Povjerenje u digitalne repozitorije i njihove procese zaštite e-gradiva

Hrup, Bea

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
SMJER ARHIVISTIKA
Ak. god. 2023./2024.

Bea Hrup

Povjerenje u digitalne repozitorije i njihove procese zaštite e-gradiva

Diplomski rad

Mentor: prof. dr. sc. Hrvoje Stančić

Zagreb, lipanj 2024.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Za moju najveću potporu koja me gleda odozgo.

Sadržaj

1. Uvod

Brze promjene i razvoj informacijske i komunikacijske okoline, sve kompleksnije informatičko okruženje, stvaranje novih normi te novi korisnici i njihovi zahtjevi doprinijeli su stvaranju digitalnih repozitorija. S razvojem digitalnih repozitorija stručnjaci se susreću s mnogim izazovima kako bi zadržali povjerenje zajednica kojima služe. Potrebno je provoditi certifikaciju digitalnih repozitorija te prepoznati norme, preporuke i primjere dobre prakse kako bi se stvorilo povjerenje u mogućnost očuvanja digitalnih zapisa.

Kako bi se steklo povjerenje potreban je decentraliziran, otvoren i transparentan model za osiguravanje porijekla i integriteta digitalnih zapisa. Repozitoriji trebaju očuvati autentične i pouzdane podatke i pritom svojim korisnicima garantirati dugotrajno očuvanje i pristup podacima te održivost. Digitalni repozitoriji zahtijevaju integraciju novih metoda, politika, normi i tehnologija. TRUST (engl. *Transparency, Responsibility, User focus, Sustainability, and Technology*) principi su temelj za provedbu najbolje prakse u digitalnom očuvanju[1]. Načela TRUST-a su sredstvo za olakšavanje komunikacije sa svim dionicima, pružajući repozitorijima smjernice za demonstraciju transparentnosti, odgovornosti, fokusa na korisnike, održivosti i tehnologije. Danas su dostupne mnoge tehnologije koje pomažu u izgradnji povjerenja u proces digitalnog očuvanja i povjerenja digitalne repozitorije općenito.

Potrebno je mnogo resursa za prikupljanje znanstvenih podataka te s takvim podacima treba pažljivo upravljati, čuvati ih i arhivirati kako bi se sačuvala njihova vrijednost za buduću upotrebu. Budući da je certifikacija način kojim se osigurava da repozitoriji budu pouzdani, World Data System (WDS) of the International Science Council (ISC) i Data Seal of Approval (DSA) razvili su CoreTrustSeal certifikaciju koja pruža temeljne zahtjeve koje digitalni repozitoriji od povjerenja[2] moraju ispuniti. Kako bi primili CoreTrustSeal certifikat, repozitoriji moraju predočiti dokaze koji pokazuju da slijede dobre prakse i ispunjavaju određene standarde.

[1] Za engleski termin *digital preservation* u ovom se radu upotrebljava hrvatski termin *digitalno očuvanje*. U stručnoj literaturi još se koristi i termin *očuvanje digitalnih sadržaja*.
[2] Za engleski termin *Trusted Digital Repository, TDR* u ovom se radu s jednakim značenjem upotrebljavaju hrvatski termini *digitalni repozitorij od povjerenja* te *pouzdani digitalni repozitorij*. U stručnoj literaturi još se koristi i termin *vjerodostojni digitalni repozitorij* no taj prijevod više odgovara engleskom terminu *Trustworthy Digital Repository.*

U radu se istražuje mišljenje digitalnih repozitorija o CoreTrustSeal certifikaciji. Istraživanje je usmjereno na percepciju digitalnih repozitorija koji su certificirani, kako bi se bolje razumio utjecaj certifikacije na njihovu vidljivost, prepoznatljivost i općenito djelovanje unutar istraživačke zajednice. Anketa je također istražila percipirane prednosti i izazove koji proizlaze iz stjecanja i održavanja CoreTrustSeal certifikata.

2. E-gradivo i njegovo očuvanje

U suvremeno doba, stvaranje i distribucija digitalnog gradiva postaje sveprisutna pojava. Međutim, zbog osjetljivosti elektroničkog gradiva, njegovo dugoročno očuvanje predstavlja značajan izazov za arhiviste. Neprestani razvoj tehnologije, brze promjene te ograničeno trajanje certifikata koji potvrđuju pouzdanost zapisa, samo su neki od problema s kojima se arhivi susreću prilikom dugoročnog očuvanja gradiva.

U digitalne zapise spadaju digitalizirani zapisi koji su prvobitno bili stvoreni na analognom mediju te zapisi koji su izvorno stvoreni kao digitalni zapisi. Proces digitalizacije u najširem smislu podrazumijeva, prevođenje analognoga signala u digitalni oblik, a u užem smislu, to je pretvorba teksta, slike, zvuka, pokretnih slika ili trodimenzionalnih oblika nekog objekta u digitalni oblik, u pravilu binaran kôd zapisan kao računalna datoteka sa sažimanjem podataka ili bez sažimanja podataka, koji se može obrađivati, pohranjivati ili prenositi računalima i računalnim sustavima.[3] Digitalizacija dijeli pojam očuvanja na dva osnovna cilja - očuvanje informacijskog sadržaja ili informacija zabilježenih u dokumentu i očuvanje fizičkog objekta, odnosno medija koji nosi informaciju. Informacijski sadržaj se digitalizira i sprema odvojeno od fizičkog objekta.[4] Digitalizacija ima mnogo primjena, od profesionalnih, poput korištenja u znanosti, inženjerstvu i medicini, do amaterskih, u koje spada digitalizacija obiteljskih albuma fotografija i slično. Danas se sve veća količina gradiva pohranjuje i distribuira u digitalnom obliku, a na globalnoj razini se ulaže sve više napora kako bi se preostalo analogno gradivo digitaliziralo i time pretvorilo u lako pretraživ i mrežno dostupan digitalni oblik, kojim bi se mogli koristiti svi potencijalni korisnici i istraživači.[5]

Informacijski objekt, u općenitom kontekstu, predstavlja svako gradivo koje pruža informaciju, bilo da je u analognom ili digitalnom obliku, a računala mogu biti samo jedan od načina njegove obrade. Digitalni objekt se odnosi na gradivo nastalo uz pomoć informacijske tehnologije, neovisno o tome je li to njegov izvoran oblik ili je gradivo koje je prethodno bilo zapisano u klasičnom obliku, postupkom digitalizacije, preneseno u digitalni oblik. Pri očuvanju, svaki oblik informacijskog objekta traži različite i specifične pristupe.[6] Digitalni

[3] *Digitalizacija. Hrvatska enciklopedija, mrežno izdanje*. Leksikografski zavod Miroslav Krleža, 2013. – 2024. https://www.enciklopedija.hr/clanak/digitalizacija (pristupljeno 15.5.2024.).
[4] Hrvoje Stančić et al., „Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31) – final report“, *InterPARES Trust*. (2018): 6. http://interparestrust.org/assets/public/dissemination/TRUSTERPreservationModel(EU31)-Finalreportv_1_3.pdf (pristupljeno 15.5.2024.).
[5] *Digitalizacija. Hrvatska enciklopedija, mrežno izdanje*., loc. cit.
[6] Hrvoje Stančić, „Arhivsko gradivo u elektroničkom obliku: mogućnosti zaštite i očuvanja na dulji vremenski rok“, *Arhivski vjesnik* 49, br. 1 (2006): 107-121. https://hrcak.srce.hr/6234 (pristupljeno 15.5.2024.).

objekti sastoje se od tokova bitova, sekvenci 1 i 0, koji zahtijevaju poseban softver i u nekim slučajevima hardver kako bi sadržaj bio razumljiv korisnicima. Digitalni objekti, poput dokumenata za obradu teksta, digitalnih slika, web-mjesta, e-pošte, skupova podataka i drugih, su krhki, lako podložni izmjenama te osjetljivi na zastarjelost i na propadanje podataka.[7] Također, digitalni objekt može se definirati kao osnovna jedinica digitalnog očuvanja koja sadrži sve relevantne informacije potrebne za reprodukciju dokumenata, uključujući metapodatke, tokove bitova i posebne skripte koje upravljaju dinamičkim ponašanjem. Navedeni podaci su inkapsulirani u digitalnom objektu i njima treba upravljati kao cjelinom. Na primjer, ako su dijelovi objekata razbacani po cijelom sustavu pohrane, postaje teško i gotovo nemoguće pratiti sve te dijelove.[8] Digitalni objekti traže stalno održavanje i oslanjaju se na složene sustave hardvera, softvera, normi i zakonskih regulativa koji se kontinuirano ažuriraju ili zamjenjuju. Očuvanje zapisa, tradicionalno, označava očuvanje fizičkog objekta, pri čemu je i sadržaj sačuvan s njim. Međutim, digitalni zapisi ovise o tehnologiji te je za njihovu upotrebu potrebna primjerena kombinacija softverskih i hardverskih rješenja. Time digitalni zapisi više nisu fizički objekti, već postaju rezultat interakcije tehnologije i podataka. Dok god su tehnologija i podaci u interakciji iskustvo objekta će trajati, stoga više osoba može istovremeno pristupiti istom zapisu o imati jednako iskustvo tog zapisa.[9]

Kao sredstvo za bilježenje i omogućavanje pristupa kulturnoj memoriji, digitalna tehnologija nudi brojne prednosti i može pomoći u ublažavanju tradicionalnog sukoba između očuvanja i pristupa. Kada su materijali pohranjeni digitalno, korisnici rade s preciznim izvornicima, primjerice slika, pohranjenim na njihovim lokalnim računalima. Ovaj način odvajanja korištenja od izvornika omogućuje višestruku i simultanu upotrebu jednog izvornika, što nije moguće s materijalima pohranjenim u bilo kojem drugom obliku. Digitalna tehnologija, također, pruža učinkovite načine pristupa. U tekstualnim dokumentima, čitatelj može pronaći potrebne informacije pretraživanjem riječi, kombinacije riječi, izraza ili ideja. Korisnici

[7] Erin Baucom, „A Brief History of Digital Preservation“, *Mansfield Library Faculty Publications.* 31. (2019): 3. https://scholarworks.umt.edu/ml_pubs/31 (pristupljeno 15.5.2024.).
[8] Ronald Jantz i Michael J. Giarlo, „Digital Preservation: Architecture and Technology for Trusted Digital Repositories“ 34, no. 3 (2005): 136. https://doi.org/10.1515/MFIR.2005.135 (pristupljeno 15.5.2024.).
[9] Magdalena Kuleš i Hrvoje Stančić, „Arhiviranje digitalnih zapisa - stanje i perspektive“, *5. kongres hrvatskih arhivista: Arhivi u Hrvatskoj - (retro)perspektiva,* ur. Silvija Babić, (Zadar: Hrvatsko arhivističko društvo, 2017.), 403. https://www.researchgate.net/publication/349647868 (pristupljeno 15.5.2024.).

također mogu prilagoditi prikaz digitalnih materijala, birajući hoće li ih gledati na ekranu, pohraniti na svoje računalo ili vanjski medij, ili ih, pak, ispisati.[10]

Digitalno očuvanje obuhvaća kombinaciju politika i radnih procesa koji omogućuju aktivno upravljanje digitalnim objektima kako bi se osigurala njihova kontinuirana autentičnost i pristup tijekom vremena. Ono uključuje prilično različite metode, vještine i rezultate i može nadopuniti tradicionalne usluge očuvanja, dok istovremeno pruža jedinstvenu i dinamičnu novu upotrebu informacija.[11] Zastarjelost je stalni izazov za stručnjake u području zaštite digitalnih podataka zbog toga što se formati datoteka neprestano ažuriraju, hardverska se oprema konstantno zamjenjuje, a softver postaje zastario. Jedna od uobičajenih strategija za borbu protiv zastarjelosti jest migracija starijih digitalnih objekata u novije formate. Tek nakon eksplozije korištenja osobnih računala i interneta u 1990-ima, te eksponencijalnog porasta broja i vrsta digitalnih objekata, poduzeti su značajni koraci prema sveobuhvatnom pristupu digitalnom očuvanju. Dugoročno očuvanje digitalnih sadržaja i njihovo održavanje je vrlo bitno kako bi ti digitalni objekti ostali dostupni budućim korisnicima.[12]

Digitalno očuvanje je ključna i neophodna komponenta digitalnog arhiviranja koja osigurava dugovječnost elektroničkih objekata unatoč promjenama generacija tehnologija. Uključuje radnje i postupke koji omogućuju tehnički i intelektualni opstanak autentičnih elektroničkih zapisa tijekom vremena, kao što su kontinuirano praćenje, konverzija, migracija i pohrana zapisa, te upravljanje metapodacima koji opisuju podrijetlo zapisa.[13]

Očuvanje digitalnih informacija predstavlja složen problem. Arhivisti, stručnjaci za digitalizaciju i ostali stručnjaci za digitalno očuvanje suočeni su s brzim promjenama u praksi stvaranja zapisa i temeljnoj tehnologiji. Oni se bore s poplavom pristiglog digitalnog gradiva u širokom spektru formata za koje tradicionalne prakse nisu posve prikladne.[14] Dok informacije zapisane na papiru ili drugim trajnim medijima mogu trajati stotinama, pa čak i tisućama godina, informacije kodirane u digitalnom obliku rijetko prežive više od desetljeća ili dva. Razlog tomu je što mediji za digitalnu pohranu poput disketa i CD-ROM-ova brzo gube

[10] Donald J. Waters i John R. Garrett, „Preserving Digital Information. Report of the Task Force on Archiving of Digital Information“, *The Commission on Preservation and Access And The Research Libraries Group* (1996): 2. https://www.clir.org/wp-content/uploads/sites/6/2016/09/pub63watersgarrett.pdf (pristupljeno 18.5.2024.).
[11] Ibid.
[12] Baucom, E., loc. cit.
[13] Marta Mihaljević, Milica Mihaljević, i Hrvoje Stančić, s.v. „digital preservation“, *Arhivistički Rječnik: HRVATSKO-ENGLESKI/ENGLESKO-HRVATSKI* (Zagreb: Zavod za informacijske studije Odsjeka za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu, 2015.), 114.
[14] Robert J. Sandusky, „How recordkeeping ensures trust in digital archives“, *Proceedings of the Association for Information Science and Technology.* ur. S. Erdelez i N.K. Agarwal, (Hoboken, NJ: Wiley. 2017.), 796. https://doi.org/10.1002/pra2.2017.14505401160 (pristupljeno 22.5.2024.).

funkcionalnost i mogu jamčiti točnost zapisanih podataka samo u relativno kratkim razdobljima. Čak i kada su podaci točni, ne postoji garancija da će hardverski i softverski sustavi na kojima su podaci kreirani opstati. Povijest digitalnih sustava obilježena je brzim zastarijevanjem i nedostatkom kompatibilnosti s prethodnim verzijama, a razvoj standarada za kodiranje dokumenata poput HTML-a predstavlja tek djelomično rješenje.[15] Svi digitalni zapisi trebaju ostati vjerodostojni, autentični, potpuni te očuvati dovoljno konteksta tijekom arhiviranja i očuvanja. Zapis je vjerodostojan kada dolazi iz pouzdanog izvora. Da bi bio autentičan, zapis treba sadržavati očuvanu povijest svog nastanka, prijenosa, korištenja i očuvanja tijekom vremena. Kada se zapisu pridruži vrijeme i mjesto nastanka, detalji o korisniku, naslov, predmet i sadržaj, tada se može reći da je zapis potpun. Na kraju, kontekst kojeg valja očuvati, predstavlja međusobne veze između pojedinih zapisa te okolinu u kojoj je zapis stvoren.[16]

Arhiviranje i očuvanje digitalnih zapisa predstavlja jedinstven izazov zbog dugotrajnosti tih aktivnosti. Problem dugotrajnog čuvanja i održavanja digitalnih informacija može se promatrati kao očuvanje zapisa kako bi se spriječila zastarjelost tehnologije na kojoj se temelje. Digitalni objekti zahtijevaju kontinuirano održavanje i ovise o složenom sustavu hardvera, softvera i normi koje se neprestano mijenjaju, dopunjuju ili zamjenjuju. Za razliku od analognih zapisa, digitalni zapisi podložniji su propadanju zbog brzog razvoja informacijske tehnologije. Očuvanje digitalnih zapisa uključuje više od pukog čuvanja računalne datoteke, cilj je omogućiti pristup sadržaju uz osiguravanje očuvanja njegovih ključnih karakteristika.[17]

[15] David M. Levy, „ Heroic measures: reflections on the possibility and purpose of digital preservation“, *Digital libraries 98: the Third ACM Conference on Digital Libraries, June 23-26, 1998, Pittsburgh, PA* (New York: Association for Computing Machinery, 1998,), 152. https://doi.org/10.1145/276675.276692 (pristupljeno 15.5.2024.).
[16] Kuleš, M., Stančić, H., op.cit. 402.
[17] Stančić, H. et al., loc. cit.

3. Povjerenje u institucije

Povjerenje je temeljno, ali istovremeno možda i najmanje shvaćeno svojstvo digitalnih repozitorija koji pohranjuju i čuvaju arhivsko gradivo. To je najvažnija karakteristika digitalnih repozitorija dizajniranih za čuvanje i isporuku arhivskih dokumenata koji imaju trajnu vrijednost za korisnike.[18] Povjerenje se može promatrati kao prihvaćanje, odobrenje ili poštovanje koje se traži ili koje se može dati. Korisnici su ti od kojih se povjerenje traži i oni će kroz istraživanje i osobno iskustvo donijeti konačnu prosudbu o tome je li njihovo povjerenje zasluženo ili ne. Ne samo da korisnici moraju procijeniti vjerodostojnost informacija, već se i pružatelji tih informacija moraju zabrinuti zbog mogućnosti zlouporabe njihovih podataka.[19]

Koncept povjerenja proučavao se u raznim disciplinama poput psihologije, sociologije i ekonomije. Međutim, budući da su istraživači iz različitih područja pristupali pojmu povjerenja kroz svoje disciplinske perspektive, bilo je teško postići potpuni konsenzus o definiciji povjerenja. Ipak, postojali su brojni pokušaji definiranja pojma iz perspektive različitih disciplina.[20] Mayer i suradnici predložili su definiciju povjerenja kao „spremnost jedne strane da bude ranjiva na postupke druge strane na temelju očekivanja da će druga strana izvršiti određenu radnju važnu za povjerenika, bez obzira na sposobnost nadziranja ili kontrole te druge strane.“[21] Slično tomu, Doney i Cannon su definirali povjerenje kao „spremnost na oslanjanje na drugoga.“[22] Rousseau i suradnici su 1998. godine izvijestili da su „očekivanja i spremnost na ranjivost“ bitne komponente svih definicija povjerenja bez obzira na disciplinu i definirali povjerenje kao „psihološko stanje koje uključuje namjeru da se prihvati ranjivost na temelju pozitivnih očekivanja namjere ili ponašanja drugog.“[23] Povjerenje se također može izvesti iz ponovljene interakcije između dvije strane tijekom vremena, što se klasificira kao relacijsko

[18] Devan Donaldson i Paul Conway, „User Conceptions of Trustworthiness for Digital Archival Documents“, *Journal of the Association for Information Science and Technology,* 66. (2015): 2428. https://doi.org/10.1002/asi.23330 (pristupljeno 18.5.2024.).
[19] Adolfo G. Prieto, „From conceptual to perceptual reality: trust in digital repositories“, *Library Review* 58. (2009): 593-594. http:// doi.org/10.1108/00242530910987082 (pristupljeno 18.5.2024.).
[20] Ayoung Yoon, „End users' trust in data repositories: definition and influences on trust development.“ *Arch Sci* 14, (2014): 17-34. https://doi.org/10.1007/s10502-013-9207-8 (pristupljeno 18.5.2024.)
[21] Roger C. Mayer, James H. Davis, i F. David Schoorman, „An Integrative Model of Organizational Trust.“ *The Academy of Management Review* 20, no. 3 (1995): 712. https://doi.org/10.2307/258792. (pristupljeno 20.5.2024.).
[22] Patricia M. Doney, i Joseph P. Cannon, „An Examination of the Nature of Trust in Buyer-Seller Relationships“, *Journal of Marketing* 61, no. 2 (1997): 39. https://doi.org/10.2307/1251829. (pristupljeno 20.5.2024.).
[23] Denise M. Rousseau, Sim B. Sitkin, Ronald S. Burt, i Colin Camerer, „Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust“, *The Academy of Management Review* 23, no. 3 (1998): 395. http://www.jstor.org/stable/259285. (pristupljeno 20.5.2024.).

povjerenje. Na kraju, postoji povjerenje utemeljeno na instituciji, u kojemu je povjerenikov osjećaj sigurnosti baziran na osiguranju strukture, jamstvima, propisima ili pravnim sustavima.[24]

Institucije odgovorne za očuvanje nedigitalnog gradiva već uživaju visoku razinu javnog povjerenja jer su tijekom godina pouzdano sačuvale veliki dio ljudske povijesti. Iako očuvanje digitalnih informacija predstavlja drukčije izazove i zahtijeva nova rješenja, korisnici će vjerojatno imati određenu razinu povjerenja u uspjeh kulturnih institucija, temeljen na njihovim dosadašnjim postignućima. Do sada su arhivi, knjižnice i muzeji pokazali da mogu stvarati i omogućiti pristup digitalnim materijalima. Korisnici sada očekuju da će te institucije nastaviti razvijati sustave koji podržavaju dugoročni pristup gradivu, a institucije će zadržati povjerenje korisnika sve dok osiguravaju pouzdan pristup informacijama. Arhivima, knjižnicama i muzejima su povjereni objekti i gradivo koji dokumentiraju vrijednu kulturnu baštinu. Povjereno im je da očuvaju gradivo za buduće generacije te da pružaju pristup tom gradivu kako bi se dokumentirala i otkrila povijest te poticalo širenje znanja. Kulturne institucije izvrsne su u očuvanju velike količine podataka u obliku fizičkih objekata, no, s obzirom na to da su digitalne informacije i objekti manje opipljivi i mnogo promjenjiviji od drugih materijala, povjerenje i pouzdanost mogu biti teže dokazivi.[25]

Danas se ustanove više ne mogu oslanjati na prethodno dobiveno povjerenje javnosti zbog same institucije. Sada je naglasak na kvalitetnom funkcioniranju ustanove i digitalnog arhiva koji ustanova koristi te je zbog toga vrlo važno stalno unaprjeđivanje procesa unutar ustanova, struktura i sustava koji ih podržavaju, kao i proizvoda tih procesa. Dobro osmišljeni procesi i sustavi za upravljanje i čuvanje gradiva značajno doprinose povećanju pouzdanosti ustanova koje stvaraju gradivo. Vjeruje se da su operacije institucija kvalitetne i dosljedne, a rezultati njihova rada pouzdani i učinkoviti, tek kada javnost stekne visok stupanj povjerenja u te institucije. Na taj način se stvara povjerenje u službeno gradivo koje nastaje u tim institucijama.[26]

Društvu su potrebni arhivi kojima se može vjerovati. Arhivisti očekuju da ih se smatra čuvarima autentičnih zapisa s neupitnom cjelovitošću i nepromjenjivošću, međutim, digitalno

[24] Yoon, A., loc.cit.
[25] „Trusted Digital Repositories: Attributes and Responsibilities“, An *RLG-OCLC* Report (Mountain View, CA: Research Libraries Group, 2002.), 8-9. www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf. (pristupljeno 18.5.2024.).
[26] Arian Rajh, Hrvoje Stančić, Bojan Romčević i Marin Vitaljić, „Koncept rješenja za osiguranje i očuvanje vjerodostojnosti zapisa u upravnim organizacijama prilikom razvoja državnog računalnog oblaka i državnog digitalnog arhiva“, *Arhivski vjesnik* 61, br. 1 (2018): 70. https://hrcak.srce.hr/216936 (pristupljeno 18.5.2024.).

doba dovodi u pitanje tu pretpostavku. Priroda digitalnih zapisa omogućava njihovu laku izmjenu i trenutno širenje. U eri lažnih vijesti, može se reći da javnost ima puno pravo manje vjerovati digitalnim sadržajima. Dok je papirnate zapise vrlo teško izmijeniti bez ostavljanja tragova, stotine digitalnih dokumenata mogu se modificirati u samo nekoliko trenutaka i bez ikakvih tragova. Manipulacija digitalnim sadržajem za stvaranje lažnih dokumenata, fotografija te audio i video zapisa, postala je, u posljednjih nekoliko godina, sve jednostavnija, napose sa sve širom dostupnošću alata umjetne inteligencije (AI). Još jedan problem predstavljaju promjene koje nastaju zbog propadanja digitalnih objekata tijekom vremena, jer formati datoteka postaju zastarjeli i sadržaj se migrira u modernije formate. Ovo je legitimna izmjena digitalnog objekta i dio je standardne arhivske prakse, pri čemu većina arhiva odlučuje zadržati izvorni format zapisa. Ipak, korisnik ne može biti siguran u vjerodostojnost digitalnih zapisa.[27] Tijekom procesa digitalizacije i upravljanja digitalnim izvornicima potrebno je uzeti u obzir sve troškove dugoročnog očuvanja. Ti troškovi ne uključuju samo operativne troškove tehnologije i prostora za pohranu, nego bi trebali uključivati i troškove rada, sigurnosnih kopija, licencija, konverzija formata, ali i nefinancijske utjecaje poput društveno-političkih koristi i rizika te prikladnosti tehnologije. Arhivi bi, kao institucije kojima korisnici tradicionalno vjeruju, trebali nastojati uspostaviti sustave koji mogu prihvatiti i na vjerodostojan način dugotrajno čuvati digitalno gradivo. Uz to, da bi stekli povjerenje, digitalni arhivi moraju se znati uhvatiti u koštac s modernim gradivom i njegovim dugotrajnim očuvanjem, te svojim zaposlenicima osiguravati kontinuirano obrazovanje u skladu s novim tehnologijama kako bi mogli unaprijediti vlastite vještine potrebne za digitalizaciju i očuvanje digitalnog gradiva. Osim toga, postoji i mogućnost da arhivi zaposle već educirane stručnjake koji će implementirati svoja znanja u rad arhiva, do boljeg uključivanja u procese digitalne transformacije te pružanja usluga korisnicima na što višoj razini.[28]

Krajnji korisnici, koji nisu uključeni u stvaranje i održavanje digitalnih objekata koje koriste, vjerojatno su najmanje informirani o procesu stvaranja i očuvanja tih objekata. Zbog toga imaju najveću sumnju oko autentičnosti i pouzdanosti digitalnih objekata. Arhivisti koji brinu o digitalnim sadržajima trebaju krajnjim korisnicima pružiti informacije o autentičnosti i

[27] Alex Green, Mark Bell, John Sheridan, John P. Collomosse, Tu Bui, Alan W. Brown, Jamie Fawcett, Olivier Thereaux and Jeni Tennison, „Using blockchain to engender trust in public digital archives“, *iPRES 2018 15th International Conference on Digital Preservation,* (Boston: 2018.), Green-iPRES-2018.pdf (surrey.ac.uk) (pristupljeno 18.5.2024.).

[28] Hrvoje Stančić, „Digitalizacija i upravljanje digitalnim izvornicima“, *Utjecaj digitalizacije na arhivsku praksu*, ur. Radoslav Zaradić, (Zagreb: Hrvatsko arhivističko društvo, 2023.). 14.,26. https://urn.nsk.hr/urn:nbn:hr:131:583191 (pristupljeno 18.5.2024.)

pouzdanosti tih objekata. Postoje dva potencijalna načina za komunikaciju o pouzdanosti digitalnih objekata s krajnjim korisnicima: prikazivanjem metapodataka o očuvanju koji se odnose na autentičnost i pouzdanost digitalnih objekata ili uporabom znakova ili simbola za označavanje autentičnosti i pouzdanosti digitalnih objekata. Metapodaci o očuvanju mogu biti vrlo složeni i često pružaju detaljnije informacije o samim digitalnim objektima. Stoga znakovi ili simboli koji potvrđuju autentičnost i pouzdanost mogu biti učinkovitiji način komunikacije s krajnjim korisnicima nego prikazivanje metapodataka o očuvanju.[29]

Korisnici imaju povjerenje u arhive, knjižnice i muzeje kada je riječ o tradicionalnom i analognom gradivu, međutim, kada se govori o digitalnom gradivu, institucije i njihovi stručnjaci to povjerenje trebaju zavrijediti. Dolazi do promjene točke kojoj korisnici vjeruju jer se prelazi s koncepta gdje su zaposlenici kulturnih institucija posrednici između korisnika i gradiva na direktan pristup korisnika gradivu. Kako bi korisnici stekli povjerenje u kulturne institucije i njihov način očuvanja e-gradiva, institucije moraju biti transparentne i korisnicima osigurati uvid u to kako je neki izvor nastao te kako je bio očuvan. S obzirom na to da danas bilo tko može postaviti bilo koji podatak bilo gdje na internet, vrlo je bitno da kulturne institucije svojim korisnicima omoguće uvid u podrijetlo i kontekst nastanka gradiva.

[29] Devan Ray Donaldson, „Users' Trust in Trusted Digital Repository Content*", iPRES 2011. 8th International Conference on the Preservation of Digital Objects* (Singapore: 2011.), 20. https://scholarworks.iu.edu/iuswrrest/api/core/bitstreams/2f6d301a-e51d-4793-8b06-3c5b9460c5eb/content (pristupljeno 20.5.2024.).

4. Digitalni repozitoriji od povjerenja

Arhivi, knjižnice i muzeji se, kao tradicionalni čuvari kulturne baštine, aktivno bave metodama i strategijama za očuvanje digitalne građe. To je veliki izazov jer kulturne institucije brzo stvaraju, pretvaraju i dobivaju gradivo u velikom broju različitih formata, od tekstualnih dokumenata do fotografija i elektroničkih zapisa. Kako zbirke rastu, rastu i potrebe povezane s njihovim održavanjem i dugoročnom održivošću. Nužni ishod ovog procesa bio je razvoj digitalnih arhiva i repozitorija. Komisija za očuvanje i pristup (engl. *Commission on Preservation & Access*, CPA) i Research Libraries Group (RLG) su 1994. godine oformile radnu skupinu za arhiviranje digitalnih informacija i započele zajednički rad na opisivanju i istraživanju prirode digitalnih repozitorija od povjerenja (engl. *Trusted Digital Repositories*, TDR).[30]

Izvješće RLG-a o digitalnim repozitorijima od povjerenja pruža temelj i okvir za razumijevanje i primjenu ključnih koncepata digitalnog očuvanja. Koncept „digitalnog repozitorija od povjerenja" temelji se na dva glavna zahtjeva: repozitorij mora imati uspostavljene politike, standarde i tehnološku infrastrukturu koji zajedno omogućuju učinkovito digitalno očuvanje te repozitorij mora biti pouzdan sustav, odnosno sustav softvera i hardvera za koji se može pouzdano očekivati da će slijediti određena pravila i standarde.[31] Predložena definicija za digitalni repozitorij od povjerenja je: „repozitorij čija je misija pružiti pouzdan i dugoročan pristup digitalnim resursima kojima upravlja određenoj zajednici, sada, ali i u budućnosti."[32] Pouzdani digitalni repozitoriji mogu imati različite oblike, neke ustanove mogu odlučiti izgraditi lokalne repozitorije, dok druge mogu odlučiti upravljati logičkim i intelektualnim aspektima repozitorija te ugovoriti s organizacijom treće strane pohranu i održavanje repozitorija.

Glavni nalazi izvješća CPA/RLG iz 1996. uključivali su ove ključne točke[33]:

- Dugoročno očuvanje digitalnih informacija primjereno zahtjevima budućih istraživanja i učenja zahtijevat će složenu infrastrukturu koja može podržati distribuirani sustav digitalnih arhiva.

[30] „Trusted Digital Repositories: Attributes and Responsibilities", op. cit. 1.
[31] Jantz, R., Giarlo, M. J., op. cit. 196.
[32] „Trusted Digital Repositories: Attributes and Responsibilities", op. cit. 5.
[33] Ibid.

- Bitna komponenta infrastrukture digitalnog arhiviranja je postojanje dovoljnog broja pouzdanih organizacija sposobnih za pohranu, migraciju i pružanje pristupa digitalnim zbirkama.
- Potreban je proces certifikacije za digitalne arhive kako bi se stvorila opća klima povjerenja u pogledu očuvanja digitalnih informacija.

Konačno izvješće radne skupine iznijelo je dvije ključne preporuke za očuvanje digitalnih informacija: uključivanje stvaratelja sadržaja u proces digitalnog arhiviranja i uspostavljanje mreže pouzdanih i certificiranih digitalnih arhiva. Prva preporuka tražila je da stvaratelji sadržaja surađuju s arhivistima i upraviteljima zapisa kako bi se očuvali važni atributi digitalnih objekata, uključujući sadržaj, nepromjenjivost, referentni integritet, porijeklo i kontekst, kroz cijeli životni ciklus digitalnog objekta. Ovo predstavlja razliku u pristupu arhiviranju tradicionalnih papirnatih zapisa i elektroničkih zapisa. Dok je rana intervencija bila, i ostaje, važna praksa za upravljanje zapisima, arhivisti su rijetko stupali u interakciju sa stvarateljima sadržaja prije završetka aktivnog vijeka zapisa, ili čak prije nego što su zapisi uopće stvoreni. Druga preporuka naglašava potrebu za certifikacijskim programom za digitalne repozitorije kako bi se osiguralo da repozitoriji budu pouzdani u pohranjivanju i omogućavanju dugoročnog pristupa digitalnim objektima za buduće istraživače. Ova usmjerenost na certifikaciju dovela je do razvoja koncepta digitalnih repozitorija od povjerenja.[34]

Povjerenje igra ključnu ulogu u očuvanju digitalnih sadržaja. Iako institucije poput arhiva, knjižnica i muzeja uživaju povjerenje u vezi s očuvanjem tradicionalnog gradiva, tek trebaju steći povjerenje kada je riječ o očuvanju digitalnih sadržaja. Digitalni repozitorij, koji uključuje takve sadržaje, mora zadovoljiti nekoliko važnih uvjeta kako bi bio vjerodostojan. Svaka institucija koja želi steći povjerenje korisnika u pogledu dugoročnog očuvanja autentičnih digitalnih sadržaja mora: prihvatiti odgovornost za dugoročno očuvanje, zadovoljavati organizacijske i operacijske odgovornosti, dokazati financijsku održivost, imati lako provjerljivu politiku, praksu i provedbu, potom imati organizacijski sustav koji podržava dugoročnu održivost repozitorija te dizajnirati sustave u skladu s prihvaćenim normama, konvencijama i standardima kako bi se osiguralo kontinuirano upravljanje, pristup i sigurnost pohranjenog gradiva te uspostaviti metodologije za evaluaciju sustava koje ispunjavaju očekivanja zajednice u pogledu povjerenja. Institucije stječu povjerenje korisnika ne samo svojim vanjskim karakteristikama i posvećenošću dugoročnom očuvanju autentičnih digitalnih

[34] Baucom, E., op. cit. 5-6.

zapisa, već i praktičnim, unutarnjim karakteristikama sustava za očuvanje. Uspostava elemenata sustava kao što su elektronički potpisi i postojani identifikatori dodatno povećavaju razinu povjerenja korisnika. Primjena koncepta postojanih identifikatora omogućuje pravilno imenovanje i organizaciju očuvanih objekata, čime se osiguravaju aktivnost i nepromjenjivost veza prema izvorima, što je ključno za dugoročno očuvanje i citiranje.[35]

Za očuvanje budućih znanstvenih istraživanja, repozitoriji moraju preuzeti odgovornost za digitalno gradivo na tri razine: razumijevanje vlastitih lokalnih potreba, prepoznavanje podijeljenih odgovornosti s drugim organizacijama te razumijevanje koje odgovornosti mogu biti podijeljene i kako. Digitalno gradivo varira od jednostavnih tekstualnih datoteka do složenih multimedijskih resursa, pri čemu gradivo koje je izvorno nastalo u digitalnom obliku predstavlja veći izazov jer njegova digitalna priroda predstavlja i njegovu informativnu vrijednost. Odluke o očuvanju digitalnih objekata ne smiju se odgađati jer to može rezultirati složenijim i skupljim postupcima, s obzirom na to da su digitalne informacije prolazne i zahtijevaju aktivno upravljanje od samog stvaranja gradiva. Digitalno očuvanje uključuje pravne izazove vezane uz prava na softver i sustave koji se koriste za stvaranje digitalnih datoteka, te odgovornosti za dugoročno očuvanje trebaju biti jasno definirane u licencnim sporazumima. Očuvanje digitalnih objekata zahtijeva stalna financijska ulaganja jer uključuje upravljanje tehnološkim promjenama, standardizaciju resursa i redovite analize. Važno je razumjeti glavne troškove i integrirati ih u postojeću praksu, te osigurati potrebne vještine i znanje za učinkovito očuvanje.[36]

Digitalni repozitoriji od povjerenja mogu se klasificirati kao pouzdani prvenstveno zato što ispunjavaju ili premašuju očekivanja i potrebe zajednica korisnika za koje su dizajnirani. Oni uzimaju u obzir jedinstvenu radnu kulturu i praksu svojih zajednica te su dizajnirani da budu upotrebljiva i vjerodostojna sredstva za širenje informacija. Zajednice korisnika su najvrjednija komponenta u osiguravanju pouzdanosti digitalnog repozitorija. Stoga je važno proučiti njihovu percepciju povjerenja kao čimbenika koji je ključan za uspjeh digitalnih repozitorija. Povećanjem i jačanjem percepcije povjerenja koje imaju zajednice korisnika, koncept i potencijal digitalnog repozitorija od povjerenja postaje sve veći.[37]

---

[35] Hrvoje Stančić, „Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata“, (doktorska disertacija, Filozofski fakultet, Zagreb, 2006.), 162.
[36] „Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources”, An *RLG-OCLC* Report, (Mountain View, CA: Research Libraries Group, 2001.), 18. https://www.oclc.org/content/dam/research/activities/trustedrep/attributes01.pdf (pristupljeno 20.5.2024.).
[37] Prieto, A. G., op. cit. 603.

4.1. Atributi digitalnog repozitorija od povjerenja

Atributi digitalnog repozitorija od povjerenja koji pružaju osnovu za očekivanje pouzdanosti repozitorija. Stručna zajednica smatra da bi ti atributi trebali biti[38]:

1. usklađenost s Referentnim modelom za otvoreni arhivski informacijski sustav (OAIS),
2. Administrativna odgovornost,
3. Organizacijska održivost,
4. Financijska održivost,
5. Tehnološka i proceduralna prikladnost,
6. Sigurnost sustava,
7. Proceduralna odgovornost.

U nastavku se navedeni atributi digitalnog repozitorija od povjerenja detaljnije tumače.

4.1.1. Usklađenost s OAIS modelom

Pouzdani digitalni repozitorij mora osigurati usklađenost cijelog sustava repozitorija s OAIS referentnim modelom. Ovaj model pruža zajednički okvir za opisivanje i usporedbu arhitekture kao i djelovanje digitalnih arhiva, uključujući funkcionalni model i model informacija za stvaranje metapodataka koji podržavaju dugoročno održavanje i pristup. Više riječi o OAIS referentnom modelu bit će u jednom od narednih poglavlja.

4.1.2. Administrativna odgovornost

Administrativna odgovornost podrazumijeva da digitalni repozitorij od povjerenja može dokazati svoju predanost implementaciji normi i najboljih praksi koje utječu na njegovo djelovanje, uključujući fizičko okruženje, procedure sigurnosnih kopija i oporavka te sigurnosne sustave. Također, redovito mora uključivati vanjske stručnjake za validaciju i/ili certificiranje svojih procesa.

[38] „Trusted Digital Repositories: Attributes and Responsibilities“, op. cit. 13-15.

4.1.3. Organizacijska održivost

Organizacije koje žele uspostaviti digitalni repozitoriji od povjerenja, uspostavit će ga na način koji demonstrira njegovu održivost. Njihove misije odražavat će dugoročnu posvećenost očuvanju, upravljanju i pristupu digitalnim kulturnim dobrima. Njihova pravna i poslovna praksa bit će transparentna, a razina stručnosti odgovarajućeg osoblja na visokoj razini.

4.1.4. Financijska održivost

Digitalni repozitorij od povjerenja mora dokazati svoju financijsku održivost tijekom vremena, uz održiv poslovni plan, godišnje preglede poslovanja i financija te primjerene operativne proračune i rezerve.

4.1.5. Tehnološka i proceduralna prikladnost

Digitalni repozitorij od povjerenja mora nabaviti odgovarajući hardver i softver za sve funkcije gradiva, uključujući prihvat, pohranu i pristup. On se mora pridržavati relevantnih normi i najbolje prakse te redovito prolaziti vanjske revizije.

4.1.6. Sigurnost sustava

Sustavi korišteni u radu digitalnog repozitorija od povjerenja moraju biti dizajnirani tako da osiguravaju sigurnost digitalnog gradiva, uz politike i planove za pripremljenost, odgovor i oporavak u slučaju katastrofe, a posebnu pozornost moraju posvetiti integritetu podataka.

4.1.7. Proceduralna odgovornost

Digitalni repozitorij od povjerenja odgovoran je za sve relevantne politike i procedure, koje moraju biti dokumentirane i dostupne na zahtjev. Uspostavljeni mehanizmi nadzora osiguravaju kontinuitet operacija, a strategije očuvanja moraju biti zabilježene i opravdane u kontekstu najbolje prakse.

Odgovornosti digitalnog repozitorija od povjerenja obuhvaćaju prihvaćanje odgovarajućih informacija stvaratelja sadržaja i nositelja prava, stjecanje dovoljne kontrole nad informacijama radi dugoročnog očuvanja, definiranje i razumijevanje svoje ciljane zajednice

korisnika, osiguranje da informacije budu razumljive toj zajednici, praćenje dokumentiranih politika i procedura te omogućavanje pristupa svim sačuvanim informacijama. Ključne točke uključuju pravna pitanja, metapodatke, provjeru autentičnosti, vođenje evidencije, jedinstvenu identifikaciju materijala i stalni pristup. Također, repozitorij treba slijediti norme u stvaranju digitalnih resursa i osigurati kontinuirano praćenje tehnologije i promjena u zajednici. Ove odgovornosti pomažu organizacijama u uspostavi pouzdanih arhivskih usluga, što je ključno u današnjem tehnološkom okruženju.[39]

[39] „Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources", op. cit. 25-34.

5. TRUST principi

Kako je informacijska i komunikacijska tehnologija postala sveprisutna u suvremenom društvu, korisnici sve više ovise o digitalnim podacima i repozitorijima koji omogućuju pristup i korištenje takvih resursa. Repozitoriji moraju zadobiti povjerenje zajednica korisnika kojima namjeravaju služiti te dokazati da su pouzdani i sposobni učinkovito upravljati gradivom koje posjeduju.

Digitalni repozitoriji od povjerenja temelje se na TRUST (engl. *Transparency, Responsibility, User focus, Sustainability, and Technology*) principima. Ovi principi služe kao osnova za implementaciju najboljih praksi u digitalnom očuvanju. Načela TRUST-a su sredstvo za olakšavanje komunikacije sa svim dionicima, pružajući repozitorijima smjernice za demonstraciju transparentnosti, odgovornosti, fokusa na korisnike, održivosti i tehnologije. Digitalni repozitorij od povjerenja koji se temelji na TRUST principima zahtijeva da očuvani podaci budu FAIR (engl. *Findable, Accesssible, Interoperable, and Reusable*). FAIR načela naglašavaju važnost dobre prakse kako bi podaci bili pronalazivi, dostupni, interoperabilni i ponovno iskoristivi. Za ostvarenje ovih ciljeva i dugoročnog očuvanja gradiva, potrebni su pouzdani digitalni repozitoriji s održivim upravljanjem, pouzdanom infrastrukturom i sveobuhvatnim politikama. Digitalni repozitoriji od povjerenja aktivno čuvaju podatke, prilagođavajući se tehnološkim promjenama i zahtjevima korisnika, čime osiguravaju njihovu trajnu vrijednost. Oni trebaju uživati povjerenje korisnika i preuzeti odgovornosti za upravljanje podacima te demonstrirati ključne sposobnosti za omogućavanje pristupa i ponovnu iskoristivost podataka.[40]

Načela TRUST-a su mnemotehnika kojom se podsjeća dionike digitalnih repozitorija na potrebu razvoja i održavanja infrastrukture za poticanje kontinuiranog upravljanja gradivom i osiguravanje buduće uporabljivosti tog gradiva.

5.1. Transparentnost

Kako bi korisnici mogli odabrati najprikladniji repozitorij za svoje korištenje, važno je da mogu lako pronaći i pristupiti informacijama o opsegu, ciljnoj korisničkoj zajednici, politikama i mogućnostima određenog digitalnog repozitorija. Transparentnost u ovim područjima pruža priliku za upoznavanje s repozitorijem i razmatranje njegove prikladnosti za specifične

[40] Dawei Lin, Johnatan Crabtree, Ingrid Dillo, et al., „The TRUST Principles for digital repositories“, *Sci Data* 7, 144. (2020): 1 https://doi.org/10.1038/s41597-020-0486-7 (pristupljeno 20.5.2024.)

zahtjeve korisnika, uključujući pohranjivanje, očuvanje i pronalaženje podataka. Kako bi postigli usklađenost s ovim načelom, repozitoriji bi trebali osigurati da su misija i opseg repozitorija jasno navedeni. Uz to, i sljedeći aspekti trebaju biti transparentno objavljeni:

- uvjeti korištenja repozitorija i pohranjenog gradiva,
- minimalno razdoblje digitalnog očuvanja e-gradiva,
- bilo koje relevantne dodatne značajke ili usluge, na primjer sposobnost odgovornog upravljanja osjetljivim podacima.

Jasno komuniciranje politike repozitorija i posebnih uvjeta njegova korištenja, informiraju korisnike o svim ograničenjima koja mogu utjecati na njihovo korištenje gradiva ili repozitorija. Također, mogućnost jednostavne procjene može li repozitorij odgovorno upravljati osjetljivim podacima, korisnicima može pomoći u odlučivanju hoće li koristiti te dostupne podatkovne usluge.[41]

5.2. Odgovornost

Digitalni repozitoriji od povjerenja preuzimaju odgovornost za upravljanje svojim podatkovnim zbirkama te za služenje svojoj korisničkoj zajednici. Odgovornost se demonstrira kroz: poštivanje metapodatkovnih i standarda za očuvanje, pružanje podatkovnih usluga korisničkoj zajednici, upravljanje pravima intelektualnog vlasništva stvaratelja podataka, zaštitu osjetljivih i klasificiranih podataka te sigurnost sustava i njegovog sadržaja.

Korisnici repozitorija trebaju imati povjerenje da će pružatelji gradiva osigurati sve metapodatke u skladu s normama zajednice, što znatno poboljšava pronalaženje i korisnost gradiva. Repozitorij provjerava integritet dostupnih podataka i metapodataka, što potencijalne korisnike uvjerava da će zbirke podataka vrlo izvjesno biti interoperabilne s drugim relevantnim skupovima podataka. Kako pružatelji usluge digitalnog repozitorija od povjerenja tako i korisnici moraju imati povjerenje u to da će gradivo ostati dostupno tijekom vremena te da se ono može citirati i referencirati u znanstvenim publikacijama.[42]

[41] Ibid. 2-3.
[42] Ibid. 3.

5.3. Fokus na korisnike

Digitalni repozitorij od povjerenja treba biti usmjeren na svoju ciljanu korisničku zajednicu, prilagođavajući se njezinim očekivanjima i potrebama, bez obzira na to što svaka zajednica ima specifične zahtjeve. Repozitoriji trebaju omogućiti svojoj zajednici pronalaženje, istraživanje i razumijevanje podataka. Korisničko iskustvo se može poboljšati tako da repozitoriji potaknu korisnike da potpuno opišu gradivo prilikom njegova pohranjivanja i potaknu ih da daju povratne informacije u slučaju problema s gradivom do kojih može doći nakon što gradivo već bude stavljeno na raspolaganje korisnicima.

Repozitoriji igraju ključnu ulogu u primjeni i provođenju normi korisničke zajednice, olakšavajući interoperabilnost i ponovnu upotrebljivost podataka. To uključuje provedbu metapodatkovnih shema, formata datoteka, kontroliranih rječnika i ontologija. Pouzdani repozitorij može dokazati pridržavanje ovog načela implementacijom i objavljivanjem metrike o korištenju i svojim korisnicima, pružanjem mogućnosti za lakše, jasnije i jednostavnije pronalaženje podataka te praćenjem i prepoznavanjem promjenjivih očekivanja zajednice te odgovaranjem na njih.[43]

5.4. Održivost

Osiguravanje održivosti digitalnog repozitorija od povjerenja nužno je za omogućavanje neprekidnog pristupa njegovim vrijednim podatkovnim zbirkama za sadašnje i buduće korisničke zajednice. Kontinuirani pristup podacima ovisi o sposobnosti repozitorija da pruža usluge tijekom vremena te da odgovori, na promjenjive zahtjeve korisničke zajednice, novim ili poboljšanim uslugama.

Digitalni repozitorij od povjerenja može demonstrirati održivost svojih zbirki kroz: dovoljno planiranje za ublažavanje rizika, kontinuitet poslovanja, oporavak od katastrofe, potom osiguranje financiranja koje omogućuje kontinuiranu upotrebu i održavanje poželjnih svojstava za zaštitu i očuvanje gradiva te osiguranje funkcioniranja upravljanja procesima zaštite e-gradiva i digitalnog očuvanja kako bi podatkovni resursi ostali pretraživi, dostupni i upotrebljivi u budućnosti.[44]

[43] Ibid.
[44] Ibid.

5.5. Tehnologija

Repozitorij ovisi o interakciji ljudi, procesa i tehnologije kako bi podržao sigurne, trajne i pouzdane usluge. Njegove aktivnosti i funkcije podržavaju se softverom, hardverom i tehničkim uslugama. Zajedno, oni pružaju alate za omogućavanje isporuke TRUST principa.

Pouzdani repozitorij može demonstrirati prikladnost svojih tehnoloških sposobnosti putem implementacije relevantnih i primjerenih normi, alata i tehnologija za upravljanje i zaštitu e-gradiva te posjedovanjem planova i mehanizama za detektiranje, sprječavanje i odgovaranje na kibernetičke i fizičke sigurnosne prijetnje.[45]

Sveukupno gledajući, TRUST principi imaju utjecaj na dionike unutar i izvan zajednice korisnika podataka. Kada repozitoriji i stvaratelji podataka prihvate FAIR načela i implementiraju TRUST principe, korisnici repozitorija dobivaju izravnu korist kroz kontinuirane i poboljšane mogućnosti za učinkovito korištenje podataka.

[45] Ibid.

6. Norme i preporuke za digitalne repozitorije

Dugoročno očuvanje digitalnog gradiva, tako da se zadrže i njegove osnovne karakteristike autentičnosti, pouzdanosti, dostupnosti, integriteta i uporabljivosti, zahtjeva oslanjanje na relevantne norme, a uz to, obično, i na nacionalni pravni okvir. Digitalni repozitoriji od povjerenja trebaju pratiti smjernice za upravljanje digitalnim gradivom kako bi osigurali uspješno dugoročno očuvanje i dostupnost gradiva korisnicima.

6.1. ISO 9000

ISO 9000 grupacija normi odnosi se na komponente upravljanja organizacijom i pripadajućim sustavima, a sastoji se od svjetske norme za sustave upravljanja kvalitetom, ISO 9001 i niza pratećih normi o upravljanju kvalitetom. Opisuje osnovne pojmove i načela upravljanja kvalitetom koji se mogu primijeniti na organizacije koje teže trajnom uspjehu te osigurava povjerenje korisnika u sposobnost organizacije da dosljedno isporučuje svoje usluge. Također, pruža smjernice za poboljšanje uspješnosti organizacije kroz usmjerenost na korisnika, vodstvo, procesni pristup, upravljanje odnosima te donošenje odluka na temelju dokaza. Fokus je na osiguravanju trajnog uspjeha organizacije u promjenjivom okruženju, istovremeno pružajući jedinstven temelj za proizvode i usluge organizacije. ISO 9000 grupacija normi se bavi komponentama osiguranja kvalitete unutar organizacije i upravljanja sustavom koje, iako vrijedne, nisu posebno razvijene za procjenu pouzdanosti organizacija koje upravljaju digitalnim repozitorijima.[46]

6.2. ISO/IEC 27002:2022

ISO/IEC 27002 je međunarodna norma koja pruža smjernice, za informacijsku i kibernetičku sigurnost te zaštitu privatnosti, koje je potrebno uspostaviti, implementirati i unaprijediti u sustav organizacije. Nudi najbolju praksu i kontrolne ciljeve za ključne aspekte kibernetičke sigurnosti poput kontrole pristupa, kriptografije, sigurnosti ljudskih resursa i odgovora na incidente. Ova norma služi kao praktičan vodič za organizacije koje žele učinkovito zaštititi svoje informacijske resurse od kibernetičkih prijetnji. Slijedeći smjernice ISO/IEC 27002, organizacija može proaktivno upravljati rizicima kibernetičke sigurnosti i zaštititi kritične

[46] *HRN EN ISO 9000 - Upravljanje kvalitetom,* Hrvatski zavod za norme, https://www.hzn.hr/default.aspx?id=43 (pristupljeno 22.5.2024.).

informacije od neovlaštenog pristupa i gubitka. U digitalnom okruženju koje se brzo mijenja, ISO/IEC 27002 postaje ključan alat za suočavanje s izazovima informacijske sigurnosti, osiguravajući zaštitu osjetljivih podataka i jačanje povjerenja među dionicima, klijentima i partnerima. Implementacija kontrola i smjernica ISO/IEC 27002 norme označava proaktivan pristup sigurnosti informacija, smanjujući rizik od povreda osobnih podataka, neovlaštenog pristupa te potencijalnih financijskih i reputacijskih šteta.[47]

6.3. ISO 15489

ISO 15489 uspostavlja temeljne pojmove i načela za stvaranje, prikupljanje i upravljanje zapisima. Ova se norma primjenjuje na zapise u bilo kojem formatu, strukturi ili tehnološkom okruženju, tijekom vremena. Ona obuhvaća važne aspekte kao što su: zapisi, sustavi zapisa, metapodaci, kontrole, dodijeljene odgovornosti, praćenje, obuka, analiza poslovnog konteksta, identifikacija zahtjeva za zapisima, zapisi i procesi za stvaranje, prikupljanje i upravljanje zapisima.[48] Norma govori kako svaki sustav za upravljanje zapisima mora očuvati autentičnost, pouzdanost, cjelovitost i upotrebljivost zapisa. Naglašava se da sustav mora rutinski prikupljati sve zapise, organizirati ih prema poslovnim procesima, štititi od neovlaštenog pristupa, služiti kao glavni izvor informacija o akcijama, osigurati pristup dokumentima i metapodacima, biti usklađen s poslovnom politikom i zakonima te pokrivati sve poslovne aktivnosti organizacije.[49]

6.4. ISO 14721

ISO 14721:2012 definira referentni model za otvoreni arhivski informacijski sustav (engl. *Open Archival Information System*, OAIS). To je koncepcijski okvir unutrašnje organizacije repozitorija. Prema OAIS referentnom modelu, otvoreni informacijski sustav definiran je kao: „arhiv koji uključuje organizaciju, osoblje i sustave koji su i preuzeli odgovornost da sačuvaju informacije i učine ih dostupnima određenoj zajednici.“[50] OAIS pruža preporuke za

[47] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls* (International Organization for Standardization, 2022). https://www.iso.org/standard/75652.html (pristupljeno 22.5.2024.).
[48] ISO 15489-1:2016, *Information and documentation - Records management*, Part 1: Concepts and principles, (International Organization for Standardization, 2016). https://www.iso.org/standard/62542.html. (pristupljeno 22.5.2024.).
[49] Tomislav Ćepulić, „Međunarodni standard ISO 15489 „Information and documentation - Records management“.“ *Arhivski vjesnik* , br. 44 (2001): 80. https://hrcak.srce.hr/9342 (pristupljeno 22.5.2024).
[50] ISO 14721:2012, *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*, (International Organization for Standardization, 2012). https://www.iso.org/standard/57284.html (pristupljeno 22.5.2024.).

uspostavljanje arhiva koji omogućuju dugoročno očuvanje i pristup informacijama, posebice onim digitalnim. On nudi koherentan i sveobuhvatan okvir načela i terminologije za upravljanje arhivskim informacijskim sustavima. Međutim, sukladnost s referentnim modelom OAIS ne jamči pouzdanost. Za procjenu pouzdanosti potrebno je obratiti pažnju na dodatne elemente spremišta, uključujući odgovarajuće upravljanje, resurse i sigurnost.[51]

Arhivi i repozitoriji koji su organizirani prema OAIS modelu, imaju šest osnovnih zadataka, odnosno odgovornosti[52]:

- pregovaranje o preuzimanju i samo preuzimanje odgovarajućih podataka od stvaratelja,
- ostvarivanje dovoljne razine kontrole nad prethodno preuzetim podacima kako bi se jamčilo očuvanje na dulji period,
- odlučivanje koje zajednice trebaju postati ciljnom korisničkom zajednicom te tako razumjeti podatke koji su isporučeni,
- osiguravanje neovisnosti razumijevanja isporučenih podataka od strane ciljnih zajednica korisnika,
- praćenje dokumentiranih politika i procedura čime se osigurava očuvanje podataka od svih slučajnosti i omogućuje diseminacija informacija kao autentičnih kopija originala, ili onih kopija kojima se original može provjeriti,
- osiguravanje dostupnosti očuvanih podataka ciljnim korisničkim zajednicama.

Usklađivanje s OAIS principima, posebice kroz implementaciju funkcionalnih i informacijskih modela, ključno je za osiguranje dugoročnog očuvanja digitalnih objekata i uspostavu digitalnog repozitorija od povjerenja. OAIS je postao standardni jezik među stručnjacima za digitalnu pohranu, omogućavajući koherentno razumijevanje i primjenu najbolje prakse u različitim profesionalnim kontekstima.

6.5. ISO 16363:2012

ISO 16363:2012 je norma za provjeru i certifikaciju digitalnih repozitorija od povjerenja koji je proizašao iz OAIS norme. Služi kao metoda za ocjenu usklađenosti određenog arhivskog informacijskog sustava s OAIS-om. To je norma, temeljena na dokumentu TRAC (engl. *Trustworthy Repositories Audit & Certification*), koja pruža kriterije za procjenu pouzdanosti digitalnih repozitorija. Ova norma definira zahtjeve i smjernice za osiguranje dugoročne

[51] Dawei, L., Crabtree, J., Dillo, I. et al., op. cit. 2.
[52] ISO 14721:2012, loc. cit.

pohrane digitalnih informacija, uključujući organizacijsku infrastrukturu, upravljanje rizicima, sigurnosne mjere i tehničke kontrole. Cilj joj je omogućiti procjenu i certifikaciju repozitorija kako bi se osigurala njihova sposobnost za trajno očuvanje i pristup digitalnim objektima, čime se povećava povjerenje korisnika i drugih zainteresiranih strana.[53]

Mjerni podaci TRAC-a[54] podijeljeni su u tri kategorije koje ispituju usklađenost s OAIS-om:

- organizacijska infrastruktura - administrativne, kadrovske, financijske i pravne funkcije repozitorija,
- upravljanje digitalnim objektima - rukovanje digitalnim objektima od unosa do pristupa,
- upravljanje infrastrukturnim i sigurnosnim rizicima - tehnologija koja se koristi za rukovanje unesenim objektima.

Arhiv mora zadovoljiti sve navedene kategorije i njihove dijelove prema ovoj normi kako bi dobio oznaku sukladnosti s OAIS-om.

Norme i preporuke igraju ključnu ulogu u osiguranju dugoročnog očuvanja digitalnog gradiva unutar digitalnih repozitorija. One pružaju okvir za standardizirane postupke koji osiguravaju dosljednost, kvalitetu i pouzdanost očuvanja. Primjenom ovih normi, institucije mogu dokazati svoju sposobnost u upravljanju i zaštiti digitalnih objekata, što povećava povjerenje korisnika i stvaratelja sadržaja. Dugoročno očuvanje zahtijeva kontinuiranu prilagodbu i reviziju prakse u skladu s tehnološkim promjenama, a norme i preporuke osiguravaju smjernice za ove prilagodbe. U konačnici, uspostavljanje i pridržavanje ovih normi ključno je za očuvanje digitalnog naslijeđa za buduće generacije.

[53] ISO 16363:2012*, Space data and information transfer systems - Audit and certification of trustworthy digital repositories*, (International Organization for Standardization, 2012). https://www.iso.org/standard/56510.html (pristupljeno 22.5.2024.).
[54] Consultative Committee on Space Data Systems, *Audit and Certification of Trustworthy Digital Repositories: recommended practice* (Washington DC: Consultative Committee on Space Data Systems, 2011). https://doi.org/10.25607/OBP-1451 (pristupljeno 22.5.2024.).

7. Certifikacija

Pouzdanost se dokazuje kroz dokaze koji ovise o transparentnosti, pa stoga repozitoriji, da bi se mogli smatrati vjerodostojnima, moraju pružiti transparentne, poštene i provjerljive dokaze o svojoj praksi. Tako dionici mogu biti sigurni da repozitoriji osiguravaju cjelovitost, autentičnost, točnost, pouzdanost i dostupnost podataka tijekom duljih razdoblja. Pouzdanost nije jednokratno postignuće i ne može se uzeti zdravo za gotovo bez redovite revizije i certifikacije. Rani dokumenti povezani s revizijom i postupkom certifikacije digitalnog repozitorija priznavali su da se status pouzdanosti samo djelomično postiže revizijom. Certifikacija za digitalne repozitorije uključuje puno više od dokumentacije kriterija. Ona mora prepoznati norme i najbolje prakse relevantne za zajednicu repozitorija, kao i one industrije upravljanja informacijama i sigurnosti u cjelini. Drugim riječima, revizija i certifikacija digitalnih repozitorija od povjerenja ne mogu postojati u vakuumu.[55]

Certifikacija daje objektivan i važan doprinos povjerenju različitih dionika u digitalne repozitorije. Kako bi procijenili i poboljšali kvalitetu svoje profesionalne prakse, repozitoriji se oslanjaju na niz međunarodnih certifikacijskih normi koje pokrivaju temeljnu, proširenu ili formalnu razinu certifikacije. Ove norme fokusiraju se na četiri glavna područja procjene: organizaciju, upravljanje digitalnim objektima, tehničku infrastrukturu i upravljanje sigurnosnim rizicima. Norme se razlikuju po broju i složenosti svojih zahtjeva, s intenzitetom procjena te s obzirom na to tko ju i gdje provodi. Postoji unutarnja certifikacija koja može uključivati samoprovjeru ili provjeru koju provodi nadležna unutarnja služba te vanjska certifikacija koju može provoditi recenzentska skupina, neka ustanova na državnoj razini koja ima licencu za izdavanje certifikata ili nezavisna certifikacijska institucija. Odabir mehanizma certificiranja ovisi o potrebi, volji i sposobnosti repozitorija da ulaže u svoju daljnju profesionalizaciju i pouzdanost.[56]

Postoje najmanje dva modela certifikacije. S jedne strane, tu je model revizije koji se koristi, primjerice, za ovjeravanje službenih repozitorija dokumenata tijela državne i javne uprave. Oni su podložni periodičnoj i rigoroznoj inspekciji kako bi se osiguralo da ispunjavaju svoju misiju. S druge strane, postoji model koji djeluje, na primjer, u zajednici za očuvanje. Sudionici tvrde da se pridržavaju normi koje je odgovarajuća agencija potvrdila kao valjane i primjerene, te

[55] Elizabeth Yakel, Ixchel M. Faniel, Adam Kriesberg and Ayoung Yoon, „Trust in Digital Repositories“, *Int. J. Digit. Curation* 8 (2013): 145. https://doi.org/10.2218/IJDC.V8I1.251 (pristupljeno 25.5.2024.).
[56] Dawei, L., Crabtree, J., Dillo, I. et al., loc. cit.

korisnici zatim svojom upotrebom potvrđuju jesu li proizvodi i usluge stvarno u skladu s tim normama.[57]

Godine 1999. stručnjaci su se okupili na Arhivskoj radionici o normama prihvata, identifikacije i certificiranja (engl. *Archival Workshop on Ingest, Identification, and Certification Standards*, AWIICS) kako bi započeli razvoj normi posebno prikladnih za potrebe digitalnih repozitorija. Tijekom rasprave, identificirana su četiri opća pristupa certificiranju[58]:

1. Individualna certifikacija koja se ponekad naziva i certifikacijom osoblja. Tradicionalno, arhivisti su certificirani kombinacijom obrazovanja, stručnog ispita i radnog iskustva. Ne postoji nikakav ekvivalent za elektroničko arhiviranje ili upravljanje digitalnim repozitorijem.
2. Certifikacija arhivskog programa ili ustanove može se postići kombinacijom samoevaluacije, korištenjem standardiziranih popisa za provjeru i kriterija te inspekcije na licu mjestu, tipične za akreditaciju programa.
3. Certifikacija procesa ocjenjuje metode i postupke koji se mogu podvrgnuti kvantitativnim ili kvalitativnim smjernicama za pridržavanje unutarnjim i vanjskim zahtjevima.
4. Certifikacija podataka bavi se postojanošću ili pouzdanošću podataka tijekom vremena i sigurnošću podataka. Certifikacija za postojanost podataka uključuje unutarnju i vanjsku kontrolu kvalitete putem norme kao što je ISO 9000:2000 i priručnika o postupcima. Također obuhvaća dokumentiranje procesa za migraciju podataka, stvaranje i održavanje metapodataka, ažuriranje podataka ili datoteka i provjeru autentičnosti novih kopija. Politike certificiranja javnih ključeva i okviri praksi certificiranja bavili su se sigurnošću podataka, međutim, zbog brzog razvoja e-trgovine, nisu obuhvaćali digitalno arhiviranje. Ovaj okvir, koji se bavi autentifikacijom korisnika i komunikacijom korisnika u transakcijama e-trgovine, rješava pitanja kontrole pristupa za repozitorije i uklanja potrebu za dodatnom certifikacijom sigurnosti podataka.

Predstavnici zainteresiranih zajednica i stručnjaci su bili oni koji trebaju razviti program za certificiranje digitalnih repozitorija od povjerenja. Prvi korak tog procesa je određivanje potrebe za certifikacijskim tijelom jer se neki programi certificiranja temelje na samoprocjeni, dok drugi ovise o procjeniteljima trećih strana. Potrebno je odvagnuti prednosti i nedostatke

[57] Waters D. J., i Garrett, J. R., op. cit. 49.
[58] „Trusted Digital Repositories: Attributes and Responsibilities“, op. cit. 33-34.

oba pristupa i odlučiti koji je najprikladniji. Nakon toga, potrebno je identificirati atribute za mjerenje, analizirati ih i razviti kontrolne liste ili alate za objektivnu procjenu usklađenosti, koristeći primjerice preliminarnu kontrolnu listu. Također, treba se postići dogovor oko učestalosti certifikacije, odnosno koliko dugo certifikacija vrijedi, kao i o vremenskom okviru i povezanim procesima za recertifikaciju. Konačno, potrebno je definirati uvjete za opoziv certifikacije, s obzirom na to da u nekim programima certifikacija automatski istječe nakon određenog razdoblja, odnosno u slučaju da je proces recertifikacije neuspješan. Ovi koraci, kao dio inicijative OAIS, ključni su za osiguranje dugoročne pouzdanosti i sigurnosti digitalnih repozitorija.[59]

Postupak certifikacije odvija se na više razina i može se primijeniti na različite segmente cjelokupnog procesa očuvanja. Ovaj postupak omogućuje ne samo vrednovanje i potvrđivanje kvalitete određenih dijelova procesa, već i postizanje različitih razina certifikacije. Institucija koja želi izgraditi povjerenje korisnika u svoje postupke očuvanja može odlučiti certificirati samo jedan segment svog procesa ili postići određenu razinu kvalitete. Iako bi idealno bilo da sve institucije koje čuvaju elektroničko gradivo postignu najviši stupanj kvalitete u svim segmentima, realnije je očekivati da će se postupno prilagoditi i standardizirati svoje postupke kako bi s vremenom dobile certifikate viših razina.[60]

Postupkom provjere kvalitete za stjecanje certifikata određene razine treba utvrditi koliko institucija koja čuva elektroničko gradivo zadovoljava određene kriterije i zahtjeve. To uključuje ne samo očuvanje elektroničkih objekata, već i provođenje dokumentiranih i propisanih postupaka. Radni dokument „An Audit Checklist for the Certification of Trusted Digital Repositories“ strukturira segmente razvoja u četiri faze: planiranje, propisivanje postupaka, implementacija i procjena kvalitete. Dokument je važan jer opisuje i strukturira elemente za analizu tijekom certifikacije, uključujući organizaciju, funkcije, procese, korisničke skupine i tehnološku infrastrukturu.[61]

[59] „Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources”, op. cit. 16-17.
[60] Stančić, H., „Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata“, op. cit. 181-182.
[61] Ibid. 186.

Certifikacijski program pruža temelj za povjerenje zbog toga što postavlja potrebne kriterije i koristi mehanizme za procjenu i mjerenje. Kulturne institucije certifikacijom mogu dobiti alat za ocjenu postojećih usluga, a repozitoriji jasno definirane najbolje prakse ili norme koje trebaju zadovoljiti kako bi surađivali s kulturnim institucijama. Proces certifikacije stvara povjerenje u institucije koje su prošle certifikaciju, što je od ključne važnosti kako za stvaratelje e-gradiva, tako i za njegove korisnike.

8. CoreTrustSeal

Certifikacija gradi povjerenje među dionicima, jača reputaciju repozitorija i dokazuje pridržavanje dobre prakse. Također pruža mjerilo za usporedbu i pomaže u određivanju snaga i slabosti repozitorija. Samoprocjena je korisna čak i ako repozitorij ne želi aplicirati za certifikaciju, jer omogućuje pregled i poboljšanje unutarnjih procesa. Usvajanje CoreTrustSeal certifikata za digitalne repozitorije od povjerenja služi kao primjer poboljšanja koja su napravljena kako bi se osiguralo da digitalni repozitoriji postignu svojstva TRUST principa. Stjecanje certifikacije i dovršetak revizija mnogih digitalnih repozitorija dokazuje da postoji želja da se repozitoriji percipiraju kao pouzdani.

CoreTrustSeal je neprofitna organizacija koja pruža certifikaciju za digitalne repozitorije od povjerenja. Ova se certifikacija temelji na ujedinjenim zahtjevima kataloga DSA-WDS (engl. Data Seal of Approval - World Data System) koji odražava ključne karakteristike pouzdanih repozitorija. CoreTrustSeal nastao je u rujnu 2017. godine i zamijenio DSA certifikaciju (osnovanu 2009. godine) i WDS certifikaciju (pokrenutu 2011. godine). Proces certifikacije uključuje internu samoprocjenu repozitorija, koju pregledavaju članovi zajednice. Ako je samoprocjena zadovoljavajuća, odbor CoreTrustSeal-a dodjeljuje certifikat koji vrijedi tri godine. Certificirani repozitoriji poboljšavaju kvalitetu i transparentnost svojih procesa, izgrađuju povjerenje korisnika i dionika te slijede najbolje prakse u upravljanju gradivom.[62]

8.1. Zahtjevi CoreTrustSeal-a

Zahtjevi CoreTrustSeal-a[63] opisuju karakteristike potrebne za digitalni repozitorij od povjerenja. Svaki zahtjev prati uputstvo za odgovore i dokaze koje podnositelji moraju pružiti kako bi se omogućila objektivna recenzija te podnositelji moraju odgovoriti na sve zahtjeve. Podnositelj mora naznačiti razinu usklađenosti za svaki zahtjev:

- u tijeku - repozitorij se nalazi u fazi implementacije,
- implementirano - zahtjev je u potpunosti implementiran od strane repozitorija.

Razine usklađenosti su pokazatelj samoprocijenjenog napretka podnositelja, ali recenzenti procjenjuju usklađenost na temelju odgovora i pratećih dokaza. Recenzent može smanjiti

[62] Ingrid Dillo i Lisa de Leeuw, „CoreTrustSeal“, *Mitteilungen Der Vereinigung Österreichischer Bibliothekarinnen Und Bibliothekare* 71, 1. (2018):162-164. https://doi.org/10.31263/voebm.v71i1.1981. (pristupljeno 30.5.2024.).
[63] CoreTrustSeal Standards and Certification Borad, „Coretrustseal Requirements 2023-2025.“ Zenodo, 2022. https://doi.org/10.5281/zenodo.7051012 (pristupljeno 30.5.2024.).

razinu usklađenosti na „u tijeku“ i pružiti objašnjenje podnositelju u povratnoj informaciji. Svi zahtjevi procijenjeni kao „u tijeku“ moraju sadržavati izjavu podnositelja o planiranim radnjama i vremenskim okvirima za postizanje „implementiranog“. Recenzent neće povećati samoprocijenjenu razinu usklađenosti s „u tijeku“ na „implementirano“. Certifikacija može biti odobrena čak i ako su neki zahtjevi „u tijeku“. Prilikom obnove CoreTrustSeal-a, recenzenti će očekivati napredak od „u tijeku“ do „implementirano“ ili jasna objašnjenja zašto to nije moguće.

Odgovori koje pružaju podnositelji moraju biti dokazani javnim poveznicama na web stranice. Konačne verzije uspješnih prijava postaju javni dokumenti. Ova razina transparentnosti važna je jer certifikacijski proces ne uključuje posjet revizora na licu mjesta. Osobe koje čitaju prijave, trebaju moći razumjeti izjave odgovora bez detaljnog čitanja povezanih dokaza. Kada se kao dokaz koriste duži dokumenti ili isti dokaz podržava više od jednog zahtjeva, podnositelj mora jasno navesti koje su relevantne sekcije i citirati informacije u svom odgovoru.

CoreTrustSeal certifikacija vrijedi tri godine od datuma izdavanja certifikata. Organizacija s dobro upravljanim poslovnim procesima i evidencijama trebala bi moći podnijeti ponovnu prijavu s minimalnim izmjenama. Značajnije izmjene mogu biti potrebne ako: organizacija, njezina zbirka podataka, tehnička infrastruktura ili odabrana zajednica dožive značajne promjene ili zahtjevi CoreTrustSeal-a budu ažurirani na načine koji utječu na podnositelja. Zahtjevi CoreTrustSeal-a podliježu pregledu i reviziji svake tri godine, no to ne utječe na uspješnog podnositelja sve dok ne zatraži obnovu.

Trenutno su na snazi zahtjevi od 2023. do 2025. godine, a oni se dijele na 16 zahtjeva raspoređenih u 3 kategorije što se pobliže analizira u nastavku.

8.1.1. Organizacijska infrastruktura

1. Misija i opseg djelovanja: repozitorij ima izričitu misiju omogućiti pristup i sačuvati digitalne objekte.
2. Upravljanje pravima: repozitorij održava sva primjenjiva prava i prati usklađenost s njima.
3. Kontinuitet usluge: repozitorij ima plan za osiguranje stalnog pristupa i očuvanja svojega gradiva i metapodataka.

4. Pravni i etički zahtjevi: repozitorij u najvećoj mogućoj mjeri osigurava da se gradivo i metapodaci stvaraju, čuvaju, čine dostupnima i koristite u skladu s pravnim i etičkim normama.
5. Upravljanje i resursi: repozitorij ima odgovarajuće financiranje i dovoljan broj osoblja kojim se upravlja koristeći jasan i učinkovit sustav upravljanja.
6. Stručnost i smjernice: repozitorij usvaja mehanizme za osiguranje stalne stručnosti, smjernica i povratnih informacija, uključujući unutarnje i vanjske informacije.

8.1.2. Upravljanje digitalnim objektima

7. Podrijetlo i autentičnost: repozitorij jamči autentičnost digitalnih objekata i pruža informacije o podrijetlu.
8. Pohrana i procjena: repozitorij prihvaća gradivo i metapodatke na temelju definiranih kriterija kako bi se osigurala relevantnost i razumljivost za korisnike.
9. Plan očuvanja: repozitorij preuzima odgovornost za dugoročno očuvanje na planski i dokumentiran način.
10. Osiguranje kvalitete: repozitorij se bavi tehničkom kvalitetom i usklađenošću s normama te osigurava da je krajnjim korisnicima dostupno dovoljno informacija za procjenu kvalitete.
11. Tijek rada: upravljanje digitalnim objektima odvija se prema definiranim tijekovima rada, od prihvata pa do pristupa.
12. Pronalaženje i identifikacija: repozitorij omogućuje korisnicima da pronađu digitalne objekte i citiraju ih na postojan i odgovarajući način.
13. Ponovno korištenje: repozitorij omogućuje ponovnu upotrebu digitalnih objekata tijekom vremena, osiguravajući da su dostupne odgovarajuće informacije za njihovo razumijevanje i korištenje.

8.1.3. Informacijska tehnologija i sigurnost

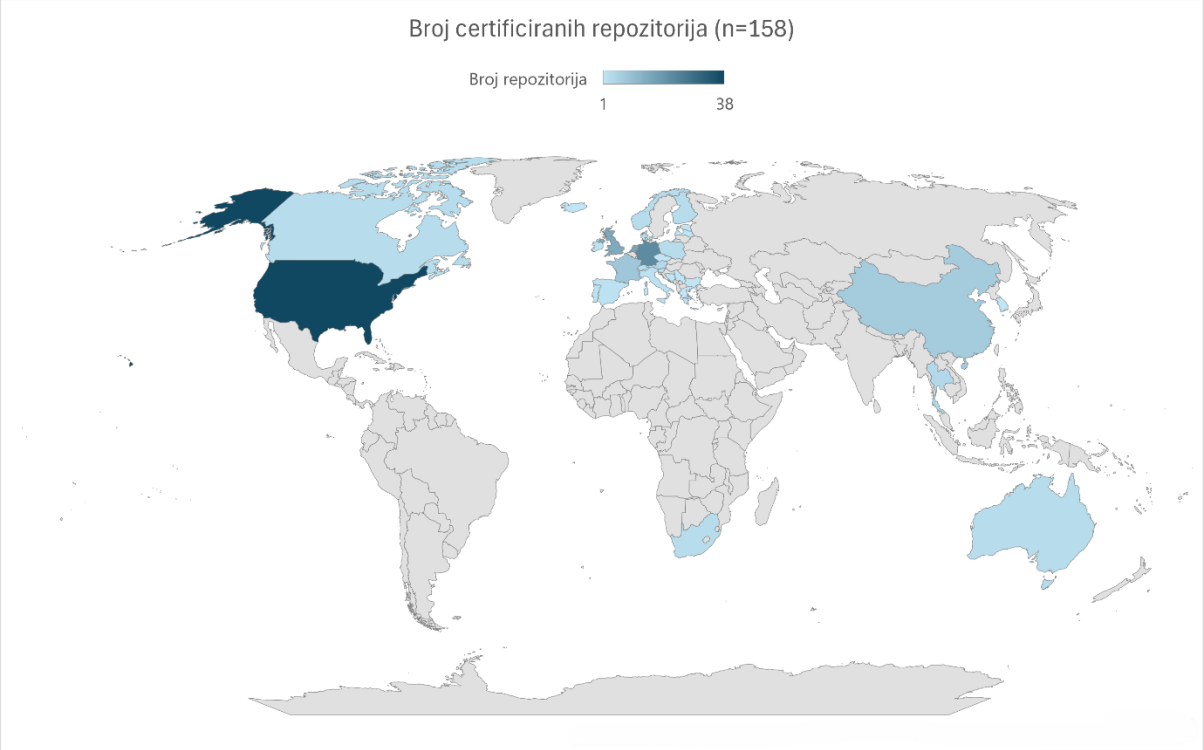
14. Pohrana i integritet: repozitorij primjenjuje dokumentirane procese kako bi osigurao pohranu i cjelovitost gradiva i metapodataka.
15. Tehnička infrastruktura: repozitorijem se upravlja na dobro podržanim operativnim sustavima te softverima i hardverima koji odgovaraju uslugama koje se pružaju zajednici korisnika.
16. Sigurnost: repozitorij štiti objekt i njegovo gradivo, metapodatke, proizvode, usluge i korisnike.

Proces prijave za certifikaciju počinje kada podnositelj prijave preda svoju samoprocjenu, odnosno izjave za svaki zahtjev putem za to namijenjenog obrasca. Svaka izjava mora biti potkrijepljena dokazima. Odbor CoreTrustSeal-a tada dodjeljuje dva neovisna recenzenta iz zajednice nositelja CoreTrustSeal certifikata. Recenzenti preuzimaju odgovornost i time postaju kandidati za izbor u Odbor CoreTrustSeal-a. Komentare i povratne informacije o ocjenama procjenjuje Odbor te se certifikat CoreTrustSeal dodjeljuje u razdoblju od tri godine ili se prijava vraća podnositelju na daljnju doradu i dopunu. Samoprocjene i konačni komentari recenzenata objavljuju se na mreži nakon dodjele CoreTrustSeal-a.[64] Svaki podnositelj plaća naknadu od 3.000 eura kako bi pokrio troškove rada, održavanja i razvoja certifikacijskih usluga. Naknada se od veljače 2024. godine povećala s 1.000 na 3.000 eura. S obzirom na to da je skok u cijeni prilično velik, u bliskoj budućnosti će se moći vidjeti hoće li takav rast cijene imati utjecaja na broj repozitorija koji će se htjeti certificirati ili obnoviti certifikaciju.

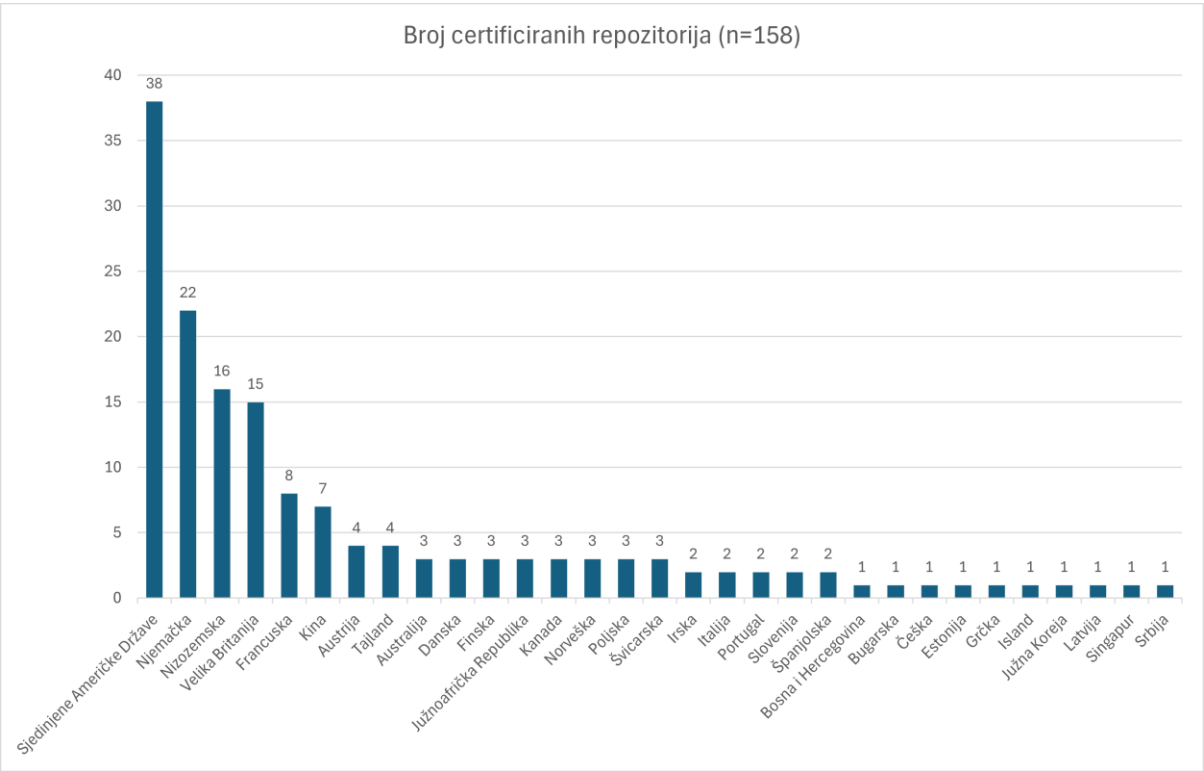
8.2. Repozitoriji s CoreTrustSeal certifikatom

Prema podacima s web stranice CoreTrustSeal-a[65], do svibnja 2024. godine je čak 158 digitalnih repozitorija steklo ovu certifikaciju. Neki su repozitoriji prethodno bili certificirani, ali nakon isteka nisu obnovili certifikat, drugi su obnovili svoj certifikat nakon njegova isteka, a postoje i repozitoriji koji su trenutno certificirani po prvi puta. Svi se ti repozitoriji nalaze u jednoj od 31 različite države. Najveći broj certificiranih repozitorija nalazi se u SAD-u, ukupno njih 38, što predstavlja otprilike 24 % svih digitalnih repozitorija s CoreTrustSeal certifikatom. Slijede Njemačka s 22 repozitorija (14 %), Nizozemska sa 16 repozitorija (10 %) i Velika Britanija s 15 repozitorija (9 %). Grafikon 1 prikazuje kartu svijeta koja ilustrira distribuciju certificiranih repozitorija. Najtamnija boja označava zemlje s najvećim brojem certificiranih repozitorija, pri čemu je SAD na vrhu s 38 repozitorija, dok najsvjetlija boja označava zemlje s najmanjim brojem certificiranih repozitorija, odnosno po jednim repozitorijem. Grafikon 2 prikazuje precizne brojčane podatke o certificiranim repozitorijima po državama. Ovi podaci prikazuju sve repozitorije koji su u nekom trenutku stekli CoreTrustSeal certifikat, neovisno o tome jesu li ga produžili ili ne.

[64] Hervé L'Horus, Mari Kleemola, i Lisa de Leeuw, „CoreTrustSeal: From Academic Collaboration to Sustainable Services“, *IASSIST Quarterly* 43, 1. (2019):8. https://doi.org/10.29173/iq936. (pristupljeno 30.5.2025.).
[65] *CoreTrustSeal certified data repositories*, https://amt.coretrustseal.org/certificates i *Expired CoreTrustSeal data repositories certificates*, https://amt.coretrustseal.org/expired-certificates (pristupljeno 30.5.2024.).

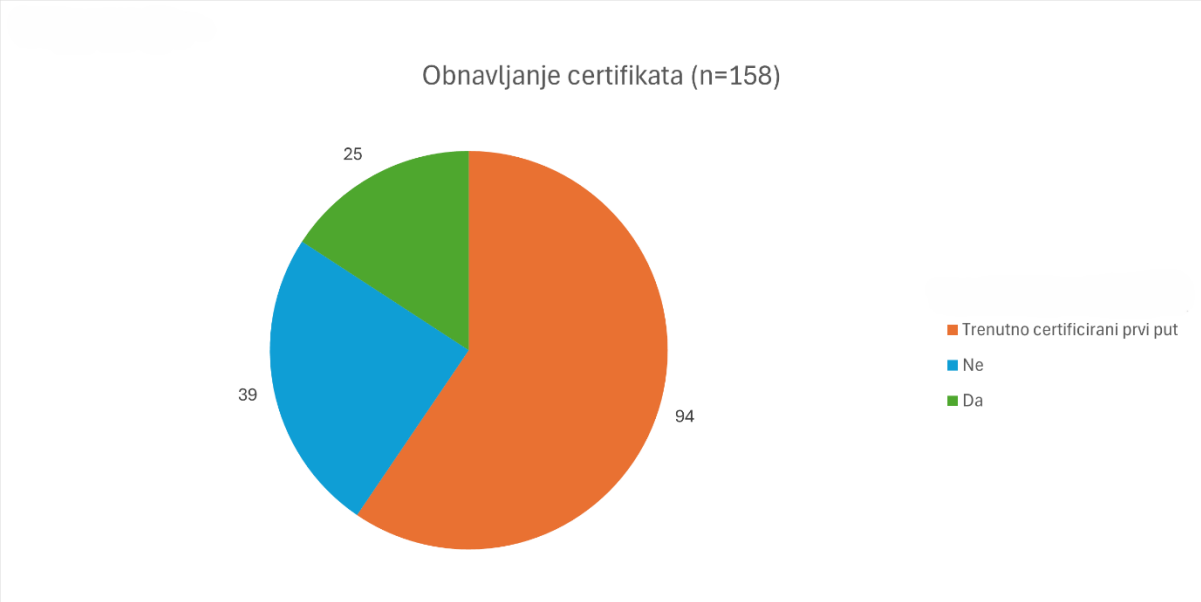


Grafikon 1. Prikaz distribucije repozitorija s CoreTrustSeal certifikatom na karti svijeta



Grafikon 2. Prikaz broja repozitorija s CoreTrustSeal certifikatom za pojedinu državu

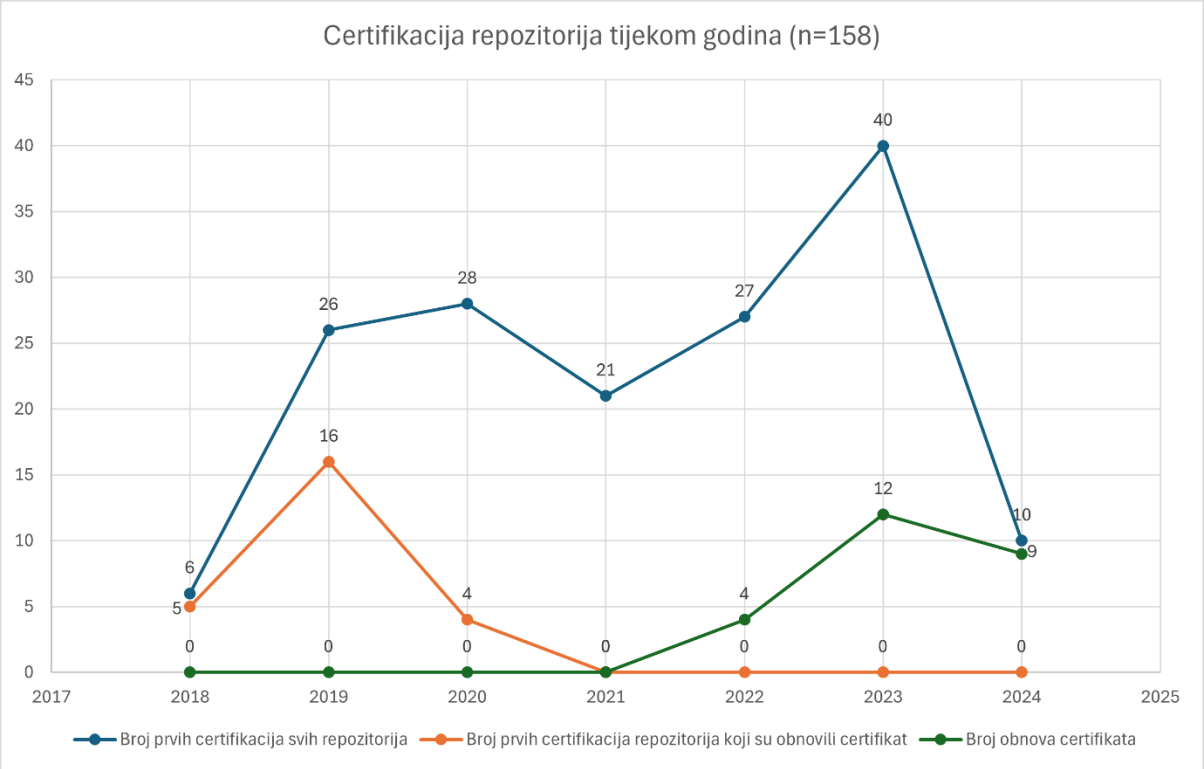
Analiza na grafikonu 3 pokazuje zanimljive trendove što se tiče obnavljanja certifikata. Prikazuju se podaci o repozitorijima koji nisu obnovili certifikat nakon njegova isteka, o onima koji ga jesu obnovili, kao i onima koji su trenutno po prvi puta certificirani. Od ukupno 158 repozitorija, 94 su trenutno certificirana po prvi puta, što čini čak 59% svih repozitorija. Broj repozitorija koji nisu obnovili certifikat iznosi 39, odnosno 25%, dok je 25 repozitorija obnovilo certifikat, što čini 16% ukupnog broja. Ovi podaci potvrđuju sve veći interes repozitorija za stjecanjem certifikacije kako bi stekli povjerenje.



Grafikon 3. Prikaz podataka o obnavljanju CoreTrustSeal certifikata

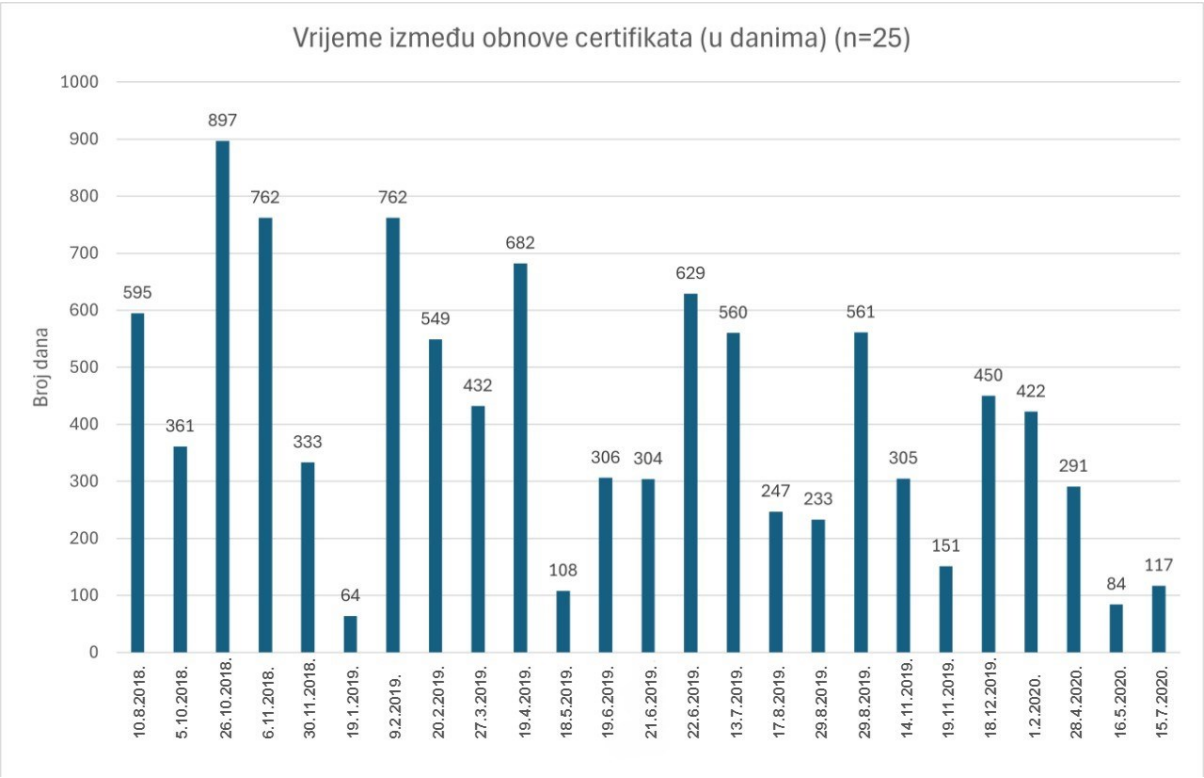
S vremenom se sve više repozitorija odlučuje za stjecanje CoreTrustSeal certifikata, pokazujući rastući trend u broju certificiranih repozitorija kroz godine. Grafikon 4 prikazuje tri krivulje koje ilustriraju ovaj rast. Plava krivulja prikazuje broj svih digitalnih repozitorija koji su po prvi put certificirani tijekom godina, tj. kada je riječ o repozitorijima koji su obnovili svoj certifikat, uključuje samo godine njihove prve certifikacije. Narančasta krivulja, prikazuje broj prvih certifikacija digitalnih repozitorija koji su kasnije obnovili svoje certifikate, a zelena krivulja prikazuje broj obnova certifikata tijekom godina. Dakle, narančasta i zelena krivulja sadrže informacije o 25 repozitorija koji su obnovili svoju CoreTrustSeal certifikaciju. Iz grafikona je vidljivo da je 2021. godine 21 digitalni repozitorij dobio CoreTrustSeal certifikat, a s obzirom na to da su narančasta i zelena krivulja na nuli, moguće je zaključiti da su svi repozitoriji te godine bili certificirani po prvi puta, a nekima od njih certifikati još uvijek traju.

Najveći broj certifikata dodijeljen je 2023. godine, njih čak 52, od kojih je 40 repozitorija certificirano po prvi put, a njih 12 je produžilo svoje prethodno stečene certifikate.



Grafikon 4. Usporedba prvih certifikacija repozitorija i obnova certifikata u periodu od siječnja 2018. do svibnja 2024.

Na kraju pregleda, donosi se prikaz perioda koji je bio potreban za obnavljanje certifikata repozitorija nakon isteka. Kao što je već navedeno (grafikon 3), 25 od 158 repozitorija obnovilo je svoje certifikate. Najduži period koji je prošao između isteka i recertifikacije iznosi 897 dana, što je više od dvije godine, dok je najkraći period iznosio 64 dana. Grafikon 5 prikazuje točan broj dana između isteka i obnove certifikata svih 25 repozitorija koji su to učinili. Podaci u grafikonu prikazani su slijeva nadesno, od repozitorija koji je najranije certificiran pa prema kasnijima, ispod svakog stupca naveden je datum prve certifikacije određenog repozitorija.



Grafikon 5. Prikaz perioda proteklog između isteka i obnove certifikata (u danima)

Vidljivo je da su repozitoriji koji su se kasnije certificirali stekli recertifikaciju u relativno kraćem roku u odnosu na ranije certificirane, međutim prosječan broj dana koji je potreban za recertifikaciju iznosi 408. Stoga se s pravom može postaviti pitanje zašto je tako dugi period potreban za recertifikaciju digitalnih repozitorija. Upravo će istraživanje koje slijedi ponuditi tražene odgovore i objašnjenja.

Svi podaci prezentirani u grafikonima 1 do 5 preuzeti su s mrežnih stranica CoreTrustSeal-a i obuhvaćaju period do 15. travnja 2024. godine. Iako će se podaci tijekom vremena posve sigurno mijenjati, ovi grafovi trenutno pružaju uvid u sadašnje stanje.

9. Istraživanje o CoreTrustSeal Certifikatu za digitalne repozitorije

9.1. Uvod, istraživački izazovi i hipoteze

U digitalnom dobu, repozitoriji igraju ključnu ulogu u očuvanju i širenju znanstvenih i stručnih podataka. Osiguravanje pouzdanosti i vjerodostojnosti ovih repozitorija ključno je za jačanje povjerenja među istraživačima i dionicima. CoreTrustSeal certifikat je međunarodno priznat standard koji procjenjuje pouzdanost digitalnih repozitorija. On pruža transparentan i provjerljiv mehanizam za repozitorije koji tako pokazuju svoju predanost održavanju visokih standarda u upravljanju i očuvanju podataka. U sklopu ovog rada provedeno je istraživanje o CoreTrustSeal certifikatu za digitalne repozitorije sa svrhom procjene utjecaja certifikata na repozitorije koji su ga stekli. U istraživanju se ispituju iskustva certificiranih digitalnih repozitorija, kako bi se razumjelo na koji način je certifikacija utjecala na njihovu vidljivost, prepoznatljivost i cjelokupno djelovanje unutar istraživačke zajednice. Istraživanje koje je provedeno metodom ankete je također, istražilo percipirane prednosti kao i izazove povezane s dobivanjem i održavanjem CoreTrustSeal certifikata.

Izazovi koji se javljaju su sljedeći:

1. Izazovno je izravno mjeriti utjecaj CoreTrustSeal certifikacije na stopu korištenja i pohrane radova u digitalnim repozitorijima zbog utjecaja mnogih istovremenih čimbenika.
2. Iako se smatra da CoreTrustSeal certifikacija poboljšava unutarnje procese i kvalitetu repozitorija, opseg i priroda tih poboljšanja nisu dobro dokumentirani ili univerzalno shvaćeni.
3. Proces CoreTrustSeal certifikacije zahtijeva puno resursa, vremena i sve je skuplji, što može obeshrabriti repozitorije od pokušaja stjecanja ili obnove certifikacije.
4. Unatoč potencijalnim prednostima, postoji nedostatak svijesti i razumijevanja među istraživačima o značaju CoreTrustSeal certifikacije, što može ograničiti njezinu percipiranu vrijednost i utjecaj.
5. Trenutni proces certifikacije smatra se opterećujućim i postoji potreba za učinkovitijim i korisnički prihvatljivijim postupcima, posebno za obnovu certifikacije.

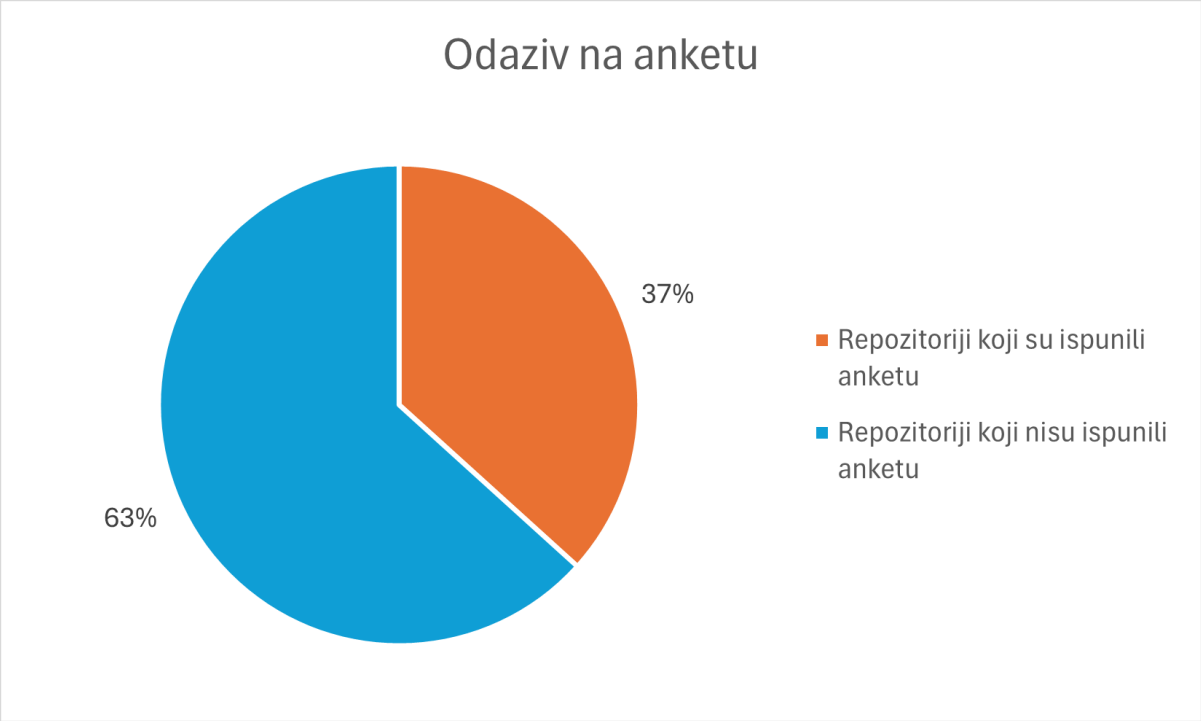
Nadalje, za potrebe istraživanja postavljene su sljedeće hipoteze:

1. Repozitoriji koji aktivno promoviraju svoju CoreTrustSeal certifikaciju imaju veći broj korisnika i pohrana u usporedbi s onima koji to ne čine.
2. Proces dobivanja CoreTrustSeal certifikacije vodi do poboljšanja u formuliranju unutarnjih procesa, dokumentaciji i ukupnoj kvaliteti repozitorija.
3. Zahtjevi za resurse i troškove za CoreTrustSeal certifikaciju su značajna prepreka za repozitorije, što utječe na njihovu odluku da traže ili obnavljaju certifikaciju.
4. Povećana svijest i razumijevanje CoreTrustSeal certifikacije među istraživačima povećava percipiranu vrijednost i značaj certifikacije.
5. Pojednostavljenje procesa CoreTrustSeal certifikacije, posebno procesa obnove, povećava zadovoljstvo procesom i smanjuje radno opterećenje za repozitorije.

Ovi izazovi i hipoteze imaju za cilj istražiti višestruke utjecaje CoreTrustSeal certifikacije na digitalne repozitorije, uključujući korištenje, prijave, unutarnje koristi, troškove, svijest i zadovoljstvo procesom. Istraživanjem ovih područja, pružit će se vrijedni uvidi u mogućnost optimizacije procesa certifikacije i povećanja njegove ukupne vrijednosti za repozitorije.

9.2. Metodologija

Metoda prikupljanja podataka u istraživanju je anketa. Anketa je provedena na engleskom jeziku i poslana na e-mail adrese svih repozitorija koji su zadobili CoreTrustSeal certifikat u cijelom svijetu. Repozitorijima koji na svojim mrežnim stranicama nisu imali navedene e-mail adrese, poziv na istraživanje poslan je putem online obrasca na kojima posjetitelji mogu ostavljati svoja pitanja. Anketa je poslana na sveukupno preko 350 e-mail adresa i 25 online obrazaca. Istraživanje je provedeno u periodu od 20. travnja do 15. svibnja 2024. godine, a za anketiranje se koristio Jotform, s pomoću kojeg su prikupljeni odgovori na pitanja. Ispitanicima je zajamčena anonimnost te da će se njihovi odgovori koristiti samo u svrhu izrade diplomskog rada te im je omogućeno da, ako žele, nakon istraživanja dobiju njegove sastavljene rezultate. Na anketu je odgovorilo 58 digitalnih repozitorija što predstavlja 37% od ukupnog broja digitalnih repozitorija koji su stekli CoreTrustSeal certifikaciju, pa se može zaključiti da je uzorak relevantan (grafikon 6).



Grafikon 6. Razdioba ispitanika koji su ispunili anketu i onih koji to nisu učinili

Anketa se sastojala od 14 pitanja i potpitanja, koja uključuju pitanja otvorenog tipa, pitanja s ponuđenim odgovorima koji se mogu izabrati te pitanja čiji se odgovori temelje na Likertovoj ljestvici s pet stupnjeva slaganja.

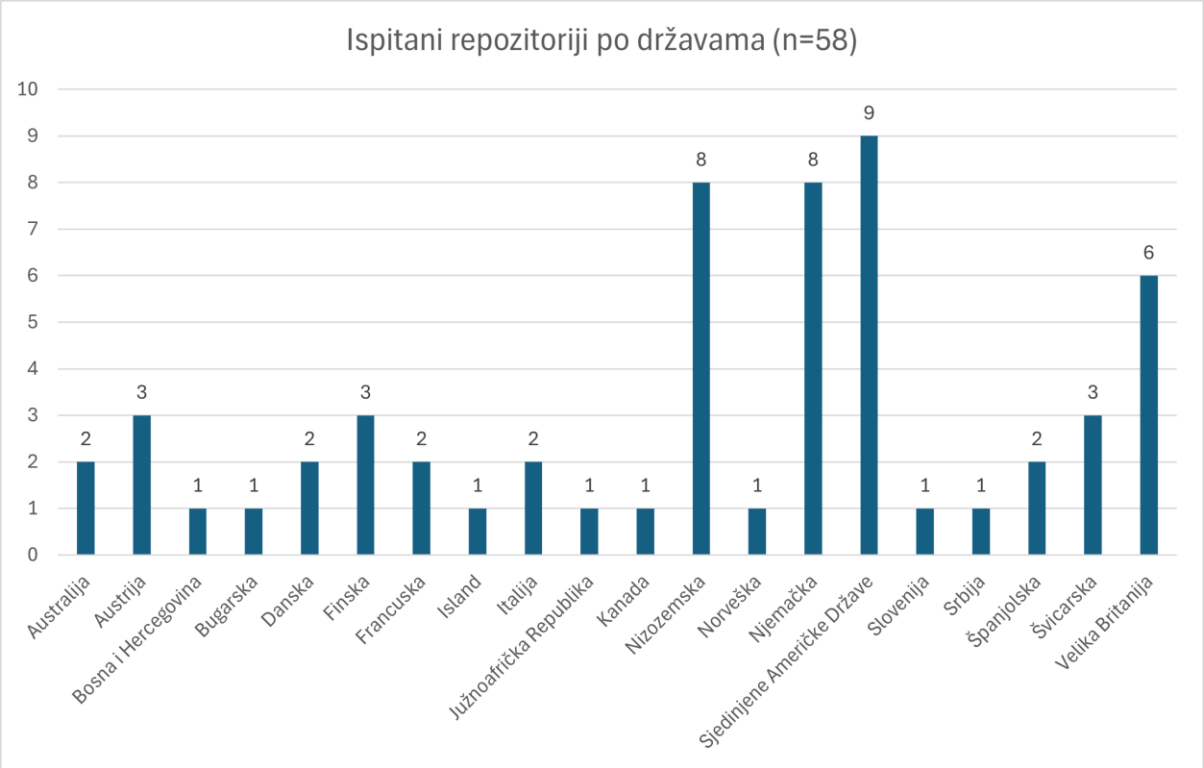
Prema Jotform analitici, može se vidjeti da je anketa imala 434 pregleda, a svi su ispitanici odgovarali na računalu koristeći pritom razne preglednike (Chrome, Firefox, Edge, Safari) i platforme (Mac OS X 10, Windows 10, Linux, Ubuntu). Prosječno vrijeme od pristupanja stranici ankete do njezina zatvaranja iznosi 58 minuta.

9.3. Rezultati

Rezultati ovog istraživanja pružaju vrijedan uvid u učinkovitost CoreTrustSeal certifikata i njegovu ulogu u jačanju vjerodostojnosti i pouzdanosti digitalnih repozitorija. U sljedećim odjeljcima predstavljaju se rezultati ankete, nudeći detaljnu analizu odgovora i ističući ključne trendove i zapažanja.

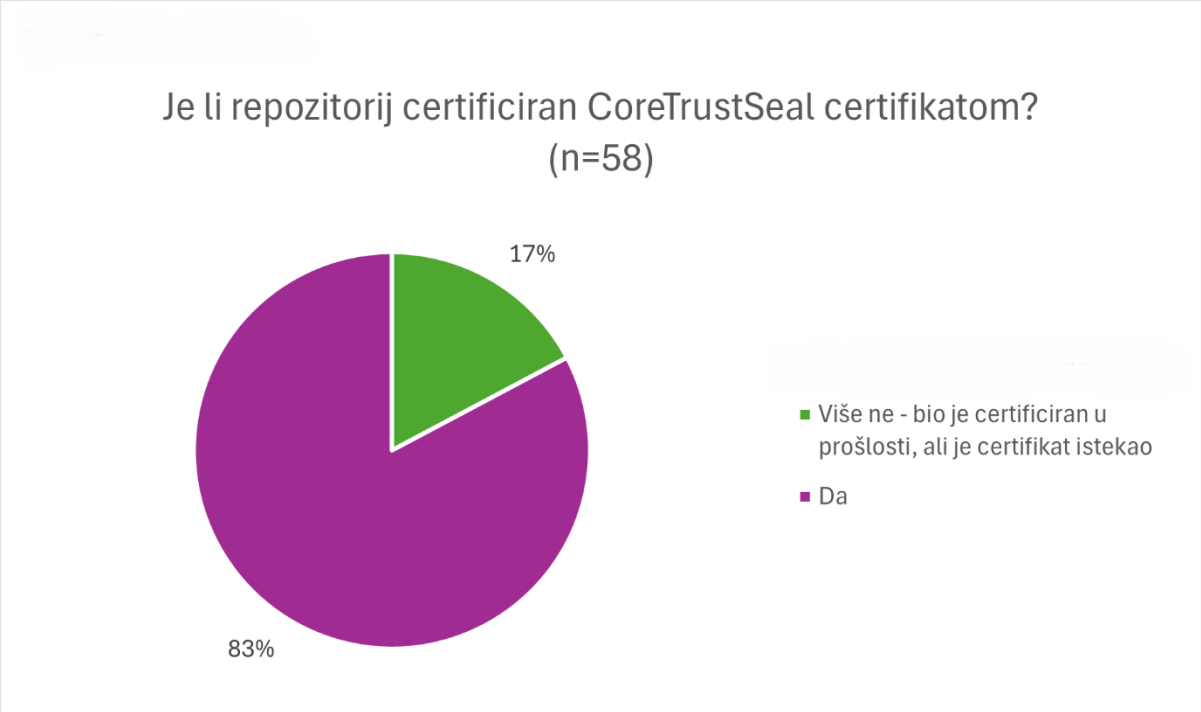
Kao što je već navedeno u ispitivanju je sudjelovalo 58 repozitorija koji su stekli CoreTrustSeal certifikat. Međutim, dva od tih repozitorija su anketu ispunili dva puta, što znači da je zabilježeno 60 odgovora na anketu. Odgovori tih repozitorija su se međusobno većinski

podudarali, ali tijekom analize podataka bit će napomenuto u kojim slučajevima je došlo do razlika. Najviše repozitorija koji su odgovorili na anketu bilo je iz SAD-a, njih devet (16%), slijede Nizozemska i Njemačka, svaka s po osam repozitorija (14%), a nakon njih dolazi Velika Britanija sa šest repozitorija (10%). U Austriji, Finskoj i Švicarskoj po tri repozitorija (5%) ispunila su ankete, a u Australiji, Danskoj, Francuskoj, Italiji i Španjolskoj taj je broj repozitorija iznosio dva (3%). Na kraju, po jedan repozitorij (2%) iz sljedećih država je sudjelovao u anketi, to su: Bosna i Hercegovina, Bugarska, Island, Južnoafrička Republika, Kanada, Norveška, Slovenija i Srbija. Prikaz ispitanih repozitorija može se iščitati na grafikonu 7.



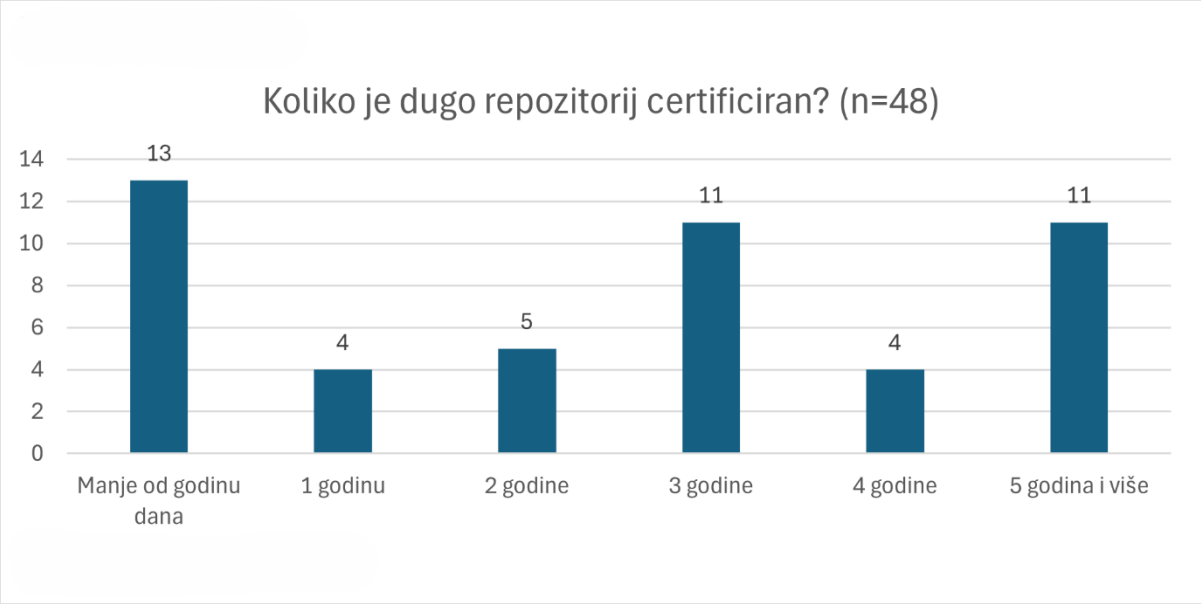
Grafikon 7. Prikaz broja repozitorija koji su sudjelovali u istraživanju po geografskoj lokaciji

Prvo pitanje bitno za analizu odnosi se na to je li repozitorij trenutno certificiran ili je u prošlosti bio certificiran, ali je certifikat istekao. Odgovori pokazuju da je 48 ispitanih repozitorija (83%) trenutno certificirano, a njih 10 (17%) je steklo certifikat u prošlosti, ali trenutno nisu certificirani jer je certifikat istekao (grafikon 8).

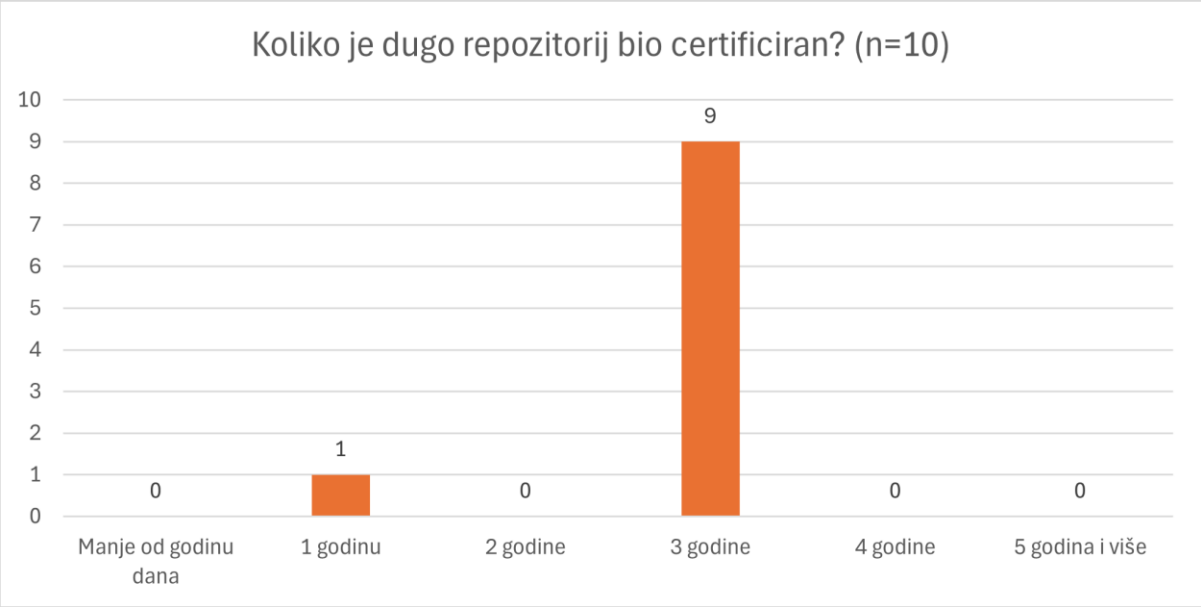


Grafikon 8. Prikaz postotka repozitorija koji su trenutno certificirani i onih kojima je certifikat istekao

Repozitorijima koji su trenutno certificirani postavljeno je pitanje o tome koliko dugo su certificirani. Ponuđeni odgovori koji su repozitoriji mogli odabrati su: manje od jedne godine, 1 godinu, 2 godine, 3 godine, 4 godine te 5 i više godina. Grafikon 9 prikazuje tu raspodjelu iz koje se može vidjeti da najveći broj ispitanih repozitorija certifikat ima manje od godinu dana, to je 13 repozitorija (27%). Godinu dana je trajanje certifikata za 4 repozitorija (8%), dok njih 5 (10%) certifikat posjeduje dvije godine. Broj repozitorija koji certifikat imaju tri godine je 11 (23%), broj onih koji su certificirani četiri godine je 4 (8%), te na kraju, broj repozitorija koji certifikat imaju pet godina ili duže od pet godina iznosi 11 (23%). Neki od repozitorija koji su odgovorili da su certificirani duže od pet godina, u taj period su uključili i Data Seal of Approval certifikaciju koja je bila preteča CoreTrustSeal-a. Isto pitanje o trajanju certifikacije postavljeno je i repozitorijima kojima je certifikat istekao. Pitanje je glasilo koliko je dugo certifikat trajao u prošlosti, a ponuđeni odgovori bili su identični. Rezultati pokazuju da je, od deset ispitanih repozitorija, samo jedan (10%) imao certifikat koji je trajao godinu dana, dok je devet (90%) bilo certificirano tri godine, što je standardno trajanje CoreTrustSeal certifikacije (grafikon 10). Razlog zašto je jedan repozitorij bio certificiran samo jednu godinu, umjesto standardne tri, nije utvrđen provedenom anketom.



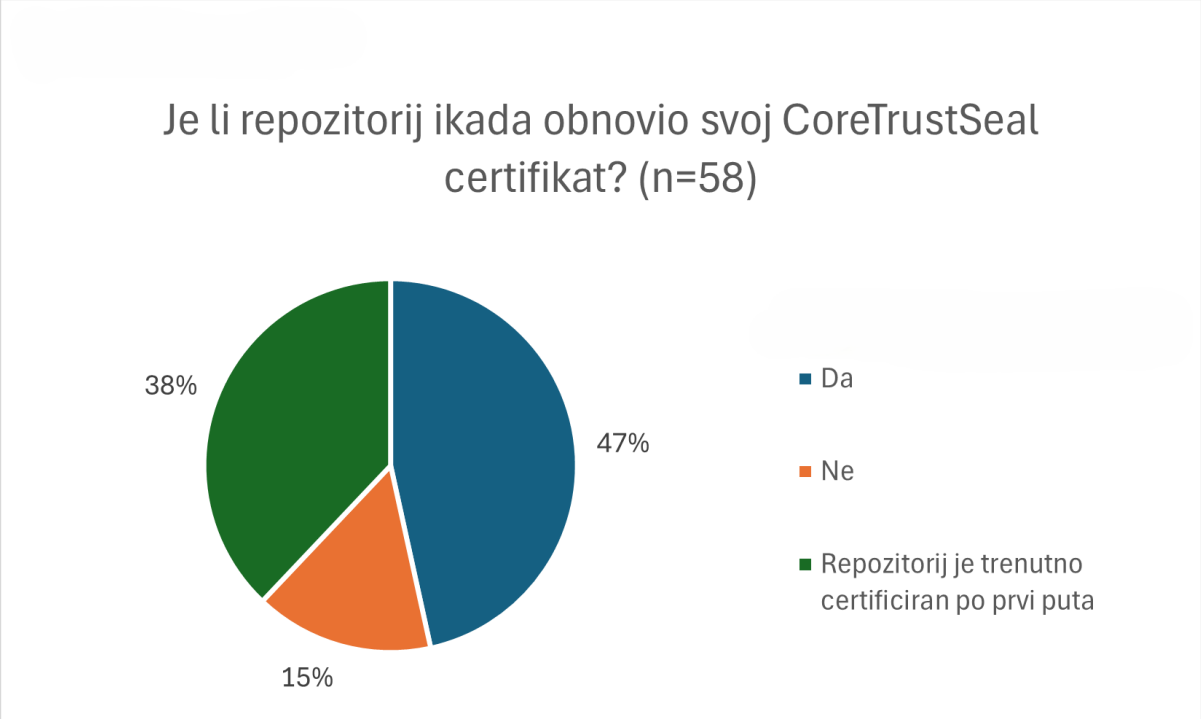
Grafikon 9. Prikaz broja trenutno certificiranih repozitorija po godinama posjedovanja certifikata



Grafikon 10. Prikaz broja repozitorija kojima je certifikat istekao i nisu ga obnovili po godinama posjedovanja certifikata

Sljedeće pitanje o obnovi certifikacije bilo je upućeno svim ispitanicima. Pitalo se jesu li repozitoriji ikada obnovili svoj certifikat, s ponuđenim odgovorima: da, ne, i repozitorij je trenutno certificiran po prvi puta. Prema odgovorima prikazanim u grafikonu 11, najveći broj

ispitanih repozitorija obnovio je svoj CoreTrustSeal certifikat, njih ukupno 27 (48%). Broj repozitorija koji nisu obnovili certifikat iznosi 9 (15%), dok je 22 ispitana repozitorija (38%) izjavilo da su trenutno prvi puta certificirani, pa tako još nisu ni imali priliku obnoviti certifikaciju. Ovdje može doći do odstupanja u uzorku budući da su dva repozitorija navela da nisu obnovili certifikat, ali iz ostalih odgovora može se pretpostaviti da su to repozitoriji koji su trenutno po prvi puta certificirani.



Grafikon 11. Razdioba repozitorija prema obnovi certifikata

Repozitoriji koji su obnovili certifikaciju bili su ispitani o glavnim razlozima obnove. Najveći broj repozitorija naveo je kao razloge recertifikacije želju za demonstriranjem kontinuirane predanosti u održavanju visokih standarda pouzdanosti i povjerenja te povećanju povjerenja i sigurnosti među trenutnim i potencijalnim korisnicima. Dodatni razlozi uključuju osiguranje stalnog usklađivanja s razvijajućim najboljim standardima u upravljanju podacima, kao i nastavak uživanja u vidljivosti i prepoznatljivosti povezanoj s CoreTrustSeal certifikatom. Neki odgovori su, također, istaknuli važnost održavanja konkurentnosti i vidljivosti unutar šire istraživačke zajednice, dok je jedan odgovor naglasio pristup mogućnostima financiranja ili institucionalne podrške vezanim uz održavanje statusa certifikacije. Nekoliko je ispitanih repozitorija dio CLARIN-a (Common Language Resources and Technology Infrastructure), europske istraživačke infrastrukture koja je usmjerena na pružanje jezičnih resursa i tehnologija

istraživačima u humanističkim i društvenim znanostima. Glavni ciljevi CLARIN-a su omogućavanje jednostavnog pristupa velikim količinama digitalnih jezičnih podataka i alata za njihovu obradu te poticanje na njihovu uporabu u istraživačkim projektima. Zbog toga je CLARIN za neke svoje repozitorije uveo obvezu CoreTrustSeal certifikacije. Neki od anketiranih repozitorija su kao razlog za obnovu certifikacije naveli ovaj obavezni zahtjev CLARIN-a.

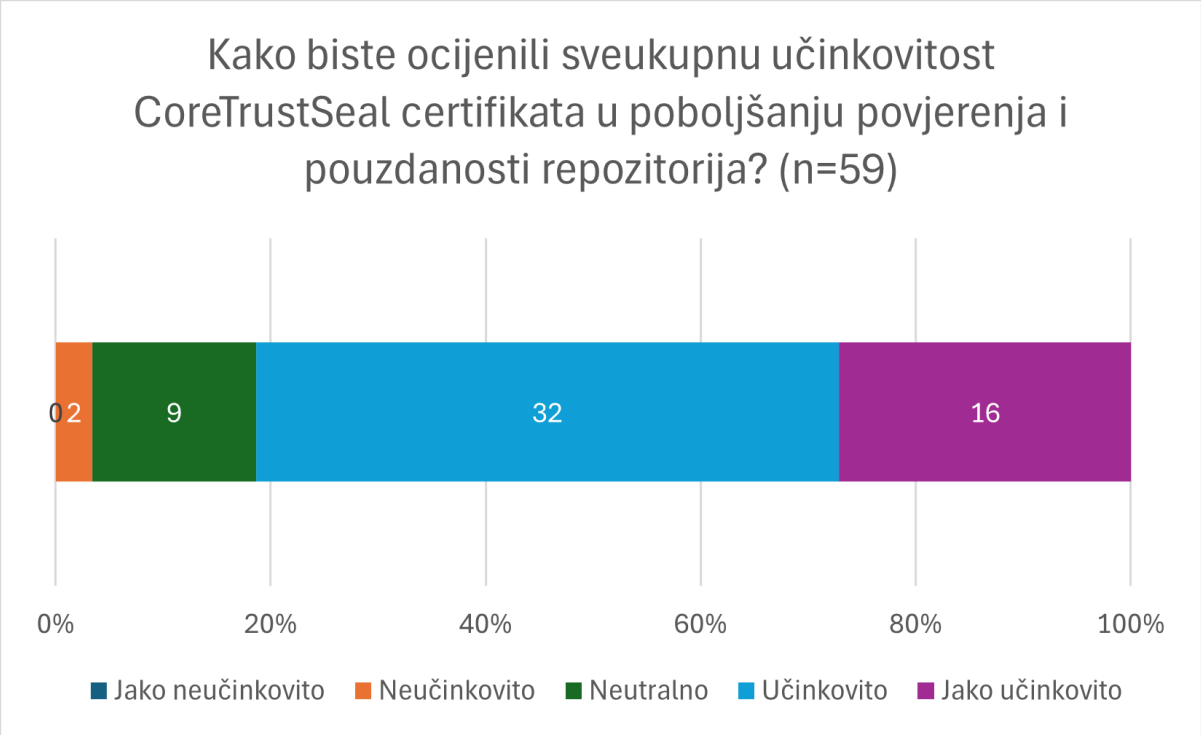
Repozitorijima koji nisu obnovili svoje certifikate postavljeno je pitanje o glavnim razlozima za takvu odluku. Većina je repozitorija, njih pet, izjavila je da su trenutno u procesu recertifikacije. Ostali razlozi uključuju percepciju nedostatka značajnih koristi od održavanja CoreTrustSeal certifikacije, financijska ograničenja ili nedostatak resursa za proces obnove, promjene u osoblju odgovornom za upravljanje zahtjevima certifikacije te percepciju da je početna certifikacija adekvatno ispunila potrebe i ciljeve repozitorija. Dva repozitorija su navela da su im certifikati još uvijek važeći, što sugerira da su u prethodnom pitanju dali pogrešan odgovor vezan za obnovu certifikata, jer su umjesto da navedu da su trenutno prvi put certificirani, izjavili da nisu obnavljali svoje certifikate.

Repozitorijima koji su trenutno certificirani po prvi put, postavljeno je dodatno pitanje o tomu imaju li nakanu obnoviti svoju certifikaciju kada ona istekne, odgovor je bio jednoglasno potvrdan (grafikon 12).

Grafikon 12. Prikaz repozitorija koji imaju nakanu obnoviti CoreTrustSeal certifikat

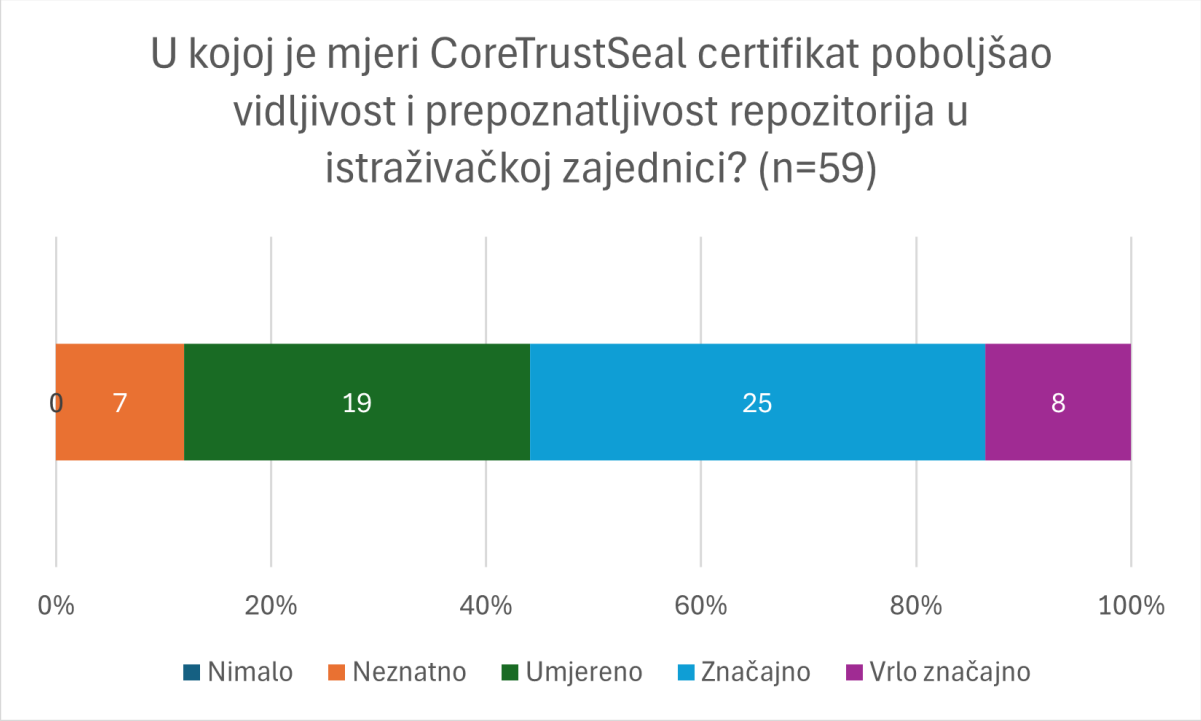
Iduća su pitanja oblikovana prema Likertovoj ljestvici. Ispitanici su na pitanja odgovarali s ocjenama od 1 do 5, pri čemu broj 1 označava najnižu, a 5 najvišu razinu. U ovom dijelu istraživanja primijećene su razlike u ocjenama kod prethodno spomenuta dva repozitorija koja su anketu ispunili dva puta. Kako bi se analizirali odgovori na pitanja za koje nije bilo moguće dobiti cjelobrojnu ocjenu nakon izračunavanja prosjeka, dodani su odgovori oba ispitanika koji su sudjelovali u anketi. Kao rezultat toga, za analizu ovih pitanja ukupan broj ispitanika povećan je na 59.

Prvo je pitanje bilo ocjenjivanje sveukupne učinkovitosti CoreTrustSeal certifikata u poboljšanju povjerenja i pouzdanosti certificiranog repozitorija. Većina je repozitorija, njih 32, ocijenila certifikaciju učinkovitom (ocjena 4), a 16 repozitorija ju je označilo jako učinkovitom (ocjena 5). Devet repozitorija je ostalo neutralno (ocjena 3), dva repozitorija ocijenila su certifikaciju neučinkovitom (ocjena 2), a niti jedan repozitorij nije ju smatrao jako neučinkovitom (ocjena 1) (grafikon 13). Analizirajući odgovore, može se zaključiti kako je CoreTrustSeal dominantno učinkovit u poboljšanju povjerenja i pouzdanosti.



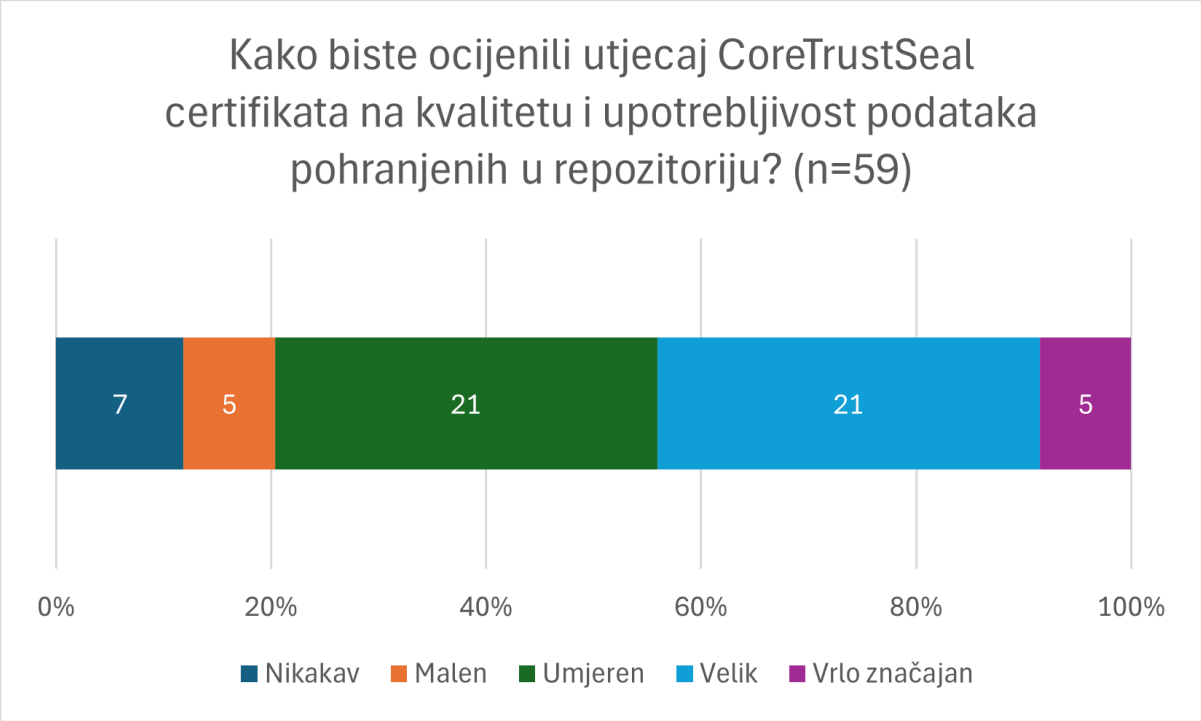
Grafikon 13. Učinkovitost CoreTrustSeal-a u poboljšanju povjerenja i pouzdanosti

Drugim pitanjem tražio se odgovor na to koliko je CoreTrustSeal certifikat poboljšao vidljivost i prepoznatljivost certificiranih repozitorija u istraživačkoj zajednici. Iz grafikona 14 može se iščitati da niti jedan repozitorij nije smatrao da vidljivost nije nimalo poboljšana (ocjena 1), sedam je repozitorija odgovorilo s neznatno (ocjena 2), dok je 19 repozitorija smatralo poboljšanje umjerenim (ocjena 3). Najveći broj repozitorija, njih 25, ocijenilo je poboljšanje značajnim (ocjena 4), a zadnjih osam repozitorija odgovorilo s vrlo značajno (ocjena 5). Dakle, može se zaključiti da je CoreTrustSeal većinom poboljšao prepoznatljivost repozitorija u istraživačkoj zajednici.



Grafikon 14. Poboljšanje vidljivosti i prepoznatljivosti repozitorija u istraživačkoj zajednici nakon CoreTrustSeal certifikacije

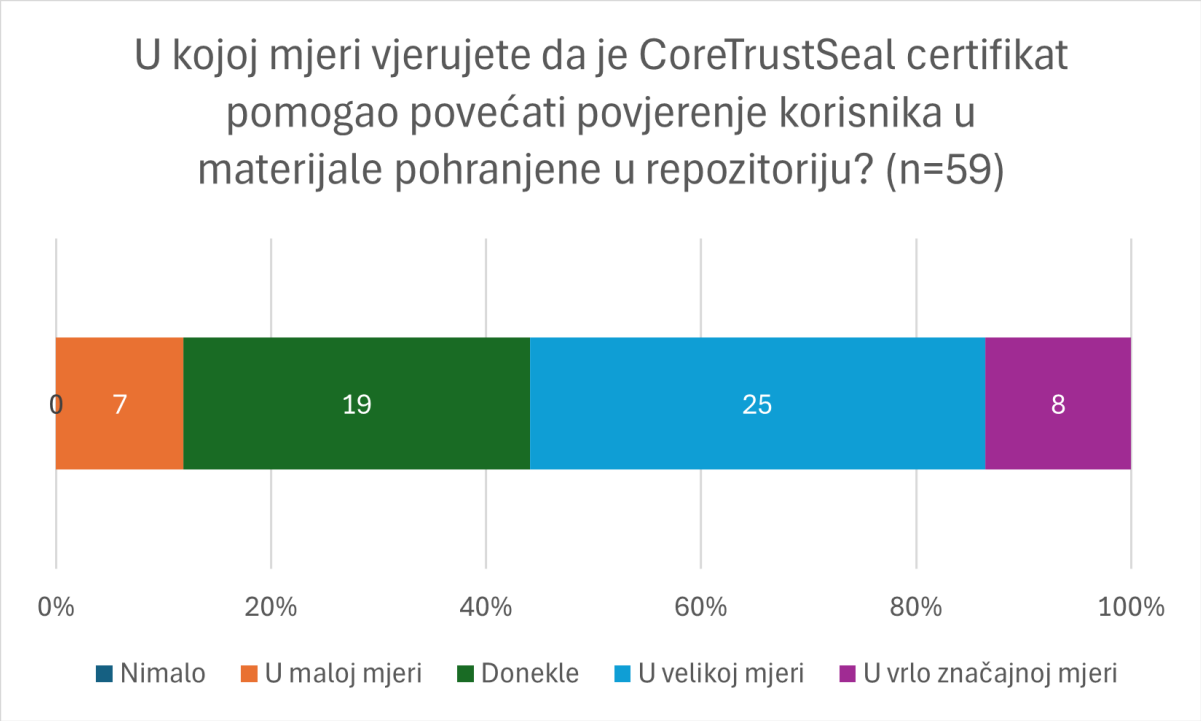
Treće pitanje je bilo procjenjivanje utjecaja CoreTrustSeal certifikata na kvalitetu i upotrebljivost podataka pohranjenih u certificiranim repozitorijima. Jednak broj repozitorija, njih 21, procijenili su utjecaj na kvalitetu i upotrebljivost podataka umjerenim (ocjena 3) i velikim (ocjena 4). Sedam je repozitorija označilo da nije bilo nikakvog utjecaja (ocjena 1), pet repozitorija smatralo je utjecaj malim (ocjena 2) i ostalih pet repozitorija utjecaj je označilo vrlo značajnim (ocjena 5) (grafikon 15). Iz ovih ocjena može se zaključiti kako većina repozitorija smatra da CoreTrustSeal ima velik ili umjeren utjecaj na kvalitetu i uporabljivost podataka koji su pohranjeni u digitalnim repozitorijima.



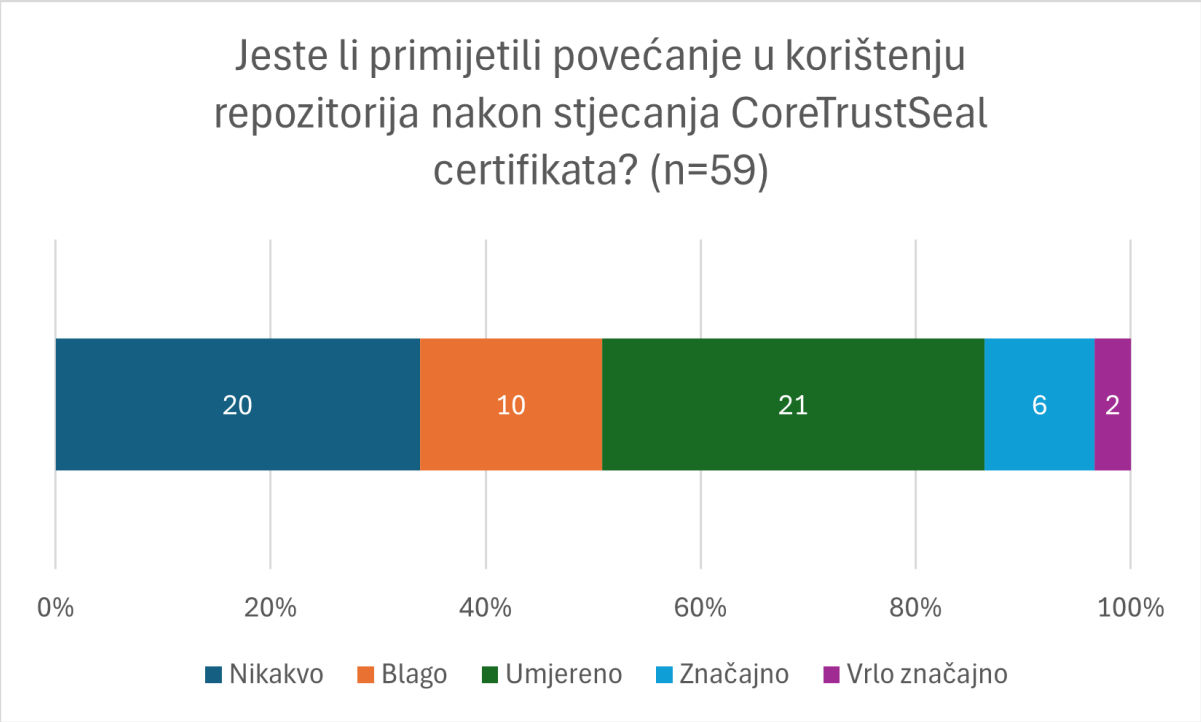
Grafikon 15. Utjecaj CoreTrustSeal certifikacije na kvalitetu i uporabljivost podataka

Četvrto pitanje odnosilo se na procjenu je li CoreTrustSeal pomogao u povećanju povjerenja korisnika u materijale pohranjene u certificiranim repozitorijima. Niti jedan repozitorij ne smatra da se povjerenje korisnika nije nimalo povećalo (ocjena 1). Sedam je repozitorija ocijenilo da je doprinijelo u maloj mjeri (ocjena 2), a 19 repozitorija smatra da se povjerenje donekle povećalo (ocjena 3). Najviše repozitorija, njih 25, smatra da je ovaj certifikat znatno doprinio povećanju povjerenja korisnika (ocjena 4), dok je osam repozitorija ocijenilo da je doprinos bio u vrlo značajnoj mjeri (ocjena 5) (grafikon 16). To ukazuje na to da većina repozitorija smatra da je CoreTrustSeal igrao važnu ulogu u jačanju povjerenja korisnika u njihovo gradivo.

Peto je pitanje bilo vezano uz povećanje korištenja repozitorija nakon dobivanja CoreTrustSeal certifikata. Iz grafikona 17 može se vidjeti da je čak 20 repozitorija odgovorilo kako smatra da povećanja nije bilo (ocjena 1), dok je njih deset osjetilo blagi porast (ocjena 2) u korištenju. Najveći broj repozitorija, njih 21, označio je povećanje umjerenim (ocjena 3), šest repozitorija vidjelo je značajno povećanje (ocjena 4), a samo dva repozitorija su povećanje označili vrlo značajnim (ocjena 5). Dok su neki ispitanici primijetili značajan porast korištenja nakon certifikacije, drugi nisu zabilježili značajne promjene, što ukazuje na to da utjecaj CoreTrustSeal-a može varirati među različitim repozitorijima i njihovim kontekstima.

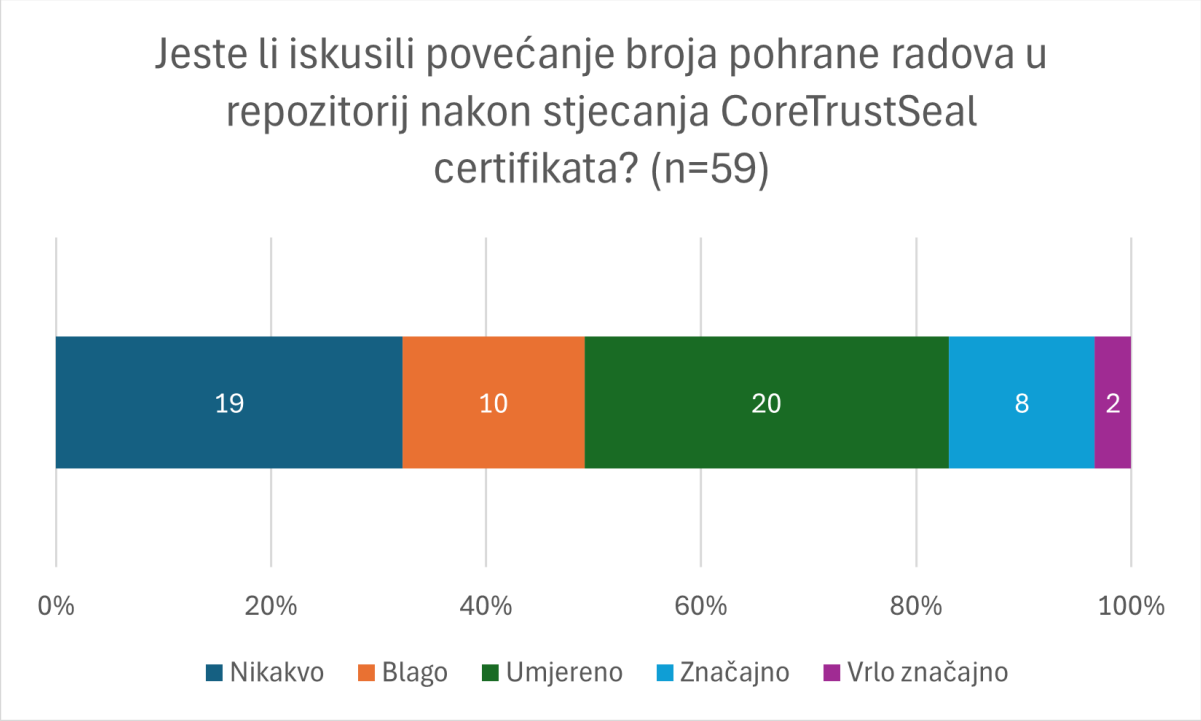


Grafikon 16. Povećanje povjerenja korisnika u pohranjeno gradivo nakon CoreTrustSeal certifikacije



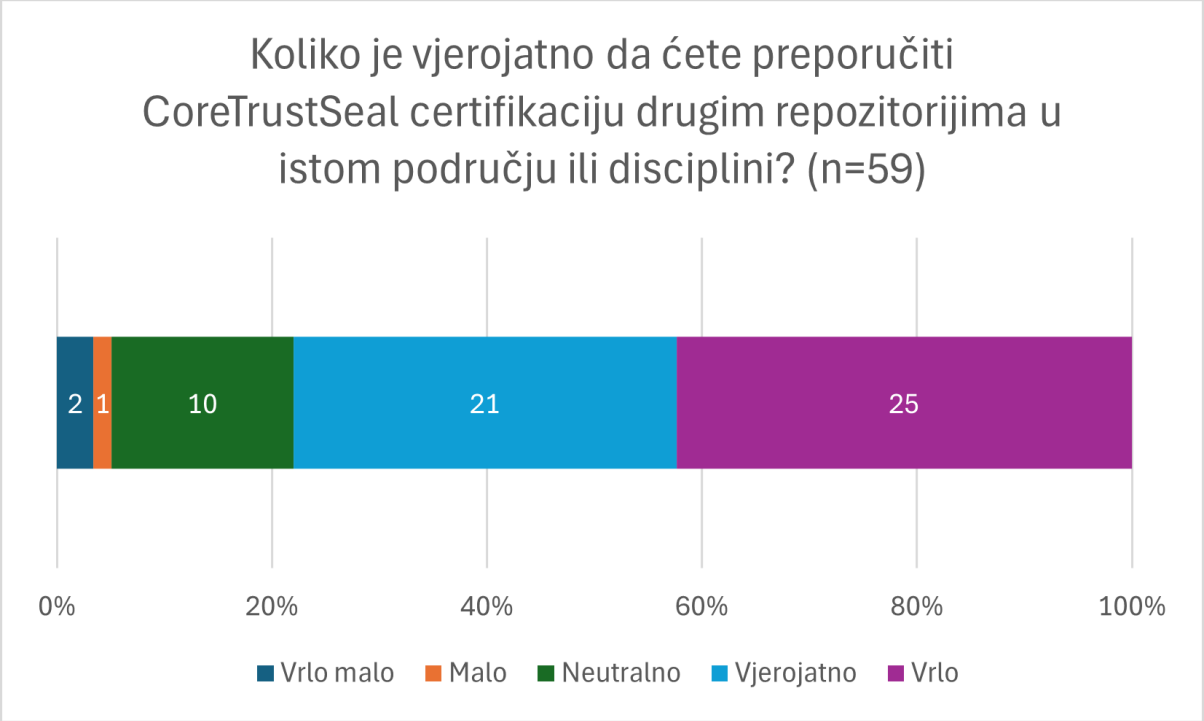
Grafikon 17. Povećanje korištenja repozitorija nakon stjecanja CoreTrustSeal certifikata

Šesto se pitanje odnosilo na iskustvo u povećanju broja radova koji su pohranjeni u repozitorije nakon CoreTrustSeal certifikata. Najviše repozitorija, njih 20, je povećanje ocijenilo umjerenim (ocjena 3), dok njih 19 nije vidjelo nikakav utjecaj (ocjena 1) u broju povećanja. Deset je repozitorija povećanje ocijenilo blagim (ocjena 2), njih osam je vidjelo značajan porast (ocjena 4) i dva repozitorija smatraju da je porast bio vrlo značajan (ocjena 5). S obzirom na odgovore, nije lako procijeniti je li baš CoreTrustSeal zaslužan za povećanje u pohranjivanju radova i gradiva u repozitorije. Kao i u prethodnom pitanju, utjecaj CoreTrustSeal-a nije jednak za svaki repozitorij, pa su tako i mišljenja podijeljena.



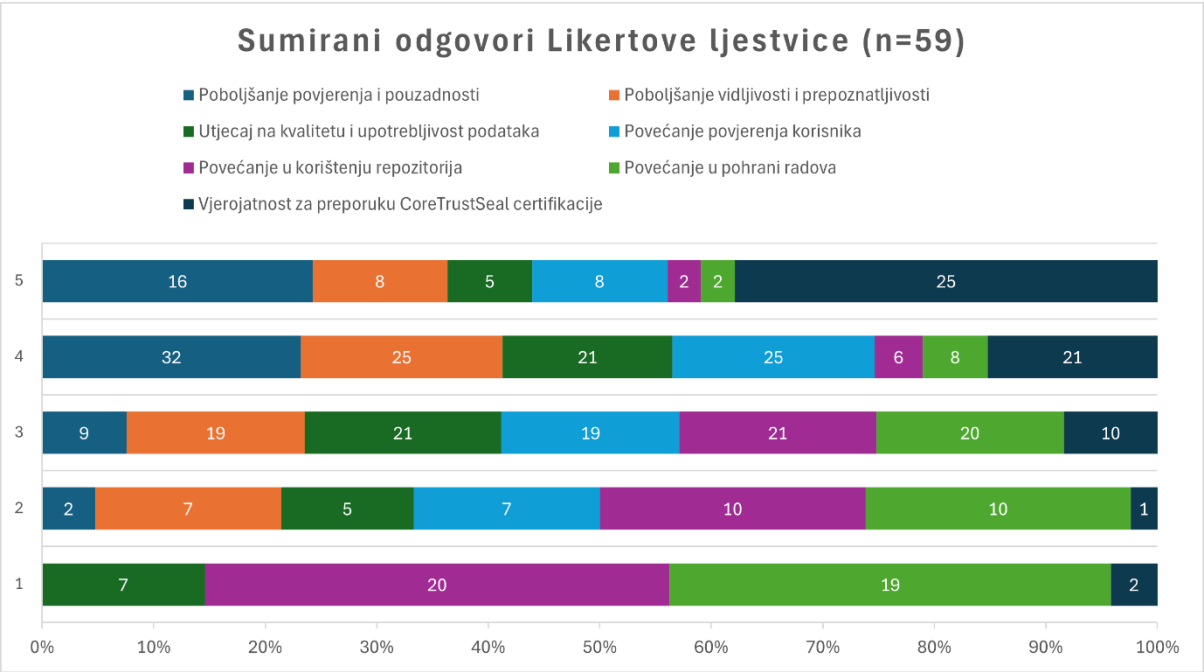
Grafikon 18. Povećanje pohranjivanja gradiva u repozitorij nakon stjecanja CoreTrustSeal certifikata

Sedmo, i ujedno zadnje pitanje ovog tipa, bilo je vezano uz preporučivanje CoreTrustSeal certifikata drugim repozitorijima u istom području ili disciplini. Dva su repozitorija odgovorila da je vrlo mala vjerojatnost (ocjena 1) da bi preporučili certifikaciju, jedan je repozitorij odgovorio da postoji mala vjerojatnost (ocjena 2), a deset repozitorija je bilo neutralno. Da bi vjerojatno (ocjena 4) preporučili CoreTrustSeal je odgovorilo 21 repozitorija, a najviše, njih 25, je odgovorilo kako bi vrlo vjerojatno (ocjena 5) preporučili certifikaciju (grafikon 19). Iz ovih odgovora može se zaključiti da je opće iskustvo s CoreTrustSeal certifikacijom izuzetno pozitivno, s obzirom na to da bi certificirani repozitoriji dominantno preporučili drugim repozitorijima u istom području i disciplini da se prijave za certifikaciju.



Grafikon 19. Vjerojatnost preporučivanja CoreTrustSeal certifikacije drugim repozitorijima

Grafikon 20 prikazuje zbirne odgovore na svih sedam prethodnih pitanja, organiziranih prema Likertovoj ljestvici.



Grafikon 20. Sumirani odgovori na sedam pitanja po Likertovoj ljestvici

Ostalo je još samo predstaviti rezultate pitanja s odgovorima otvorenog tipa. Prvo pitanje se odnosilo na primarnu motivaciju digitalnih repozitorija za CoreTrustSeal certifikacijom. Odgovori na to pitanje mogu se grupirati u devet skupina:

1. Primjena najboljih praksi

Neke organizacije su tražile certifikaciju kako bi uskladile svoje djelovanje s vlastitim savjetima o najboljim praksama, pokazujući svoju predanost pravilnom upravljanju gradivom i nastojeći poboljšati svoj repozitorij.

2. Angažman zajednice i standardi

Mnogi ispitanici istaknuli su važnost usklađivanja sa zajednicom za očuvanje podataka, pridržavanje najboljih praksi i osiguravanje kontinuiranog poboljšanja. Neki su željeli ispuniti specifične zahtjeve mreža poput CLARIN-a.

3. Osiguranje kvalitete i povjerenja

Certifikacija je viđena kao način za stjecanje vanjske potvrde njihovih praksi, osiguravajući dionicima, financijerima i korisnicima povjerenje u repozitorij i pridržavanje visokih standarda.

4. Regulatorni i financijski zahtjevi

Za neke je certifikacija bila nužna kako bi zadovoljili nacionalne ili međunarodne norme, održali uvjete za financiranje ili ispunili obveze prema dionicima i financijerima.

5. Pokazivanje predanosti

Dobivanje CoreTrustSeal certifikata također je bilo motivirano željom da se pokaže snažna predanost očuvanju podataka, upravljanju i povjerenju, čime se poboljšava njihov ugled i vjerodostojnost unutar istraživačke zajednice.

6. Operativna poboljšanja

Proces certifikacije je cijenjen zbog pomoći u strukturiranju operacija, poboljšanju dokumentacije i rafiniranju unutarnjih procesa, čime repozitorij postaje učinkovitiji.

7. Vidljivost i konkurentnost

Povećanje vidljivosti repozitorija, konkurentnosti i usklađenosti s drugim institucijama također su bile česte motivacije. Certifikacija je viđena kao način za ostanak pri vrhu u brzo razvijajućem digitalnom okruženju upravljanja gradivom.

8. Pravna i politička usklađenost

Za neke repozitorije, osobito one povezane s određenim istraživačkim infrastrukturama ili nacionalnim politikama, certifikacija je bila obvezna za usklađenost s pravnim zahtjevima ili institucionalnim politikama.

9. Podrška i suradnja

Nekoliko organizacija bilo je motivirano dostupnošću programa podrške i prilikom za suradnju i učenje od drugih certificiranih repozitorija, kako lokalno tako i međunarodno.

Drugo pitanje bilo je usmjereno na izazove s kojima su se repozitoriji susretali tijekom procesa CoreTrustSeal certifikacije. Odgovori su bili raznoliki i pokrivali širok spektar iskustava, a ona se mogu podijeliti u osam skupina:

1. Prikupljanje informacija i dokumentacija

Prilikom procesa certifikacije sakupljanje informacija i dokumentacije pokazalo se kao intenzivan proces koji zahtijeva prikupljanje informacija iz više odjela. Također su se pojavile teškoće u izbjegavanju opširnih odgovora i ponavljanja odgovora zbog pitanja kojima se preklapa spektar potrebnih odgovora. Izazovi su uključivali i pružanje povjerljive dokumentacije te one dokumentacije koja nije bila na engleskom jeziku, što je dodatno kompliciralo proces. Zbog toga se pojavila potreba za razvijanjem ili poboljšanjem unutarnje dokumentacije i politika.

2. Tehnička i sistemska pitanja

Tijekom procesa certificiranja, repozitoriji su se suočavali s nizom tehničkih izazova, uključujući probleme s portalima za podnošenje prijava i pristupnim poveznicama. Rukovanje velikim količinama informacija te osiguravanje njihove dostupnosti i razumljivosti je također velik izazov. Dodatno, susretali su se s poteškoćama u prelasku između različitih sustava ili verzija zahtjeva za prijavu, kao i sa sporim odzivnim vremenima i dugim procesima pregleda, koji su ponekad bili pogoršani nesporazumima od strane recenzenata.

3. Interpretacija i komunikacija

Digitalni repozitoriji su, tijekom procesa certificiranja, naišli na izazove u interpretaciji i komunikaciji, uključujući neizvjesnost oko dubine i specifičnosti koje su potrebne u odgovorima na prijavu, te teškoće u točnoj interpretaciji i mogućem odgovoru na zahtjeve za prijavu. Uz to, suočili su se s izazovima u jasnom komuniciranju

organizacijske strukture i odgovornosti, posebno u složenim ili distribuiranim organizacijama.

4. Ograničenja resursa i vremena

Tijekom procesa certificiranja, digitalni repozitoriji su se suočili s ograničenjima resursa i vremena, zato što je certifikacija proces koji oduzima mnogo vremena i zahtijeva značajan napor i koordinaciju osoblja. Također, morali su balansirati napore za certifikaciju sa svakodnevnim poslovnim operacijama te osigurati dovoljno resursa i vremena osoblju, što je posebno teško za male repozitorije.

5. Unutarnja koordinacija i stručnost

Izazovi internog koordiniranja i stručnosti uključuju integraciju više disciplina i osiguravanje dosljednog stila i detalja u prijavi. Također, repozitoriji su nailazili na izazove u dobivanju podrške organizacije i koordinaciji doprinosa različitih dionika, pa su se suočili s teškoćama u uspostavljanju zajedničke razine kvalitete i prakse arhiviranja među distribuiranim zbirkama

6. Specifični zahtjevi i standardi

Specifični zahtjevi i standardi izazvali su digitalnim repozitorijima određene poteškoće prilikom prijave za certifikaciju. To uključuje teškoće u usklađivanju zahtjeva s organizacijskim praksama, posebno za nedisciplinarne ili multidisciplinarne repozitorije. Dalje, postojala su pitanja koja su zahtijevala dokazivanje dugoročne održivosti i financijske sigurnosti što je za neke repozitorije bilo teško ispuniti. Također, pojavili su se izazovi u ispunjavanju specifičnih zahtjeva poput planiranja očuvanja, integriteta podataka i kontinuiteta pristupa.

7. Vanjski i kontekstualni faktori

U procesu certifikacije, repozitoriji su naišli na mnogo vanjskih čimbenika koji su im zadavali teškoće. Jedan od primjera je pandemija COVID-19 koja je iznimno utjecala na suradnju i podršku osoblja repozitorija. Drugi bitan i najčešće spomenut faktor je dugi period pregleda koji uzrokuje kašnjenje i neizvjesnost u statusu certifikacije. Također, naišlo se na razlike u razumijevanju i terminologiji između repozitorija i recenzenata.

8. Koristi i naučene lekcije

Unatoč izazovima, proces je često doveo do poboljšanja u dokumentaciji, procesima i ukupnom upravljanju repozitorijem. Prepoznata je potreba za boljim materijalima za obuku i podrške repozitorijima za buduće prijave.

9.4. Rasprava

Na temelju opsežnih povratnih informacija repozitorija o njihovom iskustvu s certifikacijom CoreTrustSeal, slijedi rasprava i odgovori na postavljene hipoteze.

Prva hipoteza (H1) bila je da će repozitoriji koji aktivno promoviraju svoju CoreTrustSeal certifikaciju imati veći broj korisnika i pohana u usporedbi s onim repozitorijima koji to ne čine. Mnogi repozitoriji su smatrali izazovnim izravno pripisati povećanje korištenja ili pohrane gradiva CoreTrustSeal certifikaciji zbog istovremenog utjecaja drugih čimbenika poput marketinških aktivnosti i obaveznih politika podnošenja podataka od strane financijera. Kao što je vidljivo iz grafikona 17 i 18 neki su ispitanici primijetili značajan porast u korištenju i pohrani nakon certifikacije, dok drugi nisu zabilježili značajne promjene. Utjecaj CoreTrustSeal-a na te vrijednosti je teško provjerljiv, pogotovo za neke od repozitorija koji od svojih početaka imaju certifikaciju i ne mogu usporediti brojke prije i nakon stjecanja certifikata. Neki repozitoriji su priznali da smatraju da bi, da su bolje promovirali CoreTrustSeal, imali više pohranjenog gradiva i povećanje u korištenju gradiva. Stoga hipoteza H1 nije ni u potpunosti potvrđena niti u potpunosti opovrgnuta.

Druga hipoteza (H2) je glasila da proces dobivanja CoreTrustSeal certifikacije vodi do poboljšanja u formuliranju unutarnjih procesa dokumentaciji i ukupnoj kvaliteti repozitorija. Ponavljajuća tema u odgovorima otvorenog tipa bila je da je većina repozitorija tijekom procesa stekla dublje razumijevanje vlastitih sustava, ističući područja za poboljšanje, posebno u sigurnosti sustava i praksama dokumentacije. Mnogo se repozitorija pohvalilo novim znanjem naučenim tijekom procesa certifikacije. Na temelju toga se može zaključiti da je hipoteza H2 potvrđena, odnosno da je proces uistinu bio koristan u poboljšanju internih procesa, dokumentacije i ukupne kvalitete repozitorija. To je viđeno kao značajna prednost, čak i ako nije izravno dovelo do povećanog broja korištenja i pohranjivanja gradiva.

Treća hipoteza (H3) bila je da su zahtjevi za resurse i troškove za CoreTrustSeal certifikaciju značajna prepreka za repozitorije, što utječe na njihovu odluku da traže i obnavljaju certifikaciju. Prema odgovorima iz ankete proces certifikacije podrazumijeva intenzivno trošenje vremena i resursa. On je opisan kao opterećujući i dugotrajan, a kašnjenja i nereagiranje od strane certifikacijskog tijela dodatno su povećavali frustraciju. Repozitoriji su u anketi iskazali potrebu za pojednostavljenjem procesa. Predložili su sustav s popisom za provjeru koji ne zahtjeva detaljnije tehničke uvide. Problem je i opseg pitanja koja se često preklapaju, dok se odgovori ne smiju ponavljati. Također, sva predana dokumentacija mora

biti na engleskom jeziku, što je rezultiralo značajnim vremenskim ulaganjem u prevođenje te dokumentacije. Financijski izazovi također predstavljaju prepreku za mnoge repozitorije. Od veljače 2024. godine cijena CoreTrustSeal certifikacije porasla je s 1.000 na 3.000 eura. Ovaj značajan porast troškova izazvao je zabrinutost među mnogim repozitorijima, posebno onima manjima, koji ističu da je omjer troškova i koristi postao manje povoljan. Neki repozitoriji izričito navode da je povećanje cijene jedan od faktora koji bi ih mogao spriječiti da obnove certifikat u budućnosti, posebno ako se pojavi nova certifikacija za repozitorije od povjerenja koja bi bila ekonomičnija. Stoga se može zaključiti da je hipoteza H3 potvrđena.

Četvrta hipoteza (H4) bila je da će povećana svijest i razumijevanje CoreTrustSeal certifikacije među istraživačima povećati percipiranu vrijednost i značaj certifikacije. Analizom rezultata prikazanih u grafikonu 14, može se zaključiti da je CoreTrustSeal u većini slučajeva poboljšao vidljivost repozitorija unutar istraživačke zajednice. Certifikacija je viđena kao vrijedan alat za demonstraciju pouzdanosti financijerima i unutar zajednice za upravljanje podacima. Posebno je cijenjena u raspravama s dionicima koji cijene standarde digitalne pohrane. Međutim, mnogi repozitoriji ističu ograničenu svijest istraživača o certifikaciji. Iako je certifikacija važna u institucionalnom i financijskom kontekstu, postoji općeniti konsenzus da istraživači često nisu svjesni ili ne pokazuju interes za status certificiranosti repozitorija. Stoga hipoteza H4 nije ni u potpunosti potvrđena niti u potpunosti opovrgnuta.

Peta, i ujedno posljednja, hipoteza (H5) je tvrdila da će pojednostavljenje procesa CoreTrustSeal certifikacije, posebno procesa obnove, povećati zadovoljstvo procesom i smanjiti radno opterećenje za repozitorije. Mnogi repozitoriji izrazili su potrebu za automatizacijom i pojednostavljenjem procesa obnove certifikacije za već certificirane repozitorije kako bi se smanjilo administrativno opterećenje. Kao što je prikazano na grafikonu 5, proces certifikacije i recertifikacije pokazao se dugotrajnim, što su ispitanici istaknuli kao glavni izazov. Jedan repozitorij čekao je čak dvije godine na potvrdu recertifikacije. Također su se pojavili problemi s promjenom zahtjeva za prijavu tijekom procesa certifikacije. S obzirom na dugotrajnost procesa, zahtjevi su se mijenjali nakon predaje početne prijave, što je rezultiralo odbijanjem prijave i potrebom za poboljšanjem u skladu s novim zahtjevima. Stoga bi pojednostavljenje procesa certifikacije, posebno recertifikacije, doprinijelo većem zadovoljstvu repozitorija, pa je tako hipoteza H5 potvrđena.

Zaključno, dok CoreTrustSeal certifikacija nudi značajne interne benefite i cijenjena je zbog svoje uloge u demonstraciji pouzdanosti, njezin izravan utjecaj na povećanje korištenja repozitorija i podnošenja podataka nije toliko jasan. Proces se smatra resursno intenzivnim, te postoje pozivi da se olakša i učini pristupačnijim. Repozitoriji cijene certifikaciju zbog poboljšanja interne kvalitete i povjerenja koje signalizira dionicima, ali također prepoznaju potrebu za boljom komunikacijom i marketingom njihovog certificiranog statusa kako bi se maksimizirali potencijalni benefiti.

10. Zaključak

Digitalizacija je neizbježno oblikovala način na koji se čuva i pristupa znanju. E-gradivo, kao ključni nositelj suvremenih informacija i spoznaja, zahtijeva adekvatne strategije očuvanja kako bi se osiguralo da budućim generacijama ostane dostupno i upotrebljivo. U tom kontekstu, povjerenje u institucije koje upravljaju digitalnim repozitorijima igra ključnu ulogu. Osim što građani očekuju da institucije osiguraju sigurnost i pouzdanost u čuvanju e-gradiva, povjerenje je temelj za uspješnu razmjenu znanja i suradnju među istraživačima.

Digitalni repozitoriji od povjerenja predstavljaju ključnu infrastrukturu u ovom kontekstu. Njihovi atributi, poput transparentnosti, sigurnosti i dugoročne održivosti, ključni su u osiguranju povjerenja korisnika. Uspješno implementirani TRUST principi, mogu poslužiti kao temelj za osiguranje integriteta i pouzdanosti digitalnih repozitorija.

Norme i preporuke za digitalne repozitorije pružaju smjernice za razvoj i održavanje visokih standarda u upravljanju e-gradivom. Certifikacija, posebno putem standarda poput CoreTrustSeal-a, predstavlja važan korak prema dokazivanju sukladnosti s tim standardima i priznavanju institucija koje ulažu napore u osiguranje visokih standarda upravljanja podacima.

Rezultati istraživanja provedenog u ovom radu dodatno potvrđuju važnost certifikacije i njen utjecaj na percepciju korisnika digitalnih repozitorija. Prikazani rezultati pružaju uvid u to kako certificirani digitalni repozitoriji percipiraju CoreTrustSeal proces certifikacije i što ističu kao ključne prednosti, izazove i preporuke za daljnji razvoj ovog važnog segmenta digitalne infrastrukture.

U cjelini, ovaj rad istražuje i naglašava važnost povjerenja u digitalne repozitorije i potrebu za kontinuiranim unaprjeđenjem praksi očuvanja e-gradiva kako bi se osiguralo da digitalna baština ostane sigurna, dostupna i relevantna za buduće generacije.

11. Literatura

1. „Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources." An *RLG-OCLC* Report. Mountain View, CA: Research Libraries Group, 2001. https://www.oclc.org/content/dam/research/activities/trustedrep/attributes01.pdf (pristupljeno 20.5.2024.).
2. Baucom, Erin. „A Brief History of Digital Preservation." *Mansfield Library Faculty Publications.* 31. (2019) https://scholarworks.umt.edu/ml_pubs/31 (pristupljeno 15.5.2024.).
3. Consultative Committee on Space Data Systems. *Audit and Certification of Trustworthy Digital Repositories: recommended practice.* Washington DC: Consultative Committee on Space Data Systems, 2011. https://doi.org/10.25607/OBP-1451 (pristupljeno 22.5.2024.).
4. *CoreTrustSeal certified data repositories*. https://amt.coretrustseal.org/certificates (pristupljeno 30.5.2024.).
5. CoreTrustSeal Standards and Certification Borad. „Coretrustseal Requirements 2023-2025." Zenodo, 2022. https://doi.org/10.5281/zenodo.7051012 (pristupljeno 30.5.2024.).
6. Ćepulić, Tomislav. „Međunarodni standard ISO 15489 „Information and documentation - Records management"." *Arhivski vjesnik* , br. 44 (2001): 77-84. https://hrcak.srce.hr/9342 (pristupljeno 22.5.2024).
7. *Digitalizacija. Hrvatska enciklopedija, mrežno izdanje*. Leksikografski zavod Miroslav Krleža, 2013. – 2024. https://www.enciklopedija.hr/clanak/digitalizacija (pristupljeno 15.5.2024.).
8. Dillo, Ingrid, i Lisa de Leeuw. „CoreTrustSeal." *Mitteilungen Der Vereinigung Österreichischer Bibliothekarinnen Und Bibliothekare* 71, 1. (2018):162-170. https://doi.org/10.31263/voebm.v71i1.1981. (pristupljeno 30.5.2024.).
9. Donaldson, Devan Ray. „Users' Trust in Trusted Digital Repository Content." iPRES 2011. 8th International Conference on the Preservation of Digital Objects (Singapore: 2011.), 20-23. https://scholarworks.iu.edu/iuswrrest/api/core/bitstreams/2f6d301a-e51d-4793-8b06-3c5b9460c5eb/content (pristupljeno 20.5.2024.).

10. Donaldson, Devan i Paul Conway. „User Conceptions of Trustworthiness for Digital Archival Documents.“ *Journal of the Association for Information Science and Technology*. 66. (2015): 2427-2444. https://doi.org/10.1002/asi.23330 (pristupljeno 18.5.2024.).

11. Doney, Patricia M., i Joseph P. Cannon. „An Examination of the Nature of Trust in Buyer-Seller Relationships.“ *Journal of Marketing* 61, no. 2 (1997): 35–51. https://doi.org/10.2307/1251829. (pristupljeno 20.5.2024.).

12. *Expired CoreTrustSeal data repositories certificates*. https://amt.coretrustseal.org/expired-certificates (pristupljeno 30.5.2024.).

13. Green, Alex, Mark Bell, John Sheridan, John P. Collomosse, Tu Bui, Alan W. Brown, Jamie Fawcett, Olivier Thereaux i Jeni Tennison. „Using blockchain to engender trust in public digital archives.“ *iPRES 2018. 15th International Conference on Digital Preservation,* (Boston: 2018.), Green-iPRES-2018.pdf (surrey.ac.uk) (pristupljeno 18.5.2024.).

14. *HRN EN ISO 9000 - Upravljanje kvalitetom.* Hrvatski zavod za norme. https://www.hzn.hr/default.aspx?id=43 (pristupljeno 22.5.2024.).

15. ISO 14721:2012. *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*. International Organization for Standardization, 2012. https://www.iso.org/standard/57284.html (pristupljeno 22.5.2024.).

16. ISO 15489-1:2016. *Information and documentation - Records management*, Part 1: Concepts and principles. International Organization for Standardization. 2016. https://www.iso.org/standard/62542.html. (pristupljeno 22.5.2024.).

17. ISO 16363:2012. *Space data and information transfer systems - Audit and certification of trustworthy digital repositories*. International Organization for Standardization, 2012. https://www.iso.org/standard/56510.html (pristupljeno 22.5.2024.).

18. ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection - Information security controls.* International Organization for Standardization. 2022. https://www.iso.org/standard/75652.html (pristupljeno 22.5.2024.).

19. Jantz, Ronald i Michael J. Giarlo. „Digital Preservation: Architecture and Technology for Trusted Digital Repositories“ 34, no. 3 (2005): 135-147. https://doi.org/10.1515/MFIR.2005.135 (pristupljeno 15.5.2024.).

20. Kuleš, Magdalena i Hrvoje Stančić. „Arhiviranje digitalnih zapisa - stanje i perspektive.“ *5. kongres hrvatskih arhivista: Arhivi u Hrvatskoj - (retro)perspektiva,* ur. Silvija Babić, 401-418. Zadar: Hrvatsko arhivističko društvo, 2017. https://www.researchgate.net/publication/349647868 (pristupljeno 15.5.2024.).

21. Levy, David M. „ Heroic measures: reflections on the possibility and purpose of digital preservation“. *Digital libraries 98: the Third ACM Conference on Digital Libraries, June 23-26, 1998, Pittsburgh, PA.* New York: Association for Computing Machinery (1998): 152-161. https://doi.org/10.1145/276675.276692 (pristupljeno 15.5.2024.).

22. L'Horus, Hervé, Mari Kleemola, i Lisa de Leeuw. „CoreTrustSeal: From Academic Collaboration to Sustainable Services.“ *IASSIST Quarterly* 43, 1. (2019):1-17. https://doi.org/10.29173/iq936. (pristupljeno 30.5.2025.).

23. Lin, Dawei, Johnatan Crabtree, Ingrid Dillo, et al. „The TRUST Principles for digital repositories.“ *Sci Data* 7, 144. 2020. https://doi.org/10.1038/s41597-020-0486-7 (pristupljeno 20.5.2024.)

24. Mayer, Roger C., James H. Davis, i F. David Schoorman. „An Integrative Model of Organizational Trust.“ *The Academy of Management Review* 20, no. 3 (1995): 709–34. https://doi.org/10.2307/258792. (pristupljeno 20.5.2024.).

25. Mihaljević, Marta, Milica Mihaljević, i Hrvoje Stančić. s.v. „digital preservation“, *Arhivistički Rječnik: HRVATSKO-ENGLESKI/ENGLESKO-HRVATSKI.* Zagreb: Zavod za informacijske studije Odsjeka za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu, 2015.

26. Prieto, Adolfo G.. „From conceptual to perceptual reality: trust in digital repositories.“ *Library Review* 58. (2009): 593-606. http:// doi.org/10.1108/00242530910987082 (pristupljeno 18.5.2024.).

27. Rajh, Arian, Hrvoje Stančić, Bojan Romčević i Marin Vitaljić. „Koncept rješenja za osiguranje i očuvanje vjerodostojnosti zapisa u upravnim organizacijama prilikom razvoja državnog računalnog oblaka i državnog digitalnog arhiva.“ *Arhivski vjesnik* 61, br. 1 (2018): 69-87. https://hrcak.srce.hr/216936 (pristupljeno 18.5.2024.).

28. Rousseau, Denise M., Sim B. Sitkin, Ronald S. Burt, i Colin Camerer. „Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust.“ *The Academy of Management Review* 23, no. 3 (1998): 393–404. http://www.jstor.org/stable/259285. (pristupljeno 20.5.2024.).

29. Sandusky, Robert. J. „How recordkeeping ensures trust in digital archives.“ *Proceedings of the Association for Information Science and Technology.* ur. S. Erdelez i N.K. Agarwal, 796–797. Hoboken, NJ: Wiley. 2017. https://doi.org/10.1002/pra2.2017.14505401160 (pristupljeno 22.5.2024.).

30. Stančić, Hrvoje et al. „Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31) – final report.“ *InterPARES Trust*. 2018. http://interparestrust.org/assets/public/dissemination/TRUSTERPreservationModel(EU31)-Finalreportv_1_3.pdf (pristupljeno 15.5.2024.).

31. Stančić, Hrvoje. „Arhivsko gradivo u elektroničkom obliku: mogućnosti zaštite i očuvanja na dulji vremenski rok.“ *Arhivski vjesnik* 49, br. 1 (2006): 107-121. https://hrcak.srce.hr/6234 (pristupljeno 15.5.2024.).

32. Stančić, Hrvoje. „Digitalizacija i upravljanje digitalnim izvornicima.“ *Utjecaj digitalizacije na arhivsku praksu*, ur. Radoslav Zaradić, 7-30. Zagreb: Hrvatsko arhivističko društvo, 2023. https://urn.nsk.hr/urn:nbn:hr:131:583191 (pristupljeno 18.5.2024.)

33. Stančić, Hrvoje. „Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata.“ Doktorska disertacija, Filozofski fakultet, Zagreb, 2006.

34. „Trusted Digital Repositories: Attributes and Responsibilities.“ An *RLG-OCLC* Report. Mountain View, CA: Research Libraries Group, 2002. www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf. (pristupljeno 18.5.2024.).

35. Waters, Donald J. i John R. Garrett. „Preserving Digital Information. Report of the Task Force on Archiving of Digital Information.“ *The Commission on Preservation and Access And The Research Libraries Group.* 1996. https://www.clir.org/wp-content/uploads/sites/6/2016/09/pub63watersgarrett.pdf (pristupljeno 18.5.2024.).

36. Yakel, Elizabeth, Ixchel M. Faniel, Adam Kriesberg and Ayoung Yoon. „Trust in Digital Repositories.“ *Int. J. Digit. Curation* 8 (2013): 143-156. https://doi.org/10.2218/IJDC.V8I1.251 (pristupljeno 25.5.2024.).

37. Yoon, Ayoung. „End users’ trust in data repositories: definition and influences on trust development.“ *Arch Sci* 14, (2014): 17-34. https://doi.org/10.1007/s10502-013-9207-8 (pristupljeno 18.5.2024.)

Popis oznaka i kratica

AWIICS - Archival Workshop on Ingest, Identification, and Certification Standards

CLARIN - Common Language Resources and Technology Infrastructure

CPA - Commission on Preservation & Access

DSA - Data Seal of Approval

FAIR - Findable, Accesssible, Interoperable, and Reusable

ISC - International Science Council

OAIS – Open Archival Information System

RLG - Research Libraries Group

SAD - Sjedinjene Američke Države

TDR - Trusted Digital Repositories

TRAC - Trustworthy Repositories Audit & Certification

TRUST - Transparency, Responsibility, User focus, Sustainability, and Technology

WDS - World Data System

Popis grafikona

Prilozi

Prilog 1 - Survey on CoreTrustSeal certification for digital repositories

Greetings, thank you for taking the time to complete this anonymous survey distributed to the repositories who have experience with the CoreTrustSeal certification. My name is Bea Hrup and I am a student conducting a research on the CoreTrustSeal certification for digital repositories for the purpose of writing a master thesis at the Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, Croatia under prof. dr. sc. Hrvoje Stančić. This survey aims at gathering insights into the experiences, motivations, and challenges of repositories that have undergone CoreTrustSeal certification. Your participation will greatly contribute to my understanding of this important aspect of data management. The responses will be used in aggregate and solely for the purposes of this master thesis research. The survey will close on 15 May 2024. In case of any further questions and/or if you want to be updated about the results of the research, please feel free to contact me via one of my emails: bea.hrup@gmail.com or bhrup@m.ffzg.hr. Thank you for your valuable input!

1. **Repository name:**

_____

2. **Repository URL:**

_____

3. **Is your data repository certified with CoreTrustSeal?**

   - ☐ Yes (continue with question → 3.1)
   - ☐ Not any more - it was in the past, but the certification period expired (continue with question → 3.2)

3.1. For how long it is certified?

- □ Less than a year
- □ 1 year
- □ 2 years
- □ 3 years
- □ 4 years
- □ 5 years or more

3.2. For how long it was certified?

- □ Less than a year
- □ 1 year
- □ 2 years
- □ 3 years
- □ 4 years
- □ 5 years or more

4. Has your data repository ever renewed its CoreTrustSeal certification?

- □ Yes (continue with question → 4.1)
- □ No (continue with question → 4.2)
- □ Data repository is currently certified for the first time (continue with question → 4.3)

4.1. What was the main reason for renewal?

- To demonstrate continued commitment to maintaining high standards of trustworthiness and reliability
- To enhance trust and confidence among current and prospective users of the repository
- To ensure ongoing alignment with evolving best practices and standards in data management and curation
- To continue benefiting from the visibility and recognition associated with CoreTrustSeal certification
- To gain access to additional funding opportunities or institutional support linked to maintaining certification status
- To maintain competitiveness and visibility within the broader research community
- It was a management decision
- Other (please specify) _____

4.2.What was the main reason for not renewing CoreTrustSeal certification?

- Financial constraints or lack of resources to support the renewal process
- Perceived lack of significant benefits or impact associated with maintaining CoreTrustSeal certification
- Shift in institutional priorities or strategic focus away from maintaining certification status
- Changes in staffing or personnel responsible for managing certification requirements
- Perception that the initial certification adequately fulfilled the repository's needs and objectives
- Challenges or difficulties encountered during the renewal process
- It was a management decision
- Other (please specify) _____

4.3. Do you anticipate renewing your CoreTrustSeal certification in the future?

- ☐ Yes
- ☐ No
- ☐ Not sure

5. **What was the primary motivation for seeking CoreTrustSeal certification for your data repository in the first place?**

_____

_____

_____

6. **What challenges, if any, did you encounter during the CoreTrustSeal certification process?**

_____

_____

_____

7. **How would you rate the overall effectiveness of the CoreTrustSeal certification process in improving the trustworthiness and reliability of your repository?**

1	2	3	4	5
Very ineffective				Very effective

8. **To what extent has CoreTrustSeal certification enhanced the visibility and recognition of your repository within the research community?**

1	2	3	4	5
Not at all				Significantly

9. **How would you rate the impact of CoreTrustSeal certification on the quality and usability of the data stored in your repository?**

1	2	3	4	5
No impact				Significant impact

10. **To what extent do you believe that CoreTrustSeal certification has helped to increase user trust and confidence in your repository's data holdings?**

1	2	3	4	5
Not at all				To agreat extent

11. **Have you experienced an increase in usage of your repository since obtaining CoreTrustSeal certification?**

1	2	3	4	5
No increase				Significant increase

12. **Have you experienced an increase in submissions to your repository since obtaining CoreTrustSeal certification?**

1	2	3	4	5
No increase				Significant increase

13. How likely are you to recommend pursuing CoreTrustSeal certification to other data repositories in your field or discipline?

1	2	3	4	5
Very unlikely				Very likely

Do you have any final comments, or an experience that you wish to share?

_____

_____

_____

Do you want to receive the compiled survey results?

- ☐ Yes
- ☐ No

Please provide your name: _____

Email: _____

14. I consent to take part in this study.

- ☐ Yes

Povjerenje u digitalne repozitorije i njihove procese zaštite e-gradiva

Sažetak

Ovaj rad istražuje ulogu povjerenja u digitalne repozitorije i njihove strategije očuvanja e-gradiva. U radu je fokus stavljen na važnost institucionalnog povjerenja kao osnove za uspješno upravljanje digitalnim gradivom. Također, analiziraju se karakteristike digitalnih repozitorija od povjerenja, istražujući kako one osiguravaju pouzdanost, sigurnost i dugotrajnu očuvanost pohranjenog sadržaja. Poseban naglasak stavljen je na primjenu TRUST principa te njihovu ulogu u izgradnji povjerenja među korisnicima digitalnih repozitorija. Također, istražuje se primjena normi i preporuka za digitalne repozitorije, s posebnim osvrtom na certifikaciju, kao što je CoreTrustSeal, te njihovu ulogu u osiguranju visokih standarda kvalitete i transparentnosti. Istraživanje provedeno na 58 digitalnih repozitorija iz cijeloga svijeta koji jesu ili su bili certificirani CoreTrustSeal certifikatom pokazuje kako oni percipiraju proces certifikacije. Cilj istraživanja je bio bolje razumjeti utjecaj certifikacije na vidljivost, prepoznatljivost i općenito djelovanje digitalnih repozitorija unutar istraživačke zajednice.

Ključne riječi: CoreTrustSeal, digitalni repozitoriji od povjerenja, certifikacija, TRUST principi, e-gradivo

Trust in digital repositories and their processes for preserving e-materials

Summary

This thesis explores the role of trust in digital repositories and their strategies for preserving e-materials. It focuses on the importance of institutional trust as the foundation for successful management of digital records. Additionally, it analyses the characteristics of trusted digital repositories, examining how they ensure the reliability, security, and long-term preservation of stored content. Special emphasis is placed on the application of TRUST principles and their role in building trust among users of digital repositories. Furthermore, it investigates the application of standards and recommendations for digital repositories, with a particular focus on certification, such as CoreTrustSeal, and their role in ensuring high standards of quality and transparency. The research conducted among 58 digital repositories throughout the world which either are or were certified by CoreTrustSeal shows their perception on the process of certification. The aim of the research was to better understand the impact of certification on the visibility, recognizability, and overall performance of digital repositories within the research community.

Key words: CoreTrustSeal, trusted digital repositories, certification, TRUST principles, e-materials