1.09 Objavljeni strokovni prispevek na konferenci
1.09 Published Professional Conference Contribution

Luka Hojnik[*]

PASTI VARSTVA OSEBNIH PODATKOV PRI UPRAVLJANJU IN HRAMBI DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA

Izvleček:

Avtor se v prispevku posveča težavam in dilemam, ki se pojavljajo pri upravljanju in hrambi arhivskega ali dokumentarnega gradiva v zvezi z varstvom osebnih podatkov, ki jih gradivo vsebuje. Področje varstva osebnih podatkov velikokrat predstavlja precejšen zalogaj, tako v organizacijskem kot izvedbenem smislu. V zvezi z roki hrambe gradiva, ki vsebuje osebne podatke, avtor opozarja na nujnost bolj kompleksno strukturiranega klasifikacijskega načrta. Prav tako opozarja na napačno tolmačenje ali nepoznavanje pravnih podlag za obdelavo osebnih podatkov in s tem tudi pravnih podlag za hrambo gradiva, ki takšne podatke vsebuje. Vprašanja informacijske varnosti v zvezi z zunanjim izvajanjem storitev upravljanja in hrambe gradiva so postala ponovno aktualna v tem času, ko se številne storitve selijo v oblak. Tudi v pogodbenem odnosu med lastnikom gradiva in izvajalcem storitve v oblaku je potrebno jasno opredeliti pravice in obveznosti glede obdelave tako hranjenega gradiva in s tem osebnih podatkov, ki jih takšno gradivo vsebuje. Informacijsko pravo bi po mnenju avtorja moralo slediti razvoju informacijske tehnologije ter se ustrezno odzvati na nove izzive, ki iz tega razvoja izhajajo.

Ključne besede:

varstvo osebnih podatkov, obdelava, upravljanje, hramba, dokumentarno gradivo, arhivsko gradivo, informacijska družba, informacijsko pravo, oblak, storitve, digitalizacija, varnost, sistem

Abstract:

Personal Data Protection in Relation to Records and Archives Management and Storage

In the present article, the author deals with problems and dilemmas which occur when managing and storing archives or records in reference to the protection of personal data they contain. The field of personal data protection often represents a huge organizational and executive problem. Regarding retention periods of documents which contain personal data, the author points to the urgency of a more complexly structures filing plan. He also emphasized the incorrect interpretation or ignorance of law regulation for the processing of personal data and therefore also law regulations for storing documents which contain them. Questions of information security regarding outsourced services of records management and storage are again present since numerous services are transferred to the cloud. The contract relation between the documents' owners and providers of cloud-services has to clearly define the rights and obligations considering the processing of stored documents and personal data contained in them. Information law should therefore follow the development of information technology and adequately react to new challenges.

Key words:

personal data protection, processing, managing, storage, records, archives, information society, manager of personal data, information law, cloud, digitalization, security, system

[*] *Luka Hojnik, univ. dipl. prav., vodja pravne pisarne v družbi MFC.2 d. o. o. , Litostrojska cesta 44B, 1000 Ljubljana, Slovenija.*

UVOD

Pred pisanjem tega prispevka sem veliko razmišljal o tem, kako bi to, sicer zelo aktualno tematiko predstavil na način, ki bi vsakogar, ki se ukvarja z upravljanjem in hrambo gradiva, napeljal na razmišljanje o izrednem pomenu varstva osebnih podatkov v postopkih upravljanja in hrambe vseh vrst gradiva, ki vsebuje osebne podatke. V resnici pa nisem pred lahko nalogo, saj področje – kljub svoji navidezni simpatičnosti in relativni jasnosti v teoriji – za tiste, ki ga udejanjamo v praksi, velikokrat predstavlja kar precejšen zalogaj, tako organizacijski kot izvedbeni. Tudi zato sem se odločil, da bom tokrat v svojem prispevku opozoril predvsem na pasti (probleme, dileme, zaplete, težave in kar je še takega), v katere se lahko ujame nič hudega sluteči upravljavec gradiva, ki vsebuje osebne podatke.

Prispevek je tako neke vrste logično nadaljevanje prispevka izpred dveh let[1], v katerem sem pojasnjeval predvsem osnove varstva osebnih podatkov pri upravljanju in hrambi gradiva ter se nekoliko bolj polemično lotil nekaterih ustaljenih (in čestokrat tudi zmotnih) predstav o pravilnem določanju rokov hrambe gradiva in obliki klasifikacijskega načrta kot izhodišča za strokovno pravilno in zakonito upravljanje z gradivom.

Zlahka ugotovimo (in če sami slučajno še nismo, nam dajo to vedeti na vsakem koraku), da smo se že davno tegá preobrazili v informacijsko družbo in da ta družba ni več zgolj družba računalnikov in njihovih variacij, temveč predvsem družba interneta in informacijskih tehnologij, povezanih z njim. Tako se v zadnjih letih naša življenja ne vrtijo več okrog bivanja na tleh, temveč čedalje pogosteje živimo in delamo v oblakih. Da, navkljub vsej prizemljenosti (v katero pa spričo dnevnih dogodkov doma in po svetu upravičeno kdaj pa kdaj tudi podvomim), se torišče dogajanja v svetu informacijskih tehnologij seli na svetovni splet, na internet, v *"oblačno družbo"* oz. t. i. *"cloud society"*. In ker v "oblačni družbi", tako kot pri tleh, težko preživimo brez takšnih in drugačnih vsebin oz. dokumentov, tudi te seveda selimo tja gor, v oblake. To pa seveda ponovno sproža številna pravna in dejanska vprašanja s področja varstva osebnih podatkov, ki se jih bom prav tako dotaknil v tem prispevku, saj bi jih bilo ob vsem pompu, ki se dandanašnji ustvarja okrog njih, skrajno ignorantsko izpustiti, pri čemer pa vemo, da še od starorimskih časov naprej velja: *"Ignorantia iuris nocet"* oz. *"nepoznavanje prava škoduje"*. Zato je čas, da se iz sveta oblakov in pravnih fikcij preselimo k našim pastem.

NEOBSTOJEČ ALI NEPOPOLN KLASIFIKACIJSKI NAČRT

Klasifikacijski načrt je osnovni in najpomembnejši šifrant za razvrščanje dokumentarnega in arhivskega gradiva. Je temeljno navodilo za upravljavca gradiva, saj v njem evidentira predvsem to, katere vrste gradiva hrani in kakšni so roki hrambe tega gradiva. Opaziti je, da se podjetja (subjekti zasebnega prava) le redko odločajo za izdelavo klasifikacijskega načrta, če pa že, ga izdelajo le večja. Velikokrat pri tem uporabijo kar javno dostopne vzorce, zato jih podjetja pogosto tudi obravnavajo na način, na kakršnega so do njih prišla, in se ne zavedajo pravega pomena takšnega notranjega akta za njihovo poslovanje. Predvsem pa se ne zavedajo

[1] *Hojnik, L. (2010). Varstvo osebnih podatkov pri upravljanju in hrambi dokumentarnega in arhivskega gradiva, Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 9. Zbornik referatov dopolnilnega izobraževanja s področij arhivistike, dokumentalistike in informatike v Radencih 2010 (str. 515-520). Maribor: Pokrajinski arhiv.*

dejstva, da kvalitetno izdelan klasifikacijski načrt vodi do urejenega arhiva, ne glede na to, v kakšni obliki je gradivo hranjeno.

Obvezni del klasifikacijskega načrta so tudi roki hrambe gradiva, ki pa morajo biti pravilno določeni, sicer nam klasifikacijski načrt ni v nobeno korist oz. lahko postane celo vzrok različnih pravnih sankcij, ki lahko organizacijo doletijo v primeru hrambe gradiva, ki je daljša od predpisanih rokov hrambe. To zlasti velja pri gradivu, ki vsebuje osebne podatke, saj za hrambo osebnih podatkov velja, da se smejo hraniti le tako dolgo, kot to določa posamezni področni zakon (če je pravna podlaga za obdelavo v zakonu), do preklica soglasja posameznika (če je pravna podlaga v privolitvi posameznika) oz. v vseh ostalih primerih le, dokler je to potrebno za dosego namena, zaradi katerega so bili osebni podatki zbrani, pridobljeni oz. drugače obdelovani. Tako določeni roki so torej maksimalni in ne minimalni, kot to velja pri večini drugega gradiva, ki osebnih podatkov ne vsebuje.

V izogib scenariju, po katerem bi lahko prišlo do kakršnihkoli pravnih sankcij za organizacijo, ki bi gradivo, ki vsebuje osebne podatke, hranila dlje od dovoljenega roka hrambe, bo pogosto potrebno klasifikacijski načrt strukturirati bolj kompleksno, globlje, če bo potrebno tudi na raven posameznega dokumenta (ki vsebuje osebne podatke). Samo tako bomo namreč lahko zagotovili, da bo klasifikacijski znak opravljal vlogo razločevalca dokumentov v sistemu klasične ali elektronske hrambe glede na različne roke hrambe za posamezne dokumente, kar bo omogočalo zakonito obdelavo takšnega dokumentarnega gradiva oz. njegovo (pravočasno) izločanje po poteku rokov hrambe.

NEOBSTOJEČA ALI NAPAČNO TOLMAČENA PRAVNA PODLAGA ZA OBDELAVO OSEBNIH PODATKOV

Naslednja past, v katero se po naših izkušnjah ujamejo številni subjekti v zasebnem in javnem sektorju, pa je gotovo napačno tolmačenje pravnih podlag za obdelavo osebnih podatkov in s tem tudi pravnih podlag za hrambo gradiva, ki takšne podatke vsebuje. V praksi se namreč dogaja, da organizacije gradivo z osebnimi podatki hranijo na zalogo, z mislijo, da bo morda nekoč že še prav prišlo. Takšno razmišljanje je do neke mere seveda razumljivo in upravičeno tedaj, ko imajo za to pristojni opravka z arhivskim gradivom, gradivom, ki je trajnega pomena za znanost, kulturo, družbo nasploh in ga praktično v nobenem primeru ni dovoljeno uničiti. V vseh ostalih primerih, ko gre za hrambo dokumentarnega gradiva, pa lahko takšno razmišljanje hitro privede to težav. Te se najprej pokažejo v pomanjkanju prostora, nepreglednosti in neurejenosti gradiva, ki zaradi tega postaja čedalje težje dostopno, s tem pa seveda tudi neuporabno, pri čemer vemo, da je prav uporabnost gradiva njegova najbolj bistvena lastnost. Ker zmanjkuje ustreznih prostorov, se višek tako nakopičenega gradiva hitro znajde v popolnoma neustreznih prostorih, kar predstavlja dodatno nevarnost za njegovo poškodbo ali celo uničenje.

Če takšno gradivo vsebuje osebne podatke, pa je problem lahko še večji. Z neurejenostjo arhiva se poveča njegova nepreglednost, gradivo ni ustrezno popisano, nihče ne skrbi za redno izločanje gradiva, ki mu je potekel rok hrambe, ker pa se takšno gradivo zaradi prostorske stiske pogosto znajde tudi v neprimernih prostorih, se rado zgodi, da imajo tam dostop do njega tudi nepooblaščene osebe, ki se po teh prostorih gibljejo. Skratka, ponovno so ogrožene temeljne lastnosti, ki jih mora gradivo izpolnjevati, organizacija pa je tako lahko celo večkratno v prekršku zaradi nezakonite obdelave osebnih podatkov. Potrebno je namreč poudariti, da po terminologiji zakonodaje s področja varstva osebnih podatkov tudi hramba gradiva, ki

osebne podatke vsebuje, predstavlja obdelavo le- teh[2]. Ta pa je dovoljena le, če zanjo obstoji ustrezna pravna podlaga, ki pa se nekoliko razlikuje glede na to, ali je lastnik gradiva (upravljavec osebnih podatkov) pravna oseba zasebnega ali javnega prava.

ZVOP-1 namreč obdelavo osebnih podatkov v javnem sektorju regulira strožje kot v zasebnem[3]. Pravna oseba javnega prava tako sme osebne podatke obdelovati le v primeru, da takšno obdelavo in osebne podatke, ki se lahko obdelujejo, določa zakon, razen v nekaterih izjemnih primerih, ki se nanašajo na obdelavo osebnih podatkov nosilcev javnih pooblastil oz. če gre za obdelavo osebnih podatkov posameznikov, ki so z javnim sektorjem sklenili pogodbo ali pa so z njim v fazi sklepanja pogodb.

Če so upravljavci v javnem sektorju precej omejeni pri zakoniti obdelavi osebnih podatkov, pa je okvir, v katerem smejo osebne podatke obdelovati organizacije v zasebnem sektorju, vendarle nekoliko širši. Tako velja, da v kolikor gradivo pravne osebe zasebnega prava v papirni ali digitalni obliki vsebuje osebne podatke, sme pravna oseba te podatke obdelovati le ob predpostavki, da je izpolnjena vsaj ena od navedenih pravnih podlag[4]:

- zakonodaja (pooblastilo oz. dovoljenje za obdelavo določa že sam zakon);
- osebna privolitev posameznika (pooblastilo oz. dovoljenje za obdelavo upravljavec pridobi od posameznika, na katerega se osebni podatki nanašajo);
- pogodba (obdelava osebnih podatkov je potrebna za sklenitev pogodbe ali za izvedbo njenega predmeta);
- uresničevanje zakonitih interesov zasebnega sektorja (vendar le v primeru, da ti interesi očitno prevladajo nad interesi posameznika, na katerega se osebni podatki nanašajo).

Obdelava (in s tem seveda tudi hramba) dokumentarnega gradiva, ki vsebuje osebne podatke, tako ni dopustna v nobenem drugem primeru. V kolikor lastnik gradiva (upravljavec osebnih podatkov) tega ne upošteva, je lahko podvržen upravnim, civilnim in kazenskim sankcijam.

NEPREPOZNAVANJE POGODBENE OBDELAVE OSEBNIH PODATKOV

Pri izvajanju pregledov organizacij v javnem in zasebnem sektorju z vidika urejenosti na področju informacijskega prava pogosto opazimo, da se organizacije ne zavedajo, da gre v številnih primerih, ko izvajanje določenih storitev poverijo zunanjim izvajalcem (npr. računovodskim servisom, kadrovskim agencijam, odvetniškim družbam, podjetjem za izterjavo, detektivskim agencijam, vzdrževalcem strojne in programske opreme, podatkovnih zbirk, izvajalcem zajema in hrambe gradiva ipd.), za pogodbeno obdelavo osebnih podatkov. Z zunanjimi izvajalci imajo sklenjene pogodbe o izvajanju storitev, pri čemer pa je področje varstva osebnih podatkov v njih pogosto zelo splošno urejeno ali celo izpuščeno.

---

[2] *Hojnik, L. (2010). Varstvo osebnih podatkov pri upravljanju in hrambi dokumentarnega in arhivskega gradiva, Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 9. Zbornik referatov dopolnilnega izobraževanja s področij arhivistike, dokumentalistike in informatike v Radencih 2010 (str. 515-520). Maribor: Pokrajinski arhiv.*

[3] *9. člen Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

[4] *10. člen Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

Redko naletimo na organizacijo, ki ima z vsemi svojimi pogodbenimi obdelovalci sklenjene posebne pogodbe o obdelavi osebnih podatkov, z vsemi elementi, ki jih predpisuje ZVOP-1[5] in jih navajamo v nadaljevanju tega prispevka na primeru zunanjega izvajanja e- hrambe gradiva.

Ponudniki spremljevalnih storitev in storitev hrambe dokumentarnega in arhivskega gradiva v razmerju do naših strank zelo pogosto nastopamo v vlogi pogodbenih obdelovalcev osebnih podatkov, zato je izrednega pomena, da se tako mi kot naše stranke zavedamo pomena varovanja osebnih podatkov in da oboji dosledno spoštujemo zahteve zakonodaje s tega področja.

TUDI PRI STORITVAH V OBLAKU LAHKO GRE ZA POGODBENO OBDELAVO OSEBNIH PODATKOV

Mnogo organizacij v javnem in zasebnem sektorju je že ugotovilo, da je smiselno za upravljanje z gradivom, izvajanje hrambe gradiva v papirni in digitalni obliki ter za izvajanje povezanih, spremljevalnih storitev (urejanja, zajema oz. pretvorbe, izločanja in uničevanja gradiva) najemati zunanje izvajalce, ki imajo znanje, vrhunsko opremo ter primerne prostore za izvajanje teh storitev. V praksi se je namreč pokazalo, da s tem organizacija lahko ogromno prihrani, hkrati pa znatno zmanjša tveganje, da bi prišlo do poškodbe, uničenja ali zlorabe gradiva.

In prav vprašanja informacijske varnosti v zvezi z zunanjim izvajanjem storitev so postala ponovno aktualna v tem času, ko se številne storitve selijo v oblak. Ker bi za naštevanje vseh storitev, ki se danes že ponujajo v oblaku, potreboval več prostora, kot ga je na voljo na straneh tega zbornika, in glede na to, da vendarle govorimo o upravljanju z gradivom, se bom omejil izključno na storitev "hrambe gradiva v oblaku", ki pravzaprav ni nič drugega kot to, kar ponudniki na trgu ponujamo že vrsto let, tj. hramba gradiva v digitalni obliki na naši infrastrukturi, z možnostjo dostopa strank (lastnikov gradiva) do tega gradiva prek spletnega vmesnika, ob upoštevanju varnostnih standardov, praktično od koderkoli.

Ker gre v vseh primerih izvajanja storitve, pri kateri lastniki gradiva v takšen oblak pošiljajo gradivo, ki vsebuje osebne podatke, za pogodbeno obdelavo teh podatkov s strani izvajalca (ponudnika storitve v oblaku), je seveda nujno potrebno, da med lastnikom gradiva (upravljavcem osebnih podatkov) in izvajalcem storitve v oblaku (v našem primeru e-hrambe gradiva, sicer pa katerekoli storitve, povezane z obdelavo osebnih podatkov), obstaja pogodbeni odnos, v katerem je potrebno jasno opredeliti pravice in obveznosti glede obdelave tako hranjenega gradiva in s tem osebnih podatkov, ki jih takšno gradivo vsebuje.

Lastnik gradiva in pogodbeni obdelovalec morata skleniti pogodbo o obdelavi osebnih podatkov (obvezno v pisni obliki), ki mora vsebovati tudi dogovor o postopkih in ukrepih, s katerimi bodo podatki zavarovani pred slučajnim ali namernim nepooblaščenim uničevanjem, njihovo spremembo ali izgubo ter nepooblaščeno obdelavo[6]. ZVOP-1 pa še določa, da so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena zakona[7].

---

[5] *11. člen v povezavi s 24. členom Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

[6] *24. člen Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

[7] *25. člen Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

Zavarovanje osebnih podatkov je po določbi prvega odstavka 24. člena ZVOP-1 opredeljeno kot sklop organizacijskih, tehničnih in logično-tehničnih postopkov in ukrepov, 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:

1. varujejo prostori, oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani ter kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

Zgoraj navedeno velja za odnos lastnika gradiva in pogodbenega obdelovalca v Sloveniji oz. na območju EU (ter na območju držav, za katere je Informacijski pooblaščenec ugotovil, da zagotavljajo enako raven varstva osebnih podatkov, kot jo zagotavljajo države EU, npr. Švica, Hrvaška, delno ZDA, ko gre za iznos organizacijam, ki delujejo po načelih t. i. "Varnega pristana"). Ker pa vemo, da danes številne storitve v oblaku ponujajo tudi ponudniki izven območja EU (iz t. i. tretjih držav), pri katerih ni vedno jasno, kje se bodo podatki v resnici nahajali, je ključnega pomena, da opozorimo na to, da je v primeru najema storitev pri takšnih ponudnikih nujno pridobiti čim več informacij o ponujeni storitvi ter tudi o lokaciji strežnikov, na katerih se bodo podatki hranili.

V primeru, ko bi lastnik gradiva želel, da se to hrani izven območja EU in zgoraj navedenih držav, je iznos gradiva (in s tem osebnih podatkov v njem) mogoč izključno ob upoštevanju določb ZVOP-1, ki se nanašajo na iznos osebnih podatkov v tretjo državo. Te namreč natančno določajo protokol in posebnosti urejanja pogodbenega odnosa[8] med lastnikom gradiva (upravljavcem osebnih podatkov), ki želi podatke iznašati iz območja EU v tretjo državo, in takšnim ponudnikom, ki podatke hrani na lokaciji izven EU (v tretji državi)[9].

---

[8] *Po določbi 1. odstavka 63. člena ZVOP-1 je posredovanje osebnih podatkov, ki se obdelujejo ali se bodo obdelovali šele po opravljenem posredovanju v tretjo državo, dopustno v skladu z določbami tega zakona in pod pogojem, da državni nadzorni organ izda odločbo, da država, v katero se iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov. Po določbi 3. odstavka 63. člena ZVOP-1 pa omenjena odločba ni potrebna, če je tretja država na seznamu tistih držav iz 66. člena tega zakona, za katere je ugotovljeno, da delno zagotavljajo ustrezno raven varstva osebnih podatkov, če se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrezna raven varstva. Med tovrstne primere držav, pri katerih je ugotovljeno delno ustrezno varstvo osebnih podatkov, na podlagi odločbe Pooblaščenca sodijo tudi ZDA, vendar le za tiste organizacije, ki so se zavezale dogovoru Varni pristan (angl. Safe Harbor). Evropski režim varstva osebnih podatkov se namreč precej razlikuje od režima ZDA, od koder prihaja nekaj največjih ponudnikov zunanjega računalništva v oblaku, nekateri medsebojni dogovori, kot je dogovor Varni pristan, pa naj bi omogočili lažjo izmenjavo podatkov med tema različnima režimoma. Varni pristan omogoča upravljavcem osebnih podatkov, da svoje podatke posredujejo upravljavcem ali pogodbenim obdelovalcem iz ZDA (kot so npr. Google, Amazon ipd.), če so se ta podjetja zavezala k spoštovanju načel Varnega pristana. Obširnejša razlaga dostopna na spletnih straneh Urada informacijskega pooblaščenca, mnenje št. 0712-1/2011/3460 z dne 21. 12. 2011.*

[9] *63.-71. člen Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

NEPOOBLAŠČEN DOSTOP DO OSEBNIH PODATKOV V ZBIRKAH GRADIVA

Kot eno od pogosto zaznanih pomanjkljivosti sistema varstva osebnih podatkov v organizacijah, lahko izpostavimo tudi nepooblaščen dostop do gradiva, ki vsebuje osebne podatke. Ponavadi se z določitvijo uporabniških pravic oz. pravic dostopov na ravni dokumentnih sistemov, sistemov e-hrambe in nasploh v informacijskih sistemih organizacij dostopi dokaj ustrezno obvladujejo, medtem ko se ta vidik zanemarja pri dostopu do gradiva v papirni obliki, ki ga organizacije hranijo v svojih prostorih.

Pogosto namreč naletimo na primere, ko se po arhivu organizacije lahko sprehodi vsakdo od zaposlenih, ki pač potrebuje (ali pa tudi ne) določen dokument. Samo večje organizacije imajo organizirano specializirano arhivsko službo, ki je pooblaščena za upravljanje z gradivom, oz. to upravljanje poverijo specializiranemu zunanjemu izvajalcu, ki bodisi na lokaciji organizacije ali v lastnih prostorih s sklopom tehničnih, organizacijskih in logično-tehničnih postopkov in ukrepov skrbi za vse vidike varstva gradiva v hrambi ter za naročnika tudi vodi in mu omogoči vpogled v postopke upravljanja z gradivom ter v evidence sledljivosti vseh obdelav gradiva oz. akcij na podatkih.

ZVOP-1 upravljavcem predpisuje, da morajo zagotoviti takšen sistem varstva osebnih podatkov, da bodo do njih dostopali le tisti posamezniki znotraj organizacije, ki so za to upravičeni in ki te podatke potrebujejo za opravljanje svojih delovnih nalog. V notranjem predpisu organizacije (ZVOP-1 določa, da je to pravilnik o varstvu osebnih podatkov) morajo biti poleg postopkov in ukrepov za zavarovanje osebnih podatkov tako določene tudi osebe, ki so odgovorne za posamezne zbirke osebnih podatkov, ter osebe, ki lahko zaradi narave svojega dela obdelujejo določene osebne podatke. To z drugimi besedami pomeni, da se bo zelo redko zgodilo, da bodo imeli dostop do gradiva, ki vsebuje osebne podatke, vsi zaposleni v neki organizaciji.

PREMAJHNA ZAVEST O VODENJU SLEDLJIVOSTI OBDELAV OSEBNIH PODATKOV

Področje vodenja evidenc sledljivosti obdelav osebnih podatkov je večna tema, ki pri upravljavcih zbirk osebnih podatkov vselej vzbudi precejšnje ogorčenje in negodovanje, sploh ko beseda nanese na njihovo dolžnost vodenja sledljivosti vseh obdelav osebnih podatkov, tudi vpogledov v gradivo, ki vsebuje osebne podatke. In to ogorčenje je resnici na ljubo do določene mere celo razumljivo in upravičeno, saj so sistemi, ki omogočajo takšno vodenje sledljivosti, relativno dragi, kar pomeni, da si jih lahko privoščijo le večje organizacije, še dražja pa kmalu postane strojna oprema, na kateri se shranjujejo sledi obdelav (t. i. dnevniki obdelav oz. "log"-datoteke), saj se morajo le-te hraniti za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi morebitnega nedopustnega posredovanja ali obdelave osebnih podatkov[10].

Zgoraj navedeno pa ne velja zgolj za osebne podatke, ki jih vsebuje gradivo v digitalni obliki, temveč tudi za tiste, ki jih vsebuje gradivo v papirni obliki, se pravi vse gradivo, ki se v organizacijah tipično hrani v priročnih in stalnih arhivih. Tudi za obdelavo osebnih podatkov v tem gradivu so lastniki gradiva dolžni voditi evidenco sledljivosti obdelav, ki skladno z definicijo ZVOP-1 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,

[10] *5. točka 1. odst. 24. čl. Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje. Pri tem je lahko obdelava ročna ali avtomatizirana (glede na uporabljena sredstva obdelave). Ker je ZVOP-1 tehnološko nevtralen, tudi ne predpisuje, v kakšni obliki naj bi se takšna evidenca sledljivosti vodila, zato je to prepuščeno iznajdljivosti upravljavcev osebnih podatkov.

Da pa bi kljub vsemu področje vodenja sledljivosti obdelave osebnih podatkov nekako ohranili v mejah obvladljivega, vselej svetujemo, da upravljavci temeljito razmislijo o ustroju sistema dodeljevanja uporabniških pravic za dostop do osebnih podatkov, le-te omejijo do mere, ki še omogoča normalno delo in poslovanje organizacije ter s tem znatno zmanjšajo tudi število uporabnikov, pri katerih je potrebno voditi evidence sledljivosti. Nenazadnje je bil to tudi namen ZVOP-1, ki izhaja iz tega, da naj se osebni podatki obdelujejo izključno za namen, zaradi katerega so bili zbrani, in da naj se dostop do njih omogoči zgolj tistim uporabnikom znotraj organizacije, ki ga nujno potrebujejo pri svojem delu.

NEUSTREZNO ZAVAROVANJE GRADIVA, KI VSEBUJE OSEBNE PODATKE

Zadnji vidik varstva osebnih podatkov pri upravljanju gradiva, na katerega bi želel opozoriti v tem prispevku (še zdaleč pa ne zadnji nasploh!), pa je zavarovanje osebnih podatkov.

Pri pregledu stanja arhivov v organizacijah javnega in zasebnega sektorja ter ob prevzemih gradiva na lokacijah naročnikov namreč pogosto ugotovimo, da se gradivo hrani v popolnoma neustreznih prostorih. Posebej zaskrbljujoče pa je, da ujetnik takšnih prostorov ni zgolj dokumentarno gradivo, temveč tudi zbirke arhivskega gradiva, ki so tako izpostavljene dejavnikom, ki jih lahko fizično poškodujejo ali celo uničijo (vlaga, glodalci, neustrezna temperatura, prevelika izpostavljenost svetlobi, izpostavljenost dejavnikom tveganja za požar ali poplavo – neustrezna el. napeljava, lesene police, kletni prostori, nevzdrževane vodovodne ali celo kanalizacijske cevi itd.). Velikokrat pa so zbirke gradiva tudi povsem neustrezno zavarovane pred nepooblaščenim dostopom, kar na široko odpira možnosti zlorab, manipulacije vsebine gradiva, neupravičene seznanitve z osebnimi podatki ipd. S tem organizacije kršijo tako pravila arhivske zakonodaje (in stroke) kot tudi pravila, ki veljajo na področju varstva osebnih podatkov. Zato kaže opozoriti, da bi moralo biti zavedanje o skrbi za kakovostno upravljanje dokumentarnega in arhivskega gradiva na višji ravni. Uspešnega, predvsem pa učinkovitega poslovanja podjetja v zasebnem sektorju ali delovanja organizacije v javnem sektorju si namreč brez urejenega področja upravljanja z gradivom pač ni mogoče predstavljati.

Posebej zaskrbljujoče pa je, da je stanje na tem področju precej slabo tudi v organizacijah, ki v svojih prostorih ustvarjajo in hranijo velike količine gradiva, ki vsebuje občutljive osebne podatke (npr. zdravstvene), za katere zakonodaja predvideva posebno strog režim varstva s številnimi dodatnimi zahtevami, ki jih morajo upravljavci pri tem izpolnjevati[11].

Stanje je nekoliko boljše pri gradivu v digitalni obliki. ZVOP-1 od upravljavcev (in pogodbenih obdelovalcev) zahteva, da se varujejo prostori, oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami, ter aplikativna programska oprema, s katero se obdelujejo osebni podatki. Hkrati pa morajo

[11] *13. in 14. čl. Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. l. RS, št. 94/2007).*

preprečevati nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih. Današnji dokumentni sistemi in sistemi za e-hrambo, ki jih organizacije uporabljajo v kombinaciji s sodobno strojno opremo, večinoma omogočajo zadovoljivo raven varstva gradiva, pri čemer pa je potrebno ponovno poudariti, da je ključna pravilna nastavitev in uporaba takšnega sistema, redno vzdrževanje strojne in posodabljanje programske opreme, varnost omrežja, ustrezno opremljeni strežniški prostori in izdelan sistem varnostnega kopiranja, načrtovanje ukrepov informacijske varnosti v skladu z oceno tveganja ter postopanje v skladu z varnostno politiko organizacije in načrtom neprekinjenega poslovanja. Seveda pa ne smemo prezreti dejstva, da so najbolj varni sistemi tisti, ki jih upravljajo in uporabljajo dovolj izobraženi ter usposobljeni uporabniki.

SKLEP

Jasno je, da je splet postal osrednji medij v svetu informacijskih tehnologij in da bo čedalje manj informacijskih sistemov, ki bi delovali zgolj lokalno, izolirano od spleta in možnosti, ki jih ta ponuja. Tudi največje svetovne organizacije ugotavljajo, da je ključ do učinkovitejšega poslovanja dajanje čedalje večjega nabora storitev v zunanje izvajanje. Pri vsem tem nekoliko zmoti le podatek, da je v svetovnem merilu še vedno relativno visok delež podjetij, ki naj ne bi povsem zaupala storitvam v oblaku. Prepričan sem, da se bo ta procent v kratkem spremenil, saj ponudniki storitev ogromno vlagamo v ozaveščanje, krepitev zaupanja, izobraževanje ter ne nazadnje tudi v infrastrukturo, ki je že zdaj na nivoju, kakršnega si posamezna organizacija v svojih prostorih praktično ne more privoščiti.

V prispevku sem poskušal podati odgovore na nekaj najbolj pereča vprašanja, s katerimi se v praksi srečujemo upravljavci gradiva, ki vsebuje osebne podatke. Pred vse, ki delamo na področju informacijskega prava, pa sodobne informacijske tehnologije nenehno postavljajo številne strokovne izzive, ki odpirajo povsem nova vprašanja ter dileme, o katerih doslej morda niti nismo razmišljali. To hitro razvijajoče se področje predstavlja velik izziv tudi za zakonodajalca, saj bo moral zakonodajni okvir prilagoditi nekaterim povsem novim konceptom pridobivanja, uporabe in razširjanja podatkov ter informacij.

SUMMARY

PERSONAL DATA PROTECTION IN RELATION TO RECORDS AND ARCHIVES MANAGEMENT AND STORAGE

It is clear now, that internet has become the main and central medium in the information technology world. Today it is hard to imagine a modern information system which would work in local information environments only, completely isolated from the web and from the possibilities, offered by the web. Outsourcing of services to the providers who offer them in a "cloud" is realized to be the optimal choice by more and more organisations worldwide. But as the technologies advance, many legal problems in the field of information law, arise.

Today´s information society is overflowed with different categories of personal data and other important information regarding our lives. Many of them are

frequently monitored by the authorities, especially after the anti-terrorist laws are being enforced in many countries around the world.

In this article I am emphasizing the importance of personal data protection within the processes of management and retention of documents and archives. I try to answer the most common questions and address the most common problems and dilemmas, which arise in the usual working environment of an avarage personal data controller (who is also the owner of documents and archives).

Despite the fact, that the personal privacy is defined as one of the fundamental human rights in international law, in the Slovenian Constitution and Personal data protection law, violations still occur, mostly due to unlawful processing of personal data, overrunning data retention periods, misinterpretation of legal grounds for personal data processing, non-recognized personal data processors, unauthorised access to the documents and archives that contain personal data, low level of perception of data processing auditing, inadequate security of premises and/ or hardware, where documents and archives are being stored, etc.

Information law should be able to react to numerous new concepts in information technology development and should be able to accept new challenges that appear in such a development. It should be able to suggest and finally form an adequate legislative framework, which would provide, on the one hand, enough rights, space and possibilities to data controllers and on the other hand still ensure an adequate level of individual´s privacy protection in usage of prospecting *"new age information technology services"*.