

## ZUNANJE IZVAJANJE ELEKTRONSKEGA ARHIVIRANJA

**Branko Godec**\*

**UDK: 004:930.25**

*Branko Godec: Zunanje izvajanje elektronskega arhiviranja. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Zbornik referatov z dopolnilnega izobraževanja, Maribor 8/2009, str. 387–404.*

*Izvirnik v slovenščini, izvleček v slovenščini in angleščini, povzetek v angleščini.*

Vsak subjekt, ki se odloča za varno hrambo digitalnega gradiva, bi se moral neodvisno od izvedbe (lastna ali zunanja) zavedati posledic nepravilno izvajane e-hrambe, zato je dobro poznavanje zakonodaje s tega področja ključnega pomena. Če bo subjekt e-hrambo zaupal zunanjemu izvajalcu, se naj pred tem dobro seznanj z ustreznostjo izvajanja storitve. Priporočljivo je, da si pred odločitvijo pri ponudniku natančno ogleda način izvajanja storitve in infrastrukturo za zagotavljanje storitve. E-hramba je področje, ki ga je treba dobro poznati, zato se z odločitvami ne splača brezglavo hiteti, ampak je treba temeljito preučiti razpoložljive možnosti.

**UDC: 004:930.25**

*Branko Godec: Outsourcing of Electronic Archiving. Technical and Field Related Problems of Traditional and Electronic Archiving. Conference Proceedings, Maribor 8/2009, pp. 387–404.*

*Original in Slovenian, abstract in Slovenian and English, summary in English.*

Each subject who decides for a safe preservation of digital records, should, independently from the kind of implementation (own or outsourcing), be aware of the consequences of incorrect execution of e-storage. Therefore it is of a great importance to have the knowledge about the legislation in this field. If the subjects entrust e-storage to outsourcers they should be well acquainted with their service performance adequacy. Before making a final decision, it is advisable to thoroughly examine the manner of service performance and the infrastructure, which supports it. E-storage is a field, which we have to know very well; therefore decisions should be made cautiously and with a lot of deliberation.

*Ključne besede: e-hramba, zakonodaja, zunanje izvajanje, outsourcing, varna hramba.*

### 1 KAJ JE TREBA VEDETI

#### 1.1 PREDHODNA ANALIZA

Preden se javnopravni ali poslovni subjekt odloči, da bo pristopil k izvajanju zajema in hrambe digitalnega gradiva, mora pripraviti natančno predhodno analizo, s katero bo ugotovil, ali razpolaga z vsemi potrebnimi viri, ki mu bodo omogočali zakonsko skladno izvajanje e-hrambe. Tako mora izvesti pripravo na zajem in hrambo, v kateri mora popisati vire gradiva, pripraviti študijo upravičenosti, študijo izvedljivosti ter analizo tveganj in ukrepe za njihovo zmanjševanje. Na podlagi rezultatov, ki jih ugotovi v okviru predhodne analize, se lahko subjekt odloči, ali bo e-hrambo izvajal v lastni režiji ali pa bo te storitve raje najemal pri ponudnikih storitve e-hrambe.

Zelo pomemben del predhodne raziskave je tudi študija upravičenosti, ki upošteva stroške vzpostavitve, upravljanja in uporabe e-hrambe, pri kateri pa subjekti prepogosto ne upoštevajo vseh dejavnikov, ki generirajo stroške.

---

\* *Mag. Branko Godec, vodja Službe za informacijske storitve v Sektorju za informatiko, Pošta Slovenije d.o.o., Slomškov trg 10, SI-2000 Maribor, Slovenija.*

### 1.1.1 DEJAVNIKI, KI SE UPOŠTEVAJO PRI PRIPRAVI NA ZAJEM IN HRAMBO

Če subjekti ne razpolagajo z infrastrukturo, so investicije v sistem e-hrambe vselej zelo velike. Subjekti, ki se odločajo za lastno izvajanje e-hrambe, v stroškovnih analizah največkrat pozabijo upoštevati vse dejavnike. Navadno se osredotočijo zgolj na stroške nakupa strojne in programske opreme za e-hrambo, ki sicer predstavljajo le del stroškov.

Treba je upoštevati tudi investicije v sisteme, ki preprečujejo zunanje vdore v sistem e-hrambe in jih sestavljajo požarne pregrade, sistemi za zaznavo in preprečevanje vdorov, protivirusni sistemi itn. Stroški vzpostavitve sistema e-hrambe se nadaljujejo z investicijami v prostore, kjer je ta oprema nameščena. Priporoča se uporaba varnih podatkovnih centrov, saj nudijo najvišjo stopnjo zaščite nameščene IT-opreme in s tem tudi hranjenega gradiva. Nadalje je treba upoštevati še stroške za vzpostavitev podpornih sistemov, kot so avtonomni protipožarni sistemi, klimatski sistemi za zagotavljanje delovne temperature IT-opreme, sistemi tehnične varnosti (videonadzor, senzorji gibanja, vrata s kontrolo pristopa, varnostne cone itn.). Prepogosto se pozablja tudi na stroške dodatnih storitev, med katere spadajo stroški komunikacijskih povezav, stroški storitev za zagotavljanje avtentičnosti in celovitosti hranjenega gradiva (npr. varni časovni žig, kvalificirana digitalna potrdila itn.) ter stroški zagotavljanja fizične varnosti. Vsekakor je pri analizi stroškov treba upoštevati tudi amortizacijo vseh navedenih sistemov in predvsem stroške njihovega vzdrževanja, ki še zdaleč niso majhni.

Vsekakor pa se pri stroških pozablja na pripravo in ažurno vzdrževanje organizacijskih ukrepov. Ti skupaj s tehničnimi ukrepi ustvarjajo pogoje za pripravo notranjih pravil za zajem in hrambo digitalnega gradiva. Še bolj se pri tem pozablja, da so notranja pravila »živa stvar«. Zaradi ugotovljenih pomanjkljivosti, tehnološkega napredka, sprememb zakonodaje, organizacijskih in kadrovske sprememb idr. jih je treba redno posodabljeti. Zgolj pripraviti in sprejeti notranja pravila še zdaleč ni dovolj, saj mora subjekt napisane postopke tudi dejansko izvajati. Le na ta način je lahko zajem in hramba digitalnega gradiva tudi zakonsko skladna. Da lahko vse to zagotovi, mora imeti subjekt tudi ustrezno število primerno izobraženih in usposobljenih ljudi. Hkrati mora skrbeti, da se to osebje nenehno usposablja. Pri tem ne gre zgolj za usposabljanje za delo z dokumentarnim gradivom, pač pa tudi za področje zagotavljanja neprekinjenega poslovanja ter novih IT-tehnologij, ki so kakorkoli zajete pri zagotavljanju e-hrambe.

### 1.2 NOTRANJA PRAVILA ZA IZVAJANJE ZAJEMA IN HRAMBE

Zakonodaja določa, da mora vsaka oseba, ki izvaja zajem in hrambo digitalnega gradiva, pripraviti in sprejeti notranja pravila, s katerimi natančno opredeli vse organizacijske in tehnične postopke, ki jih pri tem izvaja. Da je kompleksnost priprave notranjih pravil res velika, dokazuje dejstvo, da notranjih pravil ni sprejel in pri Arhivu RS potrdil še nobeden subjekt, ki ne predstavlja ponudnika storitve. Še večjo težavo predstavlja dejansko izvajanje organizacijskih in tehničnih postopkov e-hrambe v praksi. Kot je bilo že omenjeno, za zakonsko skladno izvajanje ni dovolj zgolj napisati notranja pravila, ampak je treba te postopke tudi dejansko izvajati, kar pa mnogokrat predstavlja velike težave.

Po drugi strani je treba upoštevati, da sta obseg in kompleksnost notranjih pravil v veliki meri odvisna tudi od tega, ali subjekt postopke glede e-hrambe izvaja sam ali pa storitve najema pri ponudnikih teh storitev. V kolikor vse postopke izvaja sam, mora v notranjih pravilih zajeti vse zahteve zakonodaje in jih pri izvajanju e-

hrambe tudi dejansko upoštevati. Kadar pa subjekt storitve e-hrambe najame pri zunanjem ponudniku, ni potrebe po implementaciji kompleksnih tehničnih in organizacijskih ukrepov pri izvajanju e-hrambe v lastno okolje. S tem se odgovornost za pravilno in zakonsko skladno izvajanje e-hrambe prenese na ponudnika. Subjekt in ponudnik morata razmejitev vseh odgovornosti glede izvajanja e-hrambe zavesti v medsebojnem pravnem aktu (npr. pogodbi). V tem primeru se subjekt v lastnih notranjih pravilih sklicuje na določbe medsebojnega pravnega akta, v katerih zahteve iz zakonodaje glede e-hrambe zagotavlja ponudnik. Da bi subjekt lahko zaupal ponudniku, da ta dejansko izvaja e-hrambo, ki je skladna z zakonodajo, mora imeti ponudnik najmanj sprejeta in pri arhivu RS potrjena notranja pravila za izvajanje e-hrambe. Še boljše pa je, da subjekt storitve najema pri ponudniku, ki je storitev e-hrambe tudi akreditiral, vendar o tem nekoliko kasneje.

### 1.2.1 POMEMBNEJŠA PODROČJA NOTRANJIH PRAVIL

Natančne zahteve zakonodaje, ki jih subjekt mora opredeliti z notranjimi pravili, so zavedene v KONTROLNEM SEZNAMU za potrjevanje notranjih pravil in preverjanje njihovega izvajanja ter preverjanje izpolnjevanja pogojev za pridobitev akreditacije storitve v skladu z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih, ki je objavljen na spletni strani Arhiva RS.

V nadaljevanju so navedena nekatera pomembnejša področja, ki se za izvajanje e-hrambe opredelijo z notranjimi pravili. Tako je treba natančno opredeliti organiziranost osebja za izvajanje e-hrambe ter definirati njihove vloge, pooblastila in odgovornosti. Natančno se mora opisati vse postopke, ki opredeljujejo organizacijsko in tehnično izvajanje e-hrambe. Treba je pripraviti in redno vzdrževati oceno tveganj pri izvajanju e-hrambe, ki mora zajemati najmanj strojno in programsko opremo, prostore, varovanje in človeške vire. Podatki o vseh informacijskih virih za izvajanje e-hrambe morajo biti ustrezno dokumentirani, ta popis pa se mora ažurno vzdrževati. Delovanje informacijskega sistema za izvajanje varne hrambe je treba redno spremljati in to spremljanje ustrezno dokumentirati. Natančno se morajo opredeliti postopki ravnanja z informacijskimi sredstvi, ki določajo nabavo, namestitve, testiranje, prenos iz testnega v produkcijsko okolje in zamenjavo informacijskih sredstev. Posebej mora biti opredeljen postopek odstranitve in uničenja nosilcev podatkov, na katerih se hrani digitalno gradivo. Vsak ponudnik, ki izvaja storitve e-hrambe, mora imeti sprejeto informacijsko varnostno politiko oz. sistem varovanja in upravljanja varovanja informacij (SUVI). Za izvajanje e-hrambe se mora pripraviti, vzdrževati in vaditi načrt neprekinjenega poslovanja (BCP). Potrebno je opredeliti, kako se zagotavlja varnostno kopiranje in restavriranje v primeru okrevanja po katastrofi.

Navedeni so le najpomembnejši postopki, ki morajo biti opredeljeni v notranjih pravilih. Ponovno je treba opozoriti, da se e-hramba izvaja na zakonsko skladen način šele tedaj, ko se v notranjih pravilih opredeljeni postopki tudi dejansko izvajajo. Vsak subjekt, ki izvaja zajem in hrambo, mora sproti ažurirati vse spremembe in dopolnitve notranjih pravil, vedno pa takrat, ko se spremeni vsebina notranjih pravil (zamenjava opreme, sprememba v organiziranosti, postopkih izvajanja itn.), ko se spremenijo veljavni predpisi, ko to zahteva tehnološki napredek ali spoznanje stroke ali ko se ugotovijo pomanjkljivosti obstoječih notranjih pravil.

## 2 PONUDNIKI OPREME IN STORITEV

Pri ponudnikih za področje e-hrambe je treba ločiti med ponudniki storitev e-hrambe in ponudniki opreme za e-hrambo. Ponudniki storitve e-hrambe izvajajo vse ali del postopkov e-hrambe, ponudniki opreme pa zgolj dobavljajo programsko ali strojno opremo za izvajanje e-hrambe.

### 2.1 REGISTRACIJA PONUDNIKA

Z registracijo ponudnik storitve ali opreme le priglasi, da bo opravljal določeno dejavnost na področju zajema in hrambe digitalnega gradiva, za kar pa ni potrebno posebno dovoljenje. Ponudnik opreme in storitev mora na podlagi 83. člena Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) in 29. člena Uredbe o varstvu dokumentarnega in arhivskega gradiva svojo dejavnost prijaviti Arhivu RS najmanj osem dni pred začetkom opravljanja dejavnosti.

Zahteva za registracijo ponudnika opreme, storitev ali spremljevalnih storitev se na predpisanem obrazcu vloži pri Arhivu RS. Arhiv RS le preveri popolnost prijave in z upravno odločbo odredi vpis ponudnika v register ponudnikov, ki je brezplačno dostopen na spletni strani Arhiva RS, pri tem pa ponudnika dodatno ne preverja.

Če želijo ponudniki programske ali strojne opreme dokazati, da je njihova oprema skladna s področno zakonodajo, morajo opremo akreditirati pri Arhivu RS, vendar o tem nekoliko kasneje. Pomembno je vedeti, da ponudniki storitve e-hrambe ali spremljevalnih storitev, ki so zgolj registrirali svojo storitev, predstavljajo organizacijo z nižjo stopnjo urejenosti poslovanja. To v prenesenem pomenu pomeni, da morajo v primeru pravnega spora glede avtentičnosti in celovitosti hranjenega gradiva dokazati, da je bila e-hramba izvedena na zakonsko skladen način.

### 2.2 NOTRANJA PRAVILA PONUDNIKOV STORITVE E-HRAMBE ALI SPREMLJEVALNIH STORITEV

Če želijo ponudniki storitve e-hrambe ali spremljevalnih storitev doseči status organizacije z višjo stopnjo urejenosti poslovanja, morajo za področje svojega delovanja sprejeti notranja pravila in jih posredovati v potrditev Arhivu RS. Ko Arhiv RS prejme notranja pravila v presojo, ugotavlja, ali so skladna z zakonom ZVDAGA in podrejenimi predpisi. Arhiv RS v primeru skladnosti notranja pravila potrdi, v nasprotnem primeru pa potrditev zavrne. Nema lokrat je bilo slišati očitke, da Arhiv RS »noče« potrditi notranjih pravil katerega od ponudnikov, čeprav so po njihovem mnenju ta skladna z zakonodajo. Na tem mestu je treba poudariti, da je za presojo, ali so notranja pravila skladna za zakonodajo, izključno pristojen Arhiv RS. Arhiv RS v te namene zaposluje ustrezno število strokovnjakov, ki presojo vršijo po področjih, za katera so pristojni. Navadno takšni očitki prihajajo s strani ponudnikov, ki niso dovolj usposobljeni, da bi lahko pripravili dovolj kvalitetna notranja pravila ter vpeljali potrebne postopke za zakonsko skladno izvajanje storitev e-hrambe ali spremljevalnih storitev. V takšnih primerih je vedno najlažje prevaliti krivdo na organe, ki vršijo presojo skladnosti z zakonodajo. Dokaz, da je notranja pravila možno potrditi in da Arhiv RS opravlja presojo notranjih pravil na profesionalen način, je prav seznam sprejetih notranjih pravil ponudnikov, ki je objavljen na spletnih straneh Arhiva RS. Pri tem je treba še dodati, da se prav na podlagi regulatorne vloge Arhiva RS pri potrditvi notranjih izvaja ločitev na ponudnike, ki zakonsko skladnost pri izvajanju e-hrambe dosegajo, in tiste, ki je ne.

Ponudnik z višjo stopnjo organiziranosti torej zagotavlja zakonsko skladno izvajanje storitve e-hrambe ali spremljevalne storitve. V primeru pravnega spora glede avtentičnosti in celovitosti hranjenega gradiva ponudniku ni treba dokazovati, da je bila e-hramba izvedena na zakonsko skladen način, saj se gradivu, ki ga hrani takšen ponudnik, avtentičnost in celovitost prizna že na podlagi zakona. Vendar je treba opozoriti, da se v primeru, ko obstaja utemeljen dvom, da ponudnik e-hrambe ali spremljevalnih storitev storitve ni izvajal skladno s postopki iz svojih notranjih pravil, prav tako vrši dokazovalni postopek, da je bila e-hramba ali spremljevalna storitev izvedena na zakonsko skladen način.

### 2.3 AKREDITACIJA PROGRAMSKE IN STROJNE OPREME

Za pravilno izvajanje zajema in hrambe digitalnega gradiva se zahteva, da subjekti ali ponudniki e-hrambe in spremljevalnih storitev uporabljajo tako strojno kot tudi programsko opremo, ki zadostuje zahtevam zakonodaje. Ponudniki, ki dobavljajo katero od vrst te opreme, lahko zakonsko skladnost programske ali strojne opreme dokazujejo z akreditacijo. Tako mora ponudnik opreme v akreditacijskem postopku predstavnikom Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorjem informacijskih sistemov dokazati, da je oprema, ki jo ponuja, skladna z zakonodajo. Preverjanje se vrši na podlagi ustreznega kontrolnega seznama. Tako so zahteve zakonodaje za programsko opremo zbrane v Kontrolnem seznamu za preverjanje usklajenosti programske opreme z ZVDAGA (KSpSW, različica 1.1), za strojno opremo pa v Kontrolnem seznamu za preverjanje skladnosti strojne opreme z ZVDAGA (KSpHW, različica 1.0). Oba seznama sta objavljena na spletnih straneh Arhiva RS.

V primeru izpolnitve vseh zakonskih zahtev Arhiv RS ponudniku programske ali strojne opreme podeli akreditacijo za obdobje enega leta. Ponudnik mora akreditacijo vsakoletno obnavljati, saj v nasprotnem primeru akreditacija poteče. V te namene predstavniki Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorji informacijskih sistemov enkrat letno preverijo, ali ponudnik dobavlja opremo, ki je skladna z ZVDAGA in zahtevami s področja arhivske dejavnosti ter pravili stroke. V primeru izpolnjevanja vseh pogojev se akreditacija opreme podaljša.

Subjekti naj ne nasedajo izjavam ponudnikov opreme, da je z nakupom akreditirane opreme zagotovljena zakonska skladnost zajema ali hrambe. Subjekt ali ponudnik e-hrambe oziroma spremljevalnih storitev, ki uporablja akreditirano programsko in akreditirano strojno opremo, ima zagotovljeno le, da mu ta oprema omogoča zakonsko skladno izvajanje tistih postopkov, ki jih pri izvajanju zajema ali hrambe vrši ta oprema. Omenjeno še zdaleč ne pomeni, da akreditirana oprema zagotavlja zakonsko skladen način izvajanja zajema ali hrambe. Pri tem je treba namreč upoštevati še zelo veliko drugih dejavnikov, ki jih zahteva zakonodaja. Tako mora vsa oprema biti nameščena v primernih prostorih, ustrezno varovana pred fizičnim in logičnim dostopom nepooblaščenih oseb, pred požarom, izlitjem vode, ustrezno nadzorovana s strani pooblaščenih oseb, ki morajo biti ustrezno usposobljeni, zagotavljati mora ustrezno dostopnost do gradiva, biti varovana pred računalniškimi vdori in napadi računalniških virusov itn. Nadaljevali bi lahko z vsemi zahtevami, ki jih za zakonsko skladnost moramo opredeliti z notranjimi pravili. Pri tem ne smemo pozabiti, da je pravilen način izvajanja zajema ali hrambe vedno daleč najbolj odvisen od pooblaščenega osebja, ki pri tem izvaja ustrezne organizacijske ukrepe, tehnološki ukrepi, ki se izvajajo z akreditirano programsko in akreditirano strojno opremo, pa so jim pri tem le v pomoč.

Pri programski opremi pa mora biti naročnik pozoren tudi na to, za katero področje je predmetna programska oprema akreditirana. Akreditirana programska oprema lahko podpira posamezne funkcionalnosti pri postopkih e-hrambe in postopkih spremljevalnih storitev in sicer:

- A Infrastrukturalna programska oprema: zajema sistemsko programsko opremo in sistem za upravljanje podatkovne baze.
- B Podpora posameznim funkcionalnostim pri postopkih e-hrambe in podpora spremljevalnih storitev, v kateri so zajeti:
  - B.a Upravljanje dokumentarnega gradiva v fizični obliki,
  - B.b Zajem in pretvorba izvorne analogne v digitalno obliko,
  - B.c Množični zajem (enkratno dejanje za večje sklope) in podpora hrambe istovrstnega gradiva (en rok hrambe, en klasifikacijski znak),
  - B.d Podpora trajne hrambe za gradivo, ki se ne spreminja (read only),
  - B.e Podpora e-hrambe.
- C Podpora celotnemu postopku upravljanja gradiva v digitalni obliki (arhivsko in dokumentarno gradivo).

Za primer navedimo, da programska oprema, akreditirana za podporo trajne hrambe gradiva, ki se ne spreminja (read only), ne omogoča e-hrambe gradiva, ki se lahko nadzorovano spreminja (npr. format XML). Takšna oprema torej ne zagotavlja hrambe gradiva, ki je izvirno nastalo v digitalni obliki, kar je treba pri implementaciji in izvajanju postopkov zajema in hrambe tudi dejansko upoštevati. V tem primeru se mora subjekt zavedati, da bo z naročeno akreditirano programsko opremo rešil le hrambo tistega digitalnega gradiva, ki se ne spreminja. Po drugi strani pa izvirno nastalo digitalno gradivo, ki je v formatih XML, ODF, open XML (MS Office 2007), Auto CAD itn., v primeru zakonsko skladne hrambe omogoča nadzorovano spreminjanje oziroma dopolnjevanje obstoječih dokumentov in izdajo v novi verziji. Ponudniki, ki ponujajo le »read only« opremo, bodo seveda trdili, da se hranjeno gradivo tako ne sme spreminjati, kar je le delna resnica, saj se vsako gradivo lahko dopolni in izda ter hrani v novi verziji. Poglejmo stvari še z drugega zornega kota. Danes vso gradivo izvirno nastane v digitalni obliki, se nato natisne na papir, potrdi, podpiše in pošlje naslovniku. Tam se s pomočjo skenerja zajame in pretvori v »read only« digitalno obliko, ki ne omogoča dodatnih sprememb gradiva, torej se hrani le slika tega dokumenta. V dokaj bližnji prihodnosti bo ta vmesna faza dokumentnega toka, ki se trenutno večinoma vrši na papirnih dokumentih, vedno bolj izgubljala svoj primat, saj se bo večina gradiva med subjekti izmenjevala v digitalni obliki. Hkrati je pri subjektih vedno bolj prisotno e-poslovanje, kjer vso gradivo izvirno nastaja in se tudi izmenjuje v digitalni obliki (npr. eDMS, ERP, CRM, e-bančništvo, e-VEM, e-računi, moja.posta.si itn.), zato ga je v takšni obliki potrebno tudi hraniti. Seveda obstaja možnost, da se to gradivo pred hrambo pretvori v »read only« obliko, vendar sama pretvorba pomeni dodatne stroške. Hkrati je treba upoštevati tudi to, da je v »read only« obliko pretvorjeno gradivo slabše kvalitete in zaseda več pomnilniške kapacitete kot izvirno digitalno gradivo, kar pomeni tudi večji strošek hrambe. Hkrati proces pretvorbe v »read only« obliko po nepotrebnem zelo obremenjuje informacijski sistem, saj je z vidika procesorske obremenitve zelo potraten. Najbolj kritična pa je izguba osnovne funkcionalnosti izvirnega digitalnega gradiva, saj se s takšno pretvorbo izgubi nadaljnja možnost izvajanja nadzorovanih sprememb in dopolnitev tega gradiva. Kakršnakoli pretvorba »read only« oblike v obliko, ki se lahko spreminja, se izvaja z zahtevnimi in dragimi OCR postopki, pri katerih pa obstaja tudi možnost napak pri pretvorbi. Zelo poenostavljen primer glede gradiva, ki se spreminja, je iz vsakodnevnega pisarniškega poslovanja, kjer uporabnik zaradi

potreb po dopolnitvah novo verzijo dokumenta (npr. odločbe) tvori na podlagi predhodne verzije obstoječega dokumenta, saj je večina vsebine praktično identična, vsa ostala vsebina pa se le prilagodi na dejanski primer.

## 2.4 AKREDITACIJA STORITVE HRAMBE ALI SPREMLJEVALNE STORITVE

Akreditacija storitve hrambe ali spremljevalne storitve pomeni najvišjo stopnjo zakonske skladnosti. Ponudnik, ki želi pristopiti k akreditaciji storitve, mora predhodno izpolniti vse do sedaj navedene pogoje. Tako mora storitev e-hrambe ali spremljevalne storitve registrirati, mora imeti sprejeta in pri Arhivu RS potrjena notranja pravila za področje izvajanja storitve, uporabljati mora ustrezno akreditirano strojno opremo ter uporabljati programsko opremo, ki je akreditirana za vsa področja, ki jih s storitvijo zagotavlja.

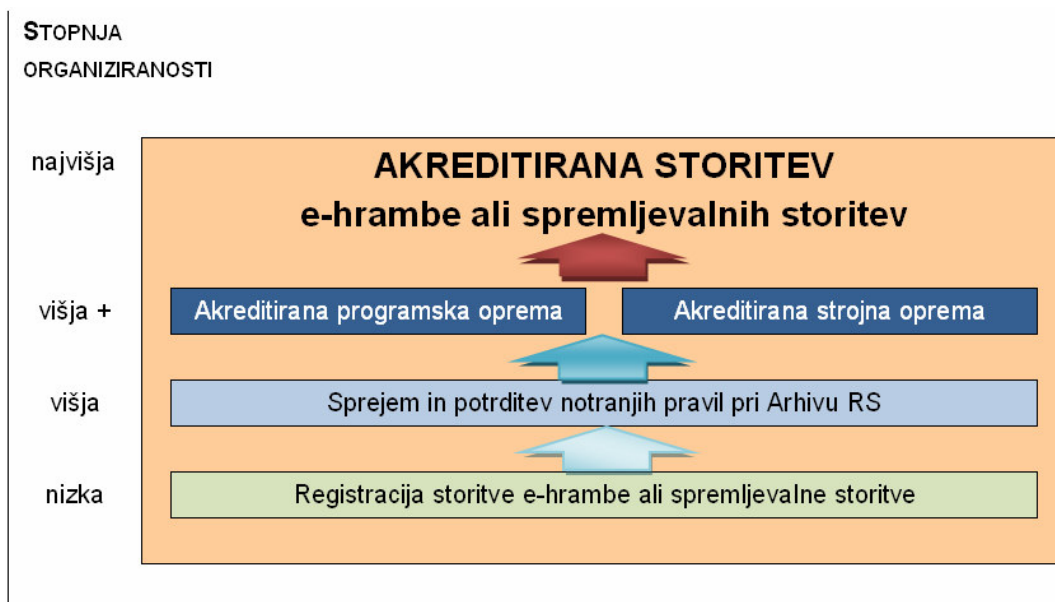
V akreditacijskem postopku mora ponudnik storitve hrambe ali spremljevalne storitve predstavnikom Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorjem informacijskih sistemov dokazati, da storitve izvaja skladno s postopki, ki jih je opredelil z notranjimi pravili, ki jih je potrdil Arhiv RS. Preverjanje se vrši na lokaciji ponudnika na podlagi ustreznega kontrolnega seznama. Pri tem se razen samega načina izvajanja storitve e-hrambe dejansko preverja tudi resničnost navedb ponudnika v notranjih pravilih glede načina namestitve programske in strojne opreme, lokacij, prostorov, fizično-tehničnega varovanja, informacijske varnosti itn.

Zahteve zakonodaje za akreditacijo storitve hrambe ali spremljevalne storitve so zbrane v Kontrolnem seznamu za potrjevanje notranjih pravil in preverjanje njihovega izvajanja ter preverjanje izpolnjevanja pogojev za pridobitev akreditacije storitve v skladu z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih, ki je objavljen na spletni strani Arhiva RS. Omenjeni kontrolni seznam služi tudi kot podlaga za samooceno ponudnika, ali e-hrambo oziroma spremljevalno storitev dejansko izvaja po postopkih, ki jih je zavedel v svojih notranjih pravilih. V nadaljevanju akreditacijskega postopka posamezne kontrolne točke navedenega kontrolnega seznama služijo za dejansko preverjanje izvajanja e-hrambe ali spremljevalnih storitev, ki jo vršijo predstavniki Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorji informacijskih sistemov.

V primeru izpolnitve vseh zakonskih zahtev, Arhiv RS ponudniku storitve e-hrambe ali spremljevalnih storitev podeli akreditacijo za obdobje enega leta. Ponudnik mora akreditacijo vsakoletno obnavljati, saj v nasprotnem primeru akreditacija poteče. V te namene predstavniki Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorji informacijskih sistemov enkrat letno preverijo, ali ponudnik storitve izvaja skladno z ZVDAGA in zahtevami s področja arhivske dejavnosti ter pravili stroke. V primeru izpolnjevanja vseh pogojev se akreditacija storitve podaljša. Ponudnik, ki ima veljavno akreditirano storitev e-hrambe ali spremljevalne storitve, predstavlja organizacijo z najvišjo stopnjo organiziranosti. Ker ima potrjena notranja pravila, zagotavlja zakonsko skladno izvajanje storitve, hkrati pa pravilnost oziroma zakonsko skladnost izvajanja storitve vsakoletno preverijo predstavniki Arhiva RS in z njihove strani pooblaščenim preizkušenim revizorji informacijskih sistemov. V primeru pravnega spora glede avtentičnosti in celovitosti hranjenega gradiva ponudniku ni treba dokazovati, da je bila e-hramba izvedena na zakonsko skladen način. Gradivu, ki ga hrani ponudnik z veljavno akreditacijo storitve e-hrambe, se avtentičnost in celovitost prizna že na podlagi zakona, v primeru pravnega spora glede avtentičnosti in celovitosti gradiva pa ni potrebno preverjati

pravilnosti izvajanja e-hrambe, saj to vsakoletno izvaja Arhiv RS, ki je regulator na področju e-hrambe.

Slika v nadaljevanju na grafičen način prikazuje, da akreditacija storitve e-hrambe ali spremljevalnih storitev zajema vse do sedaj naštetе pogoje, zato predstavlja najvišji nivo ponudnika teh storitev.



*Slika 1: Stopnja organiziranosti ponudnikov storitev e-hrambe ali spremljevalnih storitev*

### 3 ZUNANJE IZVAJANJE STORITEV E-HRAMBE - DA ALI NE

Zunanje izvajanje storitev, ki je pri nas bolj znano pod tujko »outsourcing«, je v tujini dokaj uveljavljena praksa. V Sloveniji se mnogi poslovni in javnopravni subjekti le s težavo odločijo, da bodo katerega od svojih poslovnih procesov dali v zunanje izvajanje, saj želijo večino teh opravljati sami. V primeru, ko so predmet zunanjega izvajanja storitev e-hrambe in spremljevalnih storitev, je lahko težava v tem, da dokumentarno gradivo mnogokrat vsebuje zaupne informacije o poslovanju subjekta, podatke o naročnikih, osebne podatke, podatke o zaposlenih in druge pomembne informacije, ki za subjekt predstavljajo poslovno skrivnost. Razkritje teh informacij predstavlja tveganje za poslovanje subjekta, zato jih le s težavo zaupajo ponudnikom storitev e-hrambe in spremljevalnih storitev.

V nadaljevanju so podana razmišljanja za posamezna pomembna področja, ki so zajeta pri izvajanju e-hrambe. Subjekt, ki bi želel e-hrambo samostojno izvajati, bi moral tako iz funkcionalnega kot iz stroškovnega vidika dobro razmisliti, ali lahko zadosti zahtevam zakonodaje ali pa je bolje, da izvajanje storitve e-hrambe zaupa za to usposobljenim kredibilnim ponudnikom.



### 3.1 PROGRAMSKA IN STROJNA OPREMA

Programska in strojna oprema predstavljata osnovo za izvajanje e-hrambe, vendar samostojno še zdaleč ne zagotavljata vsega potrebnega za njeno zakonsko skladnost.

Za nakup programske in strojne opreme se subjekti ne bi smeli odločati zgolj na podlagi cene, saj je pri tem smiselno upoštevati tudi razpoložljivo funkcionalnost te opreme ter možne načine in nivoje zagotavljanja avtentičnosti in celovitosti gradiva. Avtentičnost in celovitost se namreč zagotavlja s pravilno kombinacijo tehnično-organizacijskih ukrepov. Pri tem je treba upoštevati dejstvo, da so ob šibkih tehničnih ukrepih potrebni močni organizacijski ukrepi in obratno. Subjekt, ki se torej odloči za programsko in strojno opremo, ki zagotavlja le osnovne varnostne mehanizme za zagotavljanje avtentičnosti, mora na račun cenejših opreme okrepiti organizacijske ukrepe, kar pa dodatno obremenjuje kadrovske vire subjekta in tako podraži stroške dela, hkrati pa se zaposleni po nepotrebnem ukvarjajo z aktivnostmi, ki ne predstavljajo osnovne dejavnosti subjekta. Naročeno programsko in strojno opremo je treba ustrezno integrirati v obstoječ informacijski sistem subjekta in ga povezati z obstoječimi aplikacijami, ki generirajo digitalno gradivo. Ti postopki zahtevajo določeno strokovno usposobljenost informatikov, s katerimi subjekti mnogokrat ne razpolagajo, zato je treba najeti določene svetovalce, kar dodatno dviguje ceno uvedbe e-hrambe.

Zaradi tehnološkega napredka je programsko in strojno opremo nujno potrebno redno pregledovati, vzdrževati, posodabljati in dopolnjevati, da bo ta pravilno, zanesljivo in varno delovala. Mnogokrat se pozablja, da vzdrževanje za obdobje enega leta v povprečju predstavlja nekaj manj kot petino nabavne cene opreme, kar pomeni, da ima v nekaj več kot petih letih subjekt podvojene stroške nabave opreme. Hkrati je treba upoštevati, da amortizacijska doba IT-opreme v povprečju znaša od tri do pet let in da je po tem obdobju praktično zastarela in jo je smiselno zamenjati z novo. Seveda to za e-hrambo pomeni dodatne stroške, ki jih na začetku mnogokrat pozabimo upoštevati.

### 3.2 PRIMERNI SISTEMSKI PROSTORI

Vso strojno in programsko opremo je treba umestiti v primerne sistemske prostore, ki zadostujejo pogojem »Enotnih tehnoloških zahtev«.

Fizično in tehnično varovanje teh prostorov predstavlja osnovni kontrolni mehanizem pri zagotavljanju varnosti hranjenega gradiva. Tako mora fizično varovanje zagotavljati ustrezno usposobljena varnostna služba, skladno s pomembnostjo in ranljivostjo hranjenega gradiva pa je treba opredeliti tudi varnostna območja. Tehnično varovanje se zagotavlja z različnimi kombinacijami senzorjev gibanja, video nadzora, vrati s kontrolo pristopa, ki za odpiranje zahtevajo ustrezno kombinacijo identifikacijske kartice in šifre, ali celo različne biometrične mehanizme.

Subjekt mora zagotoviti, da lahko do strojne in programske opreme za hrambo dostopajo le člani operativnega osebja, ki so pooblaščen za vzdrževanje in upravljanje opreme za zagotavljanje e-hrambe. Hkrati je treba zagotoviti ustrezno protipožarno varovanje, ki se zagotavlja z javljalniki požara in protipožarnimi gasilnimi sistemi, ki morajo biti prilagojeni za IT sisteme, tako da ob uporabi ne ogrožajo hranjenega gradiva. Strojna in na njej nameščena programska oprema pravilno delujeta le v določenem temperaturnem območju, zato je treba poskrbeti za

ustrezno vzdrževanje delovne temperature. V te namene se uporabljajo napredni redundantni klimatski sistemi, ki morajo biti redno pregledovani in vzdrževani.

### 3.3 STROKOVNI KADER

Nikakor ne moremo mimo dejstva, da človeški faktor predstavlja zelo veliko tveganje pri izvajanju e-hrambe digitalnega gradiva. Seveda se da z naprednimi tehnološkimi in organizacijskimi ukrepi to tveganje omejiti na minimum, vendar človeškega faktorja ni možno nikoli popolnoma izključiti. Subjekt mora poskrbeti, da so člani operativnega osebja, ki delajo z dokumentarnim gradivom, ustrezno usposobljeni, ozaveščeni in tudi nadzorovani. Upoštevati je treba dejstvo, da operativno osebje prevzema veliko odgovornost glede varovanja poslovne skrivnosti, osebnih in tajnih podatkov, zavarovanja gradiva pred namernim in nenamernim uničenjem, potvorbami, zlorabami ter ostalimi možnimi zlonamernimi posegi nad hranjenim gradivom.

### 3.4 NOTRANJA PRAVILA ZA IZVAJANJE VARNE HRAMBE

Kot je že bilo omenjeno, mora po zakonodaji vsaka oseba, ki izvaja zajem in hrambo digitalnega gradiva, pripraviti in sprejeti notranja pravila, po katerih mora nato tudi izvajati in spremljati zajem in hrambo. Subjekti, ki se bodo odločili, da bodo storitve e-hrambe in spremljevalnih storitev najemali pri ponudnikih teh storitev, bodo kompleksnost priprave lastnih notranjih pravil zmanjšali na minimum. Zakonodaja daje največji poudarek ravno pri zajemu, pretvorbi ter hrambi gradiva. Če ta del e-hrambe namesto subjekta izvajajo ponudniki teh storitev, morajo zagotavljati zakonsko skladnost izvajanja e-hrambe. Pri tem je treba natančno razmejiti odgovornosti pri izvajanju e-hrambe, torej se dogovoriti glede tega, kdo je odgovoren za kateri del izvajanja e-hrambe. Iz tega razloga je zelo pomembno, da so subjekti pri sklepanju pravnega akta glede razmejitev odgovornosti zelo pozorni, kaj mora zagotavljati subjekt sam in kaj bo zagotavljal ponudnik.

Če ponudnik zagotavlja vse, kar se glede e-hrambe zahteva v zakonodaji, mora subjekt pri sebi urediti le upravljanje gradiva in pripravo na hrambo, glede ostalih potrebnih aktivnosti za zakonsko skladno izvajanje e-hrambe pa se sklicuje na ponudnika oziroma njegove odgovornosti v sklenjenem pravnem poslu. V osnovi mora subjekt pripraviti klasifikacijski in signirni načrt ter pripraviti akt, ki opredeljuje pisarniško poslovanje, v katerem natančno opiše tiste postopke izvajanja e-hrambe, ki jih bo izvajal sam. Priprava gradiva za e-hrambo navadno zajema opremljanje gradiva z določenimi metapodatki, ki so potrebni za pravilno izvajanje e-hrambe. Treba je omeniti, da navedeno predstavlja zelo poenostavljen primer, ki je v praksi bolj kompleksen, vendar še zdaleč ne tako, kot če bi subjekt moral pripraviti notranja pravila za celotno področje e-hrambe.

V primeru najema storitev e-hrambe in spremljevalnih storitev pri ponudnikih teh storitev je priporočljivo, da subjekt pristopi k pripravi tistega dela notranjih pravil, katerega področja bo zagotavljal ponudnik storitve, šele po sklenitvi pravnega posla, saj se bo v svojih notranjih pravilih glede teh področij skliceval na obveznosti ponudnika, ki so bile določene v okviru pravnega posla med subjektom in ponudnikom.

### 3.5 NEPREKINJENO POSLOVANJE IN OKREVANJE PO KATASTROFI PRI E-HRAMBI

Po zakonodaji mora vsaka oseba, ki izvaja e-hrambo digitalnega gradiva, razen ostalega imeti implementiran tudi načrt neprekinjenega poslovanja in okrevanja po katastrofi. Implementacija, upravljanje in vzdrževanje sistemov, ki na tehnološki način zagotavljajo neprekinjeno poslovanje in okrevanje po katastrofi, kakor tudi priprava in izvajanje načrta so kompleksni, zahtevajo precej znanja in aktivnosti operativnega osebja in hkrati tudi precej stanejo. Tako je tudi s tega vidika priporočljivo, da subjekti storitve e-hrambe raje zaupajo kredibilnim in za to usposobljenim ponudnikom teh storitev. Zaradi kompleksnosti zagotavljanja neprekinjenega poslovanja in okrevanja po katastrofi, je v nadaljevanju področje obravnavano z vidika, ko se ti postopki izvajajo s strani ponudnikov storitve e-hrambe. Kadar subjekt sam izvaja vse postopke e-hrambe, mora prav tako imeti pripravljen načrt neprekinjenega poslovanja, ki ga mora tudi dejansko izvajati v praksi. Zahteve subjekta glede neprekinjenega poslovanja morajo biti smiselno prilagojene glede na pomembnost in ranljivost hranjenega gradiva.

S stališča zagotavljanja storitve e-hrambe je treba poskrbeti, da je hranjeno digitalno gradivo subjektom vedno na razpolago, ko ga potrebujejo. Da bi zadostili strogim zahtevam subjektov, morajo ponudniki vzpostaviti takšen sistem e-hrambe, ki zagotavlja neprekinjeno dostopnost do digitalnega gradiva, ki v nobenem primeru ne sme biti podvrženo prekinitvam zaradi nedelovanja tehnologije. To lahko zagotovijo le, če na ustrezen način vzpostavijo sistem neprekinjenega poslovanja, ki mora biti po zakonodaji dodatno podprt tudi s primernim načinom okrevanja po katastrofi.

Ustrezna kombinacija tehničnih in organizacijskih ukrepov zagotavlja tako neprekinjeno poslovanje kot tudi okrevanje po katastrofi. Bolj dovršeni tehnični ukrepi imajo za posledico manj intenzivne organizacijske ukrepe in obratno. Napredni tehnični ukrepi po eni strani omogočajo manjšo možnost izpada storitve zagotavljanja e-hrambe zaradi nedelovanja tehnologije in tudi precej krajši čas vzpostavitve predhodnega stanja, po drugi strani pa predstavljajo visok strošek, zato je treba pri njihovem načrtovanju upoštevati še namen in pomembnost zagotavljanja neprekinjenega poslovanja in okrevanja po katastrofi. Navedeno je vodilo, da je pred implementacijo treba analizirati in opredeliti pravilno uravnoteženost med potrebnimi tehničnimi in organizacijskimi ukrepi. Pa vendar, kadar ponudnik zagotavlja hrambo digitalnega gradiva, ki vsebuje pomembne informacije, pogodbene ureditve, analize, poslovne izide, projekte, znanje, finančne izkaze in ostale podatke, ki jih subjekti nujno potrebujejo za svoje vsakodnevno poslovanje, je treba zagotoviti najvišje nivoje zagotavljanja neprekinjenega poslovanja in okrevanja po katastrofi, ki jih je možno podpreti le z najnaprednejšo tehnologijo in zanesljivimi organizacijskimi ukrepi.

#### 3.5.1 INFRASTRUKTURA, KI OMOGOČA NEPREKINJENO POSLOVANJE

Kot je že bilo večkrat omenjeno, infrastrukture storitve e-hrambe ne predstavljata zgolj ustrezna programska in strojna oprema, pač pa je treba zagotoviti tudi varne systemske prostore, sisteme za zagotavljanje neprekinjenega napajanja, izvajanje fizične in tehnične varnosti, protipožarne varnosti, zagotavljanje delovne temperature opreme in druge sisteme, ki znižujejo tveganja glede dostopnosti do digitalnega gradiva na minimum.

S stališča neprekinjenega poslovanja in okrevanja po katastrofi je treba upoštevati, da zaradi vedno večje kompleksnosti informacijskih sistemov posledično

prihaja do več težav, ki izhajajo iz osnovne infrastrukture, ki bi morala zagotavljati fizično varnost in optimalne pogoje za delovanje IT-infrastrukture. Običajno gre za napake v delovanju opreme in podpornih sistemov, kot so okoljski pogoji, energetski izpadi ipd. Ne glede na to, da se večje nesreče, kot so potres, poplava, požar ipd., pojavljajo redkeje, pa zaradi možnih katastrofalnih posledic zahtevajo še posebno skrbno načrtovanje in doslednost pri kontrolah in testih. Neprekinjeno poslovanje in okrevanje po katastrofi je praviloma osredotočeno na osnovno IT-infrastrukturo, vzporedno pa je treba zagotoviti tudi rezervni prostor za delo, komunikacije, prevoz, nujna finančna sredstva itn. Pri načrtovanju lokacij, kjer je nameščena strojna in programska oprema za zagotavljanje e-hrambe, je priporočljivo upoštevati, da se te nahajajo na območjih, ki jih najmanj ogrožajo potresi, poplave, požari in ostale naravne nesreče. Kljub temu, da zakonodaja za dolgoročno hrambo in arhivsko gradivo predpisuje, da mora biti rezervna lokacija, kjer se izvajajo varnostne kopije gradiva, najmanj 50 km oddaljena od glavne lokacije, je pri načrtovanju rezervne lokacije treba upoštevati, da se ne nahaja na istem potresnem ali poplavnem območju kot glavna lokacija.

Z ustreznim načrtovanjem sistemskih prostorov lahko izpolnimo več kriterijev za uspešno neprekinjeno poslovanje. Priporočljivo je, da se v te namene uporabijo varni podatkovni centri oz. varne celice, ki nudijo najvišjo stopnjo zaščite pred požarom, potresom, elektromagnetnimi vplivi, prahom, tekočinami, korozivnimi plini, vlomi in vandalizmom ter drugimi vplivi in posegi iz okolja. Gre za modularni, visokovarni sistemski prostor, ki je umeščen na ustrezni geografski lokaciji, ima ustrezno gradbeno ureditev, je fizično in tehnično varovan, omogoča zadostno oskrbo z električno energijo in ima vzpostavljene sisteme neprekinjenega napajanja, tehničnega hlajenja, protipožarne varnosti ter zaščite pred vdori vode. Vsi naštetih gradniki varnega podatkovnega centra omogočajo zagotavljanje visokega nivoja kakovosti storitve e-hrambe in so zelo pomembni za zagotavljanje neprekinjenega poslovanja, saj ima lahko nedelovanje kateregakoli izmed njih celo večje posledice kot odpoved nekega elementa v IT-infrastrukturi.

Ko so zagotovljene ustrezne geografske lokacije in varni sistemski prostori, je treba zagotoviti tudi ustrezno programsko in strojno opremo. Z vidika zagotavljanja neprekinjenega poslovanja je priporočljivo, da so vse aktivne komponente sistema za zagotavljanje e-hrambe najmanj podvojene in dimenzionirane tako, da preprečujejo enojno točko odpovedi. Priporočljivo je vzpostaviti vsaj dva aktivna sistema za zagotavljanje e-hrambe in jih umestiti na vsaj dveh geografsko ločenih lokacijah. Z ustrezno komunikacijsko povezljivostjo lahko takšen podvojen sistem, ne glede na geografsko razmejitev, deluje kot celota in subjektom hkrati zagotavlja storitev e-hrambe z obeh lokacij. V primeru delne ali popolne odpovedi enega od sistemov lahko sistem na »preživeli« lokaciji subjektom nemoteno zagotavlja izvajanje storitve e-hrambe, zato takšen način zelo znižuje tveganje za popolni izpad storitve.

Ne glede na to, ali ponudnik z naprednimi tehnološkimi ukrepi zagotovi neprekinjeno poslovanje in s tem tudi stalno dobavo storitve e-hrambe, pa mora po zakonodaji v primeru dolgoročne hrambe dokumentarnega gradiva (več kot 5 let) ter arhivskega gradiva na več kot 50 km oddaljeni lokaciji hraniti še varnostne kopije vsega hranjenega digitalnega gradiva subjektov, za katere izvaja storitev. Varnostno kopiranje se lahko izvaja na različne načine. Pri najenostavnejšem se na primarni lokaciji gradivo prenese na ustrezne pomnilne medije, ki se nato z ustreznim transportom dostavijo na oddaljeno lokacijo, kjer se hranijo v ustreznih prostorih. Takšen način je seveda najcenejši, hkrati pa tudi daleč najmanj varen in najmanj priporočljiv, saj je hranjeno digitalno gradivo v tem primeru najbolj ranljivo tako glede človeške napake in dostopnosti do podatkov kot tudi glede izgube gradiva.

Napredni ponudniki so implementirali napreden in mnogo varnejši sistem, ki je s primarnimi lokacijami komunikacijsko povezan in tako omogoča samodejno izvajanje varnostnih kopij, kjer izvajanje ni odvisno od aktivnosti osebja. Hkrati sistem sproti preverja zmožnost reprodukcije digitalnih varnostnih kopij. Podatki (gradivo) na varnostnih kopijah so kriptirani, tako da so zavarovani tako pri komunikacijskem prenosu kot pri hrambi. Reprodukcijska z varnostnih kopij se lahko izvede neposredno z rezervne lokacije, zato je tudi bistveno hitrejša.

### 3.5.2 NAČRT NEPREKINJENEGA POSLOVANJA

Zagotavljanje storitve e-hrambe je zelo povezano z delovanjem IT-opreme, zato je njeno hitro okrevanje zelo pomembno. Razen dobro načrtovane tehnologije pripomore k ponovni vzpostavitvi predhodnega stanja tudi dobro pripravljen načrt neprekinjenega poslovanja. Pri pripravi takšnega načrta je treba upoštevati, da subjekti pričakujejo neprekinjen dostop do gradiva, zato je izpad delovanja IT-tehnologije ponudnika e-hrambe popolnoma nesprejemljiv.

Priporočljivo je, da se pri pripravi načrta neprekinjenega poslovanja upoštevajo smernice standarda BS 25999. V načrtu neprekinjenega poslovanja mora biti natančno določeno, kdo je odgovoren za preverjanje in preizkušanje načrta, za njegovo vzdrževanje in posodabljanje ter izobraževanje in usposabljanje vključenih oseb. Za področje e-hrambe je treba opredeliti tudi zagotavljanje celovitosti digitalnih dokumentov pri prenosu prek komunikacijskih povezav in v sistemu e-hrambe. Opredeliti je treba tudi tehnološke načine, s katerimi se zagotavljata zaupnost in trajnost hranjenega digitalnega gradiva, ter načine, ki zagotavljajo razpoložljivost in dostopnost same storitve e-hrambe. V načrtu morajo biti opredeljene primarne in rezervne lokacije, natančno in po imenih mora biti opredeljeno tudi osebje za izvajanje načrta ter natančno definirane vloge ter pooblastila sodelujočih posameznikov. Načrt mora prav tako vsebovati ažuren seznam vse aplikativne in systemske opreme, ki je potrebna za zagotavljanje storitve. Treba je definirati različne situacije, ki se pojavijo ob nastopu nizke, srednje ali visoke stopnje kritičnosti ter v primeru potrebe okrevanja po katastrofi. Razen dobro pripravljene strategije je priporočljivo pripraviti različne scenarije za vzpostavitev predhodnega stanja, ki so odvisni od stopnje kritičnosti nastale situacije. Hkrati je treba opredeliti organizacijske in operativne postopke, ki zagotavljajo povrnitev sistemov in podatkov ter njihovo kontrolo obnove. Načrt mora vsebovati tudi seznam vseh v načrtu sodelujočih oseb z vsemi njihovimi kontaktnimi podatki (telefonska številka, elektronski naslov ...), da so ob nastopu izrednih dogodkov uspešno obveščeni in vpoklicani k izvajanju načrta.

### 3.6 IZBIRA PONUDNIKA

Subjekt, ki se je zaradi kompleksnosti izvajanja e-hrambe digitalnega gradiva odločil, da tega sam ne bo izvajal, lahko e-hrambo zaupa ponudniku storitev.

Pravilna izbira ponudnika je vedno najtežja. Najpogostejša napaka pri izbiri ponudnika je, da je odločitev mnogokrat bolj odvisna od cene kot od kakovosti storitve. Pred zaupanjem hrambe digitalnega gradiva v zunanje izvajanje je priporočljivo pri ponudniku predhodno preveriti način izvajanja hrambe, opremo in prostore za hrambo gradiva, načine zagotavljanja avtentičnosti in celovitosti, postopke omejevanja dostopa nepooblaščenih oseb, varnostne mehanizme in ukrepe za zavarovanje gradiva, požarno varnost, načine zagotavljanja varnostnih kopij

gradiva, hkrati pa pridobiti tudi informacijo o strokovni usposobljenosti oseb, ki bodo upravljali z gradivom subjekta.

Odločitev za ponudnika, ki ponuja opremo in storitve s šibkimi mehanizmi zagotavljanja varnosti, avtentičnosti in celovitosti, ki komaj zagotavljajo zakonsko skladnost (ali pa tudi ne), je lahko poceni, vendar je skoraj zagotovo zelo tvegana izbira. Ponudnik mora uporabljati najnaprednejšo tehnologijo za zagotavljanje varnosti, avtentičnosti in celovitosti, izkazovati finančno stabilnost ter kadrovske usposobljenosti in biti mora zaupanja vreden. Zavedati se je treba posledic, ki nastanejo, če se za gradivo ves čas hrambe ne zagotavljajo avtentičnost, trajnost, nespremenljivost, uporabnost vsebine in zmožnost reprodukcije, dostopnost le pooblaščenih uporabnikov, zavarovanje pred izgubo itn. Uporabnikom, ki slabo poznajo področje e-hrambe digitalnega gradiva, nekateri ponudniki na začetku ponudijo le osnovne storitve. Bolj ko se uporabniki spoznavajo s tem področjem, več dodatnih storitev zahtevajo od teh ponudnikov, zato je storitev mnogo dražja, kot je bila uporabniku na začetku predstavljena.

Nekateri ponudniki programske in strojne opreme mnogokrat zavajajo subjekte, da imajo z nakupom njihove opreme zagotovljeno pravno veljavo hranjenega digitalnega gradiva. Ponovno je treba opozoriti, da sta akreditirana programska in akreditirana strojna oprema le osnova za izvajanje e-hrambe, za zakonsko skladnost pa mora subjekt zadostiti še vsem ostalim zahtevam, ki jih predpisuje zakonodaja.

Minimalno, kar morajo subjekti zahtevati od ponudnika storitev e-hrambe digitalnega gradiva, je, da ima sprejeta in pri Arhivu RS potrjena notranja pravila za izvajanje e-hrambe. Seznam takšnih ponudnikov je trenutno še dokaj kratek, objavljen pa je na povezavi <http://www.gov.si/aplikacije/arhiv/earh-registri/notranjaPravilaPregled.php>.

Zakonsko skladno izvajanje e-hrambe je pri ponudniku, ki je storitev e-hrambe akreditiral pri Arhivu RS, najmanj enkrat letno preverjeno s strani Arhiva RS. Akreditacija storitve e-hrambe je sicer pogoj za hrambo digitalnega gradiva javnopравnih oseb, vendar predstavlja izbira takšnega ponudnika tudi za poslovni subjekt najmanjše tveganje. Na podlagi navedenega predstavlja ponudnik, ki je storitev e-hrambe akreditiral pri Arhivu RS, kredibilno izbiro za zunanje izvajanje e-hrambe, ki celovito zagotavlja zakonsko skladnost.

## **4 E-ARHIV POŠTE SLOVENIJE**

V nadaljevanju je opisan način izvajanja storitve e-hrambe, ki ga zagotavlja ponudnik Pošta Slovenije, katerega predstavnik je avtor tega prispevka.

### **4.1 NOTRANJA PRAVILA PONUDNIKA E-HRAMBE**

Pošta Slovenije je kot ponudnik varne hrambe dokumentarnega in arhivskega gradiva v digitalni obliki sprejela notranja pravila za izvajanje e-hrambe, ki jih je Arhiv RS tudi potrdil in vpisal v register sprejetih notranjih pravil pod ref. št. 0022/2007. E-hrambo izvaja v skladu s potrjenimi notranjimi pravili, zato se hranjenemu gradivu prizna enakost z izvornim gradivom (avtentičnost) na podlagi zakona (31. člen ZVDAGA). Za zagotavljanje storitve e-hrambe uporablja akreditirano programsko in strojno opremo, hkrati pa je tudi v postopku akreditacije storitve.

## **4.2 ZAGOTAVLJANJE AVTENTIČNOSTI IN CELOVITOSTI HRANJENEGA GRADIVA**

Funkcionalno se avtentičnost in celovitost hranjenega digitalnega gradiva zagotavlja s časovnim žigosanjem vsake posamezne enote gradiva, ki jo sistem E-Arhiv sprejme v hrambo. Pri tem se uporablja varne časovne žige, ki jih izdaja javno priznan overitelj POŠTA®CA. Z varnim časovnim žigom se digitalnemu dokumentu doda natančna informacija o času, s čimer se pravno veljavno potrdi, da je dokument obstajal v času sprejema v hrambo. Sistem E-Arhiv sam poskrbi, da se pred potekom veljavnosti obstoječega varnega časovnega žiga gradivo ponovno časovno žigosa. Takšen način lahko ohranja avtentičnost gradiva ves čas hrambe, saj z vsakim ponovnim časovnim žigosanjem podaljša veljavnost digitalnega gradiva do datuma poteka veljavnosti novega varnega časovnega žiga.

Ob vstopu gradiva v E-Arhiv se samodejno preverja veljavnost kvalificiranega digitalnega potrdila vsakega digitalno podpisanega dokumenta in veljavnost kvalificiranega digitalnega potrdila, uporabljenega za zagotavljanje varnega sporočilnega kanala.

## **4.3 ZAGOTAVLJANJE VARNOSTI HRANJENEGA GRADIVA**

Visok nivo varnosti hranjenemu gradivu zagotavljajo napredni tehnični in organizacijski ukrepi.

### **4.3.1 DOSTOP UPORABNIKOV IN ADMINISTRATORJEV DO APLIKACIJE SISTEMA E-ARHIV**

Pooblaščen uporabniki stranke lahko do storitve E-Arhiv dostopajo le z uporabo veljavnega kvalificiranega digitalnega potrdila. Tudi administratorji Pošte Slovenije, ki skrbijo za upravljanje s storitvijo, se morajo za prijavo v sistem E-Arhiv identificirati s kvalificiranim digitalnim potrdilom.

### **4.3.2 REVIZIJSKE SLEDI**

Vsi dogodki na nivoju posameznega dokumenta, celotnega sistema in varnosti se beležijo in trajno hranijo v obliki revizijskih sledi, ki se verižno časovno žigosajo z varnim časovnim žigom, kar zagotavlja njihovo verodostojnost.

### **4.3.3 NEPREKINJENO POSLOVANJE IN OKREVANJE PO KATASTROFI**

Vse aktivne komponente sistema E-Arhiv so že lokalno podvojene. Hkrati je podvojen še celoten sistem e-hrambe, ki v gručnem načinu vzporedno deluje na dveh geografsko ločenih primarnih lokacijah. V primeru večje oz. popolne odpovedi sistema na eni lokaciji sistem na drugi lokaciji v celoti prevzame delovanje in nemoteno zagotavlja izvajanje storitve.

Za potrebe okrevanja po katastrofi na več kot 100 km oddaljeni lokaciji samodejno poteka tudi varnostno kopiranje vsega hranjenega gradiva. V primeru nastopa katastrofe in popolnega uničenja sistema E-Arhiv na obeh primarnih lokacijah, se reprodukcija hranjenega gradiva zagotavlja iz varnostnih kopij na rezervni lokaciji. Na ta način se vsaka enota gradiva hrani na treh ločenih lokacijah, kar zagotavlja visoko stopnjo varnosti naročnikovega gradiva pred izgubo.

#### 4.3.4 VARNI TRANSPORTNI KANAL

Prenos digitalnih dokumentov v sistem E-Arhiv se izvaja prek varnega transportnega kanala, ki deluje na sporočilno osnovani varnosti (message based security), kjer se vsak posredovani digitalni dokument skupaj z metapodatki posreduje v obliki sporočila, ki je kriptirano in digitalno podpisano. Sporočilo se kriptirano in digitalno podpisano prenaša skozi celotno omrežje (tudi lokalno), torej od uporabniške aplikacije do aplikacije sistema E-Arhiv. Takšen način prenosa dokumentov je mnogo varnejši od SSL načina zaščite komunikacijskega kanala, kjer se med komunikacijskimi napravami uporabnika in ponudnika storitve kriptira le transportni kanal, sporočila (digitalno gradivo) pa se po tem kanalu in tudi v lokalnem omrežju prenašajo v običajni, nekriptirani obliki.

#### 4.3.5 INFORMACIJSKA IN FIZIČNO TEHNIČNA VARNOST

Sistem E-Arhiv je varovan z večnivojskim sistemom za preprečevanje vdorov, ki ga sestavljajo zunanje in notranje požarne pregrade, ISA strežniki ter sistem za zaznavo in preprečevanje vdorov (IDS in IPS konektorji), ki zaznava in po potrebi zavrača neželen podatkovni promet v katerikoli logični točki omrežja ponudnika, prek katerega se gradivo prenaša v sistem E-Arhiv. Vse naprave informacijskega sistema za zagotavljanje storitve E-Arhiv so varovane z naprednim protivirusnim sistemom, ki se redno posodablja.

Do komponent lahko fizično dostopajo le pooblaščen vzdrževalci, nameščene pa so v varnih podatkovnih centrih, ki zagotavljajo visok nivo zaščite pred potresom, elektromagnetnimi vplivi, plini, tekočinami, prahom, vlomi in drugimi okoljskimi vplivi. Fizična varnost se zagotavlja s kombinacijo senzorjev gibanja in video nadzora. Aktivna protipožarna zaščita se zagotavlja s posebnim, IT-prilagojenim gasilnim sistemom, ki ne ogroža IT-opreme in življenja ljudi.

#### 4.4 INFRASTRUKTURA SISTEMA E-ARHIV

Celotna potrebna infrastruktura za zagotavljanje storitve e-hrambe digitalnega gradiva je v lasti Pošte Slovenije. Potrebna strojna in programska oprema je nameščena v varnih podatkovnih centrih, ki se nahajajo na geografsko ločenih lokacijah, ki so medsebojno komunikacijsko povezane. Z opremo lastnega overitelja POŠTA®CA se zagotavljata potrebno časovno žigosanje digitalnih dokumentov ter izdaja potrebnih kvalificiranih digitalnih potrdil.

#### 4.5 NAPREDNOST REŠITVE

Za zagotavljanje storitve se uporablja akreditirana programska oprema, ki predstavlja celovito rešitev za storitev e-hrambe digitalnega gradiva, je podprta z mednarodnimi standardi, je storitveno usmerjena ter načrtovana in zgrajena z uporabo zadnjih spletnih ter srednjenivojskih tehnologij razvoja programske opreme. Programska oprema je modularna in na programskem nivoju preprečuje obstoj kritične točke odpovedi, je poljubno skalabilna, neodvisna od formata vhodnih dokumentov in podpira širok nabor metapodatkov, od katerih je del tudi uporabniško nastavljivih, tako po imenu kot po tipu vrednosti. Z različnimi možnostmi hitrosti posredovanja dokumentov v hrambo strankam omogoča izbiro med različnimi nivoji storitve glede na njihove potrebe.



Prav tako akreditirana strojna oprema rešitve uporablja napredna diskovna polja, arhivske robotske knjižnice, strežnike dokumentnega cevovoda in ostale informacijske storitve Pošte Slovenije, ki omogočajo varno in pravno veljavno storitev e-hrambe digitalnega gradiva.

Glede na arhitekturo programske opreme je omogočena poljubna skalabilnost strojne opreme, ki je konfiguracijsko dimenzionirana tako, da preprečuje obstoj enojne točke odpovedi. Implementiran je koncept okrevanja po katastrofi. Celotna arhitektura temelji na upravljanju s podatki po konceptu ILM.

## **4.6 E-HRAMBA DIGITALNEGA GRADIVA**

### **4.6.1 FORMAT DIGITALNEGA GRADIVA**

Sistem E-Arhiv lahko v hrambo sprejme katerikoli format digitalnega dokumenta, ki je razen tega lahko tudi kriptiran. Gradivo je lahko zajeto v fizični obliki in pretvorjeno v digitalno obliko ali pa je že v izvorni obliki nastalo in bilo zajeto kot digitalno gradivo. V obeh primerih je pomembno, da sta zajem in morebitna pretvorba v ustrezno digitalno obliko zakonsko skladno izvedena.

### **4.6.2 LOGIČNI IN FIZIČNI DOKUMENT**

Osnovno entiteto sistema E-Arhiv predstavlja logični dokument, ki vsebuje metapodatke in enega ali več fizičnih dokumentov. Fizični dokument vedno pripada natančno enemu logičnemu dokumentu in vsebuje metapodatke ter binarno ali tekstovno reprezentacijo dokumenta in predstavlja dokument v pravem pomenu besede (\*.pdf, \*.xml, \*.tiff, \*.docx itn.).

### **4.6.3 ČASOVNO ŽIGOSANJE**

Sistem E-Arhiv z varnim časovnim žigom časovno žigosa vsak fizični dokument, ki ga sprejme v hrambo, in ga samodejno ponovno časovno žigosa pred potekom veljavnosti obstoječega varnega časovnega žiga. Prav tako sistem E-Arhiv časovno žigosa in digitalno podpiše vsak dokument, ki ga posreduje iz sistema e-hrambe (npr. vpogled v dokument, ki se izvaja na strankinem sistemu).

### **4.6.4 POSREDOVANJE GRADIVA V SISTEM E-ARHIV**

Digitalno gradivo se iz strankinega sistema za upravljanje z dokumenti posreduje v varno hrambo prek varnega transportnega kanala velikih kapacitet, kar omogoča posredovanje obstoječe zbirke digitalnega gradiva kot tudi redno (on-line) posredovanje digitalnega gradiva v hrambo. Posredovanje digitalnega gradiva v e-hrambo se ne zaračunava posebej, ampak je že zajeto v ceni storitve.

### **4.6.5 HRAMBA NA RAZLIČNIH MEDIJIH**

Sistem E-Arhiv omogoča hrambo digitalnega gradiva na hitrih medijih, ki omogočajo takojšen dostop do gradiva, in hrambo na cenovno ugodnejših počasnih medijih, ki omogočajo zakasnen dostop, ki je ranga nekaj minut.

#### 4.6.6 DOSTOP UPORABNIKOV

Do gradiva, ki je hranjeno v sistemu E-Arhiv, lahko dostopa poljubno število strankinih uporabnikov. Število uporabnikov, ki dostopajo do sistema, se ne zaračunava posebej. Vsak uporabnik, ki želi dostopati do sistema, se mora identificirati z veljavnim kvalificiranim digitalnim potrdilom za pravne osebe (subjekta, ki je naročnik storitve), ki je vezano na tega uporabnika (ime in priimek uporabnika). Omogočen je dostop s katerimkoli v Sloveniji priznanim kvalificiranim digitalnim potrdilom za pravne osebe.

#### 4.7 PRILAGODITEV STRANKINEGA SISTEMA NA SISTEM E-ARHIV

Ker gre za povezavo aplikacij, ki v celoti komunicirajo na nivoju B2B, je treba prilagoditi določen del subjektovega informacijskega sistema. V te namene se subjektu posreduje E-Arhiv SDK (angl. Software Developer Kit), ki razen namestitvenega paketa vsebuje tudi potrebno razvijalsko specifikacijo, primere namestitev in ostalo potrebno dokumentacijo za uporabo storitve E-Arhiv. Namestitveni paket SDK omogoča tudi osnovno praktično preizkušanje storitve na testnem okolju, kot je npr. pošiljanje gradiva v hrambo in pridobivanje gradiva iz hrambe.

### 5 ZAKLJUČEK

Vsak subjekt, ki se odloča za varno hrambo digitalnega gradiva, bi se moral neodvisno od izvedbe (lastna ali zunanja) zavedati posledic nepravilno izvajane e-hrambe, zato je dobro poznavanje zakonodaje s tega področja ključnega pomena. Če bo subjekt e-hrambo zaupal zunanjemu izvajalcu, se naj pred tem dobro seznanijo z ustreznostjo izvajanja storitve. Priporočljivo je, da si pred odločitvijo pri ponudniku natančno ogleda način izvajanja storitve in infrastrukturo za zagotavljanje storitve. E-hramba je področje, ki ga je treba dobro poznati, zato se ne splača brezglavo hiteti z odločitvami, ampak je treba temeljito preučiti razpoložljive možnosti.

### SUMMARY

#### OUTSOURCING OF ELECTRONIC ARCHIVING

Acceptance of legislation in the field of safe preservation of digital documentary and archival material, which is simply named e-archiving, opened a completely new dimension in safe preservation. Digital material is a subject of change, forgery and other malicious interventions, therefore this kind of material authenticity and integrity must be guaranteed all the time of safe preservation, which is assured with advanced technological and organizing measures. Complexity of safe preservation is proved by very extensive legislation, which in the archival area demands very rigorous requests for IT technology and location for their implementation. At the same time legislation demands additional organizing measures for the process of capturing, transformation and safe preservation of digital documents. These reasons are a cause for the existence of legitimate questions, whether the public and private sector is capable to perform legislation's demands on safe preservation, or is it better for them to outsource this services and hire them at credible providers of safe preservation. On the other side some organizations and also providers treat legislation's demands to simply, which can lead to incorrigible consequences for organizations and providers.