Klasična in nova paradigma varovanja občutljivih podatkov v arhivih

Miroslav NOVAK, *Ph.D., Asist. Prof.*
Regional Archives Maribor, Glavni trg 7, SI-2000 Maribor
e-mai: miro.novak@pokarh-mb.si

Traditional and a New Paradigm of Protection of Sensitive Data in the Archives

ABSTRACT

Current practice of protection of (sensitive) data in the archives is based on the controlled restriction and use of archival material. It can be defined as the potential capability of consistent and long-term management of their statuses. A new paradigm of sensitive data protection is upgrading the traditional paradigm and it covers the protection of sensitive data in the whole segment of archival metadata. According to the new paradigm properly captured and professional maintained archival metadata, become an important basis for the protection of (sensitive) archival data. This can be defined as a complex professional task that must be consistently implemented in all procedures and policies of each archival institution.

Key words: archival material, archival data, sensitive data, protection, archival information system

Classico e nuovo modello di protezione dei dati sensibili nella pratica archivistica

SINTESI

La pratica corrente di protezione dei dati (sensibili) negli archivi si basa sulla restrizione controllata e l'uso di materiale d'archivio. Essa può essere definita come potenziale capacità di gestione coerente ed a lungo termine del loro status. Un nuovo modello di protezione dei dati sensibili aggiorna il modello tradizionale e copre la protezione dei dati sensibili in tutto il segmento dei metadati di archiviazione. Secondo il nuovo modello, i metadati professionali correttamente catturati professionalmente mantenuti diventano una base importante per la protezione dei dati d'archivio (sensibili). Questo può essere definito come un incarico professionale complesso che deve essere implementato in modo coerente in tutte le procedure e le politiche di ciascuna istituzione archivistica.

Parole chiave: materiale d'archivio, dati d'archivio, dati sensibili, protezione sistema archivistico informatico

Klasična in nova paradigma varovanja občutljivih podatkov v arhivih

IZVLEČEK

Dosedanja praksa s področja varovanja (občutljivih) podatkov v arhivih temelji na kontroliranem omejevanju dostopa in uporabe arhivskega gradiva. Opredeljujemo jo kot stopnjo zmožnosti konsistentnega in dolgoročnega upravljanja množice njihovih statusov. Nova paradigma varovanja občutljivih podatkov pa nadgrajuje klasično predvsem v metapodatkovnem segmentu. Skladno z njo postajajo ustrezno zajeti in strokovno obravnavani arhivski metapodatki pomembna osnova celovitega upravljanja (občutljivih) podatkov v arhivih. To pa predstavlja kompleksno strokovno nalogo, ki jo je potrebno konsistentno izvajati v vseh postopkih in politikah sleherne arhivske ustanove.

Ključne besede: arhivsko gradivo, arhivski podatki, občutljivi podatki, varovanje, arhivski informacijski sistem

1 Uvod

Splošna paradigma varovanja podatkov v arhivih, še posebej občutljivih, temelji na spoznanju, da so ti izpostavljeni zlorabi ali uničenju, zato je potrebno permanentno spremljati mnoge dejavnike tveganja na fizičnem in/ali logičnem podatkovnem nivoju. V ta namen je razvitih mnogo postopkov in standardov, njihova implementacija pa je v veliki meri tudi zakonsko urejena, saj so neposredne arhivske strokovne aktivnosti varovanja podatkov praviloma formalizirane v različnih pravnih, organizacijskih, postopkovnih in drugih aktih. Te pa so realizirane skozi mnoge varnostne, kulturne, kadrovske, prostorske, organizacijske, postopkovne in druge politike v arhivih in arhivskih ustanovah.

Podatki v arhivih so lahko odtujeni sami po sebi ali skupaj z nosilci in sredstvi za zapisovanje, ali pa so manipulirani na kontekstnem ali vsebinsko logičnem nivoju. Iz tega lahko izpeljemo arhivsko strokovno izhodišče, da njihovo neposredno varovanje temelji na selektivnem omejevanju dostopa in uporabe arhivskega gradiva v najširšem pomenu besede.

V dosedanji arhivski teoriji in praksi je opredeljeno "**varovanje podatkov**", tako da se zavarujejo:

- nosilci podatkov, vključno z njihovimi okolji;
- zapisi podatkov na medijih, vključno z vsebinami, ki so predmet arhivskih strokovnih obravnav (arhivsko gradivo);
- zapisi podatkov na medijih, vključno z vsebinami, ki so rezultat izdelave informativnih pomagal (prim.: *Klasinc, str. 155-158*).

Ne glede na uporabljene metode in načine varovanja podatkov se arhivisti v praksi pogosto srečujejo z mnogimi problemi identifikacije dejavnikov tveganja ter načini njihovega omejevanja. Omejene možnosti njihovega natančnega in permanentnega identificiranja na dolgo dobo pa predstavljajo dodaten dejavnik tveganja pri izvajanju arhivskih strokovnih aktivnosti.

V nadaljevanju tega prispevka bodo predstavljene osnovne norme varovanja podatkov v arhivih s posebnim ozirom na teoretično razumevanje definicije občutljivih podatkov, ki izhaja iz slovenske arhivske zakonodaje in zakonodaje s področja varovanja občutljivih podatkov. Na podlagi praktičnih primerov bo utemeljena potreba za nadgradnjo obstoječe arhivske paradigme razumevanja in varovanja podatkov z novimi zahtevami in funkcionalnostmi. Na ta način bi vzpostavili sistem, po katerem bi dolgoročno ustrezneje zaščitili njihovo integriteto v času in prostoru tako za njihove fizične kot tudi elektronske oblike. Sistem tovrstne zaščite bi moral biti konsistenten ne glede na okolje, v katerem se nahajajo podatki, kot tudi na njihovo pozicijo v življenjskem ciklu arhivskih in drugih dokumentov.

2 Terminologija in problem definicij podatkov v arhivih

Za poglobljeno razumevanje obravnavanega problema je potrebno definirati osnovne pojme. Tako lahko za potrebe tega prispevka uporabimo definicijo pojma, po kateri je "**podatek**" *dejstvo, ki o določeni stvari kaj pove ali se nanjo nanaša* (*SSKJ, 2014*). Iz te lahko izpeljemo definicijo "**arhivski podatek**". Tega definiramo kot podatek, ki izhaja iz arhivskega gradiva in ga je potrebno dolgoročno ohraniti in varovati ter mu zagotavljati celovitost, dostopnost in uporabnost v skladu z zakonom (prim. *ZVDAGA, 4. do 6. člen*).

Definicijo pojma "**osebni podatek**" za potrebe tega prispevka povzemamo po Zakonu o varstvu osebnih podatkov, ki ga opredeljuje kot *katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen* (*ZVOP-1, 6. člen*).

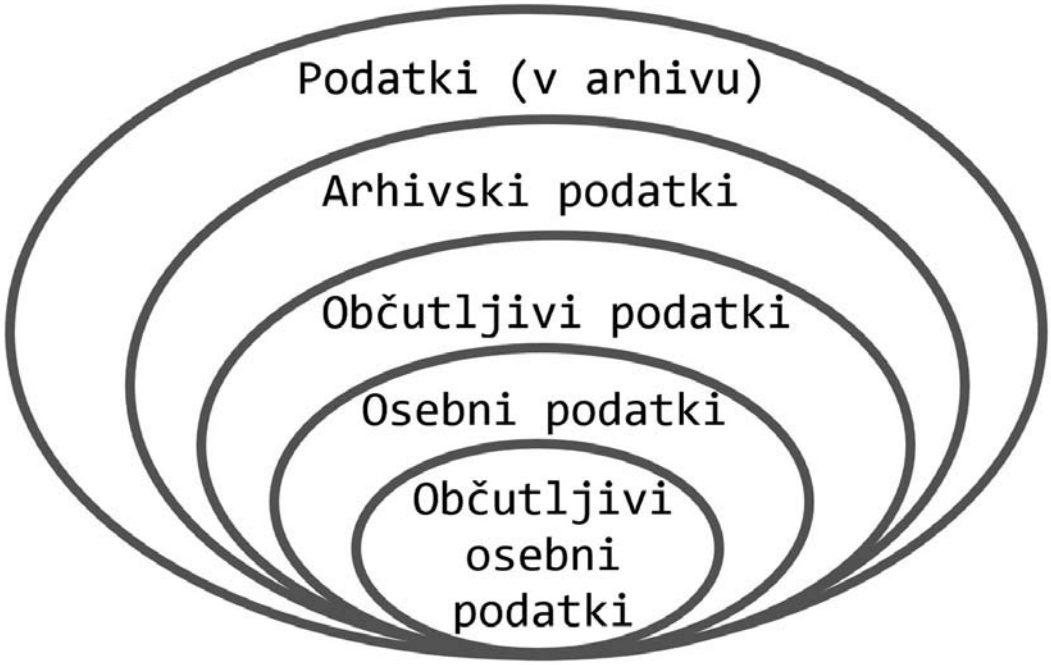
"**Občutljivi osebni podatek**" je po istem zakonu določen kot *podatek o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na 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* (*ZVOP-1, 6. člen*).

V slovenski arhivski teoriji in praksi pojem "**občutljivi podatki**" uporabljamo kot generičen pojem za osebne podatke, tajne podatke, poslovne tajnosti, davčne tajnosti itd. V nadaljevanju tega

prispevka ga bomo uporabili za vse vrste podatkov, katerih nepooblaščena uporaba ali sprememba bi povzročila ugotovljivo škodo in jim arhivski strokovni delavci morajo posvečati posebno pozornost, tako v procesih arhivskih strokovnih opravil kot tudi pri uporabi arhivskega gradiva.

Pojem "**osebni podatek**" kot ga razume slovenska arhivska stroka, je opredeljen v 65. členu ZVDAGA druga alineja[1] (*ZVDAGA, 65. člen*). Določba člena se sicer nanaša na nedostopnost arhivskega gradiva in vendar ga opredeli s pomočjo nekoliko modificirane definicije "**občutljivi osebni** podatek" po ZVOP1.

Terminološke razlike opredeljevanja pojma "**osebni podatek**" in "**občutljiv osebni podatek**" kot ju opredeljujeta ZVOP in ZVDAGA, je potrebno v arhivski praksi upoštevati in pri tem uporabljati tista določila in opredelitve, ki so oblikovane v ZVDAGA.



Slika 1: Model sistematizacije podatkov v arhivih

Podatke v arhivih lahko sistemiziramo na različne nivoje. Primer na sliki 1 predstavlja njihovo pseudo-hierarhično sistemizacijo njihovih statusov od najširšega do najožjega pojma. Pri tem ugotovimo, da imajo ti praviloma različne statuse. Opredeljeni so glede na njihove vsebinske ali pojavne oblike, ali na njihove postopkovne, pravne ali druge zahteve. Iz tega sledi, da ima posamezen podatek v arhivu vsaj enega ali več statusov, ki opredeljujejo eno ali več zahtev glede njegovega ohranjanja, varovanja in uporabe. Statusi podatkov se lahko spreminjajo glede na njihova težišča[2], lahko pa se posameznim podatkom ali množici podatkov ti v času in prostoru odvzamejo ali dodajo[3].

1. Javno arhivsko gradivo v javnih arhivih, ki vsebuje osebne podatke, ki se nanašajo na: zdravstveno stanje, spolno življenje, žrtev kaznivih dejanj zoper spolno nedotakljivost, zakonsko zvezo, družino in otroke, storilca kaznivih dejanj in prekrškov, razen kaznivih dejanj in prekrškov oseb, zoper katere je bil voden postopek zaradi nasprotovanja nekdanjemu enopartijskemu režimu, versko prepričanje in etnično pripadnost postane dostopno za javno uporabo 75 let po nastanku gradiva ali 10 let po smrti posameznika, na katerega se podatki nanašajo, če je datum smrti znan, če ni z drugimi predpisi drugače določeno.

2. Tipično spreminjanje težišča statusa predstavlja sprememba roka nedostopnosti, do katerega pride zaradi spremembe v zakonodaji.

3. Status podatka se mora spremeniti brž ko preteče z zakonom določeno obdobje njegove nedostopnosti ali se pojavi z zakonom določena zahteva po njegovi nedostopnosti.

Upravljanje statusov podatkov v arhivih predstavlja kompleksne intelektualne, postopkovne in tehnološke postopke in s tem povezane odločitve. To se razlikuje glede na tipe statusov in jih je potrebno izvajati dolgoročno in dosledno. V tem kontekstu lahko razumemo varovanje občutljivih podatkov kot integralni del upravljanja podatkov v arhivih.

3 Klasična paradigma varovanja (občutljivih) podatkov v slovenskih arhivih

Skrbniki arhivskega in dokumentarnega gradiva se v Sloveniji, podobno kot drugod v svetu, skozi daljše obdobje soočajo z različnimi incidenti s področja varovanja podatkov in s tem tudi občutljivih podatkov. Svoje poslanstvo na tem področju izvajajo na različne tehnološko tehnične, organizacijske, postopkovne načine (prim.: *Novak, 2011*). Ocenjujemo, da je v Sloveniji kljub izvedbenim problemom, na splošno zagotovljena zadovoljiva stopnja varovanja tovrstnih podatkov.

Ne glede na zgornjo oceno, pa je potrebo ugotoviti, da na področju varovanja občutljivih podatkov v arhivih ne moremo govoriti o obsežni in dolgoročni praksi, kot jo poznajo npr. slovenski restavratorji in konservatorji, ki postopke materialnega varstva arhivskega gradiva kontinuirano izvajajo že več kot šestdeset let (*Vodopivec Tomažič, 2016*). Prav pomanjkanje prakse, predvsem pa poglobljene teorije s tega področja, odpira mnoge praktične probleme. Te je potrebno ad hoc reševati, rezultati tovrstnih rešitev pa niso vedno skladni z arhivskimi strokovnimi in drugimi pričakovanji.

Intenzivno urejanje obravnavanega področja sega nekako v zadnje desetletje prejšnjega stoletja in sovpada z dejanskim začetkom razvoja sodobne slovenske informacijske družbe. To pa seveda ne pomeni, da se arhivski strokovni delavci v preteklosti niso ukvarjali s problemi zaščite integritete posameznikov, ki je izhajala iz ohranjenega arhivskega gradiva. Tovrstne probleme so reševali v okviru širšega področja uporabe arhivskega gradiva (*Žontar, str. 140-148*). Razloge za tako sistemsko rešitev je potrebno iskati v formulaciji varstva osebnih in drugih občutljivih podatkov iz prvega slovenskega zakona o varstvu osebnih podatkov[4]. V njem je bilo opredeljeno, da bo varovanje osebnih in drugih občutljivih podatkov iz arhivskega in dokumentarnega gradiva ali v zvezi z njim urejala zakonodaja s področja arhivske dejavnosti. To pa je v praksi lahko tudi pomenilo relativno svobodno interpretacijo določil v zvezi z dostopnostjo arhivskega gradiva oz. varovanjem občutljivih podatkov tako na strani uporabnikov kot tudi na strani arhivskih strokovnih delavcev in ne nazadnje političnih elit. To nerazumevanje je doživelo epilog najprej na referendumu leta 2011 in nato še enkrat leta 2014 (prim. *Cvelfar, 2015*).

Varovanje občutljivih podatkov v arhivskem in dokumentarnem gradivu urejata 63., 64. in 65. člen Zakona o varstvu arhivskega in dokumentarnega gradiva in arhivih. 63. in 64. člen ZVDAGA tako urejata zajem in vodenje uporabnikov in uporabe arhivskega gradiva v arhivih. Drugi odstavek 64. člena opredeljuje, da je potrebno nastale evidence in z njimi povezane osebne podatke v arhivih hraniti trajno. 65. člen ZVDAGA ureja roke nedostopnosti arhivskega gradiva, in sicer za javno arhivsko gradivo v javnih arhivih, ki vsebuje tajne podatke ali davčne skrivnosti oz. osebne podatke, ter za arhivsko gradivo v javnih arhivih, ki je nastalo pred konstituiranjem Skupščine Republike Slovenije pred 17. majem 1990.

Sodobnih zahtev upravljanja z občutljivimi podatki v arhivih, ki izhajajo iz potreb in zahtev informacijske družbe, ni mogoče več uresničevati zgolj z omejevanjem dostopa do tovrstnih podatkov na nivoju arhivskega gradiva. S sistemskimi spremembami statusa tovrstnih podatkov lahko arhivska praksa nevede krši z zakonom opredeljene pravice, ki izhajajo iz varovanja občutljivih podatkov. Saniranje nastale škode, predvsem glede na velike količine metapodatkov v elektronski obliki, pa lahko predstavlja velike izgube predvsem človeških potencialov v arhivih.

4 Nova paradigma varovanja podatkov v arhivih

Analiza z zakonom določenih občutljivih podatkov v arhivih oz. v arhivskem gradivu pokaže, da se ti pojavljajo in obstajajo na različnih ravneh in v različnih kontekstih:

4. Zakon o varstvu osebnih podatkov, Ur. l. RS 58/1999 opredeljuje v 5. členu 4. alineja, da se določbe tega zakona **ne uporabljajo** za osebne podatke, vsebovane v knjigah, publikacijah in drugih gradivih, ki se shranjujejo v muzejih, knjižnicah, arhivih in podobnih javnih ustanovah, ter so javna in splošno dostopna (ZVOP, 1999).

- prvo raven predstavljajo tisti občutljivi podatki, ki se nahajajo v arhivskem gradivu,
- drugo raven opredeljujejo občutljivi podatki, ki se nahajajo v meta-podatkovnem arhivskem informacijskem sistemu,
- tretjo raven predstavljajo občutljivi podatki, ki se nanašajo na uporabnike in uporabo arhivskega gradiva in
- četrto raven oblikujejo občutljivi podatki s področja managementa arhivske ustanove.

Za potrebe tega prispevka bomo abstrahirali tretjo in četrto raven. Na teh dveh ravneh je glede na prvo in drugo raven mogoče identificirati relativno omejeno količino tovrstnih podatkov, vendar to ne pomeni, da jih v praksi sistemsko ni potrebno ustrezno varovati[5]. V nadaljevanju se bomo tako osredotočili le na prvo in drugo raven občutljivih podatkov v arhivih.

Če nekoliko natančneje analiziramo relacijo med arhivskim gradivom, ki vsebuje občutljive podatke (prva raven) in pripadajoča informativna pomagala (druga raven), potem lahko ugotovimo, da je smer migracije občutljivih podatkov praviloma iz arhivskega gradiva v smeri proti arhivskim informativnim pomagalom. Ko se občutljivi podatki pojavijo na drugi ravni, ti lahko migrirajo znotraj nje npr. iz informativnih pomagal neposredno v kontekstne vsebine (KV). Pri tem velja, da je relacija med občutljivimi podatki (OP) v arhivskem gradivu (AG) in tistimi v kontekstnih vsebinah vedno (KV) posredna, relacija med arhivskimi informativnimi pomagali in arhivskim gradivom pa neposredna.

Slika 2: Model migracij občutljivih podatkov prve in druge ravni

Na podlagi zgornjega modela (slika 2) lahko določimo prvo in drugo skupno točko varovanja vseh vrst občutljivih podatkov v arhivih. Prvo tako predstavlja varovanje arhivskega gradiva v fizičnem ali elektronskem okolju, drugo pa opise arhivskega gradiva v metapodatkovnem arhivskem informacijskem sistemu. Predlagan model varovanja občutljivih podatkov pa ne predstavlja le informacijsko-tehnološke rešitve delovanja arhivskega informacijskega sistema, ampak predvsem novo, drugačno fa-

5. V arhivih moremo identificirati naslednja področja zbiranja in obdelovanja osebnih podatkov po ZVOP1 na tretjem in četrtem nivoju:
- Uprava arhiva zbira in obdeluje podatke o zaposlenih v arhivih tipično s programskimi orodji Office, na fizičnih nosilcih podatkov, v okviru računovodskih programskih paketov, v aplikaciji za nadzor delovnega časa, sistemih za nadzor dostopa v različne prostore arhiva itd.
- Video nadzorni sistemi začasno shranjujejo zajete podatke o gibanju zaposlenih in uporabnikov tipično od vhoda v stavbo do čitalnice in v določenih predelih čitalnice. Podatki se zbirajo in obdelujejo in kratkoročno shranjujejo v namenski strojni in programski opremi.
- Čitalniška služba arhiva zbira podatke o uporabnikih arhivskega gradiva in z njimi povezano uporabo arhivskega gradiva – tipično v okviru sistema scopeArchiv, sicer na fizičnih medijih ali v splošno namenski strojni in programski opremi.
- Knjižnica zbira osebne podatke o uporabnikih knjižničnega gradiva tipično v okviru sistema COBISS.SI.
- Arhivisti zbirajo in obdelujejo osebne podatke o osebah za potrebe identifikacije arhivskega gradiva v procesih zajemanja podatkov in poznejše obdelave ter uporabe arhivskega gradiva tipično v okviru sistema scopeArchiv, sicer na fizičnih medijih ali v splošno namenski strojni in programski opremi.
- Javno pooblastilo: osebne podatke za potrebe identifikacije oseb in arhivskega gradiva za zagotavljanje pravic posameznikov iz arhivskega gradiva.

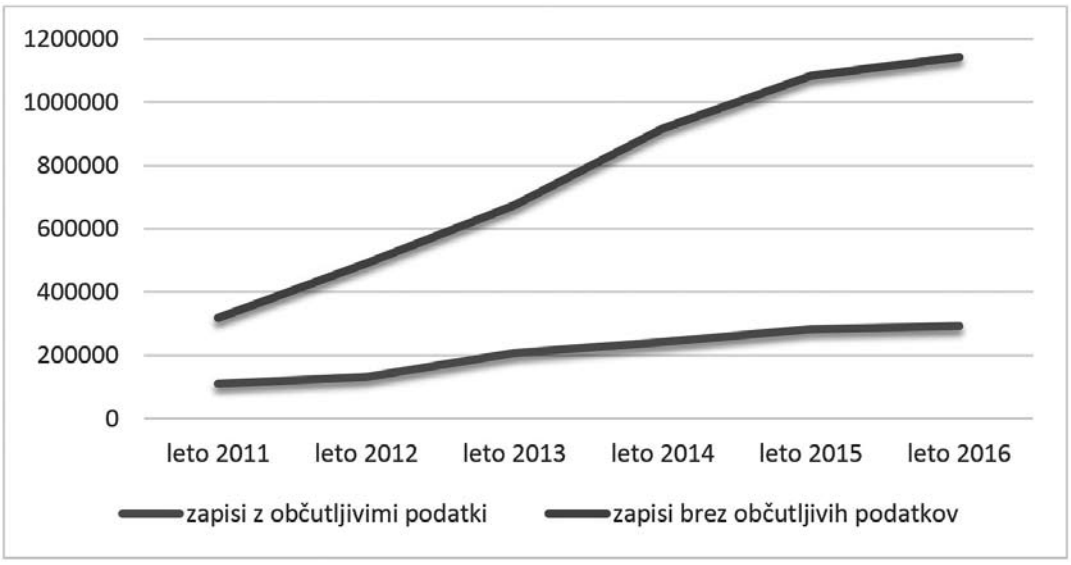
seto oblikovanja postopka popisovanja arhivskega gradiva in s tem povezanih aktivnosti in rešitev varovanja občutljivih podatkov znotraj metapodatkovnega arhivskega informacijskega sistema.

Pomembnost tovrstne strokovne usmeritve utemeljujemo z neposrednimi statističnimi podatki, ki so bili zajeti v obdobju od 2010 do 2016 v okviru sistema SIRAnet. Nanašajo se na opise arhivskega gradiva s statusom "občutljivi podatki[6]" v relaciji do opisov arhivskega gradiva brez statusa posebnega varovanja. V prvo kategorijo spadajo opisi predvsem s področja pravosodja in sociale. Drugo kategorijo pa sestavljajo podatki prvenstveno z ostalih področij.

Za razumevanje sistema varovanja občutljivih podatkov v arhivskem metapodatkovnem informacijskem sistemu je potrebno razumeti splošno logiko dinamičnega upravljanja statusov na nivoju informacijskega sistema in s tem opredeliti neposredno interakcijo med statusom "občutljivi podatek" in statusom "dostopno preko spleta". Pri tem velja, da morata biti izpolnjena vsaj dva pogoja za dostopnost opisa arhivskega gradiva s statusom "občutljivi podatek". Opis mora imeti status "zaključen", kar pomeni, da mora vsebovati z arhivskimi strokovnimi standardi predvidene vsebine. Ob tem mora preteči predvideni rok varovanja občutljivih podatkov.

Statistični podatki iz podatkovne zbirke SIRAnet kažejo, da je odnos med opisi s statusom občutljivi podatki in opisi brez tega statusa skozi daljše obdobje v različnih razmerjih. To je razumljivo, saj se politika zajemanja podatkov iz arhivskega gradiva dinamično spreminja glede na nove prevzeme ali druge arhivske strokovne zahteve. V obravnavanem primeru velja, da je bil v prvih letih zajet vsak tretji zapis, ki je vseboval občutljive podatke. V zadnjih letih se je to razmerje spremenilo, tako da vsak četrti zajeti zapis vsebuje občutljive podatke. To pomeni, da je v sistemu do sedaj zajetih nekaj več kot 25% vseh opisov arhivskega gradiva s statusom občutljivi podatki od skupnega števila 1,2 M zapisov.

Za uspešno varovanje take množice občutljivih podatkov je potrebno vzpostaviti sistem popisovanja in zajemanja vseh vrst arhivskega gradiva v skladu z usmeritvami večstopenjskega popisovanja. To pomeni, da je potrebno zajeti vertikalno in horizontalno vse podatke posameznega nivoja z različnimi statusi varovanja in zaščite, vključno z osebnimi in drugimi občutljivimi podatki. Proces njihovega zajemanja pa je potrebno zaključiti, npr. z določanjem statusa zapisa "zaključeno".



Slika 3: Dinamika zajemanja opisov v SIRAnet podatkovni zbirki

Zajeti občutljivi podatki dobijo v meta podatkovnem arhivskem informacijskem sistemu status

6. V statistiki so kot občutljivi podatki upoštevani osebni podatki, tajni podatki, poslovna tajnost, davčna tajnost in določila zasebnega izročitelja.

javne nedostopnosti. Ta pa ni trajen, ampak ima vedno določeno dobo njegovega upoštevanja. Zato pa mora biti vzpostavljen tak informacijski sistem, ki je sposoben upravljanja s statusi zapisov občutljivih podatkov in z njimi povezanimi kontekstnimi metapodatki. Status na nivoju zapisa se mora sistemsko in samodejno spremeniti, brž ko mu poteče datum prenehanja nedostopnosti. S tem pa se morajo ustrezno spremeniti tudi vsi statusi v povezanih kontekstnih zapisih, ki so posredno ali neposredno povezani z zapisi, ki vsebujejo občutljive podatke.

Arhivski podatki imajo v praksi vedno več statusov, zato je potrebno določiti njihova težišča. V primeru, ko imajo vsi statusi ista težišča, potem velja pravilo, po katerem samo en status, ki onemogoča uporabo podatkov, opredeljuje celoto opisa in z njo povezane opise kot nedostopne.

5 Pasti varovanja občutljivih podatkov

Vedno več pokazateljev kaže na to, da klasična paradigma varovanja občutljivih podatkov v arhivih ne more več popolnoma zadovoljevati mnogih sodobnih informacijskih potreb in zahtev obravnavanega področja. Na daljše obdobje je zato povsem neprimerno t. i. selektivno popisovanje npr. le tistega gradiva, ki ne vsebuje občutljivih podatkov. Prav tako je neosnovano zamolčanje ali prikrivanje podatkov iz arhivskega gradiva. Znane so tudi druge manj primerne arhivske strokovne rešitve tega problema. Omenimo naj samo zajemanje in ohranjanje občutljivih arhivskih podatkov le na posameznih lokalnih računalniških sistemih, brez doslednega permanentnega izvajanja varnostnega kopiranja teh podatkov.

Arhivisti se podobno kot drugi uporabniki informacijske tehnologije srečujejo z različnimi grožnjami od tehničnih in drugih napak na medijih. Te običajno povzročajo neposredno uničenje zbranih podatkov. Ob tem se pojavljajo še različne vrste kraje podatkov, vključno z množico namernih ali nenamernih brisanj zajetih podatkov pa vse do problemov, ki jih povzročajo t. i. izsiljevalski virusi. Slednji za arhivsko strokovno javnost predstavljajo nove skrbi in dodatne postopke preverjanja ohranjenih podatkov. Če so ti manipulirani z izsiljevalskimi virusi, se podatki še vedno nahajajo na opremi pod kontrolo arhivistov, datoteke v mapah je mogoče videti, tudi odpreti jih je mogoče, vendar jih ni mogoče prebrati in interpretirati, ker so podatki šifrirani. Postopek njihovega reševanja je kompleksen in ni vedno uspešen, tudi če žrtev plača zahtevano vsoto in dobi orodje za njihovo dešifriranje (*Ransomware, 2016*).

Podobno kot v okviru klasične paradigme se tudi v okviru nove paradigme varovanja občutljivih podatkov pojavljajo novi dejavniki tveganja. Za osnovno razumevanje njihove kompleksnosti sta v nadaljevanju predstavljena dva primera iz prakse. Prvi se nanaša na poskus nekontrolirane odtujitve podatkov iz podatkovne zbirke SIRAnet, drugi pa na zagotavljanje integritete preko spleta objavljenih osebnih podatkov na podlagi manipuliranja med zahtevami ZVOP1 in ZVDAGA.

V okviru slovenskega vzajemnega arhivskega informacijskega sistema so se sredi leta 2015 soočili z velikim številom neavtoriziranih zahtev iz podatkovne zbirke, ki pa jih v sistemu zaradi varnostnih mehanizmov ni bilo mogoče do konca izvesti. Te smo opazili kot izredno povečano obremenitev procesorjev, delovnega pomnilnika in diskovnih kapacitet. Izvedeni pa so bili s pomočjo programske kode, ki je sicer znana pod imenom webcrawler (prim.: *Baiju, 2016*). Rešitev tega problema predstavlja požarni zid nove generacije s potrebno programsko opremo, ki zna filtrirati promet v omrežju tako na nivoju vrat, internetnih naslovov kot tudi na nivoju aplikacij.

Nekaj mesecev pred poskusi vdora je starejša občanka zahtevala v pristojni arhivski ustanovi, nato še pri predajniku arhivskega gradiva, da se iz javno dostopne podatkovne zbirke izbriše podatek o tem, da pristojni arhiv hrani dokumentacijo o njenem šolanju. Gradivo je bilo prevzeto po postopku in v skladu z zakonodajo in popisano po ustaljenem in preizkušenem vzorcu[7], ki je uveljavljen za tovrstne tipe arhivskega gradiva tudi z drugih področij[8]. Vse strokovne razlage in utemeljitve niso zadosto-

7. Vzorec opisa popisne enote je bil: priimek in ime, letnica rojstva, tip dokumentacije in ustvarjalec dokumentacije. Na metodološko podoben način rešujemo problem razločevanja »soimenjakov«, ki pa se ne pojavlja zgolj pri osebnih imenih, ampak tudi pri zemljepisnih imenih ali pri opredeljevanju stvarnih gesel s pojavom homonimov itd. Na ta način je zagotovljena pragmatična identifikacija nižjih popisnih enot arhivskega gradiva v sistemu.

8. Tako so npr. popisi matičnih listov učencev skozi daljše obdobje ali personalne mape zaposlenih v velikih podjetjih

vale, zato je sprožila postopek pri državnem nadzorniku za varstvo osebnih podatkov. Nadzornika niso toliko zanimali sami podatki kot dejstvo, od kod je arhiv pridobil te podatke. Obsežni pisni zagovor je zadostoval, da je pristojna arhivska ustanova dobila potrditev, da objavlja preko spleta podatke, kot so npr. leto rojstva in ime, ki niso predmet varovanja po ZVOP1 ampak po ZVDAGA in so torej javno dostopni. Ta primer kaže na večplastnost problema opredeljevanja in upravljanja osebnih podatkov v arhivih, ki pa niso vedno opremljeni tudi s statusom "občutljivi podatki". Hkrati primer nakazuje, da se pojem "varovanje občutljivih podatkov" mora razumeti kot varovanje podatkov samih po sebi vključno z njihovo integriteto. Kar pomeni, da jih je v skladu z zakonodajo potrebno objaviti, ko jim preteče z zakonom določeno obdobje varovanja.

6 Zaključek

V času pred intenzivno implementacijo informacijske tehnologije na področju obravnavanja podatkov v arhivih so prevladovali v segmentu njihovega varovanja dejavniki tveganja, ki so bili fizikalnega, kemičnega ali biološkega izvora. Sporadično so se pojavljali dejavniki tveganja, ki so izhajali iz vsebinskih in kontekstno logičnih danosti. V zadnjih desetletjih pa so se pojavili novi dejavniki tveganja varovanja predvsem občutljivih podatkov. V tem kontekstu naj omenimo le informacijsko- tehnološke dejavnike in s tem povezane postopke varovanja podatkov. Še posebej pa je potrebno izpostaviti tiste, ki izhajajo iz sodobne področne zakonodaje. Ta na eni strani zagotavlja varovanje integritete zasebnosti posameznikov, na drugi pa ureja obveznosti v zvezi z dostopom javnosti do informacij javnega značaja (*Novak, 2015*). K temu pa je potrebno dodati še določila zakonodaje s področja arhivske dejavnosti.

V obstoječi, klasični paradigmi varovanja občutljivih podatkov je bilo smiselno zaščititi predvsem arhivsko gradivo. Razlogov je veliko. Izpostavimo naj samo: omejeno količino izdelanih vsebinskih in kontekstnih metapodatkov o arhivskem gradivu, arhivsko strokovno izhodišče po katerem so originalna fizična informativna pomagala valorizirana kot arhivsko gradivo itd.

Z večanjem števila opisov arhivskega gradiva na nižjih popisnih nivojih se veča tudi število zapisov o arhivskem gradivu, ki vsebujejo občutljive ali potencialno občutljive podatke. Z občutljivimi podatki iz arhivskega gradiva so povezani tudi mnogi zapisi v metapodatkovnem arhivskem informacijskem sistemu npr. v normativnih zapisih. Te morajo arhivski strokovni delavci tako kot one iz arhivskega gradiva ustrezno strokovno obravnavati. Prav zato varovanje občutljivih podatkov, ki bi bilo omejeno zgolj na arhivsko gradivo, ni več zadostno.

Nova paradigma varovanja občutljivih podatkov mora razširiti sistem zaščite občutljivih podatkov tako na nivoju arhivskega gradiva kot tudi na nivoju celotnega metapodatkovnega arhivskega informacijskega sistema. Zdi pa se, da tudi to ne bo zadostovalo, če varovanje ne po izvedeno tudi na sistemih, ki so povezani z arhivskim informacijskim sistemom. Rešitve morajo biti izvedene tako na formalno pravnem, postopkovnem kot tudi tehnološko tehničnem nivoju. Drugo plat tega problema pa predstavlja človeški faktor. Arhivi so dolžni permanentno oblikovati, razvijati in promovirati varnostno kulturo ne samo pri zaposlenih, na primer s promoviranjem Kodeksa arhivske etike (*Code of Ethics, 1997*) ali Univerzalne deklaracije (*Universal Declaration on Archives, 2011*), ampak tudi pri obstoječih uporabnikih z doslednim izvajanjem čitalniške službe v arhivskih ustanovah ter s tem povezanimi pravili uporabe arhivskega gradiva (prim.: *Navodilo, 2014*) in izobraževanja oz. ozaveščanja sedanjih in bodočih uporabnikov v arhivi že od vrtca oz. osnovne šole pa vse do tretjega življenjskega obdobja (prim.: *Aristovnik & Horvat, 2011*).

Bibliografija

Aristovnik, B., & Horvat, M. (2011). Učna ura v Zgodovinskem arhivu Celje in Pokrajinskem arhivu Maribor. *Primeri različnih praks v slovenskih arhivih : zbornik referatov : 25. zborovanje*, str. 60-78.

Baiju, N. (2016). Top 50 open source web crawlers for data mining. Pridobljeno 15.8.2016 iz Big Data Made Simple: http://bigdata-madesimple.com/top-50-open-source-web-crawlers-for-data-mining/.

Code of Ethics (1997). *ICA Bulletin,* No. 47 (1997-1). Pridobljeno 8.8.2016 iz http://www.pokarh-mb.si/si/p/1/17/kodeks-etike.html.

izvedeni v več deset tisoč zapisih.

Cvelfar, B. (2015). O dostopnosti arhivskega gradiva v javnih arhivih pred in po uveljavitvi ZVDAGA-A. *Arhivi na razpotju : zbornik referatov* : 27. zborovanje, str. 8-17.

Klasinc, P. P. (1992). *Materialno varovanje klasičnih in novih nosilcev informacij*. Maribor: Mednarodni inštitut arhivskih znanosti pri Pokrajinskem arhivu Maribor.

Navodilo za uporabo arhivskega gradiva v čitalnici Pokrajinskega arhiva Maribor. (14.8.2014). Pridobljeno 8. 8. 2016 iz http://www.pokarh-mb.si/uploaded/datoteke/citalniki_red_2014_pam.pdf.

Novak, M. (2011). Tveganja in ukrepi v arhivih ob naravnih in drugih nesrečah. Pridobljeno 8.8.2016 iz *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*: http://193.2.142.10/fileadmin/www.pokarh-mb.si/pdf_datoteke/Radenci2011/24_Novak_2011.pdf.

Novak, M. (2015). Dolgoročna hramba, valorizacija in uporaba računov, eračunov ter drugih hibridnih oblik dokumentacije. Pridobljeno 8.8.2016 iz *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja:* http://www.pokarh-mb.si/uploaded/datoteke/Radenci/radenci2015/481-494_novak_2015.pdf.

Ransomware. (15.8.2016). Pridobljeno 17.8.2016 iz Wikipedia, the free encyclopedia: https://en.wikipedia.org/wiki/Ransomware.

SSKJ, 3.0. (2014). Pridobljeno 17.8.2016 iz Fran, slovarji Inštituta za slovenski jezik Frana Ramovša ZRC SAZU: http://www.fran.si/iskanje?View=1&Query=podatek.

Universal Declaration on Archives. (2011). (Adopted at the General Assembly of the International Council on Archives, Oslo, September 2010. Endorsed by 36th Session of the General Conference of UNESCO Paris). Pridobljeno 8.8.2016 iz http://www.ica.org/en/universal-declaration-archives-adopted-annual-general-meeting-oslo.

Vodopivec Tomažič, J. (2016). Materialno varovanje arhivskega gradiva v Sloveniji v obdobju 1956-2016. Pridobljeno 14.8.2016 iz *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*: http://www.pokarh-mb.si/uploaded/datoteke/Radenci/radenci_2016/331-341_vodopivec_2016.pdf.

ZVDAGA (2014). *Zakon o varstvu arhivskega in dokumentarnega gradiva*. Pridobljeno 10.8.2016 iz Pravno informacijski sistem: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4284.

ZVOP (1999). *Zakon o varstvu osebnih podatkov*. Pridobljeno 10.8.2016 iz Uradni list RS: http://www.uradni-list.si/1/objava.jsp?sop=1999-01-2792.

ZVOP-1 (2007). *Zakon o varstvu osebnih podatkov*. Pridobljeno 16.8.2016 iz Uradni list RS, št. 94/2007: http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690.

Žontar, J. (1984). *Arhivistika*. Ljubljana: Dopisna delavska univerza Univerzum.

SUMMARY

Traditional archival paper based paradigm of sensitive data protection in the archives is derived from awareness that with long-term protection of the data carriers and on them written contents the archival material and with it related archival information aids can also be successfully protected, including the protection of sensitive data from archival material as well as from the metadata archival information system. Regardless from the used methods and the ways of data protection in frame of the traditional archival paradigm, today's archivists are increasingly faced with the problem of the identification of the various risk factors and their combinations by data protection. In real situations archivists cannot always react appropriate to all protection's problems due to the amount of archival materials or/and current technological, organisational and other features. It is also known, that in practice, the problems which are of physical, chemical or biological origin are generally easier identified than other risk factors. A new paradigm takes over all the elements of traditional archival paradigm and adds some new. New elements can be defined as requirements to ensure the integrity of all data generated and preserved in the archives regardless of their status. This means that it is necessary for all types of data, which are defined as publicly available, to ensure their availability in accordance with applicable law. The data, which by law are not publicly accessible yet, it is necessary to protect during the whole duration of their protection, not just in the strict sense but to protect their integrity through a long term period. From the archival point of view this is possible only with the consistent control of statuses of the sensitive and other data in the metadata archival system during long time period.

Tipology: 1.01 Original Scientific Article

Submitting date: 01.02.2016

Acceptance date: 20.02.2016