KOFETKE.

Zasebni arhivi in pravica do pozabe

Kako naj se hramba in brisanje uredita v zbirki znanja pomočnika?



ZASEBNOST IN BRISANJE

Zemljevid, ki zajema izvirnike, indekse, povzetke, varnostne kopije in odstranjevanje dostopa.

BRALNA IZDAJA

september 2026
Lokalna izdaja · september 2026

Viri preverjeni 23. septembra 2026.

Shramba znanja pomočnika je pogosto opisana, kot da bi bila en sam predal: dodamo dokumente, po njih iščemo, nato ob neuporabnosti pritisnemo izbriši. V praksi gre za majhen sistem kopij in izpeljanih gradiv. Dokument lahko obstaja kot naložen izvirnik, izvlečeno besedilo, deli za iskanje, iskalni indeks, ustvarjen povzetek, predpomnjen odgovor, varnostna kopija in revizijski zapis. Odstranitev enega vidnega elementa je lahko potrebna, vendar ni isto kot odstranitev vseh povezanih artefaktov.

To razlikovanje ni izgovor za nedoločeno hrambo. Je osnova poštenega hranjenja in brisanja. Odgovorna zasnova pove, kaj obstaja, zakaj obstaja, kdo lahko do tega dostopa, kdaj se pregleda in kaj zahteva za izbris spremeni v vsaki plasti. Pove tudi, kdaj je odgovor odvisen od veljavnega prava, pogodbe z obdelovalcem, zadržanja zaradi pravnega spora ali tehničnega urnika varnostnih kopij.

Arhiv je zemljevid, ne ime mape

Vzemimo **Studio Javor**, izrecno izmišljeno majhno oblikovalsko podjetje. Za iskanje informacij po odobrenih projektnih datotekah uporablja zasebnega pomočnika. Zaključen projekt stranke ima štiri izvirne datoteke: brief, podpisano obvestilo o spremembi, zapis sestanka in preglednico. Pomočnik iz vseh štirih izvleče besedilo in vsako razdeli na štiri dele za iskanje. Za vsako datoteko ustvari kratek povzetek projekta ter shrani iskalni indeks za dele.

Število artefaktov je že večje od števila izvirnikov:

```
4 izvirniki
+ 4 datoteke izvlečenega besedila
+ (4 datoteke × 4 deli) = 16 delov za iskanje
+ 16 indeksnih vnosov
+ 4 povzetki
= 44 aktivnih artefaktov za popis
```

Ta aritmetika je izmišljen prikaz, ne trditev o zasnovi shrambe konkretnega izdelka. Nekateri sistemi hranijo manj objektov; drugi več različic, vektorskih predstavitev, predpomnilnikov ali dnevnikov. Bistvo je, da mora »izbriši projekt« določiti, katere plasti ukaz doseže.

Uporaben zapis je zemljevid sredstev, ne le seznam imen datotek. Vsaki plasti dodeli vlogo in pravilo hrambe.

Plast	Izvirnik
Primer v Studiu Javor	Naloženo podpisano obvestilo o spremembi
Glavni namen	Dokaz o predloženem dokumentu
Meja dostopa	Lastnik projekta in imenovano osebje
Dejanja ob koncu življenjske dobe	Izbrišemo ali prenesemo v omejeno hrambo, če je utemeljena

Izvleček

Primer v Studiu Javor	Besedilo, ustvarjeno iz obvestila
Glavni namen	Iskanje in pregled
Meja dostopa	Storitveni račun pomočnika; projektno osebje
Dejanja ob koncu življenjske dobe	Izbrišemo z izvirnikom, razen če je ločeno utemeljeno

Indeks

Primer v Studiu Javor	Deli za iskanje in vektorji
Glavni namen	Iskanje pomembnih odlomkov
Meja dostopa	Samo iskalna storitev
Dejanja ob koncu življenjske dobe	Odstranimo vnose in znova zgradimo prizadeti indeks

Povzetek

Primer v Studiu Javor	Štirje ustvarjeni povzetki projekta
Glavni namen	Hitrejša orientacija
Meja dostopa	Projektno osebje
Dejanja ob koncu življenjske dobe	Izbrišemo ali znova ustvarimo le iz dovoljenega vira

Predpomnilnik	
Primer v Studiu Javor	Nedavni odgovor ali predogled
Glavni namen	Kratkoročna zmogljivost
Meja dostopa	Storitveni proces; kratek rok poteka
Dejanja ob koncu življenjske dobe	Pustimo, da poteče, ali hitro počistimo

Varnostna kopija	
Primer v Studiu Javor	Šifriran dnevni posnetek
Glavni namen	Obnova po incidentu
Meja dostopa	Skrbnik kopij, ne vsakdanji uporabniki
Dejanja ob koncu življenjske dobe	Poteče po urniku kopij; vmes je izven uporabe

Zapis o brisanju	
Primer v Studiu Javor	ID zahteve, obseg, datum, rezultat
Glavni namen	Dokaz o operaciji
Meja dostopa	Skrbnik z omejenim dostopom
Dejanja ob koncu življenjske dobe	Hranimo le, dokler je utemeljeno; zmanjšamo identifikacijske podatke

Zemljevid vsaki plasti daje drugačen odgovor na vprašanje »čemu služi?«. To vprašanje pride pred izbiro roka hrambe. Povzetek ni izvirnik; vektorski indeks ni neškodljiv samo zato, ker ga človek težko prebere; varnostna kopija ni aktivna zbirka znanja. Če jih obravnavamo kot eno samo kategorijo, zabrišemo tveganje in odgovornost.

Hramba se začne z namenom in dostopom

Pravilo hrambe naj ima štiri dele: namen, sprožilni datum, trajanje ali točko pregleda in dejanje ob koncu. »Projektne podatke hranimo nekaj časa« ni pravilo. »Aktivni brief hranimo do zaključka projekta; nato omejimo dostop in preverimo pravno ali pogodbeno podlago za nadaljnjo hrambo« je bliže pravilu.

Načelo omejitve shranjevanja v GDPR določa, da se osebni podatki v obliki, ki dopušča identifikacijo, ne hranijo dlje, kot je potrebno za namene obdelave, ob navedenih pogojih za daljše shranjevanje v javnem interesu, za raziskovanje ali statistiko.[1] Člen 17 določa pravico do izbrisa v opredeljenih okoliščinah, tudi kadar podatki niso več potrebni, vendar navaja tudi izjeme, kadar je obdelava potrebna, na primer zaradi zakonske obveznosti, nalog v javnem interesu ali pravnih zahtevkov.[1]

Te določbe niso univerzalni časovnik, ki bi vsaki slovenski organizaciji povedal natančno število let za hrambo posamezne datoteke. Pravno podlago, sektorska pravila, pogodbe, davčne ali računovodske obveznosti, pravila javnih arhivov in okoliščine spora lahko odgovor spremenijo. Praktični zemljevid arhiva naj zato vsebuje polje **retention_basis** in po potrebi osebo, ki ga je odobrila. »Morda bo kdaj uporabno« ni dovolj natančna podlaga.

Dostop naj se spremeni, preden izgine vsaka fizična kopija. Ko se projekt zaključi, lahko Studio Javor odstrani projekt iz običajnega iskanja, prekliče dostop osebju in prepreči, da bi ga pomočnik uporabljal v novih odgovorih. Odstranitev dostopa zmanjša takojšnjo izpostavljenost. Ne pomeni pa, da je bil izvirnik, izpeljan

artefakt ali varnostna kopija že izbrisan. Stanje mora povedati natanko to: **removed from active retrieval; backup expiry pending 2026-06-30**, ne zgolj **deleted**.

Tudi območje omejene hrambe potrebuje namen in varovalo. Če je treba podpisan zapis hraniti zaradi konkretne obveznosti ali zahtevka, ne sme ostati v širokem korpusu za iskanje pomočnika samo zato, ker je nekje še shranjen. Prenesimo ga na ločeno mesto, omejimo dostop, beležimo izjemen priklic in določimo datum pregleda. Izjema hrambe mora zožiti podatke in občinstvo, ne pa ohraniti popolne kopije zaradi udobja.

Brisanje je delovni tok z ločenimi izidi

Zahteva za izbris lahko pride, ker se je projekt končal, ker je oseba uveljavila ustrezno pravico, ker pogodba zahteva vrnitev ali odstranitev ali ker je poteklo notranje pravilo hrambe. Pri sprejemu zahteve določimo prosilca in obseg, ne da bi zbirali nepotrebne nove podatke. »Izbrišite vse o meni« ni vedno tehnično dovolj natančno; organizacija lahko potrebuje projektno oznako, naslov ali drug varen način za iskanje zapisov. Preverjanje identitete mora biti sorazmerno tveganju zahteve.

Nato ustvarimo načrt brisanja, ki sledi zemljevidu sredstev. Pri ozki zahtevi za en zaključen projekt bi lahko bili izidi za Studio Javor takšni:

```
izvirniki / izvlečki
  → odstranimo iz aktivne shrambe
deli / indeksni vnosi
  → izbrišemo; preverimo aktivno iskanje
povzetki / predpomnilniki odgovorov
  → izbrišemo ali pustimo poteči; preverimo predoglede
aktivna dovoljenja
  → prekličemo osebju, integracijam in žetonom
kopija z omejeno hrambo
  → ohranimo le z dokumentirano izjemo
varnostne generacije
  → zapišemo datum prepisovanja; damo izven uporabe
zapis brisanja
  → hranimo metapodatke rezultata po lastnem pravilu
```

Puščice niso obljube, da vsak sistem ponuja vsako operacijo. So točke preverjanja. Oseba, odgovorna za shrambo, mora znati pokazati, katere operacije so se izvedle, katerih plasti ni bilo, katere so v čakanju in zakaj. Neuspešna ponovna gradnja indeksa ali nedostopen tretji obdelovalec sta živi izjemi, ne dokončano brisanje.

Zapisa o brisanju ne zamenjujmo z izvirnimi osebnimi podatki. Majhen zapis z omejenim dostopom lahko vsebuje sklic zahteve, ciljni sistem, datume dejanj, utemeljitev izjeme in potek varnostne kopije. Ne sme hraniti popolne kopije izbrisanega projekta »za revizijo«. Če potrebujemo stabilen žeton za ujemanje, da se izbrisan zapis ne obnovi iz varnostne kopije, ga zasnujmo previdno, dokumentirajmo njegov namen in presodimo, ali je tudi sam osebni podatek. Ta članek ne predpisuje ene same sheme žetona.

Varnostne kopije spremenijo časovnico, ne dolžnosti načrtovanja

Varnostne kopije obstajajo za obnovo po izgubi ali okvari, zato lahko po čiščenju živega sistema vsebujejo zgodovinsko kopijo. Nastali zamik moramo opisati, ne prikriti. Informacijski pooblaščenec Združenega kraljestva v smernicah po UK GDPR navaja, da je treba ob veljavni zahtevi za izbris ukrepati v varnostnih kopijah in živih sistemih; ugotavlja, da lahko podatki v kopiji ostanejo do prepisovanja in poudarja, da morajo biti medtem »izven uporabe«.[3] To je usmeritev regulatorja iz drugega pravnega režima, uporabljena kot primer operativne zasnove, ne kot navedba slovenskega prava.

V registru kopij Studia Javor bi lahko pisalo, da se šifrirani dnevni posnetki hranijo 30 dni. Če je projekt odstranjen iz žive shrambe na dan 0, lahko najnovejša kopija, ki ga vsebuje, ostane do načrtovanega prepisovanja. Običajni uporabniški račun, iskalni proces pomočnika in postopek obnove te kopije v tem času ne smejo dati na voljo za rutinsko delo. Če po brisanju obnovimo varnostno kopijo, postopek obnove potrebuje preverjanje brisanja po obnovi; sicer lahko sistem projekt tiho znova vnese.

Zaupanja vredno stanje loči te dogodke:

Stanje	Pomen	Česar ne pomeni
active access removed	Običajni uporabniki in iskanje ne dosežejo elementa	Element je fizično odsoten povsod

Stanje	Pomen	Česar ne pomeni
live copy deleted	Imenovane aktivne shrambe so opravile odstranitev	Vse kopije in obdelovalci so čisti
backup beyond use	Kopija je omejena do načrtovanega poteka	Danes je bila prepisana
retained under exception	Imenovan, dokumentiran namen še velja	Cel projekt ostane široko izključiv
deletion blocked	Opredeljen sistem ali obdelovalec ni mogel zaključiti	Zahteva je bila tiho opuščena

Varnostna kopija tudi ni samodejno varna metoda brisanja. Trenutni NIST-ov vodnik za sanitizacijo nosilcev opredeli sanitizacijo kot postopek, ki za določeno raven vloženega napora onemogoči dostop do ciljnih podatkov na nosilcu.[2] Besedilo se nanaša na nosilce podatkov in odločitve o sanitizaciji, ne na popoln program skladnosti za osebne podatke. Kljub temu je koristen opomnik: brisanje zapisa v aplikaciji, potek posnetka v oblaku in sanitizacija naprave, ki jo zavržemo, so različni tehnični dogodki z različnimi dokazi.

Če se strojna oprema ponovno uporablja, popravlja ali zavrže, potrebuje odločitev o nosilcu lastni obseg: kateri nosilci, katera metoda, kakšno preverjanje, kdo jo je izvedel in kakšni dokazi ostanejo. Ne pišimo »varno izbrisano«, kadar je bilo edino opaženo dejanje preklic uporabniškega računa.

Povzetki, indeksi in navidezni spomin pomočnika

Izpeljano gradivo odpre težko, a običajno vprašanje: ali lahko povzetek ali indeks še vedno razkrije informacije iz izbrisanega izvirnika? Odgovor je odvisen od sistema. Povzetek lahko ponovi ime, odločitev ali značilno besedno zvezo. Iskalni deli očitno hranijo izbrano besedilo. Vektorska predstavitev sama po sebi morda ni berljiva človeku, vendar je lahko del mehanizma za pridobivanje, povezanega z virom. Varni operativni privzeti pristop je popisati in odstraniti vsak izpeljani element, ki ostaja povezan z izbrisanim virom, nato pa preveriti iskanje.

Preverjanje ne zahteva ponavljanja poizvedb z občutljivim besedilom. Uporabimo odobren skrbniški račun in interni sklic zapisa. Po odstranitvi preverimo, da izvorni identifikator ne vrne nobenega aktivnega rezultata iskanja; pregledamo števila indeksnih vnosov; potrdimo odsotnost ID-ja povzetka; in preverimo, da na novo ustvarjen odgovor nima dovoljene poti do odstranjenega gradiva. Rezultat preverjanja zapišemo, ne da bi izvirno vsebino kopirali v skupno opombo za zagotavljanje kakovosti.

Ne trdimo, da je splošnonamenski model »pozabil« vir samo zato, ker je bil projekt odstranjen iz iskalnega indeksa. Iskalna shramba, predpomnilnik pogovora in naučeni model so ločeni možni mehanizmi. Ta članek obravnava shrambo znanja s popisanimi izvirniki in izpeljanimi gradivi, ne pa zagotovila o odstranitvi informacij iz vsake vrste modela ali zunanje storitve.

Če je vključen ponudnik ali obdelovalec, njegovo dokumentirano ravnanje z brisanjem, hrambo in kopijami spada v zemljevid sredstev in pregled pogodbe.

Tudi predaja obdelovalcu potrebuje enako natančen zapis. Navedimo obdelovalca, račun ali delovni prostor, poslane kategorije podatkov, predvideno operacijo, navodila za vrnitev ali izbris, razpoložljive revizijske dokaze in kontaktno osebo za izjemo. Izjava, da je dobavitelj »skladen z GDPR«, ni zemljevid konkretnega toka. Lastnik mora še vedno vedeti, ali je bila datoteka naložena, ali se je obdržala izpeljana vsebina in kaj dobavitelj po brisanju sporoči.

Ne uporabljajmo splošnega preklica dostopa kot nadomestka za ta zapis. Preklic dostopa zaposlenemu je lahko nujen in pravilen, vendar ne odstrani skupne povezave, integracijskega žetona, izvožene preglednice ali kopije pri dobavitelju. Nasprotno pa omejena kopija zaradi pravne hrambe ne dovoljuje, da celotna ekipa še naprej išče po projektu. Vsako dejanje ima ozek izid. Zemljevid arhiva je uporaben zato, ker te izide ohrani ločene, namesto da bi jih združil pod eno pomirjujočo besedo.

Zahteva ni celotna politika

Dober postopek brisanja se začne veliko prej kot zahteva. Pri zajemu se odločimo, ali je vsak vir primeren za pomočnika, dodamo lastnika vira, označimo občutljivost, izberemo obdobje aktivnega dostopa, navedemo sprožilec pregleda in zabeležimo znane obdelovalce. Ob zaključku najprej odstranimo širok dostop,

obdelamo izbrane plasti, spremljamo kopije in preskusimo vedenje obnove. Pri vsaki izjemi zapišemo natančen razlog, obseg in datum naslednjega pregleda.

Pri izmišljenem Studiu Javor lahko mesečna evalvacija vzorči en zaključen projekt in sledi zemljevidu od izvirnika do registra varnostnih kopij. Pregledovalec preveri: ali je aktivno iskanje blokirano; ali identifikatorji ne kažejo aktivnih indeksnih vnosov; ali so dejanja za povzetek in predpomnilnik zabeležena; ali ima vsaka ohranjena kopija določen razlog in omejen dostop; ter ali register kopij navaja datum prepisovanja. Če je en odgovor neznan, stanje brisanja ni »dokončano«. Gre za izjemo, ki jo je treba rešiti.

Pravica do pozabe ni gumb z oznako »izbriši vesolje«. Tudi zapletenost ni dovoljenje za večno hranjenje vsega. Zasebni arhiv postane bolj zaupanja vreden, ko so vidne njegove plasti, meje dostopa, razlogi hrambe in stanja brisanja. Tako je pomočnik lahko uporaben, ne da bi se pretvarjal, da ena ikona za brisanje uredi vsako kopijo, izjemo in pot obnove.

Viri

Številke virov veljajo za ta vodnik. Povezave vodijo do izvirnih dokumentov. Pred uporabo preverite besedilo, pogoje uporabe in razpoložljivost storitev.

[1] Regulation (EU) 2016/679 (General Data Protection Regulation)
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[2] NIST SP 800-88r2: Guidelines for Media Sanitization
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf

[3] Right to erasure | Information Commissioner's Office
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/