Gospodarenje informacijama : koncepti i alati

Kipke, Matko

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

Matko Kipke

Gospodarenje informacijama: koncepti i alati

Završni rad

Mentor: Dr. sc. Arian Rajh, izv. prof.

Zagreb, 13. kolovoza 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.

SADRŽAJ

1. Uvod

Informacije predstavljaju organizacijama i tvrtkama veliku vrijednost, ali i veliku odgovornost. One su neophodne za funkcioniranje bilo kakve organizacije te se njihovim kvalitetnim raspolaganjem može doprinijeti radnoj efikasnosti. S druge strane, rast količine informacija te pravne obaveze i sigurnosni rizici vezani uz njih mogu ometati tijek rada organizacije. Gospodarenje informacijama je polje koje se bavi sa tim problemima s ciljem da se efikasno i standardizirano upravlja nad informacijama u organizacijama, od njihovog nastanka do izlučivanja.

2. Gospodarenje informacijama

Gospodarenje informacijama (engl. *„information governance“*) je stalno razvijajuće interdisciplinarno polje koje se bavi strategijama vezanim uz informacije i njihovo upravljanje u organizacijama i tvrtkama. Smatra se dijelom općenitijeg pojma korporativnog upravljanja (engl. „*corporate governance“*), a unutar gospodarenja informacijama se nalaze različiti koncepti iz kibernetičke sigurnosti, privatnosti podataka, spisovodstva, informacijsko komunikacijske tehnologije, sukladnost sa pravom i ekonomijom informacija (infonomika) (Blair, 2012, p. 4). Glavni cilj je maksimizirati korisnost dostupnih informacija te istovremeno smanjiti troškove i rizike vezane uz njih što zahtijeva optimizaciju, sigurnost i kontrolu nad informacijama sa strane organizacije (InfoGovWorld, 2019, p. 1).

O gospodarenju informacijama se pisalo već nekoliko desetljeća, no pravi razvoj počinje ranih 2000-tih kada ga je počeo implementirati zdravstveni sustav Ujedinjenog Kraljevstva za bolju kvalitetu podataka i sigurnost osjetljivih informacija pacijenata (Lomas, 2010, p. 184). Britanska Nacionalna Zdravstvena Služba (engl. „*National Health Service*“, NHS) je već od 2002. godine zahtijevala od zdravstvenih organizacija da implementiraju njihove alate za gospodarenje informacijama (originalno „*Information governance toolkit*“, danas se naziva „*Data security and protection toolkit*“) (NHS, 2023, p. 1). Smallwood (2018, p. 4) argumentira da je jedan od razloga veće kvalitete zdravstvenog sustava Ujedinjenog Kraljevstva nad onog od SAD-a taj što je

njihov sustav bolji u „dostavljanju odgovarajućih informacija odgovarajućim ljudima u odgovarajuće vrijeme“.

U zadnjih nekoliko godina je mnogo pravnih i tehnoloških izazova potaknulo povećani interes u disciplinu. To uključuje propise kao što su GDPR (General Data Protection Regulation) i CCPA (California Consumer Privacy Act), velike količine podataka (engl. „*Big Data“*) i rastuće shvaćanje informacija kao imovinu sa pravom vrijednošću (Smallwood, 2018, p. 3).

GDPR, koji je stupio na snagu 2018. godine, je imao najveći utjecaj, jer je zahtijevao mnogo sustavnih promjena od svih tvrtka koje su spremale osobne podatke EU i EEA stanovnika (Intersoft Consulting, 2018, p. 1). Jedna od potreba je bila napraviti inventar svih prikupljenih podataka i odrediti gdje su sve te informacije spremljene, što je zapravo jedan od prvih koraka u implementiranju programa gospodarenje informacijama. Kasnije je CCPA, inspiriran GDPR-om, zahtijevao slične postupke za sve građane savezne države Kalifornije da se uvedu do 2020. što je značilo da su i tvrtke u SAD-u morale uvesti slične promjene (Smallwood, 2018, p. 3).

„Big Data“ je isto imao veliki utjecaj, jer sa rastom količine podataka u sustavima organizacija je došlo do nove potrebe za većom kontrolom i kvalitetom istih. Mnogi su ubrzo shvatili da je čuvanje svih informacija koje imaju neodrživo i kontraproduktivno. ROT (engl. „*redundant, outdated, trivial*“) informacije su postale glavna meta u rješavanju tog problema. Takve nepotrebne informacije stvaraju velike troškove, poteškoće u elektroničkom pronalasku (engl. „*eDiscovery*“) te moguće pravne probleme, zbog čega ih je potrebno sustavno i slijedno propisima uništiti (Smallwood, 2018, p. 4).

3. Gospodarenje podacima i gospodarenje informacijske tehnologije

Osim gospodarenja informacijama postoje i pojmovi gospodarenje podacima (engl. „*data governance“*) i gospodarenje informacijske tehnologije (engl. „*IT governance“*). Ona su zasebna polja, no spadaju pod gospodarenje informacijama. Robert Seiner (prema Smallwood, 2018) definira gospodarenje podacima kao „izvršenje i provođenje

ovlasti nad definicijom, produkcijom i korištenjem podataka“. Ono se bavi sa kvalitetom podataka na najtemeljnijoj razini, da su podaci točni, precizni i jedinstveni. Tu se koriste metode kao čišćenje podataka da se maknu netočni ili korumpirani podaci te deduplikacija koja miče iz sistema redundantne pojave podataka. Seiner (2024, p. 1) predlaže takozvano „neinvazivno“ gospodarenje podacima koje se organski integrira bez previše poremećaja tijekom rada. To se postiže pomoću integriranja promjena u postojeće sustave i prakse bez ometanja istih. Te promjene se lakše prihvate unutar organizacije kada se uspostave pomoću kooperacije radnika, a ne kada ih nametnu nadređeni.

Gospodarenju informacijske tehnologije je cilj poboljšati performansu informacijskog sustava te također postići poslovnu vrijednost kroz suradnju sa poslovnim ciljevima. Fokus nije samo na razvoju softvera i održavanje sustava, već to postići sa minimalnim troškovima prateći dokazane metode razvoja i principe iz gospodarenja podataka (Smallwood, 2018, pp. 21-22). Postoji pet domena gospodarenja informacijske tehnologije koje su bitne za prepoznati za potpuno postizanje moguće vrijednosti iz sustava (Hajela, 2024, p. 1). Ovih pet domena je:

- Dostavljanje vrijednosti: realiziranje vrijednosti iz ulaganja u informacijsku tehnologiju
- Strateško usklađivanje: usklađenost strategija sa poslovnim ciljevima
- Upravljanje performanse: stvaranje i praćenje performanskih metrika
- Upravljanje resursima: efikasno korištenje budžeta, osoblja i tehnologije
- Upravljanje rizicima: identificiranje i ublaživanje rizika vezanih uz informacijsku tehnologiju

4. Zašto je gospodarenje informacijama važno?

Jedan od najvećih problema kod implementiranja programa gospodarenja informacijama je razumjeti koji su sve koristi od njega i kako ih predstaviti nadređenima. Najočitiji razlog za implementaciju bi bio prisila od strane vlade kroz različite propise i zakone koje se organizacija mora držati, no potreba za gospodarenjem informacijama bi trebala biti i to što je blagotvorno za kontinuirano funkcioniranje (Blair, 2012, p. 5).

Organizacije mogu doživjeti godišnji rast u veličini spremljenih informacija od 30% do 100%. Makar se također razvijaju i rješenja za pohranu, taj razvoj nije dovoljan da se zanemari problem prenakupljanja informacija. Cijena spremanja tih informacija je samo dio poteškoća koje one mogu donijeti, one također otežavaju pronalazak potrebnih informacija i traže kontinuirano održavanje. Često se nema konkretan plan što će se napraviti s njima, to jest, koliko dugo će se čuvati, a ta odluka samo postaje težom što se duže čeka. Moguće je da hardver ili softver za čitanje tih informacija nije više dostupan, da odjel ili djelatnici koji su stvorili te informacije više nisu prisutni ili da je teže pronaći propise vezane uz čuvanje i uništavanje takvih informacija. Također ne možemo bilo što uništiti, potrebno je uzeti u obzir poslovnu vrijednost informacija i slijediti zakone koji se tiču njihovog spremanja na određeno vrijeme. Za to je potreban program koji će prilikom nastanka informacija odrediti gdje i koliko dugo će se čuvati (Blair, 2012, pp. 10-12).

Važna je i efikasnost radnika koja se poveća sa gospodarenjem informacijama. Mnoga istraživanja dokazuju da su radnici znanja preopterećeni sa informacijama iz različitih izvora, bili oni email, pozivi ili dokumenti. Ta preopterećenost vodi do nesnalaženja i gubitka efikasnosti na poslu. Makar isprva postoji faza odbijanja procedura kojih se moraju držati, djelatnici ubrzo shvate da su pogodne za njihov svakodnevni rad i da organiziranost koja dolazi sa programom gospodarenja informacijama im olakšava posao (Blair, 2012, p. 15).

Gospodarenje informacijama također kultivira organizacijsku kulturu. Multidisciplinarna priroda gospodarenja informacijama vodi do veće kooperacije između različitih odjela u organizaciji. Stvara sistem u kojem skupine surađuju do zajedničkog cilja, gdje je temelj okvir koji određuje kako svi spremaju i koriste informacije. Prije implementacije programa česta su uska shvaćanja ciljeva između odjela organizacije, na primjer spisovodstvo je fokusirano samo na dokumentarno, najčešće papirnato, gradivo, a odjel za informacijsku tehnologiju često se ne zanemaruje sa sadržajem koji prolazi kroz sustave koje održavaju (Blair, 2012, p. 18).

Program gospodarenja informacijama daje i osjećaj sigurnosti i samouvjerenja. Ne samo zbog zaštite od različitih kibernetičkih napada koju pruža, već i zbog znanja da sve informacije koje se unište iz sistema se može pravno obrazložiti. to je osobito bitno za internacionalne tvrtke koje operiraju pod mnogim zakonodavnim jurisdikcijama i industrije koje imaju mnoge stroge propise vezane uz parnice i ostale legalne

postupke. Ako ne postoji sustav koji pomaže u olakšavanju tih briga, organizacija može završiti u stanju prenatrpanosti informacija zbog straha od uništavanja pravno važnih dokumenata.

Također je bitna buduća korist koja dolazi sa takvim programom. Blair (2012, pp. 16-17) napominje da što ranije dođe do implementacije, to bolje, jer će u budućnosti biti samo teže to postići. Što više vremena prolazi to će biti više neorganiziranih informacija i njezinih izvora. Još k tome, što ranija implementacija znači da će se organizacija moći bolje prilagoditi budućim razvojima u tehnologiji ili zakonodavstvu.

5. Program gospodarenja informacijama

Za postizanje ciljeva gospodarenja informacijama potrebno je pokrenuti stalan program unutar organizacije. Važno je napomenuti da se tu ne radi o jednokratnom projektu već o planu kojeg će se cijela organizacija morati stalno pridržavati i koji bi se trebao stalno razvijati i usavršavati. Tehnologija i zakonodavstvo se stalno mijenja i zato je važno da je program fleksibilan i u mogućnosti prilagođavanja. Smallwood (2018, p. 9) takav program uspoređuje s programom za sigurnost na radnom mjestu koji se također stalno mijenja i isto zahtijeva redovite preglede da se odredi da sve funkcionira po programu. Još jedan važan aspekt programa je kolaboracija sa ostalim odjelima, ali i s radnicima organizacije. Važno je uskladiti odjele na zajednički cilj te educirati sve radnike što se od njih očekuje da se program može pokrenuti.

Jedan od najvažnijih koraka kod uspostavljanja programa je dobiti odobrenje od upravnog odbora. Smallwood (2018, p. 69) kaže da je najbrži način dobivanja tog odobrenja kad se desi nekakva veća nesreća, ili novčana kazna ili povreda podataka. Najčešće tek onda su tvrtke zainteresirane za implementacijom, no moguće ih je i prijevremeno upozoriti o takvim prijetnjama te implementirati program prije nego što se nešto takvoga desi. Smallwood (2018, p. 70) preporučuje da se jedan od članova odbora uzme kao izvršni sponzor koji bi garantirao da se program provede i kao pomoć tijekom planiranja i odlučivanja.

Nakon toga je bitno formiranje tima i dodjeljivanje uloga. Najvažnije uloge za popuniti su te izvršnog sponzora i menadžera za program gospodarenja informacijama, no zbog multidisciplinarnosti gospodarenja informacijama također bi trebali imati i nekoga

iz odjela za informacijsku tehnologiju, nekoga iz spisovodstva, nekoga iz legalnog tima te po mogućnosti nekoga specijaliziranog za sigurnost podataka i privatnost podataka. Osim njih važno je uključiti odjele na koje bi takav program najviše utjecao i odjel za ljudske resurse koji bi kasnije pomogli u edukaciji novih strategija (Smallwood, 2018, pp. 72-73).

Program gospodarenja informacijama bi trebao imati poslovne i strateške ciljeve tvrtke na umu. Na primjer, ako tvrtka planira stjeći manje konkurente, onda bi program morao uzeti u obzir kako bi integrirao druge sustave u sadašnji. Općenito bi politike, vezane uz email, mobitele, formatiranje izvještaja ili druge, morale usmjeravati prema zajedničkom cilju (Smallwood, 2018, pp. 73-74).

Konačno, prije samog formuliranja plana za program, važno je uzeti u obzir tehnološke, financijske i zakonodavne uvjete u kojim organizacija djeluje. Pod tehnološke uvjete se trebaju razmatrati trendovi u sektoru informacijske tehnologije i bile li se te nove tehnologije, bile one softver ili hardver, mogle inkorporirati unutar informacijskog sustava tvrtke i time programa gospodarenja informacijama. Ako industrija tvrtke ili ekonomija općenito slijedi negativan trend onda je teže naći financiranje za implementaciju svih željenih dijelova programa ili čak programa uopće. U takvom slučaju najbolje bi bilo implementirati plan samo u odjelima gdje bi najviše utjecao te zatim kasnije proširiti na cijelu organizaciju. Pomoću razgovora sa legalnim timom tvrtke bi se identificirali zakoni i propisi koje treba uzeti u obzir. Razmatralo bi se koji su konkretni zahtjevi zakona, koji su dijelovi više interpretativni, koju poziciju bi tvrtka zauzela ako ima takvih dijelova, kakvi su legalni rizici i tako dalje. Smallwood (2018, p. 77) napominje da bi legalni zahtjevi trebali imati prednost nad svim ostalim uvjetima kod formiranja plana.

Sam plan bi morao uzeti u obzir sve te uvjete te doprinose svih članova tima s kojima bi se formirao plan u nekakav konačan oblik pri čemu bi izvršni sponzor pomogao u balansiranju potreba svih participirajućih odjela. Specifične politike bi se trebale definirati s time da bi se trebala prioritizirati polja prema ciljevima organizacije (Smallwood, 2018, p. 82).

6. Principi gospodarenja informacijama

Tijekom slaganja plana i politika vezano uz program gospodarenja informacijama, bilo bi pogodno služiti se nekim od mnogih setova principa koje su različiti autori ili skupine složili kao usmjeravanje za takve projekte. Ti principi mogu biti specifično za gospodarenje informacijama ili mogu biti napravljeni za neka od polja kojima se bavi i gospodarenje informacijama.

Jedan set principa vezani specifično uz gospodarenje informacijama bi bili principi Sedona konferencije (engl. „*Sedona Conference*“). Ta konferencija se sastoji od stručnjaka prava i tehnologije te slažu smjernice za područja kao što su elektronički pronalazak, upravljanje rizicima i slično. Njihovih principi za gospodarenje informacijama su napravljeni da pomognu u usmjeravanju tima i za bolje shvaćanje gospodarenja informacijama (Sedona Conference, 2019, pp. 120-154). Ti principi su:

1. Organizacije bi trebale razmotriti implementaciju programa gospodarenja informacija da bi mogli bolje koordinirati odluke oko informacija koje bi pokrivale potrebe informacija i njezine rizike te da bi optimizirali njezinu vrijednost
2. Program gospodarenja informacijama bi trebao biti dovoljno neovisan od bilo kojeg odjela da bi se osiguralo da odluke koje su donesene su u interesu cijele organizacije
3. Svi sudionici informacijskog sustava organizacije bi trebali biti uključeni u stvaranju programa
4. Svi strateški ciljevi programa bi trebali biti temeljeni na poznavanju prakse, potreba, rizika i prilika informacija
5. Program bi trebao bit složen sa pravilnom strukturom, usmjerenjem, resursima i odgovornošću koje daju prihvatljivo uvjerenje da će planirani ciljevi biti dostignuti
6. Efektivno, konzistentno i vremenski prihvatljivo uništavanje fizičkih i elektroničkih informacija koje se više ne trebaju čuvati bi trebalo biti jedna temeljna komponenta programa
7. Kada se organizacija nalazi u situaciji gdje postoje proturječni zakoni organizacija bi trebala djelovati sa dobrom namjerom uzimajući u obzir privatnost, sigurnost podataka, upravljanje rizicima i općenito dobre poslovne prakse

8. Ako je došlo do takve situacije gdje je organizacija djelovala sa dobrom namjerom pod proturječnim zakonima, sud sa autoritetom za pregled njezinih aktivnosti bi trebao djelovati sa određenom razinom razumnosti vidjevši njihovu situaciju
9. Organizacija bi trebala razmišljati o mjerama za održavanje integriteta i dostupnosti dugotrajnih informacija kroz njihov očekivani životni vijek
10. Organizacija bi trebala razmatrati korištenje nove tehnologije u svojem programu
11. Organizacija bi trebala periodično pregledati i nadograđivati svoj program da osigura da program ispunjava potrebe organizacije kroz njezin razvoj

Smallwood (2018, pp. 30-34) je napisao i svoje principe za gospodarenje informacijama. Bazirao ih je na svojem iskustvu u industriji kao konzultant koje je skupio i analizirao kroz zadnje desetljeće. Preporučuje da bilo koja organizacija koja želi uspjeh u provedbi programa gospodarenja informacijama bi se trebala držati ovih principa:

1. Cijeniti informacije kao imovinu - Isto kako organizacija ima fizičku imovinu koju cijene, tako bi se i informacije koje su prikupljene trebali smatrati vrijednim.
2. Konzultacija sa sudionicima - Oni koji rade najviše sa informacijama najbolje znaju zašto su potrebne i kako upravljati s njima
3. Integritet informacija – suradnja između organizacije i ostalih organizacija ili potrošača počiva na vjeri i to uključuje da su informacije unutar organizacije točne i sigurne
4. Organizacija i klasifikacija informacija – to ne uključuje samo dokumente koji nastaju tijekom transakcija, već bilo koje informacije unutar organizacije koje bi trebali biti kategorizirane na standardizirani način i dodijeljene sa metapodacima
5. Sigurnost i privatnost informacija – prvo bi se trebala postaviti sigurnost i tek onda se može postaviti privatnost informacija. Najvažnije informacije za takve postupke su PII (engl. „*Personally Identifible Informarion*“), PHI (engl. „*Protected Health Information*“) i PCI (engl. „*Payment Card Industry data*“) koje bi trebale biti sigurne kroz sva tri moguća stanja u kojem mogu biti: mirovanje, micanje, korištenje.
6. Dostupnost informacija – dostupnost se mora balansirati sa sigurnošću. Informacije autoriziranim korisnicima bi trebale biti lake za locirati i koristiti što

podrazumijeva intuitivno korisničko sučelje i dobru praksu iz područja upravljanja identitetom i pristupa (engl. „*identity and access management*“).

7. Kontrola informacija – organizacija mora složiti standardizirani i automatizirani proces obavještavanja o zamrzavanju radnji nad informacijama koji bi osigurao da se pravno relevantni čuvaju na propisano vrijeme.
8. Pregled programa gospodarenja informacijama – tijekom razvoja programa potrebno je postaviti mjere kojima će se moći objektivno mjeriti napredak programa i usklađenost djelatnika sa programom. Trebalo bi se i nadgledati sva aktivnost elektroničke pošte, generiranje izvještaja i slično kao mjera protiv aktivnosti koje bi bile protiv postavljenih propisa.
9. Izvršni sponzor – nikakav trud za osnivanje programa gospodarenja informacijama neće uspjeti bez odgovornog izvršnog sponzora koji će sastaviti budžet programa i usmjeravati program.
10. Mijenjanje upravljanja – za postizanje ciljeva programa potrebno je uvjeti upravni odbor da su promjene koje dovodi program potrebne i da će se dijelovi organizacije morati temeljno promijeniti
11. Kontinuirano unapređenje – napredak programa se mora konstantno nagledati te se program mora usavršavati sa znanjem stečenog od tog nadgledavanja i sa različitim promjenama koje organizacija može doživjeti kroz vrijeme.

Vidjevši da je velik dio gospodarenja informacijama spisovodstvo i upravljanje sa dokumentima, dobra je i praksa uzimanja u obzir principa iz tog područja. Ovdje bi bili bitni principi koje je složio ARMA (engl. „*the Association of Records Managers and Administrators*“) zvani GARP (engl. „*Generally accepted recordkeeping principles*“) (ARMA, 2017, p. 1). Njihov cilj je usavršiti praksu spisovodstva i glase:

1. Odgovornost – član odbora bi trebao nadgledavati spisovodstveni program i delegirati određene odgovornosti odgovarajućim djelatnicima.
2. Transparentnost – aktivnosti spisovodstva bi se trebale dokumentirati i biti dostupne prikladnim strankama
3. Integritet – program spisovodstva bi trebao imati prikladnu razinu pouzdanosti za dokumente koje se nalaze u sustavu organizacije
4. Zaštita - trebale bi postojati mjere koje će garantirati određenu mjeru sigurnosti za dokumente koji imaju povjerljive informacije

5. Usklađenost – program se treba konstruirati da je usklađen sa zakonima i propisima organizacije
6. Dostupnost – dokumenti se moraju čuvati na način da su lako dostupni autoriziranim osobljem
7. Čuvanje – dokumenti se moraju držati na određeno vrijeme prateći zakone, ali i operacionalne i poslovne potrebe
8. Izlučivanje – organizacija mora pružiti sigurno i odgovarajuće izlučivanje kada dokumenti više nisu potrebni

Sličan naziv nosi i set principa koje su zajedničkim snagama razvili CICA (engl. „*Canadian Institute of Chartered Accountants*“) i AICPA (engl. „*American Institute of Certified Public Accountants*“). GAPP (engl. „*Generally Accepted Privacy Principles*“) služe za dostizanje dobre prakse u području privatnosti informacija koja postaje sve važnije sa zakonima kao što su GDPR i CCPA (Clarke, 2017, p. 1). GAPP su:

1. Upravljanje – organizacija dodjeljuje određene odgovornosti djelatnicima za provedbu mjera za privatnost informacija
2. Obavijest – Organizacija obavijesti svoju politiku privatnosti. To uključuje svrhu zašto se osobni podaci skupljaju
3. Izbor i pristanak – organizacija predstavi izbore korisnicima i osigura eksplicitni pristanak na navedene uvjete
4. Prikupljanje – prikupljaju se podaci jedino prema već postavljenim kriterijima
5. Korištenje, čuvanje i izlučivanje - osobni podaci su dostupni samo organizaciji, čuvaju se na određeno vrijeme te zatim unište na odgovarajući način
6. Pristup – organizacija nudi mogućnost pregleda i ažuriranje osobnih podataka
7. Razotkrivanje trećim strankama – informacije se dijele sa trećim strankama samo zbog identificiranih razloga i sa pristankom pojedinca
8. Sigurnost i privatnost – informacije su zaštićene od neautoriziranog pristupa
9. Kvaliteta – organizacija održava informacije koje su točne, potpune i relevantne za identificirane ciljeve
10. Nadgledanje i primjenjivanje – organizacija nadgledava sukladnost s politikama privatnosti. Također ima spremne mjere za rješavanje sporova

Nešto što svi ti principi imaju zajedničko je što govore o bitnosti postavljanja odgovornosti unutar organizacije i što napominju da bi se program morao nadgledati i usavršavati.

7. Politike gospodarenja informacijama

Za stvaranje politika programa gospodarenja informacijama trebalo bi se služiti sa uspostavljenim modelima, principima, standardima i dobrim praksama. Moguće je da su neke od tih već prisutne u nekim odjelima pa bilo dobro iskoristiti to da se lakše prošire na cjelokupan program i time na cijelu organizaciju (Smallwood, 2018, p. 87).

Projekt EDRM (engl. „*Electronic Discovery Reference Model*“) uz suradnju sa ARMA i CGOC (engl. „*Compliance, Governance and Oversight Council*“) su razvili GRM (engl. „*Information Governance Reference Model*“). Najnovija verzija ima dodane privatnost i sigurnost kao sudionike zbog njihove povećane važnosti kroz vrijeme. Model je napravljen kao okvir putem kojeg bi se lakše shvatio program gospodarenja informacijama i za poboljšanu komunikaciju i suradnju najvažnijih odjela za program (EDRM, 2023). Osim prije spomenute privatnosti i sigurnosti to također uključuje odjele za poslovanje, pravo, informacijsku tehnologiju i spisovodstvo.

Najbolje prakse bi bilo isto važno uzeti u obzir. Smallwood (2018, pp. 91-92) je napravio svoju listu od 21 točke, no neke se preklapaju sa principima. One koje se ne ponavljaju sa prijašnjim principima i koje se ističu su:

- Poslovni procesi se trebaju redizajnirati kada se implementiraju nove tehnologije za veću učinkovitost
- Pomoću analitike poboljšati stvaranje odluka i maksimizirati vrijednost informacija
- Koristiti gospodarenje podataka za poboljšanje kvalitete podataka
- Stvoriti standardizirane metapodatke za bolji pronalazak informacija
- Napraviti plan za rizike informacija
- Zabraniti osobno spremanje elektroničke pošte
- Spremiti najvažnije dokumente kao dio dokumentarnog nasljeđa organizacije

Najvažniji alati za stvaranje politika u organizaciji bi bili standardi. To uključuje „prave“ standarde kao one koje objave tijela kao što su ISO (engl. „*International Organisation for Standardization*“) ili „de facto“ standarde kao što su Microsoft-ovi formati. Neke od koristi implementiranja standarda su osiguranje kvalitete, interoperijabilnost sa ostalim sustavima i moguće smanjenje troškova održavanja. No postoje i poteškoće koje standardi mogu donijeti kao što su smanjenje fleksibilnosti, moguća nesukladnost sa

praktičnim svijetom i „zbunjenost standardima“ zbog više standarda koji se preklapaju. Neki od standarda koji pokrivaju polja vezana uz gospodarenje informacijama uključuje ISO 31000:2009 za upravljanje rizicima, ISO/IEC 27001:2013 za upravljanje sigurnost informacija, ISO/IEC 38500:2008 za upravljanje informacijske tehnologije, ISO 15489:2016 za spisovodstvo i ISO 22301 za kontinuitet poslovanja (Smallwood, 2018, pp. 93-97).

Uzimajući u obzir sve te alate i doprinos sudionika se onda slažu specifične politike. One moraju biti precizne i dobro komuniciranje djelatnicima. Tu mogu biti pomoć politike iz srodnih organizacija, no važno je ih ne samo kopirati bez da se prilagode. Prije implementacija važno je čuti što odjeli imaju reći o tim politikama i njima se prilagoditi, jer ako oni nisu sa njima zadovoljni teže će doći do usklađenosti sa politikama (Smallwood, 2018, p. 105)

8. Gospodarenje informacijama i poslovanje

Veza programa gospodarenja informacijama i poslovanja je najočitija kod poslovnih tvrtki. Tamo je osobito bitno da se program uskladi sa poslovnim ciljevima što će povećati interes upravnog odbora za program. Na primjer, ako tvrtka traži dobru reputaciju među kupcima onda bi program se dodatno fokusirao na sigurnost i privatnost podataka (Smallwood, 2018, pp. 115-116). Općenito program bi doprinosio poslovanju organizacije tako da bi smanjio troškove informacija u sustavu i da bi našao ili poboljšao vrijednost iz informacija. Za to se mogu primijeniti koncepti iz infonomike. Infonomika je disciplina koja se zagovara za promatranje informacija kao imovinu sa vrijednošću. Najčešće tvrtke imaju kvalitetne mjere za upravljanjem fizičke imovine, ali ne i za informacije. Informacije zahtijevaju isto upravljanje nad njima, ali to upravljanje ne može biti te isto kao što je ono za fizičku imovinu zbog karakteristika informacija. Informacije ne degradiraju, ne nestanu nakon što ih iskoristimo, ne oporezuju se tijekom transakcije, lagano se dupliciraju i transportiraju (Laney, 2018, p. 20).

Točni troškovi informacija i načini kako, i za koliko, smanjiti te troškove je nemoguće točno izračunati. Troškovi informacija nije samo njihovo spremanje, već uključuje trošak održavanje, sigurnosnih programa, elektronički pronalazak i slično. Ovdje ne pomaže trend rastućeg volumena informacija koji povećava troškove spremanja, ali i

gubljenja efikasnosti zbog otežanog elektroničkog pronalaska. Pomoću modela potpunog obračuna troškova (engl. *„full cost accounting“*) za informacije se traži najtočnija procjena troškova, i onih direktnih i indirektnih. Ti troškovi mogu biti administrativni, troškovi zbog operacija i osoblja odjela informacijske tehnologije, troškovi elektroničkog pronalaska, novčane kazne, i budući troškovi kao migracije na druge sustave i slično. Jasnija slika pravih troškova informacija omogućuje upravnom odboru da prave bolje odluke o tome kako će rukovati sa informacijama u organizaciji (Smallwood, 2018, pp. 122-124).

Drugi dio poslovne sfere i gospodarenja informacijama je vrijednost koja se nalazi u njima. U poslovanju se vrijednost informacija gleda kroz njihovu ulogu u analizi odluka. One pomažu usmjeravati prema boljim odlukama, kao što je na primjer tijekom biranja investicijskih opcija. U infonomici se modeli za mjerenja vrijednosti informacija dijele na fundamentalne i financijske. Fundamentalni modeli vrijednosti se bave sa njihovom kvalitetom, dok su financijski modeli bolje namijenjeni pridodavanju ekonomske vrijednosti informacijama. Pod financijske modele spadaju troškovna vrijednost koja gleda koliko bi koštalo ako bi se te informacije izgubilo, tržišna vrijednost koja gleda koliko bi mogli dobiti za te informacije na otvorenom tržištu i ekonomska vrijednost koja uspoređuje prihode prije i poslije inkorporiranja tih informacija u analize i odlučivanje. Svi ti modeli imaju neke svoje nedostatke, na primjer neke informacije (PII, PHI, PCI) se ne može prodavati na otvorenom tržištu pa se za njih ne može dobiti tržišna vrijednost, no svejedno nam mogu pomoći u otkrivanju koje informacije je bitno čuvati i kako nam mogu pomoći u poslovanju organizacije (Laney, 2018, pp. 293-295).

Za postizanje poslovnih ciljeva pomoću informacija Smallwood (2018, pp. 127-129) predlaže 3 koraka:

1. Čišćenje – Čišćenje informacijskog sustava od ROT informacija te ostavljanje samo vrijednih informacija ili onih koje je potrebno čuvati zbog legalnih razloga. Već sa tim korakom pridonosimo poslovanju zbog smanjenja troškova vezanih uz spremanje i održavanje informacija.
2. Izgradnja i održavanje – da ne dođe do iste situacije gdje bi trebalo opet čistiti sustav od ROT informacija potrebno je izgraditi i održavati program gospodarenja informacijama koji će postaviti mjere da se to ne dogodi
3. Monetizacija – konačno treba izvući tu vrijednost iz informacija i koristiti ih za poslovne svrhe. To može biti analiza strukturiranih informacija za postavljanje

cijena, ili analiza nestrukturiranih informacija, na primjer različitih poruka elektroničke pošte djelatnika za povećano zadovoljstvo kupaca

9. Gospodarenje informacijama i pravo

Vjerojatno najvažnije polje koje ima odnos sa gospodarenjem informacijama je pravo. Pravne potrebe bi uvijek trebale imati prioritet nad ostalima, jer ako se organizacija ne drži zakona može biti novčano kažnjena ili zatvorena. Najvažnije funkcije koje program mora pravilno odrađivati su spremnost za elektronički pronalazak, politike retencije, obavještavanje o zamrzavanju radnji nad informacijama iz pravne potrebe (engl. „*legal hold notification*“) i pravno obranjivo brisanje informacija (engl. „*defensable disposition*“) (Smallwood, 2018, p. 135).

Tijekom parnica i ostalih sudskih procesa, tužitelj i tuženik pronalaze dokaze vezane uz tužbu. Svaka strana mora pronaći informacije koje se od njih traže ili objasniti zašto takav zahtjev nije prihvatljiv. Ako se ti zahtjevi ne odrade u određenom vremenskom razdoblju onda dolazi do kazna. Ti zahtjevi mogu biti za informacije i u fizičkom obliku i u elektroničkom. Elektronički spremljene informacije (engl. „*electronically stored information“*) može uključiti informacije iz elektroničke pošte, CD/DVD, pametnih telefona, tvrde diskove i slično. Zato je bitno da program gospodarenja informacijama pokriva pronalazak za sve oblike elektronički spremljenih informacija koje se koriste u organizaciji. Efektivan elektronički pronalazak informacija zahtijeva kooperaciju legalnog tima i ostalih odjela za prepoznavanje važnih informacija i njihovo čuvanje.

obavještavanja o zamrzavanju radnji nad informacijom iz pravne potrebe (engl. „*legal hold notification“*) je proces kojim se obavijeste odgovarajući djelatnici o sudskom procesu koji je pokrenut ili bude pokrenut te koje određene dokumente se toga tiču. Ti dokumenti se moraju čuvati i ne smiju se više mijenjati tako da ih mogu pregledati za to zadužena tijela. Važno je da postoje mjere koje će to osigurati i da se takav posao ne eksternalizira (Smallwood, 2018, pp. 144-145).

Na zamrzavanje radnji se nadovezuje i obranjivo izlučivanje. To je izlučivanje koje se drži regulacija i bilo bi obranjivo pred sudom. Nakon što se planom odrede koje informacije bi se htjele izlučiti potrebno je postaviti sistem koji će to regulirati. Najčešće se počinje sa elektroničkom poštom, ne samo zato što ju je mnogo, nego zato što za

nju već postoje izgrađeni sustavi za čuvanje i izlučivanje. Nakon što se uspostavi sustav i regulacije nad elektroničkom poštom se pomoću tog iskustva može lakše postaviti sustavi i za ostale dokumente. Metode koje se koriste za determiniranje koje informacije bi se trebale izlučiti su prediktivno kodiranje (engl. „*predictive coding*“) koje pomaže tijekom takve analize pomoću automatskog označivanja dokumenata i pregled uz pomoć tehnologije (engl. „*technology assisted review*“) koji koristi neke metode prediktivnog kodiranja, ali uz puno veću ljudsku intervenciju (Smallwood, 2018, pp. 153-156).

10. Gospodarenje informacijama i spisovodstvo

Spisi su među bitnijim informacijama koje možemo naići u organizacijama pa se oni, te samo spisovodstvo također pokriva sa programom gospodarenja informacijama. Specifično, program se fokusira na upravljanje elektroničkih spisa (engl. „*electronic records management*“) koje se bavi sa spisima, u elektroničkom i u papirnatom obliku, te ostalim elektroničkim dokumentima pomoću elektroničkog sustava. upravljanje elektroničkim spisima se bazira na klasičnom spisovodstvu, no mora uzeti u obzir karakteristike elektroničkog oblika. To pridonosi mnoge izazove organizaciji, uključujući stalan razvoj tehnologije, oslanjanje na odjel informacijske tehnologije i sigurnosne izazove koji dolaze sa elektroničkim oblikom. Svejedno, uspostava takvog sustava doprinosi efikasnosti organizacije, samopouzdanja djelatnika i profesionalnosti radnog okruženja (Smallwood, 2018, pp. 161-163). U uspostavi mjera vezane uz spisovodstvo trebalo bi se držati GARP principa.

Prvi korak bi bio napraviti popis vrsta dokumenata (klasa ili dugih, ovisno o okolini i propisima). Taj popis nije lista svih dokumenata koja organizacija ima, već dokument koji opisuje sve serije koje postoje. Zbog elektroničkog oblika ti spisi mogu biti u različitim serverima i mogu imati kopije zbog kojih je teže saznati koji je original. Stvaranje ovih popisa je zapravo vrsta istraživanja koja može koristiti upitnike, intervjue, inspekcije, softverske alate ili neku kombinaciju tih. Koliko je opširno to istraživanje ovisi o upotrebama inventara (Smallwood, 2018, pp. 168-182).

Primjer ovoga su popisi gradiva s rokovima čuvanja (engl. „*retention list“).* Ti popisi određuju koliko dugo će se određene vrste (klase ili podserije) spisa čuvati. Oni moraju

pokrivati sve spise unutar organizacije, uzeti u obzir pravne i poslovne potrebe te bi se trebale redovito ažurirati. U interesu organizacije je da su ti rokovi čuvanja što kraći, jer time smanjuju troškove koje uključuje čuvanje spisa na duže vrijeme. Spisi se prije određivanja rokova grupiraju prema poslovnim funkcijama kako bi se jednostavnije mogli pridodati i pratiti rokovi čuvanja. Nakon isteka rokova čuvanja spisi se izlučuju. Izlučivanje nije samo uništavanje nego može biti i predaja spisa nekom drugom tijelu, kao što je arhiv. To se također određuje pomoću popis gradiva s rokovima čuvanja (Smallwood, 2018, pp. 192-194).

11. Gospodarenje informacijama i informacijska tehnologija

Odjel za informacijsku tehnologiju je isto bitan u uspostavi programa gospodarenja informacijama. Oni su bitni da informacijski sustav organizacije (serveri, mreže, aplikacije) funkcionira. No često se taj odjel ne brine toliko o sadržaju koji prolazi kroz sustav što ih je često suzdržalo od nekih odgovornosti. Pomoću programa gospodarenja informacijama se pokuša odjel informacijske tehnologije bolje integrirati u cjelokupan plan organizacije i pomoću određenih programa bi se cilj programa bolje izveo (Smallwood, 2018, p. 211).

Gospodarenje podataka bi bio program kojim bi se poboljšala kvaliteta podatak organizacije. To je bitno zbog efikasnijeg elektroničkog pronalaska i poboljšane vrijednosti podataka. Izazov gospodarenja podataka je postići kontrolu nad velikim količinama podataka i njezino čišćenje i čuvanje. Kvaliteta koja dolazi sa tim programom je na najnižoj razini tako da svi izvještaji, analize i odluke koje prolaze iz podataka su isto kvalitetne (Smallwood, 2018, pp. 213-214).

Upravljanje informacijama je jedna funkcija iz gospodarenja informacijskim tehnologijama. Radi se o primjenjivanju različitih menadžerskih tehnika za prikupljanje, procesiranje i komuniciranje informacija. Upravljanje podacima (engl. „*master data management*“) je proces kojim se osigurava da pouzdani podaci iz jednog izvora se koriste kroz više poslovnih jedinica. Eliminiraju se nekonzistentni setovi podataka s čime se postiže „jedinstvena verzija istine“. Životni ciklus informacija (engl. „*information life cycle management*“) je funkcija upravljanja informacijama kojom se osigura

pravilno korištenje i održavanje informacija kroz njihov životni vijek. To uključuje sve od samog kreiranja, korištenja, spremanja i uništavanja ili arhiviranja. Različite informacije imaju različite vrijednosti i životne cikluse pa je bitno znati kakve vrste čuvanja one trebaju. Pod arhitekturu podataka se podrazumijeva dizajn sustava za strukturirane i nestrukturirane podatke. Što je kvalitetniji taj dizajn time je lakše procesirati i transportirati podatke među aplikacijama ili sustavima. Tijekom dizajniranja tih sustava važno je uzeti u obzir strukturu podataka, koje baze podataka se koriste te čak operacionalni sustavi na kojima se nalaze te baze.

Konačno, gospodarenje informacijske tehnologije objedinjuje sve ovo prijašnje te također mjere koje povećavaju efikasnost i vrijednost informacijskog sustava. To uključuje smanjenje troškova i razvoj softvera da se sa uloženim novcem u informacijsku tehnologiju postignu poslovni ciljevi. Za implementaciju programa gospodarenja informacijama se preporučuje uzeti jedan od standarda, najčešće COBIT ili ITIL (Smallwood, 2018, pp. 220-222)

12. Gospodarenje informacijama i privatnost i sigurnost

Privatnost i sigurnost idu jedna sa drugom. Prije uspostave privatnosti prvo se mora postaviti sigurnost. Ako se to dvoje ne uspije organizacije mogu doživjeti velike novčane i reputacijske probleme. Važnost privatnosti i sigurnosti informacija je naglo porasla nakon dolaska GDPR-a i CCPA-a, koji su kupcima dali nova prava, a tvrtkama nove izazove u kontroliranju njihovih podataka (Smallwood, 2018, p. 229).

Privatnost je drugačija od sigurnosti po tome što je subjektivna, a ne objektivna. Radi se o kontroliranju organizacije ili osobe koje su informacije javno dostupne, no koje informacije se smatraju privatnim varira. Svakako bi organizacije trebale shvatiti privatnost informacija važnom, ne samo zbog zakona koji se njih tiču, već i zato što je to nešto što je važno njihovim korisnicima ili kupcima (Smallwood, 2018, p. 230). Ovdje pomažu GAPP koje bi se organizacija trebala držati za kvalitetnu praksu privatnosti informacija.

Sigurnost informacija je ono što mora doći prije privatnosti. Ta sigurnost mora nastati kroz različite mjere protiv vanjskih, ali i unutarnjih prijetnji organizaciji. Vanjski napadi postaju sve češći, a još k tome teško ih je ponekad prepoznati da se uopće dešavaju pa time mogu trajati na duže vrijeme. Ako se napad dovoljno dobro prikrije, napadači mogu ne samo prijašnje dokumente i poruke, već i one koje trenutačno nastaju kroz vrijeme. Ti napadači mogu biti konkurenti koji će ukradene informacije koristiti za prednost u tržištu ili kriminalci koji osobne podatke korisnika prodaju na crnom tržištu. Također postoje i unutrašnje prijetnje koje mogu biti maliciozne ili slučajne greške. Maliciozni napadi su oni koji su napravljeni namjerno na štetu organizacije što uključuje oštećenje sustava ili krađu informacija. Motivi koji stoje iza toga mogu biti mržnja prema organizaciji od strane nezadovoljnih djelatnika ili špijuni koji rade neprijateljsku stranu. Prijetnje mogu biti i slučajne zbog ljudske greške, na primjer slanje krive datoteke preko elektroničke pošte (Smallwood, 2018, pp. 245-248).

Za bolju obranu protiv prijetnji, i malicioznih i slučajnih, jedna od lakših i bržih metoda za provesti je trening svijesti o sigurnosti (engl. „*security awareness training*“). Trening je dizajniran da nauči djelatnike kako na konzistentan i siguran način rukovati sa informacijama i najčešće sheme kojim napadači pokušavaju prodrijeti u sustav. To uključuje trening za obrane protiv socijalnog inženjerstva i lažnih poruka i elektroničke pošte (engl. *phishing*). Uz trening često dolaze i simulirani napadi kojima se djelatnici najbolje upoznaju sa vanjskim prijetnjama i kako na njih reagirati. Slično se radi i sa testiranjem tehničkog aspekta sigurnosti informacijskog sustava. Testiranje prodiranja (engl. „*penetration testing*“) je tehnika kojom stručnjaci kibernetičke sigurnosti traže slabosti u sigurnosnom sistemu organizacije. Metode, koje zapravo i napadači koriste tražeći slabe točke, uključuje napade grubom silom (engl. „*brute force attacks*“), iskorištavanje neažuriranih dijelova sistema i alate za probijanje lozinka. Često individualne slabe točke ne mogu izazvati velike prodore, no zajedno mogu dovesti do uspješnog napada. Međutim, napadači često traže lagane načine prodora, tako da ako nema isprva očite metode za ulazak u sustav često će se rađe fokusirati na neku drugu žrtvu (Smallwood, 2018, pp. 248-249).

Također je bitno koristiti tehnologiju kriptografije. Kriptografija je tehnika kojom se osigura da su informacija čitljive jedino onima kojima su namijenjene. To se postiže tako da se dokumenti šifriraju pomoću jednog od mnogih dostupnih algoritama i ključem koji određuje točno šifriranje i dešifriranje. Ako bi napadači došli do šifriranih

dokumenata mogli bi ih pročitati jedino ako imaju i ključ ili ako uspiju probiti šifru što je praktički nemoguće sa kvalitetnim šifriranjem. Na kriptografiji se bazira još jedan sustav, a to su digitalni potpisi, specifično infrastruktura javnog ključa (engl. „*public key infrastructure*“). Njima se determinira ako je dokument izgubio integritet (je li bio mijenjan sadržaj) i ako je osoba koja je potpisala taj dokument stvarno ta koja se predstavlja da je. To osigurava da maliciozne osobe ne mogu slati u sustav krive dokumente i time kompromitirati sustav (Brzica, 2018, pp. 39-40).

Još jedan sustav za sigurnost informacija bi bila prevencija gubitka podataka (engl. „*data loss prevention*“). Time se bave specijalizirane tvrtke koje nude programe i hardver kojima se ograničava koji dokumenti i poruke mogu napustiti sustav organizacije. To se napravi tako da se gledaju ključne riječi, koji je oblik dokument, vrijeme dana slanja i drugo. Nedostaci tog sistema su da može usporiti sustav i što ne funkcionira najbolje sa šifriranim porukama. Srodna tehnologija prevenciji gubitka podataka, i koja se sinergijski može koristiti uz nju, je upravljanje pravima informacijama (engl. „*information rights management*“). Ono stvara mjere kojima se ograničavaju koje radnje određene skupine mogu poduzeti sa informacijama. Određuje koja prava netko ima u vezi informacija, uključujući pristup, uređivanje, kopiranje i slanje elektroničkom poštom. To pruži sigurnost informacijama kroz njihov cijeli životni vijek, kroz bilo koje stanje (tijekom korištenja, tijekom slanja, tijekom mirovanja) (Smallwood, 2018, 262-268).

13. Gospodarenje informacijama i specifične tehnologije

13.1. Elektronička pošta

Elektronička pošta je često tehnologija koja proizvodi među najvećim količinama informacija u organizaciji. Često postoje već ugrađeni sustavi kojima se poruke mogu lagano upravljati, no svejedno organizacija često rade greške vezane uz njih. Često se nađu na suprotnim ekstremima gdje ili dugotrajno čuvaju sve poruke ili brišu sve poruke zanemarujući njihov sadržaj (Blair, 2012, p. 22).

Pomoću programa gospodarenja informacijama se postavljaju mjere za sigurno i efektivno korištenje elektroničke pošte. To uključuje sustave za arhiviranje elektroničke pošte koji automatski arhiviraju poruke i čuvaju ih na određeno vrijeme. To se napravi u trenutačno tijekom slanja što osigurava integritet poruka i da ostanu prihvatljive kao dokazi u legalnim procesima. Takav sustav također olakšava elektronički pronalazak specifičnih poruka što daje prednost legalnom timu u pravnim sporovima. Važno je napomenuti da bi osobno arhiviranje poruka na radnom mjestu trebalo bit zabranjeno jer narušava sigurnost sustava (Smallwood, 2018, p. 286).

13.2. Instantne poruke

Instantne poruke (engl. „*instant messaging*“) je tehnologija koja je, kao mnoge, prešla iz privatne sfere u poslovnu. Sada su instantne poruke neizbježan dio organizacijske kulture što donosi neke probleme. One se često koriste za neformalne razgovore između djelatnika i često se slabije regulirane nego elektronička pošta makar čak i u tim neformalnim razgovorima se mogu pojaviti informacije koje bi mogle naštetiti organizaciji ako bi se našle u krivim rukama (Smallwood, 2018, p. 291-293). Zbog toga Quest softvare predlaže ove politike vezane uz instantne poruke (većinom se mogu primijeniti i na elektroničku poštu):

1. Jasno objasniti svrhu instanih poruka u organizaciji djelatnicima
2. Objasniti djelatnicima da se instante poruke mogu nadgledavati sa strane organizacije
3. Definirati prihvatljive i neprihvatljive upotrebe instantnih poruka u organizaciji
4. Definirati ograničenja oko vrste sadržaja i mogućih kontakata
5. Objasniti posljedice za nepoštivanje ovih politika

13.3. Društvene mreže

Društvene mreže su kroz vrijeme postale izuzetno bitne za organizacije. One pomažu u povezivanju sa korisnicima, unapređenje pozicije na tržištu i angažman zaposlenika. Isto kao i ostale informacije organizacije, sadržaj društvenih mreža se mora kontrolirati pomoću programa gospodarenja informacijama. Taj sadržaj, i vrste internetskih stranica na kojima su objavljeni, mogu doći u mnogo oblika, no mjere kojima se

kontroliraju su za sve iste. Smallwood (2018, p. 311-312) spominje neke od dobrih politika za postaviti za društvene mreže u organizaciji:

1. Specificirati tko je autoriziran za kreiranje računa za društvene mreže za predstavljanje organizacije
2. Objasniti djelatnicima kakav utjecaj na reputaciju organizacije neprihvatljive objave mogu imati
3. Napraviti jasnu razliku između poslovnog i privatnog korištenja društvenih mreža
4. Naglasiti djelatnicima limitiranu privatnost tijekom korištenja društvenih mreža za poslovne svrhe
5. Poručiti djelatnicima da se drže dalje kontroverznih rasprava
6. Zatražiti od djelatnika da spomenu da njihova mišljenja na privatnim računima ne reprezentiraju mišljenja organizacije
7. Napraviti pravila koja reguliraju na koje načine se mogu koristiti ime i logo organizacije

13.4. Mobilni uređaji

Mobilni uređaji kao što su pametni telefoni, tableti, laptopi i slično postaju sve češći u radnom okruženju. Zbog njihove lakoće krađe i ranjivosti intercepcije dolaze novi rizici i potrebe za uspostavljanjem mjera. Dio tih prijetnji bi trebao pokriti trening svijesti o sigurnosti, no najčešće organizacije trebaju više od toga. Tu dolazi upravljanje mobilnih uređaja (engl. „*mobile device management*“) pomoću kojeg se automatiziraju postupci kao brisanje povjerenih informacija sa uređaja ili ažuriranje svih uređaja unutar organizacije. Sofisticiraniji sustavi mogu upravljati ne samo uređajima od organizacije već i osobnim uređajima djelatnika. Također raste i potreba za sustavom koji bi mogao pokriti i različite ostale uređaje koji se mnogu spojiti na Internet (engl. „*Internet of things*“) (Smallwood, 2018, pp. 324-330. Neke općenite smjernice za upravljanje mobilnim uređajima uključuje:

- Šifrirati sadržaja poruka
- Koristiti dovoljno snažne lozinke
- Postaviti automatsko gašenje nakon vremena neaktivnosti

- Ne kompromitirati sigurnosne funkcije uređaja putem hakiranja za pristup viših funkcija operativnog sustava (engl. „*jailbreaking*“)
- Zaposliti kvalificirane programere za razvijanje sigurnih aplikacija
- Pronaći stručnjaka za testiranje sigurnosti sustava i savjetovanje

14. Zaključak

S gomilanjem podataka te sa stalno razvijajućim pravnim i tržišnim okruženjima gospodarenje informacijama postaje sve bitnije za organizacije u današnje vrijeme. Ono omogućuje bolje upravljanje rizicima i prilagođavanje novim okolnostima te ostale organizacijske dobrobiti kao što su veća pouzdanost radnika tijekom obavljanja posla ili bolje surađivanje među odjelima. Iako primjenjivanje i održavanje programa gospodarenja informacijama može biti skup pothvat, i u smislu radnih sati i novčano, postaje sve očitije zašto je dobra ideja pokrenuti takav program i ne čekati prvo da se desi nekakva nesreća u obliku pravnih problema ili kibernetičkih napada. Takav program se obavezno mora unaprijeđivati kroz vrijeme zbog promjena u organizaciji ili njezinoj okolini te bi trebao obuhvatiti sve odjele i sve vrste tehnologija koje se u njima primjenjuju. Jedna tehnologija koju bi trebalo držati na oku, ne samo u sklopu gospodarenja informacijama nego i općenito, bi bila umjetna inteligencija. Ne samo što bi ona mogla biti izvor velike količine novih informacija i dokumenata u organizacijama, nego bi i zahtijevala nove politike specifične za njezinu upotrebu i njezine proizvode, oviseći za koju svrhu se koristi. Druga velika potencijalna promjena koja bi mogla zateći svijet gospodarenja informacijama bi bila daljnji razvoj tijela za zaštitu podataka i njihove suradnje sa ostalim tijelima, specifično u sklopu GDPR-a. S takvim novim valom mjera bi vidli ponovo povećani interes za implementaciju programa gospodarenja informacijama i njihovo unapređenje. No čak i da to nije slučaj, zbog samih trendova u poslovanju, kao što su sve veća birokratizacija i internacionalizacija tvrtka te sve veća svijest o vrijednosti informacija, bi mogli očekivati rast discipline. Taj rast bi mogao doći u obliku ne samo veće prisutnosti pozicija koje se bave, djelomično ili isključivo, gospodarenjem informacijama, nego i kao bolje institucionaliziranje njihove obuke. Državne vlade, organizacije i tvrtke bi trebale podržavati takav rast kojem bi one postale sveukupno efikasnije i sigurnije.

Popis literature

ARMA (2017). *The Principles*:
Preuzeto 13. kolovoza 2024: https://www.arma.org/page/principles

Blair, B (2012). *Making the Case for Information Governance: 10 Reasons Information Governance Makes Sense.* Slideshare
Preuzeto 13. kolovoza 2024: https://www.slideshare.net/btblair/making-the-case-for-information-governance-10-reasons-information-governance-makes-sense

Brzica, H. (2018). *Koncept Uspostave Elektroničkoga Arhiva U Javnoj Upravi*: Filozofski Fakultet Sveučilišta Zagreb

Clarke, I. (2017). *The 10 Generally Accepted Privacy Principles*. Linford & Company:
Preuzeto 13. kolovoza 2024: https://linfordco.com/blog/the-10-generally-accepted-privacy-principles/

EDRM, (2023). EDRM model:
Preuzeto 13. kolovoza 2024: https://edrm.net/edrm-model/current/

Hajela, S. (2024). Demystifying Information Technology (IT) Governance. Cio Index:
Preuzeto 13. kolovoza 2024: https://cioindex.com/reference/demystifying-it-governance/

Infogovworld (2019). *Information Governance: A Primer*:
Preuzeto 13. kolovoza 2024: https://infogovworld.com/ig-topics/information-governance-a-primer/

Intersoft Consulting (2018). *General Data Protection Regulation*:
Preuzeto 13. kolovoza 2024: https://gdpr-info.eu/

Laney, D. (2018). *Infonomics: How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage*. New York: Bibliomotion

Lomas, E. (2010). *Information governance: information security and access within a UK context*. Emerald Insight:
Preuzeto 13. kolovoza 2024:
https://www.emerald.com/insight/content/doi/10.1108/09565691011064322/full/html

NHS (2023). *Data Security and Protection Toolkit*:
Preuzeto 13. kolovoza 2024: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

The Sedona Conference (2019). *The Sedona Conference Commentary on Information Governance*:
Preuzeto 13. kolovoza 2024:
https://thesedonaconference.org/publication/Commentary_on_ Information_Governance

Seiner, R. (2024). *Data Governance Doesn't Have to Be Scary*. TDAN: Preuzeto 13. kolovoza 2024: https://tdan.com/data-governance-doesnt-have-to-be-scary/31878

Smallwood, R. (2018). *Information Governance: Concepts, Strategies, and Best Practices*. Hoboken: Wiley

Sažetak

Gospodarenje informacijama: koncepti i alati

Gospodarenje informacijama (*engl*. „information governance“) je stalno razvijajuće interdisciplinarno polje koje se bavi strategijama za informacije u organizacijama i tvrtkama. U ovom radu će se objasniti kako se ono razlikuje od pojmova kao gospodarenje podacima i gospodarenje informacijskom tehnologijom, kontekst nastanka i razvoj discipline te što ono sve pokriva. Gospodarenje informacijama se bavi privatnošću i sigurnošću informacija što podrazumijeva upravljanje rizicima, obranu od napada, enkripciju elektroničke pošte i ostalih metoda koje se mogu koristiti tijekom svakodnevnih aktivnosti organizacije. Također, neka od važnijih pitanja na koja će rad odgovoriti su koje dokumente je vrijedno zadržati i za koliko dugo, što s njima napraviti tijekom legalnog postupka i kako primijeniti program gospodarenje informacijama u nekoj organizaciji uzimajući u obzir njihove ciljeve i potrebe te pravno okruženje.

Ključne riječi: gospodarenje informacijama, privatnost, sigurnost, poslovanje, administracija, spisovodstvo

Summary

Information governance: concepts and tools

Information governance is a constantly evolving interdisciplinary field that develops strategies for information in organizations and companies. This paper will explain how it differs from data governance and information technology governance, the context during it's origin and what is all covered by it. Information governance deals with, among other things, with privacy and security of information which includes risk management, defense from cyber-attacks, e-mail encryption and other methods used during the everyday operations of the organization. Additionally, the paper will answer which documents to preserve and for how long, what to do with them after that period and how to apply an information governance program in an organization taking into account their goals and needs, as well as the legal landscape.

Keywords: information governance, privacy, security, business, administration, records management