih so obdelovani tudi isti povezovalni znaki.

BIOMETRIČNE ZNAČILNOSTI – so takšne telesne, fiziološke ter vedenjske značilnosti, ki jih imajo vsi posamezniki, so pa edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, deoksiribonukleinske kisline[10] ter značilne drže.

[10] DNK oziroma DNA

3.2 VARSTVO OSEBNIH PODATKOV

Zakon o varstvu osebnih podatkov določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov.

3.2.1 KAJ JE VARSTVO OSEBNIH PODATKOV

Zakon o varstvu osebnih podatkov načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku zagotovljeno varstvo osebnih podatkov, njegovo državljanstvo in prebivališče pa ne smeta biti pogoj. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo (Informacijski pooblaščenec, 2009).

Osebni podatki se lahko obdelujejo le, če je njihova obdelava določena z zakonom ali če ima upravljavec zbirke podatkov pisno privolitev posameznika. Za pravne ali fizične osebe, ki opravljajo javno službo ali dejavnost po zakonu, ki ureja gospodarske družbe, pa velja, da lahko že neposredno na podlagi tega zakona, torej brez izrecne podlage v nekem drugem zakonu ali pisne privolitve posameznika, obdelujejo osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le, če gre za osebne podatke, ki jih potrebujejo za izpolnjevanje pogodbenih obveznosti ali uveljavljanje pravic iz pogodbenega razmerja. Za državne organe, organe lokalnih skupnosti in nosilce javnih pooblastil je ureditev drugačna, saj lahko obdelujejo le tiste osebne podatke, za katere je tako določeno z zakonom. Posameznik, čigar osebni podatki se obdelujejo na podlagi njegove pisne privolitve, mora biti predhodno pisno seznanjen z namenom obdelave podatkov, njihove uporabe in časom shranjevanja (Informacijski pooblaščenec, 2009).

3.2.2 KAKO ZAVAROVATI OSEBNE PODATKE

Eden od bistvenih pogojev za učinkovito varstvo osebnih podatkov oziroma varstvo posameznika, na katerega se podatki nanašajo, je ustrezno zavarovanje osebnih podatkov. 24. členu v ZVOP-1-UPB1 določa zahteve, ki jim morajo zadostiti postopki in ukrepi za zavarovanje osebnih podatkov, v 25. členu pa upravljavce osebnih podatkov zavezuje k sprejemu akta, s katerim predpišejo organizacijske, tehnične in logično-tehnične postopke in ukrepe za zavarovanje osebnih podatkov, s katerimi se (Ainigma, 2011 in ZVOP-1-UPB1, 24. člen):

- varujejo prostori, oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;

- nepooblaščenim osebam preprečuje dostop do osebnih podatkov pri njihovem prenosu. Enako velja za prenos po telekomunikacijskih omrežjih;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani ter kdo je to storil, v obdobju, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

Za uspešno izvedbi postopkov in ukrepov varovanje, je potrebno zagotoviti, da se bodo vsi predpisani postopki in ukrepi tudi dejansko izvajali.

V podjetju Ainigma lahko pomagajo tako pri postopkih, vezanih na izvajanje varstva osebnih podatkov, kot pri postopkih in ukrepih zavarovanja osebnih podatkov tako, da:

- izvedejo usposabljanje, prilagojeno potrebam podjetja z vidika podatkov, s katerimi le-ta upravlja oziroma jih obdeluje, oziroma z vidika določenih skupin osebja, ki osebne podatke obdeluje;
- pomagajo in svetujejo pri izvedbi postopkov za zakonito obdelavo osebnih podatkov, ki jih upravljavcem zbirk podatkov nalaga ZVOP-1-UPB1;
- izdelajo ali pomagajo izdelati analizo tveganja, ki ga predstavljata obdelava in narava osebnih podatkov, ki jih podjetje obdeluje;
- izdelajo ali pomagajo izdelati posebne akte ali določbe za dopolnitev obstoječih aktov, s katerimi podjetje predpiše postopke in ukrepe za zavarovanje osebnih podatkov ter določi osebe, odgovorne za posamezne zbirke osebnih podatkov, in osebe, ki zaradi narave svojega dela lahko obdelujejo določene osebne podatke;
- pomagajo in svetujejo pri izvedbi posebnih varnostnih ukrepov za obdelavo občutljivih osebnih podatkov ter dodatnih postopkov in ukrepov za uporabo video nadzora in biometrije (Ainigma, 2011).

3.3 OBDELAVA OSEBNIH PODATKOV

Prvi odstavek 8. člena ZVOP-1-UPB1 pravi, da je osebne podatke mogoče obdelovati le, kadar je to določeno z zakonom ali na podlagi privolitve posameznika. Zakonov, ki določajo obdelavo podatkov na posameznem področju, je veliko, med njimi so:

- Zakon o centralnem registru prebivalstva,
- Zakon o evidencah na področju dela in socialne varnosti,
- Zakon o zavarovalništvu,
- Zakon o policiji,
- Zakon o Slovenski obveščevalno-varnostni agenciji,
- Zakon o obrambi,
- Zakon o osnovni šoli,

- Zakon o gimnazijah,
- Zakon o zdravstveni dejavnosti itd.

Pri obdelavi osebnih podatkov, ki je dovoljena že z zakonom, ni potrebna še dodatna osebna privolitev posameznika, na katerega se podatki nanašajo, razen v tistih primerih, ko zakon za javni sektor izrecno določa in zahteva posameznikovo privolitev.

Določba drugega odstavka 8. člena ZVOP-1-UPB1 pravi, da mora biti namen obdelave osebnih podatkov določen v zakonu. Posameznik, na katerega se nanaša obdelava osebnih podatkov, mora biti o tem predhodno pisno ali na drug ustrezen način seznanjen.

3.4 OBDELAVA OBČUTLJIVIH OSEBNIH PODATKOV

V 13. členu ZVOP-1-UPB1 je v osmih točkah taksativno določenih osem pravnih podlag, ki dopuščajo obdelavo občutljivih osebnih podatkov. To pomeni, da se lahko občutljivi osebni podatki obdelujejo zgolj in samo v osmih, taksativno določenih primerih. Podlaga za določbo tega člena je določba 8. člena Direktive 95/46/ES[11]. Po tej odločbi v prvem odstavku 8. člena države članice EU prepovedujejo obdelavo osebnih podatkov, ki kažejo na rasni ali etični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu in obdelavo podatkov v zvezi z zdravjem ali spolnim življenjem. V določbi drugega odstavka določa odmike od splošne prepovedi obdelave občutljivih osebnih podatkov iz prvega odstavka ZVOP-1-UPB1, tem določbam pa sledi omenjenih osem točk.

13. člen ZVOP-1-UPB1 temelji tudi na 6. členu Konvencije 108 Sveta Evrope, ki določa: »Avtomatizirana obdelava osebnih podatkov, ki razkrivajo rasno poreklo, politična stališča ali verska ali druga prepričanja, ter osebnih podatkov, ki zadevajo zdravje ali spolno življenje, ni dovoljena, razen če nacionalna zakonodaja za obdelavo zagotavlja ustrezne varnostne mehanizme.«[12]

Obdelava občutljivih osebnih podatkov je opisana v osmih točkah (ZVOP-1-UPB1, 13. člen):

- obdelava občutljivih osebnih podatkov je dopustna le, če je posameznik za to podal izrecno osebno privolitev. Praviloma je privolitev pisna, v javnem sektorju je določena tudi z zakonom;
- obdelava občutljivih osebnih podatkov je dopustna le, če je obdelava potrebna zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca osebnih podatkov na področju zaposlovanja v skladu z zakonom, ki določa tudi ustrezna jamstva pravic posameznika;

[11] Direktiva Evropskega parlamenta št. 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov z dne 24. 10. 1995.
[12] Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

- obdelava osebnih podatkov je dopustna le, če je nujno potrebna za varovanje življenja ali telesa posameznika, na katerega se ti osebni podatki nanašajo. Kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve iz prve točke 13. člena ZVOP-1-UPB1, ga lahko zastopa druga oseba;
- obdelava osebnih podatkov je dopustna le, če jih obdelujejo ustanove, združenja, verske skupnosti, sindikati ali druge nepridobitne organizacije s političnim, filozofskim, verskim ali sindikalnem ciljem za namene zakonitih dejavnosti. Vendar pa je obdelava teh podatkov mogoča le, če se obdelava nanaša na njihove člane ali na posameznike, ki so v zvezi s temi cilji v rednem stiku in če se ti podatki ne posredujejo drugim posameznikom ali osebam javnega ali zasebnega sektorja brez pisne privolitve posameznika, na katerega se nanašajo;
- obdelava občutljivih osebnih podatkov je dopustna le, če je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil, vendar brez očitnega ali izrecnega namena, da omeji namen njihove uporabe;
- obdelava občutljivih osebnih podatkov je dopustna le, če jih v skladu z zakonom obdelujejo zdravstveni delavci in sodelavci za namene zdravstvenega varstva prebivalstva in posameznikov ter vodenja ali opravljanja zdravstvenih služb;
- obdelava občutljivih osebnih podatkov je dopustna le, če je to potrebno zaradi uveljavljanja ali nasprotovanje pravnemu zahtevku;
- obdelava občutljivih osebnih podatkov je dopustna le, če tako določa drug zakon zaradi izvrševanja javnega interesa.

Kršitev določb 13. člena ZVOP-1-UPB1 je ustrezno sankcionirana v tretji točki prvega odstavka 91. člena ZVOP-1-UPB1.

3.5 NAMEN ZBIRANJA IN NADALJNJA OBDELAVA

Osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače (ZVOP-1-UPB1, 16. člen). To je temeljno načelo namembnosti ali načelo namenskosti. Zakon mora biti skladen z vladavino prava in posameznik mora tudi predvideti posledice zanj. Določitev namena obdelave osebnih podatkov v podzakonskem predpisu je zato protiustavna.

V Republiki Sloveniji je po pravnem redu uveljavljeno načelo stroge namembnosti zbiranja in nadaljnje obdelave osebnih podatkov. Namen mora biti namreč enak, razen če zakon ne določa drugače. Vsa nadaljnja obdelava v zgodovinske, statistične in znanstvenoraziskovalne namene se ne šteje za nezdružljivo s prvotnimi nameni pri zbiranju podatkov. Kot nadaljnja obdelava osebnih podatkov je mišljena vsaka nadaljnja uporaba ali obdelava osebnih podatkov.

Praviloma je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zato morajo biti nameni nedvoumni, določni in določeni pred zbiranjem samih podatkov.

Kršitev določb 16. člena ZVOP-1-UPB1 predstavlja prekršek po peti točki prvega odstavka 91. člena ZVOP-1-UPB1.

3.6 UPORABA ISTEGA POVEZOVALNEGA ZNAKA

ZVOP-1-UPB1 v prvem odstavku 20. člena določa, da pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja, zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva ter kazenske evidence in prekrškovnih evidenc ni dovoljenja uporaba istega povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil samo ta znak, torej kot edini znak brez dodatnih osebnih podatkov.

V praksi je treba pri pridobivanju osebnih podatkov poleg istega povezovalnega znaka (v večini primerov EMŠO) obvezno navesti še kak drug identifikacijski podatek, na primer osebno ime, kraj prebivališča ali kaj podobnega.

3.6.1 ENOTNA MATIČNA ŠTEVILKA OBČANA (EMŠO)

Zakon o centralnem registru prebivalstva (v nadaljnjem besedilu: ZCRP-UPB1) v prvem odstavku 6. člena določa, da je enotna matična številka občana (v nadaljnjem besedilu: EMŠO) v Republiki Sloveniji osebna identifikacijska številka in je identifikacija za enoznačno opredelitev posameznika. EMŠO predstavlja temeljni, z matematično metodo izračunani numerični standard. V drugem odstavku 6. člena ZCRP-UPB1 določa, da je identifikacija namenjena vodenju in vzdrževanju zbirk podatkov o prebivalstvu, povezovanju podatkov v teh zbirkah ter racionalizaciji dela državnih organov in drugih uporabnikov, ki imajo zakonsko podlago za uporabo EMŠO.

EMŠO pomeni primarni ključ za posamično identifikacijo posameznika, to pomeni, da gre za najbolj točno in osnovno identifikacijo posameznika. Iz nje je mogoče razbrati podatke o starosti posameznika, spolu, rojstnem datumu. Upravljavec centralnega registra (CRP) določi EMŠO enotno za vse osebe iz 3. člena ZCRP za državljane na podlagi podatkov iz rojstne matične knjige, za tujce pa na podlagi podatkov iz osebnega dokumenta (ZCRP-UPB1, 7. člen).

EMŠO sestavlja trinajst številk (ZCRP-UPB1, 8. člen) :

- številke od 1. do 7. mesta določajo datum rojstva (dve mesti za dan, dve mesti za mesec in tri mesta za letnico);
- številki na 8. in 9. mestu določata številko registra (šifra 50);

- številke na 10., 11. in 12. mestu pomenijo zaporedno številko oziroma kombinacijo za spol in zaporedne številke za osebe, rojene istega dne (000-499 za moške in 500-999 za ženske);
- številka na 13. mestu predstavlja kontrolno številko, izračunano po matematičnem modulu (modul 11).

EMŠO je sama po sebi osebni podatek, vsebuje pa še druge osebne podatke. EMŠO morajo po določbi prvega odstavka 9. člena ZRCP-UPB1 uporabljati upravljavci zbirk podatkov, ki jih vodijo posamezniki na podlagi zakona, na področjih statistike, notranjih zadev, zdravstvenega varstva in zavarovanja, davkov in carine, obrambe, geodetske službe, urejanja prostorov in ekološke zaščite, zaposlovanja in spremljanja delovne sile, pokojninskega in invalidskega zavarovanja, pravosodja, šolstva, socialnega varstva in drugi uporabniki, določeni z zakonom, oziroma upravljavci zbirk podatkov, določeni z zakonom, ki v teh zbirkah podatkov uporabljajo EMŠO. Vpisuje se lahko tudi v javne listne.

Vsakdo, ki pridobiva EMŠO določene osebe, je dolžan navesti zakonsko podlago in namen pridobivanja EMŠO, v primeru pisne privolitve pa posameznika seznaniti z namenom pridobivanja.

3.6.2 DAVČNA ŠTEVILKA

Zakon o davčnem postopku (v nadaljnjem besedilu: ZDavP-2-UPB4) v 33. členu z naslovom Davčna številka za davčne namene določa, da se zavezancu za davek pod določenimi zakonskimi pogoji dodeli davčna številka, ki se uporablja v zvezi z vsemi davki. Davčna številka je drugi najpogostejši povezovalni znak.

Davčna številka je uvedena oziroma vzpostavljena za potrebe postopkov davčnega organa za njihove postopke in identifikacije oziroma natančne določitve konkretnega davčnega zavezanca. Zbiranje davčne številke posameznika je upravičeno in potrebno le, kadar gre za nastanek pravnega posla, iz katerega nastane davčno razmerje. Potrebnost in upravičenost obdelave davčne številke kot osebnega podatka oziroma enoličnega identifikacijskega znaka je zato treba presojati z opisanega vidika.

3.6.3 ENOTNA MATIČNA ŠTEVILKA OBČANA (EMŠO) IN DAVČNA ŠTEVILKA SKUPAJ

Zbiranje obeh enoličnih identifikacijskih znakov je nedvomno v neskladju z načelom sorazmernosti iz 3. člena ZVOP-1-UPB1, saj je že eden od teh osebnih podatkov dovolj za nedvoumno določitev posameznika (Informacijski pooblaščenec, 2011).

Informacijski pooblaščenec ob tem napotuje tudi na odločbo Ustavnega sodišča Republike Slovenije št. U-I-229/03 z dne 9. 2. 2006, kjer je sodišče med drugim zapisalo, da popolno identifikacijo posameznika omogoča tako podatek o EMŠO kot tudi podatek o davčni

številki. Po mnenju Ustavnega sodišča RS to pomeni, da je odveč določitev kar dveh podatkov, ki omogočata popolno identifikacijo posameznika, saj zadostuje zgolj eden (Informacijski pooblaščenec, 2011).

Določba drugega odstavka 20. člena ZVOP-1-UPB1 pa pomeni izjemo, odstop od načelne določbe prvega odstavka. Določa, da se isti povezovalni znak lahko izjemoma uporabi za pridobivanje osebnih podatkov, vendar le takrat:

- če in ko je to edini podatek v konkretni zadevi, ki omogoči, da se odkrije ali preganja kaznivo dejanja po uradni dolžnosti;
- da se zavaruje življenje ali telo posameznika ali
- da se zagotovi izvajanje nalog obveščevalnih ali varnostnih organov, določenih z zakonom.

Vsa tri navedena področja ureja področna zakonodaja.

Izvajanje pregona kaznivih dejanj je urejeno v Zakonu o policiji (ZPol-UPB7, sprememba v ZPol-H) in Zakonu o državnem tožilstvu (ZDT-1). Načeloma se vsa kazniva dejanja preganjajo po uradni dolžnosti, razen tistih, za katere Kazenski zakonik (KZ) eksplicitno določa, da se preganjajo na predlog (tako imenovani predlagalni delikti) oziroma na zasebno tožbo. Zavarovanje življenja in telesa posameznika izhaja iz zakonov na področju varstva. To področje urejata Zakon o zdravstveni dejavnosti (ZZDej-I) in Zakon o zdravniški službi (ZZDrS-E). ZZDej-I določa pomen zdravstvene dejavnosti, ki obsega ukrepe in aktivnosti, ki jih po medicinski doktrini in ob uporabi medicinske tehnologije opravljajo zdravstveni delavci in sodelavci pri varovanju zdravja ter pri preprečevanju, odkrivanju in zdravljenju bolnikov in poškodovancev. ZZDrS-E pa določa, da zdravnik opravlja zdravstveno dejavnost kot zdravniško službo v skladu z Zakonom o zdravstveni dejavnosti in tem zakonom ter je temeljni odgovorni nosilec opravljanja zdravniške dejavnosti.

Izvajanje nalog obveščevalnih in varnostnih organov je urejeno v Zakonu o Slovenski obveščevalno-varnostni agenciji (ZSOVA-UPB2) in Zakonu o obrambi (ZObr-UPB1). Po 1. členu ZSOVA-UPB2 je Slovenska obveščevalno-varnostna agencija (v nadaljevanju: SOVA) samostojna službe vlade, ki opravlja s tem zakonom določene naloge. Po 2. členu ZSOVA-UPB2 je določeno, da SOVA pridobiva in vrednoti podatke in poseduje informacije iz tujine, ki so pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države, kot tudi o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev.

Določba tretjega odstavka 20. člena ZVOP-1-UPB1 je prepoved uporabe istega povezovalnega znaka na način, da se za pridobitev osebnega podatka uporabi samo ta znak, za zemljiško knjigo in sodni register.

Uporaba istega povezovalnega znaka v nasprotju z določbami 20. člena ZVOP-1-UPB1 je ustrezno sankcionirana v osmi točki prvega odstavka 91. člena ZVOP-1-UPB1.

3.7 ROK HRAMBE OSEBNIH PODATKOV

Prvi odstavek 21. člena ZVOP-1-UPB1 določa, da se osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbrali ali nadalje obdelovali. Ta določba je nadgradnja temeljnih načel, ki so zapisana v 2. in 3. členu ZVOP-1-UPB1.

Zakon o policiji (ZPol-UPB7) v 63. členu določa roke hrambe za vsako posamezno evidenco osebnih podatkov. Pri tem izhaja iz namena, zaradi katerega se evidence vodijo in nadalje vzdržujejo (izvajanje policijskih pooblastil). Podatki iz 1., 6., 7., 8., 14., 15., 17. in 20. točke 59. člena ZPol-UPB7 se, denimo, hranijo do ustavitve policijske preiskave oziroma do zaključka akcije varovanja ali izdaje sklepa o zavrženju kazenske odločbe. Če te ni, pa se hranijo do zastaranja kazenskega pregona. Podatki iz evidence tretje točke 59. člena ZPol-UPB7 se hranijo, dokler trajajo razlogi, zaradi katerih je bilo uvedeno iskanje ali drug zakonit ukrep, vendar najdalj do zastaranja pregona, za podatke v evidencah iz 4. in 19. točke 59. člena zakon določa absolutni rok enega leta po vnosu podatkov. 64. člen ZPol -UPB7 pa pravi, da se po preteku rokov iz 63. člena ZPol-UPB7 podatki iz policijskih evidenc obravnavajo skladno s predpisi, ki urejajo poslovanje organov javne uprave s stalno zbirko dokumentarnega gradiva oziroma ravnanje z javnim arhivskih gradivom. Dostop do teh podatkov je policistom in pristojnim osebam drugih državnih organov dovoljen le v primeru preiskovanja suma storitve kaznivega dejanja, za katero se storilec preganja po uradni dolžnosti, ali v drugih primerih, določenih z zakonom (ZPol-UPB7, 63. člen).

Tudi drugi področni zakoni opredeljujejo čas shranjevanja osebnih podatkov za določene zbirke osebnih podatkov. S tem upravljavcu osebnih podatkov bistveno olajšajo delo oziroma presojo, kdaj je namen osebnih podatkov dosežen, saj je to določil zakonodajalec.

Drugi odstavek 21. člena ZVOP-1-UPB1 določa, da je osebne podatke treba po izpolnitvi namena obdelave zbrisati, uničiti, blokirati ali anonimizirati, razen kadar so osebni podatki na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Evropsko sodišče za človekove pravice je že razsojalo o neupravičeno dolgi hrambi osebnih podatkov v primeru Amann v. Switzerland.[13] Razsodilo je, da je tudi hramba osebnih podatkov eden od vidikov pravice do zasebnosti, zato kršitev 8. člena Evropske

[13] European Court of Human Rights, Case of Aman v. Switzerland, Application no. 27798/05, sodba z dne 16. 2. 2000.

konvencije o človekovih pravicah pomenita tudi neupravičena hramba zbirke osebnih podatkov in dejstvo, da zbirka osebnih podatkov ni bila uničena v skladu z zakonom.

Kršitev določbe 21. člena je ustrezno sankcionirana v deveti točki prvega odstavka 91. člena ZVOP-1-UPB1.

3.8 ZAVAROVANJE OBČUTLJIVIH OSEBNIH PODATKOV

Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se vsem nepooblaščenim osebam onemogoči dostop do teh podatkov. Izjema so primeri, kadar je posameznik, na katerega se nanašajo občutljivi podatki, te javno objavil brez očitnega ali izrecnega namena, da omeji namen njihove uporabe (ZVOP-1-UPB1, 14. člen).

Kadar gre za prenos osebnih podatkov preko telekomunikacijskih omrežij, so podatki ustrezno varovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Glede na to, da zgolj predpisovanje postopkov in ukrepov za zavarovanje občutljivih osebnih podatkov ni dovolj, je treba poskrbeti, da se predpisani postopki in ukrepi tudi izvajajo.

Za tehnično zavarovanje nosilcev občutljivih podatkov (vseh vrst sredstev, na katerih so zapisani ali posneti podatki: listine, akti, gradiva, spisi, računalniška oprema, vključno z magnetnimi, optičnimi in drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov itd.) je priporočljivo, da se ti podatki hranijo v ognjevarnih omarah ter da so zavarovani z videonadzorom, alarmno napravo in požarno zaščito.

3.9 ZAVAROVANJE OSEBNIH PODATKOV

Določila prvega odstavka 17. člena Direktive 46/95/ES[14], ki določajo varnost obdelave in se glasijo:

»Države članice določijo, da mora upravljavec izvajati ustrezne tehnične in organizacijske ukrepe za zavarovanje osebnih podatkov pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom, predvsem kadar obdelava vključuje prenos podatkov po omrežju, ter proti vsem drugim nezakonitim oblikam obdelave.

[14] Direktiva Evropskega parlamenta št. 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov z dne 24. 10. 1995.

Taki ukrepi ob upoštevanju stanja tehnologije in stroškov za njihovo izvajanje zagotavljajo raven zaščite, ustrezno tveganju, ki ga predstavljata obdelava in narava podatkov, ki jih je potrebno varovati.« je ZVOP-1-UPB1 prenesel v svojem 24. členu z naslednjo vsebino:

- zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:
  - varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
  - varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
  - preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
  - zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
  - omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, vendar le za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov;
- v primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov;
- postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavljata obdelava in narava določenih osebnih podatkov, ki se obdelujejo;
- funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju svojih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave (ZVOP-1-UPB1, 24. člen).

Določbe, navedene v 24. členu ZVOP-1-UPB1, so zgolj osnovne zahteve, ki jim morajo zadostiti postopki in ukrepi za zavarovanje osebnih podatkov, v 25. členu pa je določeno, da so obdelovalci osebnih podatkov in pogodbeni delavci dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona.

Kršitev 24. člena ZVOP-1-UPB1 v povezavi s 25. členom po 93. členu ZVOP-1-UPB1 predstavlja prekršek. Četrti odstavek tega člena ni sankcioniran. V primeru kršitve četrtega odstavka 24. člena ostane pravna podlaga za sankcioniranje protizakonitega ravnanja Kazenski zakonik.

3.10 DOLŽNOST ZAVAROVANJA

ZVOP-1-UPB1 v prvem odstavku 25. člena določa subjekte, ki so dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona. To so vsi upravljavci osebnih podatkov ter pogodbeni delavci.

Določba drugega odstavka 25. člena ZVOP-1-UPB1 določa, da upravljavci osebnih podatkov niso dolžni zagotoviti le ustreznih postopkov in ukrepov za zavarovanje osebnih podatkov, pač pa morajo le-te tudi predpisati v svojih aktih. Upravljavci osebnih podatkov morajo v svojih aktih poleg prepisanih postopkov in ukrepov za zavarovanje osebnih podatkov določiti tudi osebe, ki so odgovorne za določene zbirke podatkov. Določiti morajo tudi osebe, ki lahko zaradi narave svojega dela obdelujejo določene osebne podatke. To pomeni, da mora predstojnik upravljavca osebnih podatkov določiti, katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov, lahko obdelujejo določene osebne podatke.

Iz 24. člena ZVOP-1-UPB1 je razvidno, da morajo upravljavci osebnih podatkov v notranjih aktih v prvi vrsti preprečiti nepooblaščeno obdelavo osebnih podatkov ter preprečiti naključno ali namerno nepooblaščeno uničenje podatkov in njihovo spremembo ali izgubo. To jim omogočajo predpisani organizacijski, tehnični in logistično-tehnični postopki ter ukrepi za zavarovanje osebnih podatkov.

Za zavarovanje osebnih podatkov so lahko notranji akti samostojni akti ali pa akti v sklopu varovanja vseh zaupnih podatkov v neki ustanovi. Dobro je, da se izdela še več izvedbenih aktov, ki podrobneje predpisujejo zavarovanje na posameznem področju. Opis zavarovanja osebnih podatkov mora biti razviden že iz 11. točke kataloga zbirke osebnih podatkov, ki ga morajo upravljavci osebnih podatkov vzpostaviti za vsako zbirko osebnih podatkov na podlagi 26. člena ZVOP-1-UPB1.

Kadar gre za zavarovanje občutljivih osebnih podatkov, ki se obdelujejo s sredstvi za avtomatsko obdelavo osebnih podatkov, je potrebna še zagotovitev s sistemom gesel za identifikacijo in avtorizacijo uporabnikov programov in podatkov. Programska oprema mora zagotoviti evidenco, s pomočjo katere bo mogoče naknadno ugotoviti, kateri uporabnik je v določenem času vnašal, spreminjal ali pa samo pregledoval osebne podatke določenega posameznika.

Mediji so edini, katerim ni treba po drugem odstavku 25. člena ZVOP-1-UPB1 zagotoviti internih aktov in določiti odgovorne osebe. To določa tretji odstavek 7. člena ZVOP-1-UPB1, vendar zgolj za osebne podatke, ki jih mediji obdelujejo za namene obveščanja, za vse druge osebne podatke, ki jih mediji obdelujejo (o svojih zaposlenih, naročnikih, honorarnih sodelavcih itd), pa veljajo določila tega zakona v celoti.

V pomoč upravljavcem osebnih podatkov je Informacijski pooblaščenec izdelal osnutek internega akta, ki ga mora imeti vsak upravljavec osebnih podatkov.

Kršitev 25. člena (v povezavi s 24. členom) predstavlja prekršek po 93. členu ZVOP-1-UPB1.

3.11 KATALOG ZBIRKE OSEBNIH PODATKOV

Upravljavci osebnih podatkov morajo za vsako zbirko osebnih podatkov, ki jih vodijo in vzdržujejo, vzpostaviti katalog zbirke osebnih podatkov. Pri tem ni pomembno, ali zbirko osebnih podatkov vodijo na podlagi zakona, na podlagi osebne privolitve, na podlagi pogodbena razmerja ali pa na kakšni drugi pravni podlagi iz 9. ali 10. člena ZVOP-1-UPB1.

»Katalog zbirke osebnih podatkov« je definicija izraza, ki je bila podana zaradi lažjega razumevanja dolžnosti upravljavcev osebnih podatkov pri opisovanju zbirk osebnih podatkov ter njihovih dolžnosti obveščanja nadzornega organa o vzpostavitvi zbirk osebnih podatkov.

Katalog zbirke osebnih podatkov mora po določbah prvega odstavka 26. člena ZVOP-1-UPB1 vsebovati 13 točk oziroma 13 taksativno določenih podatkov oziroma dejstev, ki se nanašajo na obdelavo osebnih podatkov v posamezni zbirki osebnih podatkov. Posameznik se lahko z vpogledom v katalog seznani z opisom zbirke osebnih podatkov oziroma s 13 najpomembnejšimi podatki oziroma informacijami, ki se nanašajo na obdelavo osebnih podatkov v posamezni zbirki osebnih podatkov. Upravljavec zbirke osebnih podatkov je dolžan posamezniku po določbah 30. in 31. člena ZVOP-1-UPB1 omogočiti vpogled v katalog zbirke osebnih podatkov v roku 15 dni od prejema zahteve. To pomeni, da mora upravljavec osebnih podatkov za posamezno zbirko osebnih podatkov pri sebi vedno imeti vsaj en izpisan izvod kataloga zbirke osebnih podatkov.

Katalog zbirke osebnih podatkov mora vsebovati 13 točk, pod vsako točko pa se zapišejo zahtevani podatki oziroma dejstva, ki se nanašajo na obdelavo osebnih podatkov v posamezni zbirki. Te točke so (ZVOP-1-UPB1, 26. člen):

Pod 1. točko *"Naziv zbirke osebnih podatkov"*
Primer:

- evidenca o zaposlenih delavcih,
- evidenca o stroških dela,
- centralni register prebivalstva,
- kazenska evidenca,
- evidenca o izdanih odločbah o prekrških,
- evidenca o učencih, vpisanih v osnovno šolo, njihovih starših,
- evidenca posnetkov videonadzora dostopa v poslovne prostore,

- evidenca kupcev oziroma strank v Podvig, d.o.o., itd.

Pod 2. točko *"Podatki o upravljavcu osebnih podatkov"*
Primer: Podvig (firma), d.o.o., naslov, matična številka.

Pod 3. točko *"Pravna podlaga za obdelavo osebnih podatkov"*
Primer:

- osebna privolitev posameznika,
- najemne pogodbe,
- drugi odstavek 22. člena Zakona o varstvu osebnih podatkov, itd.

Pod 4. točko *"Kategorije posameznikov, na katere se nanašajo osebni podatki"*
Primer:

- zaposleni v družbi Erazem, d.o.o., in pogodbeni sodelavci,
- učenci v osnovni šol Igorja Levca in njihovi starši oziroma skrbniki,
- storilci prekrškov,
- kupci podjetja Erazem, d.o.o., itd.

Pod 5. točko *"Vrste osebnih podatkov v zbirkah osebnih podatkov"*
Primer:

- osebno ime, naslov stalnega prebivališča, EMŠO, kraj rojstva, davčna številka, številka transakcijskega računa, datum sklenitve pogodbe,
- slikovni posnetek posameznika, datum in čas vstopa in izstopa iz poslovnih prostorov,
- osebno ime, številka in vrsta osebnega dokumenta, naslov stalnega ali začasnega prebivališča, zaposlitev ter datum, ura in razlog vstopa ali izstopa v prostore ali iz njih itd.

Pod 6. točko *"Namen obdelave"*
Primer:

- za potrebe izvajanja socialno-varstvene dejavnosti, določene z zakonom, za načrtovanja politike socialnega varstva, spremljanje stanja ter za znanstvenoraziskovalne in statistične namene,
- za sklepanje in izpolnjevanje posojilnih pogodb,
- za izvedbo nagradnih iger in izvajanje neposrednega trženja itd.

Pod 7. točko "*Rok hrambe osebnih podatkov*"
Primer:

- osebni podatki se hranijo trajno,

- osebni podatki se brišejo po preteku treh let od dneva pravnomočnosti odločbe,
- osebni podatki se hranijo deset let po prenehanju zavarovalne pogodbe, v primeru nastanka škodnega dogodka pa deset let po koncu obdelave škodnega dogodka,
- osebni podatki se hranijo deset let oziroma do preklica osebne privolitve posameznika itd.

Pod 8. točko *"Omejitve pravic posameznikov glede osebnih podatkov v zbirkah podatkov in pravna podlaga omejitve"*
Primer:

- ni omejitev pravic posameznika iz 30. in 32. člena ZVOP-1-UPB1,
- posameznik ima pravico do vpogleda v svoje osebne podatke po pravnomočni odločitvi o uvedbi kazenskega postopka, če ta ni uveden, pa po zastaranju pregona. Pravna podlaga za takšno omejitev je določena v drugi alineji prvega odstavka 62. člena Zakona o policiji, itd.

Pod 9. točko *"Uporabniki ali kategorije uporabnikov osebnih podatkov, vsebovanih v zbirki osebnih podatkov"*
Primer:

- Zavod za zdravstveno zavarovanje Slovenije, Zavod za pokojninsko in invalidsko zavarovanje Slovenije, Davčna uprava Republike Slovenije,
- osebni podatki se posredujejo neomejenemu krogu uporabnikov,
- osebni podatki se le izjemoma posredujejo sodiščem in policiji, itd.

Pod 10. točko *"Dejstvo, ali se osebni podatki iznašajo v tretjo državo, kam, komu in pravna podlaga iznosa"*
Primer:

- osebni podatki iz zbirke osebnih podatkov se ne iznašajo v tretje države,
- osebni podatki se iznašajo v Združene države Amerike, pogodbenemu delodajalcu Street, 700 New York, New York. Pravna podlaga za iznos osebnih podatkov je Pogodba o _____, št. 87/10, z dne 10. 7. 2010, ter odločba Informacijskega pooblaščenca, šifra: 120-5/2006, z dne 1. 5. 2006.

Pod 11. točko *"Splošen opis zavarovanja osebnih podatkov"*
Primer:

- prostori, v katerih se nahaja računalniška oprema, s katero se obdelujejo osebni podatki, ter druga dokumentacija, vezana na zbirko, se izven delovnega časa zaklepajo, zaklepajo se tudi v času, ko v njih ni zaposlenih. Zbirka osebnih podatkov je varovana z gesli za identifikacijo in avtorizacijo uporabnikov, ki jih imajo le za obdelavo osebnih podatkov posebej pooblaščeni delavci. Organizacijski, tehnični in logistično-tehnični postopki ter ukrepi za zavarovanje osebnih podatkov so podrobneje

določeni v Pravilniku o zavarovanju osebnih podatkov v Podvig, d.o.o., ki ga je dne 1. 5. 2006 izdala uprava družbe.

Pod 12. točko "*Podatki o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig*"
Primer:

- osebni podatki iz zbirke osebnih podatkov se ne povezujejo z uradnimi evidencami ter javnimi knjigami,
- osebni podatki iz zbirke osebnih podatkov se povezujejo s centralnim registrom prebivalstva in evidenco transakcijskih računov pri Banki Slovenije itd.

Pod 13. točko *"Podatki o zastopniku iz tretjega odstavka 5. člena tega zakona"*
Primer:

- ni zastopnika iz 5. člena Zakona o varstvu osebnih podatkov,
- zastopnik upravljavca osebnih podatkov v Republiki Slovenije je Podvig, d.o.o., Mačkova 1, 1000 Ljubljana, matična številka: 123456789.

Na spletnih straneh Informacijskega pooblaščenca (www.ip-rs.si) se nahaja posebni elektronski obrazec, s katerim upravljavci osebnih podatkov na bolj enostaven način izdelajo katalog zbirke osebnih podatkov. Prednost pri takšni izdelavi katalogov zbirk osebnih podatkov (ob upoštevanju določb 27. člena ZVOP-1-UPB1 in navodil) je, da podatke iz katalogov zbirk osebnih podatkov na enostaven način posredujejo tudi Informacijskemu pooblaščencu za namen vodenja registra zbirk osebnih podatkov.

Za točnost in ažurnost vsebine kataloga zbirke osebnih podatkov mora upravljavec v primeru spremembe katerega od 13 dejstev, ki se nanašajo na posamezno zbirko osebnih podatkov, to popraviti oziroma ažurirati tudi vsebino kataloga te zbirke osebnih podatkov.

Kršitve določb 26. člena ZVOP-1-UPB1 predstavlja prekršek po 11. točki prvega odstavka 91. člena ZVOP-1-UPB1.

4 ZAKLJUČEK

Za varovanje in zaščito dokumentov in osebnih podatkov je treba upoštevali kar nekaj zakonov, podzakonskih aktov, predpisov, internih navodil itd. Vendar upoštevanje vseh zapisanih predpisov ni dovolj. V tiskanih in elektronskih medijih beremo članke o posredovanju dokumentov ministrstva v javnost, ta dokument pa ima stopnjo tajnosti. Le kako so lahko taki dokumenti prispeli v javnost? Ali je javnemu uslužbencu po nesreči padel dokument na tla, se posredoval preko elektronske pošte ali preko faksa? Ne, javni uslužbenec je to storil zavestno, čeprav je kljub različnim osebnostnim preverjanjem zavezan k varovanju občutljivih informacij, dokumentov ali osebnih podatkov. Take zlorabe so se že dogajale in se še bodo.

Vendar pa je sistem za preprečitev zlorabe dokumentov in osebnih podatkov zelo obsežen. Vse več ljudi ima dostop do računalnikov, s tem pa se znanje in iznajdljivost posameznikov povečujeta in zlorabo je nemogoče preprečiti v celoti. Ljudje pa smo tudi naivni in lahkoverni. Problem je predvsem pri elektronski pošti, službeni ali pa osebni. Neznani pošiljatelj posreduje elektronsko pošto s prijaznim naslovom, mi ga odpremo in virus je že na našem osebnem računalniku. Tako je sedaj naš sistem dostopen nepridipravu. Ravno tako se pri nagradnih igrah preko elektronske pošte posredujejo naši osebni podatki (rojstni podatki, naslov, davčna številka, EMŠO itd.), številke osebnega računa, kreditnih kartic, kar pa lahko pripelje tudi do kraje identitete.

Kakšne pravice imamo glede snemanja s kamerami? Nadzorovan prostor mora biti označen z napisom, da je pod videonadzorom. Pravico do uporabe teh videoposnetkov ima samo pooblaščena oseba v primeru zlorabe oziroma ropa trgovine ali podjetja. Večji stanovanjski bloki imajo zaradi varnosti nameščeno kamero na vhodu v blok za spremljanje vseh ljudi, ki vstopijo in izstopijo iz bloka. Dogajanje pa 24 ur spremljajo preko določenega televizijskega kanala.

Pri varovanju in zaščiti dokumentov je najprej treba poskrbeti za ustrezne prostore. Prostori so različni glede na različne dokumente, kot so na primer stopnje tajnosti dokumentov, vrsta samega dokumentarnega gradiva, ali se varuje arhivsko gradivo ali elektronsko gradivo in podobno. Prostori morajo biti primerni glede na delo in nato še za hranjenje teh dokumentov. Poskrbeti je treba za ustrezno fizično in računalniško oziroma programsko varnost. Večja stopnja varnosti se uporablja pri občutljivih dokumentih, tako fizično kot programsko. Z občutljivimi dokumenti morajo tudi posamezniki ravnati previdno, ne pa dokumente puščati na mizi, v odklenjeni pisarni, kjer so dostopni vsem. V javni upravi to še marsikje ne deluje tako, kot je potrebno. No, ob vsej tehnološki varnosti je tu ponovno pomemben človeški dejavnik. Neprimerno obnašanje posameznika lahko privede do zlorabe dokumentov in posredovanja dokumentov, občutljivih za javnost.

Vprašalnik za dostop do podatkov EU in NATO ima tudi rubriko, kjer je treba podati finančno stanje. To so prihodki in različni krediti. Glede na finančno stanje se lahko pojavi dvom, da bi uslužbenec zaradi slabih dohodkov in kreditov dokumente EU in NATO preprodal in si s tem izboljšal finančno stanje. Ali je res treba podajati vse te podatke? Ali ni to že prevelik vdor v zasebnost posameznika? Zdi se mi, da so nekateri podatki odveč.

Ravno tako je tudi pri varovanju in varstvu osebnih podatkov pomembna varnost prostorov, kjer se ti podatki obdelujejo. Z dodatnimi gesli in omejitvijo pristopov se osebni podatki še dodatno zaščitijo. Ponovno pa je tu pomemben posameznik. Vpogled v osebne podatke, kot je na primer centralni register prebivalstva, ni kazniv, če ti podatki potem niso zlorabljeni. V javnosti so se pojavili podatki na CD-medijih tisočev komitentov, z osebnimi računi, vsemi transakcijami, ali pa so se izgubili podatki o zdravstvenem stanju tisočev prebivalcev. Ponovno je tu zatajila vsa tehnika visokega varovanja, kajti posameznik je storil napako. Ne glede na vse varovanje je vedno prisoten človeški dejavnik. V vrtcih in šolah so seznami otrok postali nepopolni, saj je zaradi varstva osebnih podatkov prepovedano skupaj objavljati otrokovo ime in priimek. Ali se je pojavila zloraba osebnih podatkov otrok, kot sta ime in priimek?

V naše vsakdanje življenje pa se lahko prikrade tehnika. To poznamo tudi iz filmov, kot je na primer nadzor z navigacijskim sistemom v avtomobilu, telefonu, nadzornimi kamerami na semaforjih ali v tunelih. Ali nas res lahko nekdo nenehno nadzoruje, od odhoda od doma pa do prihoda v službo, kaj smo kupili v trgovini (primer je kartica Mercator Pika), kje smo se vozili z avtobusom, sledi našim pogovorom po mobilnem telefonu? Lahko, če bi nekdo imel voljo in korist od tega. Vendar pa je zato posameznik zaščiten s pravicami o človeški nedostopnosti ter z zakoni in podzakonskimi akti o zlorabi dokumentov in osebnih podatkov.

Veliko pa je seveda odvisno od vsakega posameznika. Ali smo pripravljeni spoštovati obveznosti delodajalca, ali smo pripravljeni neznancu na ulici dati svojo davčno številko ali pa EMŠO pri anketi, ali bomo posredovali svoje bančne podatke po elektronski pošti, ker je prišlo do neke napake v sistemu, itd. Vsak posameznik se bo odločil po svoji volji in presoji, kaj je v tistem trenutku pomembno zanj.

LITERATURA IN VIRI

SAMOSTOJNE PUBLIKACIJE

- BREJC, Miha (2004). *Ljudje in organizacija v javni upravi.* Fakulteta za upravo, Ljubljana.
- PIRC MUSER, Nataša (2006). *ZVOP-1 s komentarjem*. GV založba, d.o.o., Ljubljana.
- mag. SIRNIK, Iztok (2007). *Informatika v upravi (prosojnice).* Fakulteta za upravo, Ljubljana.

PREDPISI

- (1995). Direktiva št. 65/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov, 24. 10. 1995.
- (2008). Kazenski zakonik (KZ-1). Ur. list RS, št. 63/94, 95/04, 55/08.
- (2007). Obligacijski zakonik (OZ-UPB1). Ur. list RS, št. 83/01, 97/07.
- (2006). Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov. Ur. list RS, št. 71/06, 138/06.
- (2011). Uredba o varovanju tajnih podatkov. Ur. list RS, št. 74/05, 48/07, 22/08, 7/11.
- (2006). Uredba o varstvu dokumentarnega in arhivskega gradiva. Ur. list RS št. 86/06.
- (2002). Uredba o vodenju in vzdrževanju centralnega registra prebivalstva ter postopku za pridobivanje in posredovanje podatkov. Ur. list RS, št. 70/00, 28/02.
- (2006). Ustava Republike Slovenije. Ur. list RS, št. 33/91, 42/97, 66/00, 24/03, 69/04, 68/06.
- (2006). Zakon o centralnem registru prebivalstva (ZCRP-UPB1). Ur. list RS št. 1/99, 39/06, 72/06.
- (2011). Zakon o davčnem postopku (ZDavP-2-UPB4). Ur. list RS, št. 18/96, 87/97, 82/98, 91/98, 108/99, 97/01, 54/04, 139/04, 25/05, 109/05, 21/06, 117/06, 125/08, 110/09, 43/10, 97/10, 13/11.
- (2004). Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1). Ur. list RS, št. 57/00, 25/04, 98/04.
- (2009). Zakon o odvetništvu (ZOdv-C). Ur. list RS, št. 18/93, 24/01, 54/08, 35/09.
- (2010). Zakon o policiji (ZPoL-H). Ur. list RS, št. 49/98, 93/01, 79/03, 110/03, 50/04, 102/94, 53/05, 70/05, 98/05, 3/06, 78/06, 107/06, 42/09, 66/09, 22/10.
- (2011). Zakon o tajnih podatkih (ZTP-D). Ur. list RS, št. 87/01, 101/03, 135/03, 28/06, 50/06, 9/10, 60/11.
- (2006). Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Ur. list RS, št. 30/06.
- (2007). Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). Ur. list RS, št. 59/99, 59/01, 86/04, 67/07, 94/07.

VIRI Z INTERNETA

- Ainigma, svetovanje za varno poslovanje, d.o.o. (2011). Dostopno 5. 6. 2011 na: http://www.ainigma.si/.
- Ainigma, svetovanje za varno poslovanje, d.o.o. (2011). Dostopno 5. 6. 2011 na: http://www.ainigma.si/page.php?id=1&cid=1.
- Ainigma, svetovanje za varno poslovanje, d.o.o. (2011). Dostopno 5. 6. 2011 na: http://www.ainigma.si/page.php?id=3&cid=2.
- Ainigma, svetovanje za varno poslovanje, d.o.o. (2011). Dostopno 5. 6. 2011 na: http://www.ainigma.si/page.php?id=3&cid=4.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). Dostopno 28. 1. 1981 na: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
- Direktiva št. 65/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov (1995). Dostopno 24. 10. 1995 na: http://eur-lex.europa.eu/LexUriServ /LexUriServ.do?uri=CELEX:31995L0046:sl:NOT.
- Gama System, d.o.o. (2011). Dostopno 6. 6. 2011 na: http://www.gama-system.si/.
- Gama System, d.o.o (2011). Dostopno 6. 6. 2011 na: http://www.gama-system. si/Content.aspx?id=10040000.
- Gama System, d.o.o. (2011). Dostopno 6. 5. 2011 na: http://www.gama-system.si/NewsItem.aspx?id=182.
- Informacijski pooblaščenec (2011). Dostopno 6. 5. 2011 na: http://www.ip-rs. si/.
- Informacijski pooblaščenec (2011). Dostopno 6. 5. 2011 na: https://www.ip-rs.si/fileadmin/user_upload/doc/Prijava_zaradi_krsitve_zasebnosti.doc.
- Informacijski pooblaščenec EMŠO, Davčna številka... (2011). Dostopno 6. 5. 2011 na: https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/emso-davcna-stevilka/.
- Inštitut za ekonomijo, pravo in informatiko (2007), Dostopno 1. 8. 2007 na: http://www.ipri-zavod.si/news.php?item.53.2.
- Judgment in the Case of Amann v. Switzerland (2000). Dostopno 16. 2. 2000 na: http://www.menschenrechte.ac.at/orig/00_2/Amann.pdf.
- Kaj je varstvo osebnih podatkov (2011). Dostopno 6. 5. 2011 na: http://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika.
- Kolokvij Arhiva RS 2006, Novosti arhivskih predpisov na področju e-hrambe, Mag. Vladimir Žumer (2010). Dostopno 13. 5. 2010 na: http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/kolokvij/ZVladimir. pdf.
- Kriptografija v internetu (2007). Dostopno januar 2007 na: http://www.ca.gov.si/kripto/kr-osn.htm/.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/delovna_podrocja/hramba_dokumentarnega_gradiva_v_ elektronski_obliki/notranja_pravila/.

- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/delovna_podrocja/hramba_dokumentarnega_gradiva_v_ elektronski_obliki/registracija/.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/E-ARHIVI/obrazci/eARS-7-0_ZAHTEVA_ZA_ AKREDITACIJO.pdf.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/uporaba_arhivskega_gradiva/o_arhivskem_ gradivu/.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://reh.ars.gov.si/index.php?page=webInterface&idDefinition=3.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: na: http://reh.ars.gov.si/index.php?page=webInterface&idD.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/uporaba_arhivskega_gradiva/dostopnost_arhivskega_ gradiva/efinition=1.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/zakonodaja_in_dokumenti/predpisi_s_podrocja_arhivske_ dejavnosti_v_sloveniji/.
- Ministrstvo za kulturo, Arhiv Republike Slovenije (2011). Dostopno 9. 5. 2011 na: http://www.arhiv.gov.si/si/uporaba_arhivskega_gradiva/dostopnost_arhivskega _gradiva/.
- Ministrstvo za notranje zadeve, Policija (2010). Dostopno 9. 5. 2010 na: http://www.policija.si/portal/.
- Novela ZVOP-1A stopila v veljavo (2007). Dostopno 22. 11. 2010 na: http://www.ipri-zavod.si/news.php?item.53.
- Republika Slovenija (2010). Dostopno 22. 11. 2010 na: http://intranet.sigov.si/.
- Uradni list Republike Slovenije (2010). Dostopno 22. 11. 2010 na: http://www.uradni-list.si/.
- Vlada Republike Slovenije, Urad Vlade RS za varovanje tajnih podatkov (2011). Dostopno 13. 5. 2011 na: http://www.uvtp.gov.si/.
- Vlada Republike Slovenije, Urad Vlade RS za varovanje tajnih podatkov (2011). Dostopno 13. 5. 2011 na: http://www.uvtp.gov.si/si/delovna_podrocja /dokumentacijska_varnost/dokumentacijska_varnost_eu/.
- Vlada Republike Slovenije, Urad Vlade RS za varovanje tajnih podatkov (2011). Dostopno 13. 5. 2011 na: http://www.uvtp.gov.si/si/delovna_podrocja /dokumentacijska_varnost/dokumentacijska_varnost_nato/.
- Vlada Republike Slovenije, Urad Vlade RS za varovanje tajnih podatkov (2011). Dostopno 13. 5. 2011 na: http://www.uvtp.gov.si/si/delovna_podrocja /industrijska_varnost/.
- Vlada Republike Slovenije, Urad Vlade RS za varovanje tajnih podatkov (2011). Dostopno 13. 5. 2011 na: http://www.uvtp.gov.si/si/delovna_podrocja /informacijska_varnost/.

PRILOGE

Priloga A: Obrazec zahteve za akreditacijo opreme in storitev za digitalno hrambo

Vir: Arhiv Republike Slovenije

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA KULTURO
ARHIV REPUBLIKE SLOVENIJE
1127 Ljubljana, Zvezdarska 1, Slovenija, p.p. 21
Tel.: +386(1)2414200; fax: +386(1)2414269
e-mail: ars@gov.si; http://www.arhiv.gov.si

ZAHTEVA ZA AKREDITACIJO OPREME IN STORITEV ZA DIGITALNO HRAMBO [1]

I. Splošni podatki [2]

1. Naziv ali osebno ime vlagatelja zahteve:
2. Sedež oziroma naslov stalnega prebivališča vlagatelja:
3. Matična številka:
4. Poštni naslov:
5. Elektronski naslov:
6. Spletni naslov (če obstaja):
7. Telefon:
8. Telefaks:

II. Podatki o opremi ali storitvah

9. Vrsta opreme ali storitve (strojna oprema, programska oprema, storitev hrambe, spremljevalna storitev):

10. Naziv storitve/opreme, kot je vpisan v register ponudnikov opreme in storitev:

11. Opis storitve:

Podpis vlagatelja ali pooblaščene osebe:
_____

V _____, dne_____

[1] Priloga 7 Uredbe o varstvu dokumentarnega in arhivskega gradiva (Ur.l. RS št. 86/2006)
[2] Vsi podatki so obvezni razen podatkov pod točko 6 in 8.

Priloga B: Funkcionalni tip programske opreme

Vir: Gama System d.o.o.

Tip programskega produkta		Funkcionalni tip programske opreme Programski produkt glede na nivo uporabe	
		Aplikacijska programska oprema	**Tržni programski produkt**
B.a	Upravljanje dokumentarnega gradiva v fizični obliki	Gama System eDocs 4.1	Gama System eDocs 4.1
B.b	Zajem in pretvorba izvorne analogne v digitalno obliko	Gama System eDocs 4.1	Gama System eDocs 4.1
B.c	Množični zajem in podpora hrambe istovrstnega gradiva	Gama System eDocs 4.1	Gama System eDocs 4.1
B.d	Podpora trajne hrambe za gradivo, ki se ne spreminja		Gama System eArchive 1.1
B.e	Podpora e-hrambe		Gama System eArchive 1.1
C	Podpora celotnemu postopku upravljanja gradiva v digitalni obliki	Gama System eDocs 4.1 + Gama System eArchive 1.1 Gama System eDocs 4.1 + IBM DR 550	Gama System eDocs 4.1 + Gama System eArchive 1.1 Gama System eDocs 4.1 + IBM DR 550

Priloga C: Prijava zaradi zlorabe osebnih podatkov informacijskemu pooblaščencu

Vir: IP-RS

INFORMACIJSKI POOBLAŠČENEC

PRIJAVA ZARADI ZLORABE OSEBNIH PODATKOV

(Pred izpolnjevanjem prijave obvezno preberite spodaj napisana navodila.)

1. Vaši podatki

Ime	
Priimek	
Vaš naslov	
Telefon	
E-pošta	

2. Podrobnosti pritožbe

Kdo je po vašem mnenju kršil pravico do zasebnosti?		
Navedite točen datum nastanka kršitve:		
Kdaj ste organizacijo opozorili na kršitev?		Prosimo, priložite kopijo opozorila, ki ste ga poslali organizaciji.
Ali ste od organizacije prejeli kakšen odgovor?	DA NE (Prosimo obkrožite)	Če ste od organizacije prejeli kakšen odgovor, ga prosimo priložite prijavi.

3. Razlogi za prijavo

(Kako je bila po vašem mnenju kršena pravica do zasebnosti? (Prosimo, bodite kar se da natančni, saj bo v tem primeru lahko Informacijski pooblaščenec obravnaval vašo prijavo bistveno hitreje kot sicer.)

4. Druga dejstva

(Opišite, na kakšen način ste organizacijo ali posameznika opozorili na kršitev in kakšen je bil odgovor.)

5. Datum

Vaš podpis

6. Obvezno preberite

- Informacijski pooblaščenec vaših osebnih podatkov, v skladu z Zakonom o inšpekcijskem nadzoru (Uradni list RS, št. 56/02, v nadaljevanju ZIN), ne bo posredoval prijavitelju.

- Informacijski pooblaščenec bo vaše podatke varoval v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 86/04, s spremembami in dopolnitvami, v nadaljevanju ZVOP-1).

- Podatek o vaši telefonski številki in elektronskem naslovu ni obvezen, priporočamo pa, da nam ju posredujete, saj se da mnogo težav rešiti tudi telefonsko.

- Končno odločbo Informacijskega pooblaščenca bomo objavili v anonimizirani obliki na spodaj napisani spletni strani.

7. Anonimna prijava

Prijavo lahko vložite tudi anonimno. V tem primeru ne vpišete svojih osebnih podatkov. Opozarjamo pa vas, da vas v tem primeru tudi ne bomo mogli obvestiti o naših ugotovitvah in dejanjih.

8. Kontakti (Tudi naslov za pošiljanje prijave)

Vošnjakova 1, p. p. 78, 1000 Ljubljana
Telefon: 01/230 9 730
Faks: 01/230 9 778

www.ip-rs.si