UPRAVLJANJE KORISNIČKIM PODACIMA U POSLOVNIM PROCESIMA

Rezek, Ivan

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

UPRAVLJANJE KORISNIČKIM PODACIMA U POSLOVNIM PROCESIMA

Ivan Rezek

Zagreb, veljača 2019.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 11.2.2019.

Predgovor

Iznimno se zahvaljujem svojoj supruzi Ivi Rezek i cijeloj obitelji na velikom razumijevanju, podršci i ohrabrenju prilikom cijelog vremena trajanja studija.

Zahvaljujem se Renatu Barišiću v. pred. na mentorstvu i vođenju kroz proces izrade završnog rada „Upravljanje korisničkim podacima u poslovnim procesima“ te mu se zahvaljujem na profesionalnom usmjerenju i savjetovanju prilikom odabira studija i karijere u trenucima kada mi je to bilo najpotrebnije.

Također se posebno zahvaljujem Danielu Beleu struč. spec. ing. comp. na vrhunskim predavanjima i trudu koji ulaže da prenese znanje svojim studentima. Zahvaljujući njegovom angažmanu danas sam tamo gdje sam očekivao biti tek za nekoliko godina. Uvelike mi je olakšao i ubrzao profesionalni razvoj.

Ivan Rezek

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Na području Europske unije je donesena uredba o zaštiti osobnih podatka te je prepoznata mogućnost stvaranja nove IT usluge koja bi olakšala nadzor, kontrole pristupa te upravljanje osobnim podacima. Ovaj rad će se temeljiti na pravnim i poslovnim pritiscima koji djeluju na organizacije unutar Europske unije i one organizacije koje posluju sa zemljama članicama Europske unije. Na temelju tih pritisaka objasnit ćemo uslugu koja bi organizacijama pomogla i olakšala rad s podacima. Za način implementacije koristit ćemo se ITIL okvirom dobrih praksi, pa ćemo našu uslugu podijeliti na strategiju usluge, dizajn usluge, tranziciju usluge, rukovanje uslugom i stalna poboljšanja usluge. Objasnit ćemo neke osnovne pojmove iz zakona, zašto je važno usklađivanje raditi na zakonskoj, procesnoj i tehničkoj razini i koje su dobrobiti svakog usklađivanja. Dati ćemo primjere na koji način bismo olakšali upravljanje podacima našim programskim rješenjem i kako povećati sigurnost implementacijom sigurnosnih politika i pravila grupa koristeći aktivni direktorij. Prikazat ćemo primjer dinamičkog maskiranja podataka u SQL serveru te objasniti koncept stalne enkripcije. Na kraju ćemo proći kako održavati uslugu te predvidjeti stalna poboljšanja naše usluge upravljanja korisničkim podacima.

Ključne riječi: ITIL, usluga, GDPR, osobni podatak, upravljanje, zaštita osobnih podataka, usklađivanje, PDCA, životni ciklus usluge

Sadržaj

1. Uvod 1

2. Strategija usluge 3

2.1. Zakonski pritisci 4

2.1.1. GDPR terminologija 5

2.1.2. Načela GDPR-a 8

2.2. Poslovni pritisci 9

2.3. Usluga upravljanja korisničkim podacima 10

2.3.1. Usklađivanje po pravnoj osnovi 11

2.3.2. Usklađivanje po procesnoj osnovi 11

2.3.3. Usklađivanje po tehničkoj osnovi 12

2.4. Podaci i njihova snaga 12

2.5. Upravljanje uslugom i ITIL prakse 13

3. Dizajn usluge 16

3.1. Utjecaji vanjskih čimbenika 16

3.2. Usklađivanje organizacije po zakonu 18

3.2.1. Definiranje dokumenata 19

3.3. Identifikacija poslovnih procesa u organizaciji 19

3.3.1. Proces 19

3.4. Tehnološka rješenja 21

3.4.1. Izvedba programskog rješenja 23

3.5. Dokumenti u fizičkom i digitalnom obliku 25

3.5.1. Postupanje i pohrana fizičkih dokumenata 26

3.5.2. Postupanje i pohrana digitalnih dokumenta i podataka 26

3.6. Metrike usluge 27
3.6.1. Metrike zakonskog usklađivanja 28
3.6.2. Metrike procesnog usklađivanja 29
3.6.3. Metrike tehničkog usklađivanja 29
3.6.4. Metrike programskog rješenja 30
4. Tranzicija usluge 32
4.1. Isporuke 32
4.1.1. Zakon i organizacija 32
4.1.2. Isporuka programskog rješenja 34
4.2. Sigurnosne preporuke i načini implementacije 35
4.2.1. Cloud pohrana podataka i pristup 36
4.2.2. Moderne tehnike rada s podacima u bazi podataka 40
4.3. Rizici 44
5. Rukovanje uslugom 46
5.1. Upravljanje kontrolom pristupa 47
5.2. Upravljanje incidentima 48
5.2.1. Nedostupnost usluge 49
5.2.2. Nepravovremeno reagiranje na promjene 49
5.2.3. Pogreške prilikom usklađivanja 50
5.2.4. Gubitak ili kompromitiranost podataka 50
5.3. Korisnička podrška 51
5.4. Upravljanje programskim rješenjem i IT problemima 51
6. Stalna poboljšavanja usluge 52
6.1. Interna poboljšanja 53
6.2. Eksterna poboljšanja 53
6.2.1. Poboljšanja zakonskog usklađivanja 54

6.2.2. Poboljšanja procesnog usklađivanja 54
6.2.3. Poboljšanja tehničkog usklađivanja 55
6.2.4. Poboljšanja programskog rješenja 55
6.2.5. Prilagodbe potrebama organizaciji 58
6.3. Prilagodbe zakonskim okvirima 58
6.4. Prilagodbe zahtjevima krajnjeg korisnika 59
Zaključak 60
Popis kratica 63
Popis slika 64
Popis tablica 65
Popis kôdova 66
Literatura 67
Prilog 68

1. Uvod

U današnje vrijeme razne organizacije sve se više bave organiziranjem i analizom informacija koje smo dobili prikupljanjem, proučavanjem i tumačenjem podataka koji proizlaze iz poslovnih procesa. Znanje stječemo razumijevanjem značenja i tumačenjem informacija što nam daje moć da prepoznamo uzorke unutar procesa te u skladu s time donosimo poslovne odluke koje utječu na cijeli naš poslovni sustav i prepoznajemo nove poslovne prilike ili moguće prijetnje našem poslovnom sustavu.

Donesene odluke su toliko dobre koliko smo dobro protumačili dobivene informacije iz podataka. Naravno, upravo zbog toga organizacije žele znati što više o svojim klijentima i konkurenciji. U te svrhe današnje tehnologije omogućavanju prikupljanje podataka na vrlo raznolik način. Neki podatke skupljaju zapisivanjem i vođenjem transakcija u bazi podataka, drugi pak koriste sustave za upravljanje odnosima s kupcima (engl. *Customer relationship management*, skraćeno CRM), treći prikupljaju podatke putem raznih anketa. Nepostojanost ili lažiranje podataka također može imati veliko značenje kada se rade razne analize podatka modernim sustavima za potporu odlučivanju.

Iz toga spoznajemo kako su podaci temelj svake organizacije počevši od onih malih koji podatke koriste u svrhu pisanja poštanskih adresa ili telefonskih poziva pa sve do multimilijunskih kompanija koje tumačenjem dobivenih informacija donose vrlo ključne i strateške odluke.

Kako ne bi došlo do zloupotrebe korisničkih podataka, postoje određene zakonske regulative koje nam govore o načinu prikupljanja i obrade korisničkih podataka. Organizacije se vrlo često znaju ne pridržavati tih zakonskih regulativa jer ih ne razumiju ili se ne boje zakonskih kazni ili u najgorem slučaju niti nisu svjesne da one postoje.

Upravljanje podacima vrlo brzo postaje zahtjevan proces, pogotovo ako se radi o velikoj količini zapisa u bazi podataka ili na nekom drugom mjestu ili čak obliku koji ne mora uvijek biti digitalan, što dodatno otežava cijeli proces upravljanja. Upravo iz tog razloga samoj obradi i čuvanju podataka se mora pokloniti velika pažnja. Gubitak istih podataka, njihova zloupotreba ili nepažljivi gubitak mogu imati katastrofalne posljedice, kako po ugled, tako i po financijsko stanje firme, a pošto to nije samo naš podatak, posljedice može imati i naš klijent koji je pravi vlasnik toga podatka.

Upravo se tu pruža mogućnost da prilikom digitalne transformacije IT organizacije prepoznaju svoju poslovnu priliku i dizajniraju usluge kako bi svojim postojećim i budućim korisnicima mogle pružiti upravo takve usluge. U ovom radu ću opisati iz perspektive IT poduzeća prepoznatu poslovnu priliku, te na primjeru prikazati kako bi takva usluga mogla izgledati, njen način implementacije u poduzeće kod naručitelja prema okviru infrastrukture informacijske tehnologije (engl. *information technology infrastructure library*, skraćeno ITIL).

2. Strategija usluge

Strategija usluge je prvi i najvažniji dio životnog ciklusa usluge u ITIL-u. Strategijom ćemo odrediti što je to korisniku bitno, što sve moramo uzeti u obzir, kako međusobno povezati komponente unutar usluge i koje su njihove međusobne zavisnosti. Također strategija nam mora odgovoriti na pitanje i zašto to radimo te na koji način ćemo tu dodanu vrijednost korisniku isporučiti. Krajnji rezultat mora biti vrijednost za korisnika. Sve to je pripremni plan i nacrt za dizajn usluge.

Svaka organizacija posjeduje određen skup podataka koje je prikupila tijekom godina poslovanja. U svome svakodnevnom poslu organizacija radi svjesno i nesvjesno s podacima koji se mogu klasificirati kao osobni podaci. Ti podaci mogu biti u digitalnom ili fizičkom formatu. Ako organizacija nije dobro organizirana i nema jasnu sliku kako, tko, gdje i kada rukuje se tim podacima, organizacija dovodi sebe, svoje djelatnike i ono najvažnije za organizaciju, svoje klijente do vrlo nezgodne pozicije ako dođe do gubitka ili zloupotrebe podataka koje su prikupili. Upravo tu smo mi prepoznali svoju poslovnu priliku da prilikom digitalne transformacije našim klijentima damo novu dodatnu vrijednost upakiranu kao novu uslugu upravljanja korisničkim podacima u poslovnim procesima. Dosadašnjim iskustvom u IT svijetu spoznao sam da mnogo organizacija nema jasno definirane poslovne procese niti delegirana prava unutar istih. Mnogi ni ne rade razliku između poslovnih procesa pa je tu još i veći problem razumijevanja pojma poslovnog procesa. Naša usluga će se morati nositi, kako sa zakonskim tako i s poslovnim pritiscima, što bi značilo da ćemo morati napraviti usklađivanja sa zakonom i s poslovnom stranom te istovremeno pružiti i implementirati nadzor nad svim procesima. Osim što će uvesti dodatnu vrijednost nadzora i upravljanja nad osobnim podacima u organizaciji, cilj je u svakom pojedinom ciklusu integracije naše usluge i educirati zaposlenike organizacije koji će raditi na našem riješenu. Druge zaposlenike koji neće imati direktan dodir s našim rješenjem treba također educirati da su i oni upoznati te da se znanju ophoditi s osobnim podacima. Ako se ne promjeni kultura u ovom cijelom integracijskom procesu i ako se svi djelatnici organizacije ne budu pridržavali procedura i pravila koje nam propisuje trenutno važeći zakon ili se ipak desi ispad i curenje podataka, organizacija će lakše i brže moći intervenirati kako joj to bude propisano trenutno važećim zakonom. Taj dio je vrlo bitan da naše rješenje definira razine odgovornosti u slučaju incidenata te koga je potrebno obavijestiti u slučaju incidenta.

2.1. Zakonski pritisci

Dana 27. travnja 2016. i nakon razdoblja prilagodbe u trajanju od 2 godine, od 25. svibnja 2018. u Europskoj uniji, što uključuje i nas kao članicu, počinje primjena „Uredbe (EU) 2016/679 Europskog parlamenta i vijeća o zaštiti u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka te o stavljanju izvan snage direktive 95/46/EZ (Uredba o zaštiti podataka)[1].

Uredba o zaštiti podataka se odnosi na sve organizacije bez obzira na njihovu veličinu ili to da su privatna ili javna poduzeća koja prikupljaju i obrađuju osobne podatke građana europske unije bez obzira gdje se sjedište organizacije nalazi. Kako mi djelujemo na području Europske unije ova se uredba odnosi direktno na nas i na naše klijente.

Uredbom o zaštiti podataka se štite temeljna prava i slobode pojedinaca, a posebno njihovo pravo na zaštitu osobnih podataka.[2] Glavni i jedini cilj ove uredbe je zaštiti privatnu osobu od zloupotrebe njihovih podataka.

Također, u uredbi se i spominju velike financijske kazne u slučaju incidenata, koje bi trebale biti dodatan motiv organizaciji da poštuje uredbu. No takve stvari ne bi trebale biti glavni motiv organizaciji da se bolje organizira i da počne razmišljati na način jesu li stvarno ti podaci potrebni. Također bi se trebali voditi i moralnim kompasom, jer ono što naša organizacija radi možemo se upitati bi li nama bilo u redu da neka druga organizacija tako rukovodi s našim podacima?

GDPR uredba je donesena od strane Europskog parlamenta i vijeća te se odnosi na sve organizacije i fizičke osobe u zemljama članicama Europske unije. To ograničenje ujedno definiraju i naše područje primjene usluge, odnosno tržište. Usluga upravljanja korisničkim podacima će biti orijentirana na organizacije iz zemalja članica Europske unije te one koje žele poslovati s organizacijama iz zemalja članica Europske unije, a njihovi poslovni procesi i aktivnosti prikupljaju podatke osoba iz europske unije.

[1] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/1
[2] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/2, Članak 1, Točka 2

2.1.1. GDPR terminologija

GDPR uredba definira termine sudionika te njihova prava, ovlasti i odgovornosti. Od iznimne je važnosti da se pridržavamo terminologije kroz našu implementaciju kako bismo pravilno uskladili našu uslugu s GDPR uredbom. Osim našeg pridržavanja kroz implementaciju potrebno je unutar organizacije uspostaviti takvu hijerarhiju prava unutar pojedinih procesa te definirati pojedine role i odgovornosti djelatnika na razini organizacije.

Osobni podatak je često spominjan pojam u našoj usluzi te je od iznimne važnosti shvatiti što to taj pojam zapravo znači. U kontekstu GDPR-a i fizičke osobe osobnim podatkom se smatra sve što se može iskoristiti za identifikaciju pojedinca, bez obzira da li smo mi ga prethodno identificirali ili ne.

Prema GDPR uredbi osobni podaci su:

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca[3]

Prema zakonu o zaštiti osobnih podatka osobni podatak je:

Svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati izravno ili neizravno, posebno na osnovi jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.[4]

Navodim nekoliko primjera:

Ime i prezime nije osobni podatak jer samo imenom i prezimenom ne možemo vezati osobu uz to ime i prezime bez dodatnih atributa. Na svijetu postoji više osoba koje dijele ime i prezime. Primjer bi bio Marko Markić, no ako bi dodali još poneki opisni atribut primjerice redovni kupac dućana Zoo u centru Zagreba i sa stalnom adresom u Sisku, već bi pobliže

[3] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/33, , Članak 4, Definicija 1
[4] Zakon o zaštiti osobnih podataka, Narodne novine, broj:106/12, članak 2. stavka 1. točka 1

opisali osobu indirektno. Samim time bismo drugim osobama mogli omogućiti identifikaciju te osobe i u tom kontekstu tada ime i prezime postaje osobni podatak.

Fotografija se smatra osobnim podatkom, i to spada u posebnu kategoriju koju nazivamo biometrijski podaci. Iako mi nismo u stanju prepoznati osobe na fotografiji, postoje algoritmi prepoznavanja lica (engl. Facial Recognition) koji svoj posao identifikacije osoba rade s izuzetnom preciznošću,. Trenutno najpoznatiji portal društvene mreže Facebook, ima ugrađen facial recognition koji milijuni ljudi dnevno koriste kako bi označili na svojim fotografijama sebe ili svoje prijatelje.

Ako bismo željeli koristiti fotografiju u marketinške svrhe, tada bismo trebali sve osobe s fotografije tražiti privolu za korištenje iste.

Dakle ono što zaključujemo, je da svaki podatak ili set podataka može jednoznačno identificirati ispitanika, smatra se osobnim podatkom. Identifikacija se može raditi direktno (ime, prezime, adresa, OIB) ili indirektno (opis osobe).

Ispitanik je fizička osoba kojoj možemo utvrditi identitet i čije podatke obrađujemo. Za sada se to odnosi na sve građane Europske unije.

Ima nekoliko načina na koje možemo definirati pojam ispitanika:

- Nositelj prava na zaštitu osobnih podataka
- Pojedinac čiji je identitet utvrđen ili se može utvrditi[5]
- Pojedinac, osoba koja je živa

Uredbom o zaštiti podataka je omogućeno svakom ispitaniku da od organizacije zatraži informaciju gdje, kada i kako se koriste njegovi podaci te što sve od njegovih podataka posjeduje organizacija. Prilikom samog zatraženog prikupljanja podataka od strane organizacije, ispitanik ima pravo odbiti dati dio ili sve podatke koji nisu legitimni interes za tu organizaciju. Isto tako ispitanik može zatražiti brisanje, izmjenu ili nadopunu podataka koje organizacija već posjeduje.

Ukratko, prava ispitanika prema GDPR uredbi su:

- Informiranje / Transparentnost
- Pristup

[5] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/33, , Članak 4, Definicija 1

- Ispravak
- Brisanje
- Ograničenje obrade
- Prijenos podataka
- Prigovor
- Isključenje automatizirane obrade

Svako od spomenutih prava ima svoje uvjete i načine ostvarivanja. Isto će biti omogućeno kroz našu uslugu.

Obrada je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje. [6]

Voditelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice. [7]

Izvršitelj obrade fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade[8].

Službenik za zaštitu osobnih podataka (engl. *Data protection officer*, skraćeno DPO) je osoba imenovana od strane voditelja i izvršitelja obrade sa zadaćom informiranja i savjetovanje cijele organizacije, kao i raspodjela odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade, a kontaktna je točka kako za nadzorno tijelo tako i za ispitanike.

---

[6] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/33, Članak 4, Definicija 2
[7] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/33, Članak 4, Definicija 7
[8] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/33, Članak 4, Definicija 8

Nadzorno tijelo je nezavisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51.[9]

Privola ispitanika je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.[10]

Uredba nam govori da bismo trebali prikupljati samo podatke koji su za nas legitimni interes, odnosno podatke koji su nam nužni za naše poslovanje i te podatke ne smijemo koristi u druge svrhe.

2.1.2. Načela GDPR-a

GDPR uredba se temelji na sljedećim načelima:

- Zakonitost, poštenost i transparentnost
    - Obrada podataka se treba izvršavati u skladu sa zakonom, transparentno i pošteno prema pravima koje ostvaruje ispitanik
- Ograničenje svrhe
    - Prikupljeni podaci se prikupljaju u određenu svrhu i to mora jasno biti napomenuto prilikom prikupljanja podataka od ispitanika i u druge svrhe prikupljeni podaci se ne smiju koristiti.
- Smanjenje količine podataka
    - Cilj je prilikom obrade sakupljati što manje podataka od ispitanika, uzeti samo najosnovnije i najnužnije što smo zamislili da nam treba, ne ispitanika zamarati dugim i iscrpnim formama za unos podataka i privolama kao što je to do nedavno bila praksa.
- Točnost
    - Svi podaci koji se obrađuju trebaju biti točni i ažurni što znači da se treba implementirati brisanje ili ispravak svih podataka koji nisu ispravni
- Ograničenje pohrane

[9] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/34, Članak 4, Definicija 21
[10] Službeni list europske unije, Uredba (EU) 2016/ 679 europskog parlamenta i vijeća, L 119/34, Članak 4, Definicija 11

    - Načelo ograničenja pohrane govori da se podaci u obliku koji omogućuje identifikaciju pojedinca trebaju čuvati samo koliko je potrebno da se obrada u čiju svrhu su prikupljeni završi. Na dulja razdoblja mogu se pohranjivati samo podaci čija obrada obuhvaća javni interes ili povijesna i znanstvena istraživanja.
- Cjelovitost i povjerljivost
    - Prilikom obrade podataka moraju se primijeniti određene sigurnosne mjere što uključuju prevencije ulaska neovlaštenih osoba u područje obrada, moraju se primijeniti tehnička sredstva kako bi se osigurala obrada da bude cjelovita, bez gubitka ili izmjene obrađivanih podataka
- Pouzdanost
    - Cijela obrada mora biti ispravno odrađena, sva prava ispitanika poštovana tijekom obrade te podaci zaštićeni od slučajnih izmjena ili curenja podataka van organizacije

Sva navedena načela GDPR-a trebaju biti prihvaćena i implementirana od strane organizacije ako organizacija želi postići usklađenost sa zakonom.

2.2. Poslovni pritisci

Kako s vremenom rastu, organizacije povećavaju broj ljudi, broj procesa, broj aktivnosti unutar pojedinih procesa. Tako bismo mogli ići u nedogled. Upravo se tu počinju primjećivati prve nesukladnosti. Ovo su smo neka od pitanja koje se mogu naći u bilo kojoj organizaciji:

- Tko sve ima pristup i kojim podacima? Mogu li svi zaposlenici organizacije doći do bilo kojeg podatka koji bi se smatrao osobnim podatkom i mogu li ga iskoristiti u neku svrhu osobnog probitka?
- Gdje se čuvaju podaci? Čuvaju li se podaci u arhivu u fizičkom obliku ili se čuvaju u bazi podataka, u tom slučaju, gdje je server?
- Nalaze li se podaci na zaštićenim lokacijama? Može li se tim lokacijama lako pristupiti te vodi li se na tim lokacijama evidencija pristupa, bilo video nadzorom ili nekim drugim načinom?
- Nalaze li se samo nužni podaci potrebni za samo jednu obradu na pojedinim dokumentima koji kolaju firmom, bilo digitalnog oblika ili fizičkog, kao npr. broj

telefona, email i adresa klijenta na radnom nalogu, ili pak kolega mailom šalje listu svojih top 10 klijenata nekome izvan ili unutar organizacije? Posjedujemo li legitimni interes za prikupljanje određenih podataka?

Također dolazimo i do pitanja odgovornosti: Tko je nadležan za upravljanje podacima u organizaciji? Dakako, na ovo zadnje pitanje će svi djelatnici organizacije pokazati na čelnu osobu organizacije, no to nikako nije ispravno. Upravo zbog toga je bitno uspostaviti i delegirati odgovornosti.

2.3. Usluga upravljanja korisničkim podacima

Usluga se sastoji od niza koraka koje treba poduzeti da bi se moglo reći da organizacija ispravno rukovodi s podacima svojih zaposlenika i klijenata, što bi značilo da je sukladna sa zakonom i Uredbom o zaštiti podataka.

Usluga će se dijeliti na tri faze usklađivanja:

- Usklađivanje po pravnoj osnovi
- Usklađivanje po procesnoj osnovi
- Usklađivanje po tehničkoj osnovi

Da bi usluga bila potpuna moramo primijeniti sve tri uskladbe istovremeno, jer su međusobno povezane i jedna drugu nadopunjuje. Pravnim usklađivanjem ćemo upoznati organizaciju što nam je uredba donijela i identificirat ćemo potrebne podatke i legitimni interes organizacije. Usklađivanjem po procesnoj osnovi ćemo identificirati procese i obrade unutar procesa, dok ćemo prilikom tehničke uskladbe primijeniti suvremena tehnološka rješenja kako bismo omogućili praćenje svih obrada i podataka unutar obrada. Također ćemo primijeniti i regulirati prava pristupa aplikacijama, bazama podataka te samim podacima unutar baza podataka. Fizičke razine pristupa i fizičko rukovanje podacima evidentirat ćemo u sklopu naše usluge kao i savjetovanje kako se bolje fizički zaštiti. Bitno je za napomenuti da dijelovi naše usluge jesu primjenjivi i na druge organizacije kao što je programsko rješenje koji ćemo pružiti, savjeti i dokumenti vezani za zakonske regulative i norme, ali sam centralni dio naše usluge, sama analiza organizacijske kulture i podjele unutar organizacije je jedinstvena za tu organizaciju i taj dio će se morati svaki puta izvršavati iznova prilikom implementacije u neku drugu organizaciju.

Ovu uslugu definira i programsko rješenje koje će biti implementirano u tehničkom dijelu usklađivanja usluge. Programsko rješenje je web aplikacija koja je jedinstvena za sve organizacije u koju uslugu implementiramo, s naglaskom da sama pohrana podataka koje ta aplikacija prikuplja o toj organizaciji nije u našoj nadležnosti.

2.3.1. Usklađivanje po pravnoj osnovi

Ovu vrstu usklađivanja ćemo koristiti da bismo mogli analizirati pravnu stranu organizacije. Analizom ćemo utvrditi upoznatost organizacije s trenutnim zakonom, razumijevanje nove terminologije i njihovo značenje te upoznata s posljedicama lošeg rukovanja podacima unutar poslovnog procesa. Cilj ove uskladbe je educirati djelatnike organizacije, upoznati djelatnike s terminologijom koju nam donosi GDPR te definirati dokumente koje će biti potrebno implementirati. Također ćemo analizirati koje sve podatke ispitanika trenutno organizacija posjeduje te ćemo uspostaviti što je legitimni interes za organizaciju, a što ne. Za sve što nam nije legitimni interes bit će potrebno sastaviti dokumente za traženja privola od ispitanika. Kod generiranja dokumenta privola morat ćemo poštivati načela ograničenja svrhe i pohrane te načelo smanjena količine podataka. Organizacija u koju implementiramo uslugu morat će se zadovoljiti s vrlo smanjenom količinom podataka.

2.3.2. Usklađivanje po procesnoj osnovi

Poslovni proces je skup povezanih aktivnosti koji rezultiraju dodatnom vrijednošću za organizaciju, poslovne partnere ili njene klijente. Proces ima svoje ulaze i izlaze, a aktivnosti možemo mjeriti.[11]

Zato je važno raditi usklađivanje procesne osnove. Njega provodimo kako bismo identificirali sve procese unutar organizacije. Fokusiramo se na one koji rade s osjetljivim podacima. Vrlo često organizacije nemaju dobro postavljene procese, pa ovom uskladbom također možemo poboljšati procese u organizaciji tako da vođenje organizacije upoznamo s njihovim propustima. Cilj ove uskladbe je identificirati sve procese, prepoznati potencijalne obrade koje se provode u procesu, ocijeniti koji su sve podaci bitni u procesu, koji ne. Tom analizom ćemo dobiti bolji uvid te smanjiti količine podataka koje prikupljamo i

[11] R. Kelly Rainer Jr., Casey G. Cegielski, Introduction to information systems, Third edition, John Wiley & Sons, Inc, USA 2011

obrađujemo. Također za svaki proces ćemo definirati i duljinu čuvanja podataka, mjesto i imenovat ćemo izvršitelja obrade za pojedini proces.

2.3.3. Usklađivanje po tehničkoj osnovi

Tehničko usklađivanje je zadnja faza, ali ujedno i najbitnija faza naše usluge. Prve dvije faze nam služe kako bismo upoznali, educirali i pripremili organizaciju da možemo početi implementaciju tehničkih rješenja koristeći suvremene tehnologije današnjice. Cilj ove uskladbe je implementirati modernu tehnologiju i najbolje prakse zaštite osobnih podataka.

2.4. Podaci i njihova snaga

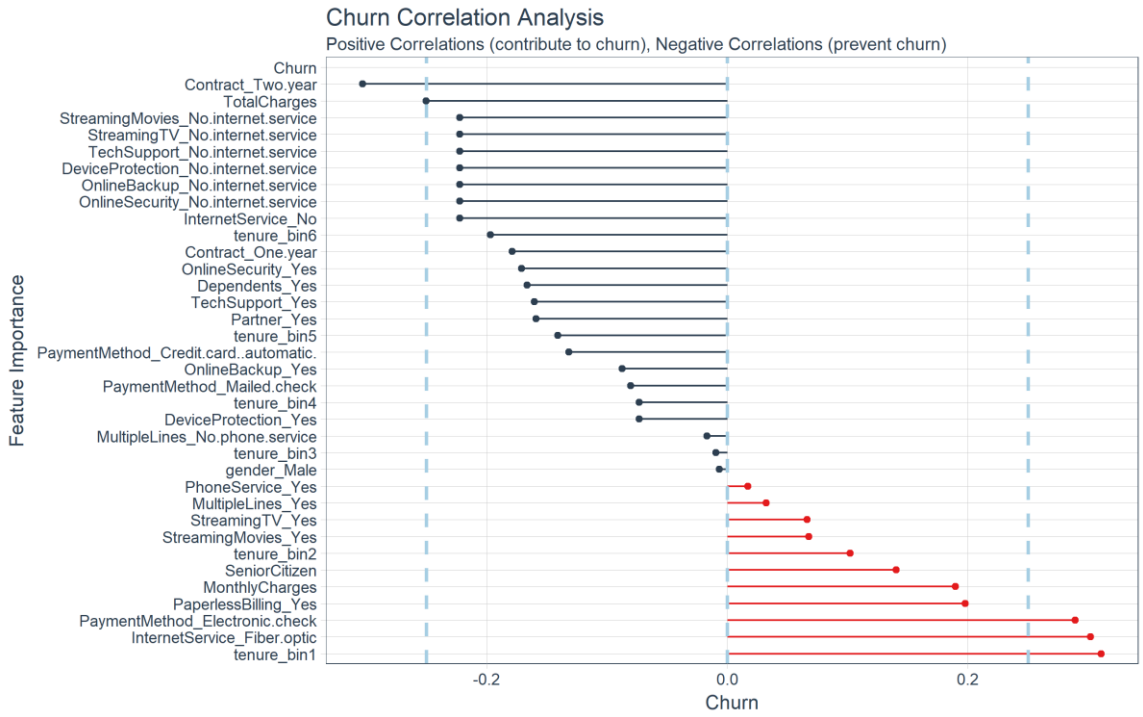
U današnje vrijeme ekonomije pokretane znanjem, organizacije sve više se oslanjaju na sustave poslovne inteligencije (engl. *Business Intelligence*, skraćeno BI) da prikupe, analiziraju i pravovremeno predstave pravu informaciju pravim ljudima, kako bi ljudi koji donose odluke u organizaciji odluke donijeli na temelju spoznaja i informacija.[12]

Kako bismo se uvjerili da su podaci zaista snaga svakog poduzeća možemo uzeti primjer telekoma. U današnje vrijeme telekomi imaju na svom raspolaganju najviše podataka.

Telekomi znaju koliko često upućujete pozive, pišete poruke, pretražujete internet. Prati se u koje vrijeme ste na internetu. Telekomi imaju velike količine i osobnih podataka. Svi ti podaci telekomu omogućavaju analizu tržišta u cilju kako to oni vole nazivati poboljšanja kvalitete usluge. U tome ima istine, ali generalno telekomi stalno analiziraju tržište u cilju povećanja prodaje.

Upotrebom moderne tehnologije, programskog koda, baza podataka te znanja iz matematike, statistike i poslovne analize vrlo se lako iz velikog seta podataka generiraju modeli koji vrlo precizno mogu predvidjeti trendove pada ili rasta prodaje. Na osnovu vaših parametara kao što su plaćanje računa, vrijeme na internetu, vaša dob, broj vaših ukućana, koliko mobilnih uređaja imate mogu se predvidjeti prekidi ugovornih obveza. Nerijetko se u tom slučaju prodaji prosljeđuju Vaši podaci i Vi dobijete ponudu koju ne možete odbiti baš kada ste odlučili promijeniti telekom operatera.

[12] Information resources managment association. Business Inteligence: Concepts, Methodologies, Tools and Applications, Liderpress TimPress, USA 2016



Slika 2.1 Primjer analize prekida ugovornog odnosa [13]

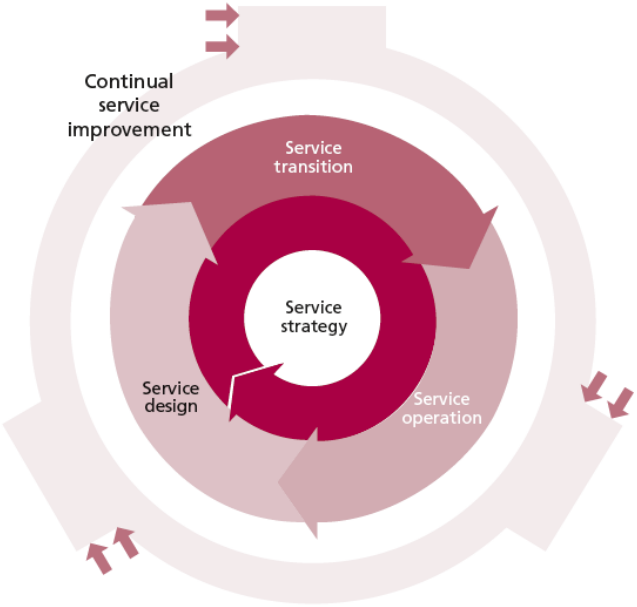
Na ovom naizgled vrlo jednostavnom primjeru objasnili smo kakvu dobrobit imamo od podataka. Svaka organizacija želi prikupiti tih podataka što više, ali takav stav nas odvraća od našeg cilja, a to je pametno, sigurno i usklađeno upravljanje podacima. Velika količina osobnih podataka se prikuplja i analizira, ali to nužno ne mora biti tako. U gore navedenom primjeru, što bi značilo da imamo osobni identifikacijski broj? Taj podatak je u ovakvim analizama nebitan, odnosno analizom vrijednosti atributa bi pokazala da taj podatak nema utjecaja na cijeli set podataka, te bi ga isključili iz daljnje analize raskida ugovornih odnosa. Ali osobni identifikacijski broj nam je vrlo bitan kod generiranja računa. Upravo se tu već vidi da se već daju poslovna analiza i financije odvojiti kao dva zasebna procesa u organizaciji i da ne obrađuju podatke na isti način.

2.5. Upravljanje uslugom i ITIL prakse

Našu uslugu ćemo implementirati koristeći najbolje prakse koje nam preporučuje ITIL. Uslugu ćemo dijeliti na faze strategije, dizajna, tranzicije, rukovanje i stalno poboljšavanje usluge. ITIL je okvir najboljih praksi skupljenih iz privatnog i pravnog sektora organizacija

[13] https://blogs.rstudio.com/tensorflow/posts/2018-01-11-keras-customer-churn/, 16. siječanj 2019.

diljem svijeta. Njegov cilj je da omogući isporuku kvalitetnih IT usluga, s posebnim naglaskom na upravljanje IT uslugom. [14]



Slika 2.2 Životni ciklus usluge prema ITIL-u[15]

ITIL se fokusira na konstantno praćenje usluge u svim ciklusima s ciljem konstantnog poboljšanja kvalitete usluge. Neki od ITIL dobrobiti:

- Povećano zadovoljstvo korisnika i naručitelja s IT uslugama
- Povećana dostupnost usluge, što vodi povećanju dobiti i prihoda
- Uštede od smanjenja prerada ili izgubljenog vremena te poboljšanog upravljanja resursima i korištenja
- Smanjenje vremena isporuke novih proizvoda i usluga
- Smanjenje rizika i bolje donošenje odluka[16]

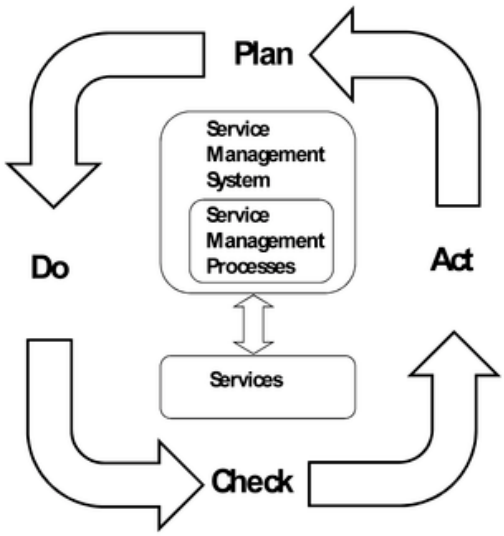
Kako bismo osigurali kvalitetu usluge, nakon što smo krajnju vrijednost isporučili korisniku, uslugu ćemo rukovoditi prema propisanoj normi ISO/IEC 20000-1:2011.

Norma ISO/IEC 20000-1:2011 je međunarodna norma čija je svrha što bolje razumijevanje i ispunjenje korisničkih zahtjeva s ciljem postizanja zadovoljstva korisnika. Implementacijom ove norme dobivano dodatnu garanciju da je naša usluga i način na koji

[14] Ahmad, N., Zulkifli, M.S. Systematic Approach to Successful Implementation of ITIL, Procedia Computer Science 17 237 – 244, 2013
[15] Hearsum, P. Introduction to ITIL Service Lifecycle; London, TSO 2011
[16] Itsmf Uk, An introductory overview of ITIL 2011, London: TSO 2012

upravljamo uslugom usklađeni s potrebama poslovanja i zahtjevima korisnika. Ona propisuje pojmove koje ćemo koristiti prilikom rukovanja uslugom kao što je sustav upravljanja uslugom (engl. Service level agreement, skraćeno SLA), što je bitan dokument u kojem ćemo jasno definirati što i kako naša usluga pokriva te kolika će biti njena dostupnost. Taj je dokument od iznimne važnosti da bi se s korisnikom uspostavila što bolja komunikacija i spriječio nepotreban i ekscesivan rad s naše strane. Ova norma se prvenstveno odnosi na nas, pružatelja usluge da se sama usluga što bolje isplanira, uspostave se politike i ciljevi unutar usluge, poboljša rukovanje, nadzor i održavanje usluge.

ISO/IEC 20000-1:2011 je komplementaran i dobro usklađen s ITIL-ovim skupom dobrih praksi, što nam donosi i dodanu vrijednost naše usluge. Ono što dijele ITIL i ISO/IEC 20000-0:2011 je životni ciklus. Norma definira ciklus planiranje, provedbu, provjere i djelovanje (engl. *Plan, Do, Check, Act* skraćeno PDCA). Upravo na principu ITIL-a pružamo svoju uslugu, a kako to određuje PDCA cijeli ITIL-ov proces ponavljamo u ciklusima.



Slika 2.3 PDCA metodologija primjenjena na upravljanje uslugom[17]

Cikluse PDCA u ovom slučaju moramo definirati u SLA, jer u prvom ciklusu mi moramo postići usklađenost organizacije s GDPR-om. PDCA je način kako ćemo pružati uslugu u danom periodu vremena zbog promjena koje mogu nastati zbog vanjskih čimbenika na našu uslugu što rezultira neusklađenošću organizacije s GDPR uredbom i važećim zakonom o sigurnosti i upravljanju osobnih podataka.

[17] ISO/IEC 20000-1:2011; https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en

3. Dizajn usluge

Dizajn usluge je dio ciklusa ITIL procesa koji se brine da su nove ili izmijenjene usluge dizajnirane tako da prate promjenjive zahtjeve koje nam poslovna okolina definira.[18] Dizajn usluge uključuje planiranje i koordinaciju aktivnosti, tehnologiju, procese, metrike.

Usluga upravljanja korisničkim podacima u poslovnim procesima zamišljena je kao ciklička usluga. To znači da samo inicijalno uvođenje naše usluge u organizaciju neće riješiti probleme te organizacije za sva vremena. Zakon se mijenja. Organizacije rastu. Tehnologija se stalno razvija. Upravo zbog toga naša usluga je zamišljena da se izvodi u ciklusima i upravo zato radimo implementaciju prema ITIL-u. Tako bi se i implementirala i naplata usluge, što bi nam omogućilo generiranje tržišnih modela u više kategorija, npr. organizacija naručitelj mogla bi odraditi implementaciju usluge kao osnovni paket usluge te tada nakon određenog vremena od nas tražiti ponovno procesne uskladbe jer je u nekom periodu organizacija narasla i uvela dodatne procese i obrade podataka.

Kako bi bili kompetentni pružiti uslugu ove razine naša vlastita organizacija mora imati stručnjake na pravnim, tehničkim, konzultantskim te prodajnim razinama. Naša organizacija unutar svojih procesa mora raditi konstantno praćenje promjena koje se događaju unutar zakonskih i tehnoloških okvira. Moraju se raditi istraživanja novih tehnologija s ciljem pružanja najboljih tehničkih rješenja s ciljem konkurentnosti na tržištu. Moramo pratiti trendove tržišta i raditi analize prethodnih znanja i spoznaje kako bismo u bilo koje vrijeme bili kompetentni implementirati navedenu uslugu prema najnovijim spoznajama. Tako će naši konzultanti uvijek imati najbolja znanja koja su im potrebna kada se nađu na lokaciji s korisnikom.

3.1. Utjecaji vanjskih čimbenika

Da bismo razumjeli u potpunosti našu uslugu moramo shvatiti i sve vanjske čimbenike koji utječu na nju. Usluga upravljanja korisničkim podacima u poslovnim procesima vrlo je zavisna o najmanje 3 vanjska čimbenika koji mogu imati vrlo snažan utjecaj na nju i moramo biti spremni djelovati i prilagoditi se novonastaloj situaciji.

[18] Hearsum, P. Introduction to ITIL Service Lifecycle; London, TSO 2011

Najbitnija tri vanjska čimbenika su:

- Izmjene zakona i zakonskih regulativa
- Promjene unutar organizacije
- Razvoj tehnologije

Nužno je shvatiti da navedena tri čimbenika utječu na organizaciju pojedinačno ili skupno. To bi značilo da ako se promijeni jedan čimbenik, promjena tog čimbenika može, ali i ne mora utjecati na druga dva čimbenika, a oni mogu imati utjecaj na našu uslugu jedan po jedan ili svi zajedno. Ako dođe do toga postoji vjerojatnost da naša usluga više nije u skladu s jednim ili više čimbenika.

Naša organizacija ima direktan uvid na dva čimbenika, a to su zakonski i tehnološki čimbenici. Ranije smo spomenuli da njih pratimo interno kroz našu organizaciju pa smo tako uvijek u korak s ta dva čimbenika. S time smo u mogućnosti i djelovati proaktivno obavještavajući naše klijente gdje smo napravili implementacije ove usluge na promjene. Sve dodatne djelatnosti oko primjene tih izmjena morali bi ugovorno dogovarati sa svakom organizacijom ako već od prije nismo potpisali ugovor.

Promjene unutar organizacije nismo u mogućnosti mi držati pod nadzorom, nego te promjene padaju na samu organizaciju da nam ih prijavi i da se definira novi ciklus uskladbe poslovnih procesa i prepoznavanja obrada unutar istih.

Idealna situacija bi bila da imamo dogovoren model, kao što to ITIL preporučuje, kroz koji radimo stalna poboljšavanja usluge gdje bi naša organizacija periodično izvodeći mjerenja koja ćemo definirati i praćenja čimbenika mogla intervenirati i konstantno raditi prilagodbe naše usluge. To bi za organizaciju koja je naručitelj usluge značilo veliko olakšanje jer bi tako znali da su uvijek usklađeni i da na pravilan način rukuju osobnim podacima.

Slika 3.1 Prikaz utjecaja vanjskih čimbenika

Već ranije smo napomenuli da ako želimo implementirati našu uslugu u neku organizaciju i reći da je ona implementirana, moramo napraviti usklađivanja na tri različite razine, a to su zakonsko, procesno i tehnološko usklađivanje.

3.2. Usklađivanje organizacije po zakonu

Da bismo mogli pružiti usklađivanje prema zakonu, naši konzultanti moraju biti u doticaju s pravnom službom. Moraju biti svjesni svih promjena koje nastaju od trenutka kada su zadnji put bili informirani. To znači da bi mi pružili ovu uslugu naši konzultanti su u trenutku pružanja usluge prošli sve potrebne edukacije kako bi ostvarili kompetentnost u zakonskim okvirima.

Usklađivanje po zakonu u organizaciji naručitelju provodimo mi kao pružatelj usluge tako da definiranim voditeljima i izvršiteljima obrade vršimo edukacije. Edukacije koje ćemo provoditi se mogu podijeliti na dvije jednostavne kategorije:

- Implementacijska (inicijalna) edukacija
- Edukacija na zahtjev

U implementacijskoj edukaciji konzultanti će objasniti GDPR uredu, dijeliti materijale s primjerima, objasniti uloge u procesima obrade. Dakle, navedeno se smatra dijelom usluge i neće se dodatno naplaćivati korisniku.

U zahtjevanoj edukaciji organizacija naručitelj definira što žele saznati i naši konzultanti definiraju edukaciju prilagođenu baš njima. Također, ova vrsta edukacije podrazumijeva dodatnu naplatu ako nije drugačije definirano u SLA.

3.2.1. Definiranje dokumenata

Tijekom usklađivanja po zakonu generiramo dokumente i pravila postupanja. Neki od dokumenata su privole, zahtjevi za brisanjem iz sustava, potvrda o postojanju podataka, itd.

Ti dokumenti su isti uz sve organizacije u koje ćemo primjenjivati našu uslugu i njih će definirati naša pravna služba. Moguće su manje preinake dokumenata kao što je privola iz razloga potrebe dodavanja određenog podatka u prikupljanje.

3.3. Identifikacija poslovnih procesa u organizaciji

Identifikacija poslovnih procesa je proces kojim provodimo detaljne analize procesa unutar organizacije, a cilj je prepoznati skupove aktivnosti, klasificirati ih pod procese te nakon toga razložiti svaku aktivnost i prepoznati koje se obrade podataka događaju unutar njih. Nakon uspješno odrađene identifikacije krenut ćemo s grupiranjem obrada i smanjenjem količine podataka tako da iz obrada izuzmemo sve podatke koji se tamo ne bi trebali naći. Ovaj proces može potrajati od nekoliko dana do nekoliko tjedana, jer što su organizacije starije i veće nakupila se veća količina podataka.

3.3.1. Proces

Do sada spominjemo procese, no obrazložimo malo što je to proces zapravo i koji su njegovi sastavni dijelovi. Definicija procesa prema ITIL-u glasi:

Proces je strukturirani set aktivnosti dizajniranih u svrhu postizanja određenog cilja. Proces uzima jedan ili više ulaza i pretvara ih u definirane izlaze.[19]

Nadodao bih još originalnoj definiciji da bi se proces aktivirao mora se desiti neki okidač i da aktivnosti unutar procesa neće uvijek generirati dobar izlaz, te da postoje i kontrolne aktivnosti koje će cijeli proces ili zaustaviti ili će dati upute kako da se proces poboljša. Proces na određen način mora biti mjerljiv. To se radi s ciljem povećanja kvalitete izlaznih

[19] Hearsum, P. Introduction to ITIL Service Lifecycle; London, TSO 2011

vrijednosti iz procesa. Aktivnosti unutar procesa može izvršavati jedna ili više osoba. Na osnovu aktivnosti unutar procesa generiraju se i poslovne funkcije.

Poslovne funkcije obično obuhvaćaju grupu ili tim ljudi i alata te resurse koje koriste kako bi izvršili neki proces ili aktivnost.[20]

Da objasnimo na kratkom primjeru:

Mi u svakoj organizaciji imamo proces upravljanja ljudskim resursima. Taj proces se sastoji od niza aktivnosti kao što su:

- Planiranje
- Zapošljavanje novih djelatnika
- Procjenu performansi djelatnika
- Promocija ili degradacija djelatnika
- Edukacije
- Otpuštanje

Sve ove aktivnosti, zavisno o veličini organizacije može obavljati jedna ili više osoba. Velike organizacije imaju i posebne odjele koji se bave ljudskim potencijalima.

Svrha i cilj ovog procesa je kvalitetno upravljati postojećim potencijalima te po potrebi privući i dobro odabrati nove djelatnike. Unutar cijelog procesa mogu se definirati kontrolne aktivnosti kojima ćemo provjeravati svaki izlaz koji pojedina aktivnost generira.

Primjer bi bilo unaprjeđenje zaposlenika. Ulaz je djelatnik, podaci o performansama djelatnika i portfolio djelatnika. Aktivnost koja validira performanse djelatnika je dala svoj izlaz u obliku pisane procjene koju su proveli nad djelatnikom tako da su pratili rokove koje je određeni djelatnik zadovoljio ili prekršio. Aktivnost koja se brine da se djelatniku ponudi promaknuće ima uvid u rezultate analize performansi i portfelj djelatnika. No umjesto da djelatniku odmah ponudi promaknuće, uvidom u portfelj djelatnika vidi da je navedenom djelatniku prije toga potrebna obuka da bi ga se promoviralo na određenu poziciju. Tu je već prikazan kontrolni mehanizam prilikom unaprjeđenja. U tom slučaju djelovat će aktivnost edukacije, zatražit će se dodatni ulazi kao što su vrijeme i sredstava za edukaciju i djelatnika će dodatno obučiti. Nakon obuke bit će promoviran ako on na to pristane. Nakon pristanka

[20] Hearsum, P. Introduction to ITIL Service Lifecycle; London, TSO 2011

zaposlenika na unaprjeđenje završili smo jedan ciklus procesa i generirali smo izlaz, a to je unaprijeđeni djelatnik.

U ovom primjeru smo objasnili kako proces funkcionira. Kako se primjenjuju ulazi, kako funkcionira sustav kontrole koji potražuje dodatne ulaze da bi na kraju dobili željeni izlaz.

Ono što je nama bitno jest prepoznati, tj. identificirati, popisati sve procese organizacije s ciljem definiranja uloga, dokumenata i podataka koji u određenom procesu postoje. Svaki je proces jedinstven, svaki rukuje s određenim setom podataka koji mu je potreban. Isto tako, svaka aktivnost u procesu koja će biti prepoznata mora biti identificirana. Moraju se znati odnosi između aktivnosti u procesu.

Da bismo proveli usklađivanje po procesnoj osnovi moramo identificirati sve procese koji se mogu prepoznati unutar organizacije u koju implementiramo našu uslugu. Identifikaciju je potrebno provoditi kod svake nove implementacije usluge u nove organizacije zbog različitosti i specifičnosti organizacija. Također, ako organizacija nad kojom je provedena identifikacija procesa i u koju se implementira naša usluga, bude izmjenjivala ili dodavala nove procese bit će potrebno izvršiti identifikaciju nad tim promijenjenim procesima ili novo dodanim kako bi se utvrdilo postoje li nove obrade, novi podaci koji se prikupljaju te tko sve sudjeluje u tom poslovnom procesu.

3.4. Tehnološka rješenja

Kao sastavni i obavezni dio naše usluge pružat ćemo i programsko rješenje koje će nam olakšati unos, izmjene, brisanja i praćenja obrada koje provodimo. Naše programsko rješenje će biti prezentirano i isporučeno krajnjim korisnicima kao web usluga s mogućnošću pohrane podataka organizacije u cloudu ili na fizičkom serveru organizacije. Naše programsko rješenje je zapravo registar osobnih podatka, koji moramo uspostaviti kako bi mogli pratiti podatke povezane uz poslovne procese, kako interne tako i eksterne.[21]Naše programsko rješenje bit će moguće implementirati i kao samostalno rješenje bez usklađivanja, ali taj dio nije dio usluge upravljanja korisničkim podacima već je samo aplikacija kojoj je definirana cijena za mjesečno korištenje.

[21] Chad Russel, Shane Fuller, GDPR for dummies, John Wiley & Sons, LTD, West Sussex, 2017

Takav model nije preporučljiv jer on ne garantira usklađenosti organizacije, već organizacija koristi samo aplikaciju koja im olakšava organiziranje obrada i praćenje pohrane podataka.

Programsko rješenje je izvedeno kao web aplikacija zbog dodatne vrijednosti koje nam web aplikacije danas donose, a to su:

- Jednostavnost implementacije
- Jednostavno održavanje
- Program kao usluga (engl. *Software as a service*, skraćeno SAAS)
- Za korištenje je potreban uređaj s web preglednikom i pristupom internetu
- Dostupnost

Za uslugu upravljanja korisničkim podacima je od iznimne važnosti da voditelji obrada ili izvršitelji u bilo koje doba mogu pristupiti našoj usluzi i istu koristiti. Korištenjem web tehnologija dobivamo tu dodatnu vrijednost da se web aplikaciji može pristupiti putem bilo kojeg uređaja koji ima pristup internetu i ima instaliran internet pretraživač. Neki od njih su računalo, prijenosno računalo, mobilni uređaj, tablet uređaj, itd.

Programsko rješenje je dizajnirano kao 3 potpuno nezavisna sloja. To su redom:

- Prezentacijski sloj ili grafičko korisničko sučelje (engl. *Graphical user interface*, skraćeno GUI)
- Poslovni sloj ili aplikacijsko sučelje (engl. *Application interface,* skraćeno API)
- Podatkovni sloj ili sloj pristupa podacima (engl. *Data Access Layer*, skraćeno DAL)

Svaki sloj je nezavisan jedan o drugom i komuniciraju međusobno koristeći današnje moderne komunikacijske protokole. Upravo ovom odvojenošću postižemo veliku fleksibilnost prilikom isporuka dodatne vrijednosti klijentu. Prva dva sloja se isporučuju kao dvije odvojene web aplikacije. Navedene aplikacije su smještene na cloud servis te postoji centralna baza podataka koja regulira pristup aplikaciji i postavkama aplikacija za svakog korisnika aplikacije. Ideja je pružiti naizgled jednu aplikaciju za sve korisnike aplikacije, u ovom slučaju to bi bile organizacije. Registracija i prijava organizacije i njenih korisnika u aplikaciju se ostvaruje putem povezivanja korisničkog računa Google ili Microsoft. Za svaku organizaciju će biti predviđene razine administratora i korisnika.

Ranije smo spomenuli da ćemo korisniku ponuditi opciju odabira lokacije baze podataka u koju će se unositi podaci o obradama. Mogućnost odabira mjesta lokacije ima dodatnu pogodnost za korisnika. Dobrobit koja proizlazi iz ove mogućnosti je ta da ako korisnik

posjeduje privatne servere, baza može biti postavljena na te servere i korisnik ne mora dodatno plaćati održavanje i smještaj baze u cloudu. Odnosno baza i njeni resursi će biti nadzirana od strane korisnika, s čime smo smanjili trošak cloud usluga, a i našeg održavanja. U tom slučaju odgovornost o zaštiti i kontroli pristupa bazi podataka pada na korisnika. Lokaciju i njene pristupne podatke za organizaciju unosit će se u naše programsko rješenje inicijalno prilikom postavljanja aplikacije za određenu organizaciju u rad. Podaci koji su vezani za korisničke račune i lokacije baza podataka će biti pohranjeni na našem serveru u cloudu u kriptiranom obliku.

Ovim načinom mi radimo s najosnovnijim setom podataka, a korisnik svoje lozinke pohranjuje i izmjenjuje kod drugih pružatelja usluge, dok mi dobivamo od tih usluga token koji ocjenjujemo i korisnici tako ostvaruju pristup do svojih podataka.

Iz korisničke perspektive korisniku prilikom uporabe programskog rješenja izgleda da ima ispred sebe jedan kompaktan proizvod koji je krojen samo za njega, dok zapravo koristiti dva sloja aplikacije koji su jedinstveni za sve korisnike tj. organizacije. Jedino što je zapravo krojeno samo za korisnika je baza podataka o njegovoj organizaciji koja je smještena na njegov server ili cloud. Struktura baze podataka koja se koristi u ovom procesu je jedinstvena za sve baze svih organizacija.

Ovdje se pruža i mogućnost proširenja našeg programskog rješenja tako da prezentacijski sloj ne mora nužno biti web aplikacija. U budućnosti otvaramo mogućnost da se razviju aplikacije za Android i iOS koje bi pritom imale mogućnost pristupa aplikacijskom sloju koji bi i dalje bio izložen kao web servis.

3.4.1. Izvedba programskog rješenja

Glavnu radnju upravljanja podacima odrađuje aplikacijski sloj koji ima pristup centralnoj bazi podataka, te temeljem unosa podataka putem grafičkog sučelja podatke obrađuje i pohranjuje na podatkovni sloj.

Prezentacijski sloj je web aplikacija pisana kao jednostrana aplikacija (engl. *Single page application,* skraćeno SPA) koristeći moderne web tehnologije. Programski jezici korišteni u izradi aplikacije su C# i JavaScript te platforme Angular 2 za JavaScript i .Net Core za C#.

Prezentacijski sloj koristi i OAuth 2.0 autorizacijski protokol kako bi se korisnik predstavio aplikacijskom sloju tko je i dobio pristup.

Aplikacijski sloj je pisan C# programskim jezikom na .Net Core platformi.

Podatkovni sloj je Microsoft SQL baza podataka.

Komunikacija između prezentacijskog sloja i aplikacijskog sloja vrši se putem hiper tekstualnog sigurnosnog prijenosnog protokola (engl. *Hyper text transfer protocol*, skraćeno HTTPS) koji za prijenos podataka koristi JavaScript objektnu notaciju (engl. *JavaScript object notation*, skraćeno JSON).

```
{
      "Datum":"2019-01-19T23:51:03+0000"
      "Proces": {
            "Id": 5,
            "Naziv": "Demo proces",
            "Voditelj": 12,
            "Obrada": {
                  "Id": 5,
                  "Aktivnost": 55,
                  "Naziv": "Demo obrada",
                  "Izvrsitelj": 224
            }
}
```

Kôd 3.1 Primjer JSON objekta za prijenos podataka

Komunikacija između aplikacijskog sloja i baze podataka se ostvaruje korištenjem Entity Framework-a. Autorizacija s korisničkom bazom podataka se ostvaruje tako da se iz naše centralne baze podataka nakon autorizacije čitaju kriptirane lozinke i lokacije baze te se tada generiraju podaci koji ostvaruju pristup na korisničku bazu podataka. Aplikacijski sloj koristeći Entity Framework generira upit na bazu podataka koristeći strukturirani upitni jezik (engl. *Structured Query Language*, skraćeno SQL) koji se izvršava na SQL serveru i izvršava se u obliku naredbi prema definiranoj bazi podataka.

Nakon što je aplikacijski sloj dohvatio tražene podatke oni se šalju u JSON formatu na prezentacijski sloj, koji prepoznaje dogovoreni format i prikazuje podatke korisniku. Isto tako prilikom unosa podataka na prezentacijskom sloju, oni se šalju u aplikacijski sloj u JSON formatu. Aplikacijski sloj tada provjerava ispravnost unesenih podataka na način zadovoljavaju li oni određene strukture i tipove podataka. Ako se ispostavi da su podaci u ispravni, iste šalje na podatkovni sloj, odnosno zapisuje ih u bazu podataka. Nakon što su podaci uspješno ili neuspješno zapisani na podatkovnom sloju, na prezentacijski sloj se ispisuje poruka o uspjehu ili neuspjehu dane radnje.

Naše programsko rješenje je formulirano na principu knjižnice – definira procese, obrade, aktivnosti obrade, odgovorne ljude u procesu, tko ima pristup tim podacima i koje razine treba imati pristup. Definira i način na koji su ti podaci pohranjeni, fizički ili digitalno s prikazom fizičke ili digitalne lokacije na kojoj su spremljeni. Sam pristup podacima organizacije naše programsko rješenje nema.

Time se ograđujemo od samog rukovanja s podacima kao što su brisanje, čitanje ili izmjena. Podaci s kojima će raditi naše rješenje su najosnovniji set podataka organizacije u koje će isto biti implementirano.

3.5. Dokumenti u fizičkom i digitalnom obliku

Svijet kakvim ga danas poznajemo posluje u dva različita svijeta. To su digitalni i fizički poslovni svijet. Tendencija danas, a i trenutni hit u svijetu je digitalna transformacija. Proces digitalne transformacije mnogi krivo shvate te misle kako je to proces koji se odradi jednom i sada smo mi digitalna organizacija, no to je daleko od istine. Proces digitalne transformacije nije proces koji može samo tako jednostavno biti implementiran i primijenjen. On se mora sustavno uvoditi i stalno se raditi na njemu da bi se organizacija maknula što više iz fizičkog u digitalni svijet. Ovaj proces ima mnogo dobrobiti, ali ono što moramo shvatiti je da organizacija se ne može samo tako maknuti iz fizičkog svijeta. Dokle god postoji zakon koji propisuje postojanje fizičkih dokumenata mi možemo digitalizirati te dokumente i pohranjivati ih u digitalnom obliku, ali ako zakon nalaže postojanje i fizičkog oblika ili organizacije imaju potrebu za postojanjem istog, mi moramo arhivirati dokumente i u fizičkom obliku.

Ovime dolazimo do zaključka da mi kao organizacija koja provodi usklađivanja možemo dati prijedloge i implementirati poboljšanja digitalnih sustava koristeći moderne tehnologije ako se radi o podacima u digitalnom obliku. No ako se radi o podacima u fizičkom obliku mi ćemo dati preporuke kako pravilno postupati s fizičkim dokumentima koji na sebi imaju osobne podatke.

Dokumente i podatke koji se nalaze na njima usklađujemo tako da ćemo prvo analizirati kakve dokumente organizacija generira, koji su sve podaci na dokumentima legitimni interes, kakva je njihova usklađenost sa zakonskom osnovom, generirat ćemo privole ako postoji potreba za time te ćemo definirati mjesta pohrane i prava pristupa. Također za

neopravdane podatke na dokumentima koji se smatraju nepotrebnima dati ćemo upute organizaciji kako da izmjene dokument da bude usklađen s GDPR regulativom.

Od iznimne je važnosti i imati na umu da moramo podržati i brisanje, nadopunu ili izmjenu podataka od fizičke osobe ako ista to zatraži.

3.5.1. Postupanje i pohrana fizičkih dokumenata

Da bi postigli usklađenost na fizičkoj razini naši konzultanti moraju fizički proći organizaciju i vidjeti kakvi se dokumenti i gdje nalaze. Vrlo često u proizvodnoj industriji organizacije imaju mnogo podataka na radnim nalozima, u medicinskoj industriji je to još izraženije jer nalazi sadrže veliku količinu povjerljivih podataka. Ne rijetko se dogodi da koji nalaz zaluta, radni nalog se izgubi ili se desi treća situacija. Tada se organizacija može naći u velikom problemima jer takvo što bi značilo curenje podataka i tešku povredu GDPR regulative.

Brisanje, nadopunu ili izmjene ćemo podržati na različite načine, zavisno o kojem se zahtjevu radi, davanjem prijedloga organizaciji kako da postupi u tom slučaju.

Brisanje, ako taj dokument na sebi ima podatke koji su klasificirani kao legitimni interes organizacije taj dokument se ne smije mijenjati. Ako dio podataka je legitimni interes, a drugi dio nije, dokument treba izmijeniti tako da se podaci koji nisu legitimni interes obrišu. Ako je dokument nebitan za organizaciju (nije ugovor ili račun), isti je moguće uništiti.

Izmjene ili promjene je moguće implementirati ispisivanjem dokumenta s novim podacima i davanjem na potpis fizičkoj osobi, a stari tom prilikom je potrebno uništiti. Istu izmjenu ili nadopunu potrebno je i evidentirati unutar programskog rješenja.

Postupanje i pohranu podataka u fizičkom obliku moći mjeriti na način da se periodički napravi nenajavljeni fizički pregled organizacije i time se utvrdi pravilno rukovanje s dokumentima koji su klasificirani kao dokumenti osjetljive prirode te uništavaju li se dokumenti kojima je istekao rok za čuvanje.

Također će se provjeriti postoji li dokument gdje se spominje fizička osoba, a u programskom rješenju postoji evidencija da želi biti izbrisana iz sustava organizacije.

3.5.2. Postupanje i pohrana digitalnih dokumenta i podataka

Digitalni dokumenti se mogu pohranjivati na razna mjesta kao što su:

- Podatkovni mediji (USB, CD, magnetna traka)
- Baze podataka (SQL, mySQL)
- Cloud servisi za pohranu (GoolgeDrive, OneDrive)

Vrlo je velika vjerojatnost da većina dokumenata koji su generirani kao fizički dokumenti postoje i u digitalnom formatu. Samim time već prilikom prvog pregleda fizičkih dokumenata znamo za pojedine dokumente gdje je potrebno odraditi izmjene dokumenata. Za sve dokumente koje nismo identificirali i analizirali prilikom fizičkog pregleda dokumenta, a postoje u digitalnom obliku, bit će potrebno odraditi analizu podatka koje sadrže. Analiza dokumenta se provodi kako bi se utvrdio legitimni interes i izbacio višak podataka iz dokumenata, a samim time dobrobit koju organizacija dobiva je smanjenje nepotrebnih podataka i privola s kojima moraju opterećivati klijente prilikom generiranja određenog dokumenta koji sadrži osobne podatke.

Ono što nam digitalni podaci daju je fleksibilnost upravljanja podacima, a to nam znači puno brže i lakše pronalaženje podataka fizičke osobe i rad s tim podatkom. No s većom dostupnošću podataka treba primijeniti moderne kontrole pristupa podatcima.

U ovom dijelu usklađivanja ćemo uključiti i naše razvojne inženjere koji, ako to bude definirano u SLA, će u skladu s najboljim praksama i tehnologijom koju nađu, na terenu primijeniti sigurnosne metode i politike. Ovdje će se također pružiti prilika za našu organizaciju, a to je prodaja i implementacija novih programskih rješenja ili licenci. Prvu procjenu će ustanoviti konzultant u pregledu na terenu i u skladu s odlukama organizacije naručitelja primijenit će se rješenje za serversku ili cloud pohranu i čuvanje dokumenata i podataka.

Moguća rješenja koja bi mogli ponuditi su licence za cloud pohrane podataka, definiranje sigurnosnih politika i prava pristupa, definirati radnje nad dokumentima i mapama, postojeće baze podataka nadograditi i ponuditi prednosti koje nam donose nove tehnologije.

3.6. Metrike usluge

S ciljem praćenja kvalitete usluge, što boljeg upravljanja uslugom te pružanja korisničke podrške moramo implementirati mjeritelje kvalitete usluge. Moramo učiniti našu uslugu mjerljivom. Kako smo uslugu do sada podijelili na tri razine usklađivanja tako ćemo kategorizirati i mjerila usluge, s posebnim naglaskom na mjerenje kvalitete programskog rješenja.

Početna točka svih mjerenja će se postaviti prilikom prvog pregleda i zatečenog stanja u organizaciji. Mi ćemo postaviti početne faktore mjerenja po svakoj kategoriji, no ako dođe do promjene vanjskih čimbenika faktore ćemo morati sukladno njima mijenjati, dodavati ili čak možda ih proglasiti nevažećim zbog novonastalih promjena.

Kada sve rezultate metrika skupimo, moći ćemo odgovoriti na pitanje:

Upravlja li organizacija korisničkim podacima u poslovnim procesima odgovorno i u skladu s GDPR uredbom?

Sve metrike a pozitivnom ocjenom zajedno odgovaraju na postavljeno pitanje sa pozitivnim odgovorom. Ako jedna metrika ukazuje na negativan odgovor usluga nije usklađena s GDPR uredbom. Ako postoji određena metrika s negativnim rezultatom, moramo analizirati element koji je uzrokovao negativnu metriku. Analizom elementa doći ćemo do razloga negativne metrike i moći ćemo djelovati na njega ili njegove dijelove kako bi u sljedećem mjerenju davao zadovoljavajući rezultat.

Metrike ćemo provoditi jednom godišnje. Organizacija također može zatražiti metrike i na zahtjev, npr. zaposlili su novog DPO, a žele utvrditi njegovo poznavanje GDPR-a ili su napravili promjene u procesima. Bitno je napomenuti da metrike vezane uz programsko rješenje pratimo konstantno i da su te metrike izdvojene od metrika vezanih uz organizaciju.

3.6.1. Metrike zakonskog usklađivanja

Zakonsko usklađivanje nam se svodi na pregledavanja dokumenata organizacije, razgovore s DPO, voditeljima i izvršiteljima obrada te ankete i ispite. Provjeravat ćemo posjeduje li organizacija svu potrebnu dokumentaciju koju propisuje zakon te ispunjava li dodatne potrebne dokumente (privole) za prikupljanje osobnih podataka.

U ovom dijelu također ćemo mjeriti i znanje sudionika u obradi tako da se istima postave anketna pitanja iz GDPR uredbe. Kako bismo utvrdili znaju li voditelj i izvršitelj svoje dužnosti i kako se vodi pojedini proces obrade konzultanti će odraditi razgovor s voditeljima i izvršiteljima obrade.

Na godišnjoj bazi DPO i voditelji obrada morat će polagati ispit o znanju i tumačenju GDPR koji ćemo mi definirati.

3.6.2. Metrike procesnog usklađivanja

Procesno usklađivanje ćemo mjeriti tako da prvo provjeravamo postoji li dokumentacija za sve poslovne procese koje organizacija provodi. To inicijalno podrazumijeva sve aktivnosti unutar procesa, okidače koji sudjeluju u procesu, mjerenja kvalitete procesa, koji su ciljevi procesa te koje se tu sve poslovne funkcije mogu u pojedinim procesima i aktivnostima naći.

Kada smo utvrdili postojanje navedenog potrebno je provjeriti ima li organizacija navedene obrade u procesima i aktivnostima. Konzultant će obaviti razgovor s DPO kako bi se raspitao postoje li novi procesi i obrade u organizaciji ili je došlo do kakvih promjena.

Provjeravat ćemo imaju li svi procesi, aktivnosti i obrade definirane voditelje i izvršitelje obrade. Također ćemo provjeriti izvršavaju li se obrade kako treba, npr. jesu li obrisani podaci nakon što ih više ne smijemo čuvati.

To ćemo provjeriti tako da uzmemo nekoliko nasumično odabranih zahtjeva iz sustava i provjeriti i jesu li obrisani s lokacija pohrane koje su navedene u programskom rješenju.

Zadnji korak mjerenja je utvrditi da su sve promjene pravilno unesene u naše programsko rješenje.

3.6.3. Metrike tehničkog usklađivanja

Tehničko usklađivanje zbog mogućnosti pohrane i obrade podataka na fizički i digitalni način moramo gledati iz te dvije perspektive.

Fizičke načine pohrane i obrade mjeriti tako da se vodimo dokumentom preporuka koje je naš konzultant dao organizaciji da moraju provesti. Fizički ćemo morati ponovno obići sve organizacijske jedinice i ustanoviti, tj. validirati stanje koje je zatečeno na terenu, sa stanjem koje je u dokumentu s preporukama. Zavisno od organizacije do organizacije bit će definirani rokovi implementacije tehničkih rješenja i kontrola pristupa, te će se izvidi raditi u skladu s njima. Također će biti definirano što je nužno potrebno implementirati i što bi bilo dobro da se implementira. Mjerit ćemo do koje je razine implementirano rješenje i poštuju li se rokovi koji su zadani. To znači da u samom mjerenju možemo imati pregled X faktora gdje X označava broj potrebnih preinaka. Svaki će se prema dokumentu preporuka posebno ocjenjivati.

Digitalni način usklađivanja obuhvaća također dokument preporuka, ali i pregled sigurnosnih politika i prava pristupa na zajedničkim serverima, bilo da su u cloudu ili lokalno

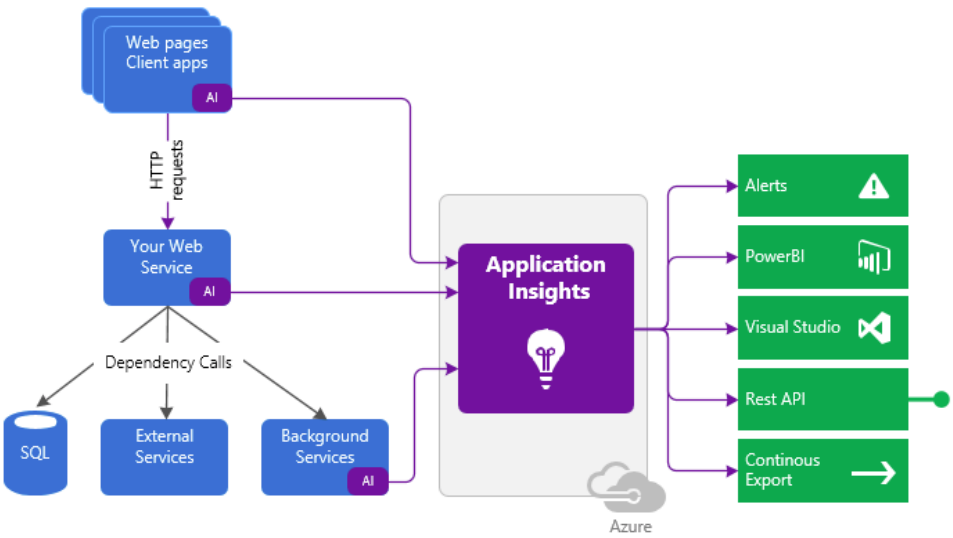
kod korisnika. Ako dokument preporuka obuhvaća nova tehnološka rješenja bit će potrebno pratiti i njihov napredak implementacije u organizaciju.

Zadnji korak mjerenja je utvrditi da su sve lokacije pohrane podataka i dokumenata s pravima pristupa pravilno upisane u naše programsko rješenje.

3.6.4. Metrike programskog rješenja

Centralni dio naše usluge se vrti oko našeg programskog rješenja, pa tako ćemo ove metrike izdvojiti kako zasebnu cjelinu. Ove metrike neće utjecati na ocjene metrika usluga implementiranih u organizaciji jer mi pružamo isto programsko rješenje za sve organizacije s kojima ćemo sklopiti ugovor.

Moramo osigurati da naše programsko rješenje radi sigurno i pouzdano 24 sata dnevno. Svjesni smo rizika koje nam donosi informacijska tehnologija i internet pa sukladno tome nad svakom komponentom našeg programskog rješenja (GUI, API i DAL) moramo implementirati alate koji će skupljati metrike i telemetriju kako bismo mogli pratiti dostupnost, opterećenje i korištenje programskog rješenja. Jedan od alata koji ćemo koristiti je Azure Application Insights.



Slika 3.2 Prikaz Azure Application insghts cloud rješenja

To je SAAS usluga koje se vrlo lako integrira u programska rješenja a omogućava praćenje i upravljanje performansi aplikacije na raznim platformama. Vrlo se lako koristi kao alat za praćenje zahtjeva na poslužitelj u web aplikacijama te nam nudi praćenje i analitiku broja zahtjeva, praćenje iznimki, metrike i telemetrije. Ovakav alat nam je potreban kako bismo

mogli optimizirati korištenje resursa na Azure platformi, prepoznati kada bi trebali povećati dostupnost aplikaciji ili čak primijetiti da se s programskim rješenjem događa nešto nepredviđeno kako bi mogli pravovremeno reagirati.

4. Tranzicija usluge

Tranzicija usluge je dio ITIL procesa čiji je cilj osigurati da nova ili izmijenjena usluga dostigne očekivanja koja su definirana u strategiji i dizajnu usluge. Ključne aktivnosti koje se provode u ovom dijelu procesa su planiranje isporuka, upravljanje rizicima, prijenos znanja postavljanje očekivanja i osiguravanje da je dodana vrijednost za organizaciju isporučena.[22]

U fazi isporuke opisat ćemo kako smo zamislili isporuku pojedinog dijela naše usluge, dotaknuti ćemo se konkretnih primjera koje ćemo predlagati našim klijentima da implementiraju u baze podatka kao što su maskiranja podataka i enkripcija. Spomenuti ćemo rizike i dati smjernice kako se njima ophoditi.

4.1. Isporuke

Isporuke su niz aktivnosti koje ćemo provoditi u sklopu procesa tranzicije, odnosno to će biti ključne radnje kako bismo dogovorenu dodanu vrijednost prenijeli korisniku.

Zavisno o dijelu usklađivanja u isporukama će biti uključeno više inženjera s više poslovnih aspekata, kao što su razvojni inženjeri, inženjeri kvalitete programskih rješenja (engl. *Software Quality Assurance Engineer*, skraćeno QA), konzultanti, inženjeri baza podatka, projekt manageri, poslovni analitičari i pravnici.

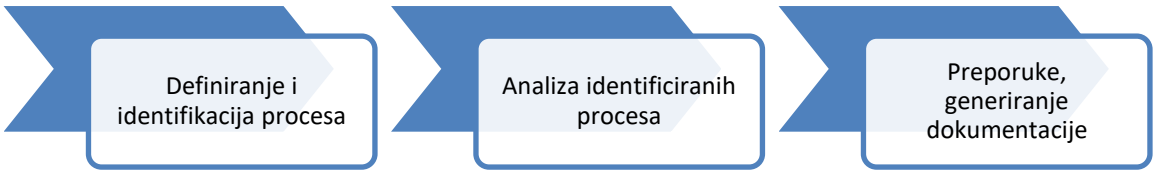
Najveći dio posla pri isporukama imat će svakako konzultanti jer će upravo oni biti stalno na terenu i radit će pojedine identifikacije i davati prijedloge organizaciji. Njima će podrška konstantno biti naša organizacija sa svojom pravnom i tehničkom službom i specijalistima iz već unaprijed pripremljenih područja bitnih za usklađivanje na svakoj osnovi.

4.1.1. Zakon i organizacija

Usklađivanje organizacije i zakona ide paralelno. To znači da naši konzultanti prvo izlaze na teren i s vodstvom organizacije prolaze kroz sve procese i dokumente u njima. Nakon što

[22] Stationery Office, ITIL 2011 Service Transition, TSO 2011.

smo s vodstvom identificirali sve procese unutar organizacije, započinjemo analize svakog pojedinog procesa.

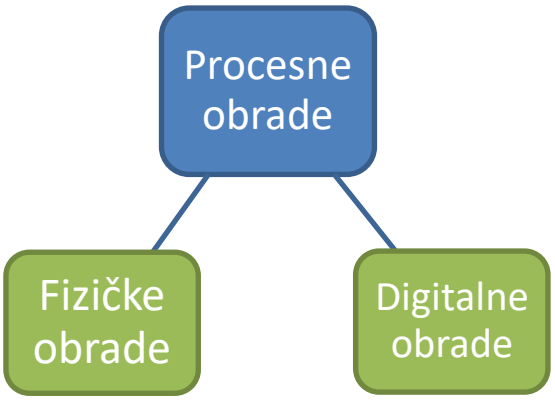


Slika 4.1 Prikaz analize procesa

Definiranje i identifikacija procesa se odvija na način:

1. Identifikacija svrhe i cilja poslovnog procesa
2. Identifikacija okidača poslovnog procesa
3. Identifikacija aktivnosti unutar procesa
4. Identifikacija sudionika procesa

Prilikom identifikacije obrada unutar procesa obrade dijelimo na fizičke i digitalne obrade. Ta podjela je od velike važnosti kako bismo kasnije što lakše rukovodili procesom. Načini rukovanja će se uvelike razlikovati zavisno od vrste obrade i njene naravi. Zavisno radi li se o fizičkoj ili digitalnoj obradi, preporuke će se odnositi na kontrole pristupa i načine prikaza podataka.



Slika 4.2 Prikaz podjele procesne obrada

Analiza identificiranih procesa obuhvaća:

1. Grupiranje procesa u skupine
2. Grupiranje aktivnosti u skupine
3. Analiza i definiranje rola te poslovnih funkcija u pojedinim aktivnostima
4. Grupiranje i klasifikacija obrada unutar aktivnosti

Prilikom zadnjeg koraka analize procesa dajemo preporuke i generiramo potrebne dokumente. To je dio gdje se počinju isprepliću zakon i organizacija. Dokumente koje moramo generirati unutar organizacije definiran nam zakon, a da bismo ih generirali i mogli kasnije pratiti sustavno kroz našu aplikaciju moramo odraditi smisleno grupiranje na procesnoj osnovi.

Po završetku analize i preporuka imamo identificirane procese, generirane dokumente, odredili smo obrade unutar aktivnosti te znamo tko treba imati pristup kojoj obradi i samim podacima. Također znamo i koji podaci se nalaze u kojim procesima. Prepoznali smo i fizičke i digitalne dokumente, podatke i obrade.

4.1.2. Isporuka programskog rješenja

Programsko rješenje postoji kao web aplikacija. Sama aplikacija se nalazi u cloudu i njoj se pristupa uz pomoć korisničkog imena i tokena. U sklopu naše usluge definirani su modeli usluge i što ona sadrži, a naše programsko rješenje je dio svakog modela usluge upravljanja korisničkim podacima jer ona i je sama srž upravljanja i informacija za pojedinu organizaciju.

Sama isporuka za sve modele ide prema sljedećim koracima:

1. Definira se SLA
2. Definiramo DPO i zamjenika DPO za nivo cijele organizacije
3. Definira se model pohrane podataka (je li baza u cloudu ili na fizičkom serveru kod korisnika)
4. Inženjeri baza podatka rade isporuku prazne baze podataka na dogovoreno mjesto i pritom se poštuju pravila informacijske sigurnosti
5. U sklopu administratorskog djela aplikacije kojem korisnik nema pristup generiraju se pristupni računi za DPO i zamjenika DPO
6. U sklopu administratorskog djela aplikacije unose se podaci o organizaciji
7. Aplikacija se povezuje s pohranom podataka
8. Naši QA inženjeri rade test programskog rješenja i baze podataka s ciljem da se uvjere da je aplikacija spremna za korištenje i unos podataka od strane korisnika
9. Omogućuje se pristup DPO i zamjeniku DPO u aplikaciju
10. Prema definiranom SLA, konzultanti provode osposobljavanje i prijenos znanja na DPO i zamjenika DPO

11. Konzultanti zajedno s DPO unose općenite podatke specifične za organizaciju, a da to nisu osobni podaci
12. Prema definiranom SLA i u trajanju koje je definirano SLA konzultanti pomažu u unosu prvih podataka u sustav na način pomoći iz prve ruke savjetima i prikazivanjem određenih radnji na demo podacima, jer tako konzultanti neće imati doticaj sa živućim podacima organizacije

Nakon što su svi koraci prošli u redu i organizacija počne koristiti naše programsko rješenje aktivno, smatramo da je isto isporučeno kao dodatna vrijednost definirana u našem dizajnu usluge.

Novije verzije programskog rješenja definirat će se u SLA te će isporuke istih ići prema planu koji će biti dogovoren između organizacije i nas pružatelja usluge.

4.2. Sigurnosne preporuke i načini implementacije

Nakon što je provedena analiza procesa i imamo čistu situaciju evidentiranu u našoj aplikaciji možemo pružiti detaljnije preporuke i u dogovoru s organizacijom provesti ih u djelo ako se radi o digitalnim obradama podataka te ako se organizacija u koju implementiramo uslugu odluči da mi odradimo taj dio posla.

Fizičke obrade smatramo manje rizičnim obradama jer na njih već možemo utjecati prilikom same identifikacije jer se pregledavaju i definiraju podaci koji se nalaze u kojem dijelu procesa. Tako se može eliminirati dosta rizika. Za primjer možemo navesti radni nalog u proizvodnom procesu. Radni nalog kao takav treba sadržavati minimalne podatke o fizičkoj osobi. Treba biti fokusiran na radni proces i podatke koji su bitni da proces ostvari taj cilj.

Konzultanti će prilikom dolaska na lokaciju organizacijske jedinice dati prijedlog na koji način ograničiti pristup povjerljivim dokumentima. To uključuje prijedlog video nadzora na lokaciji, pregradne zidove, vrata i ograničenje pristupa. Dakle, implementiranje fizičke kontrole pristupa nad definiranom lokacijom. Zavisno o veličini organizacije i broju organizacijskih jedinica imat ćemo toliko više definiranih mjesta pohrane i osoba koje pristupaju tim lokacijama. Također, konzultant će provjeravati je li na organizacijskoj jedinici primijenjena struktura procesa i identificiranih obrada u procesima.

Definirane fizičke obrade sa svim podacima o obradi konzultanti će zajedno s voditeljem obrade unositi u naše programsko rješenje u obliku da se upiše definiramo mjesto pohrane, izvršitelj i voditelja obrade.

Digitalne obrade su najrizičnije obrade upravo zbog manjka znanja o IT sigurnosti unutar organizacije. Vrlo često se dokumenti čuvaju na nekom zajedničkom serveru ili cloud mjestu za pohranu podataka, a ne postoje dobro definirane sigurnosne politike. Usluga upravljanja korisničkim podacima će pružiti preporuku da se rukovanje dokumentima ograniči implementacijom sigurnosnih politika, kontrolom pristupa i evidentiranjem svih djelatnika organizacije koji imaju ili trebaju imati pristup digitalnom dijelu organizacije. Dakle, ako djelatnik organizacije na bilo koji način pristupa na domenu organizacije i koristi bilo koju aplikaciju ili dokument koji spada pod organizaciju, on u istoj mora biti zaveden i na njega moraju djelovati sigurnosne politike.

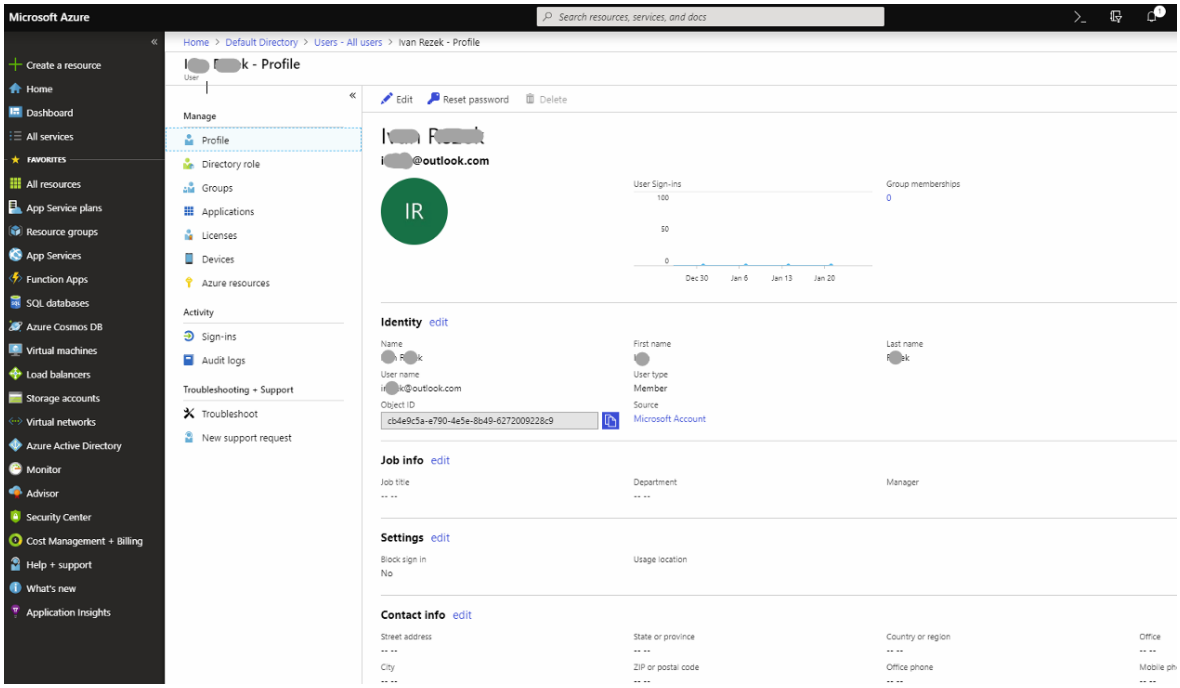
Konzultant će predložiti korištenje web pohrana podataka s ciljem povećavanja dostupnosti dokumenta. Na razini baza podataka dati će preporuke kako zaštiti podatke maskiranjem i pohranom kriptiranih podataka. Također, razine pristupa i sigurnosne politike će analizirati koje trenutno postoje te dati prijedloge za njihovo poboljšanje i unaprjeđenje prema svojem dosadašnje stečenom iskustvu. Ako se organizacija odluči za prihvaćanje danih prijedloga, mi ćemo im ponuditi implementaciju istih. U tom slučaju u proces će se uključiti odjel IT-a s našim stručnjacima za predložene implementacije. Prijedlozi će biti bazirani na Microsoftovim tehnologijama, jer naši stručnjaci su specijalisti upravo za Microsoft rješenja.

4.2.1. Cloud pohrana podataka i pristup

U današnje doba kada je bitna dostupnost dokumenta nema boljeg načina da se dokument distribuira od cloud usluga. Na svijetu postoje pružatelji usluga kao što su Google, Amazon, Microsoft koji imaju razvijene usluge za pohrane dokumenta, kako za serversku pohranu kod klijenta tako i za cloud pohranu.

Ponajprije konzultant će evidentirati posluje li organizacija tako da postoji centralni Windows server ili organizacija koristi online Microsoftova rješenja i jesu li sva računala koja se koriste, uređaji unutar domene organizacije. Na temelju inicijalne analize generirat će preporuke kako poboljšati i centralizirati upravljanje objektima koje posjeduje organizacija, a to su računala, printeri, mobilni uređaji i najvažnije djelatnici. Kao najbolje rješenje ponudit će Azure aktivni direktorij (engl. *Azure Active Directory,* skraćeno Azure

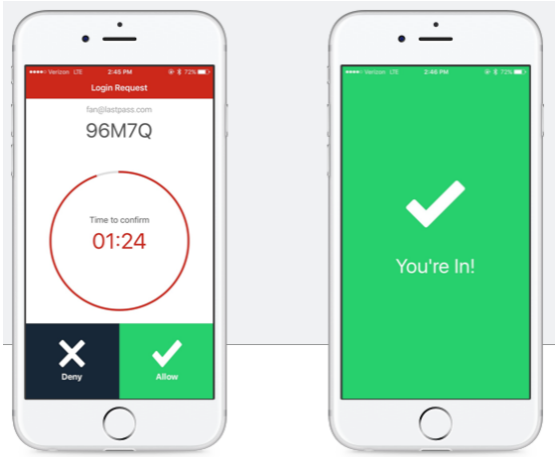
AD)[23] ako organizacija želi ići u smjeru cloud usluga ili Active Directory ako organizacija ne želi koristiti cloud usluge. Veliki naglasak će ići u smjeru cloud usluga.



Slika 4.3 Prikaz sučelja Azure AD- User Profile[24]

Azure AD je cloud inačica AD-a čiji je cilj omogućiti centralno mjesto za korisnike unutar poslovne domene. Kada imamo djelatnike organizacije zavedene u bilo Azure AD ili AD na temelju članstva security grupa možemo im ostvariti ili zabraniti pristup na određene datoteke ili direktorije. Azure AD nam nudi mogućnost da koristimo i multifaktor autentikaciju. Multifaktor autentikacija podrazumijeva jaču razinu sigurnosti prijave u aplikacije kao što su mail servisi, poslovne aplikacije, korištenje online poslovnih aplikacija. On funkcionira tako da se od nas traži pristupna lozinka i korisničko i te treći faktor koji je dodatna razina. Dakle, radi na principu nešto što znam, nešto tko sam i nešto što imam. Najčešće se za multifaktor postavljaju mobilni uređaji.

[23] Active Directory ili AD je Microsoftov servis za upravljanje direktorijima unutar domene. Preko AD-a se mogu autorizirati i autenticirati korisnici i računala unutar poslovne domene. Microsoft je također napravio i cloud rješenje a ono se zove Azure AD.
[24] Izvor Azure AD www.portal.azure.com



Slika 4.4 Primjer multifaktor notifikacije na android mobilnom uređaju[25]

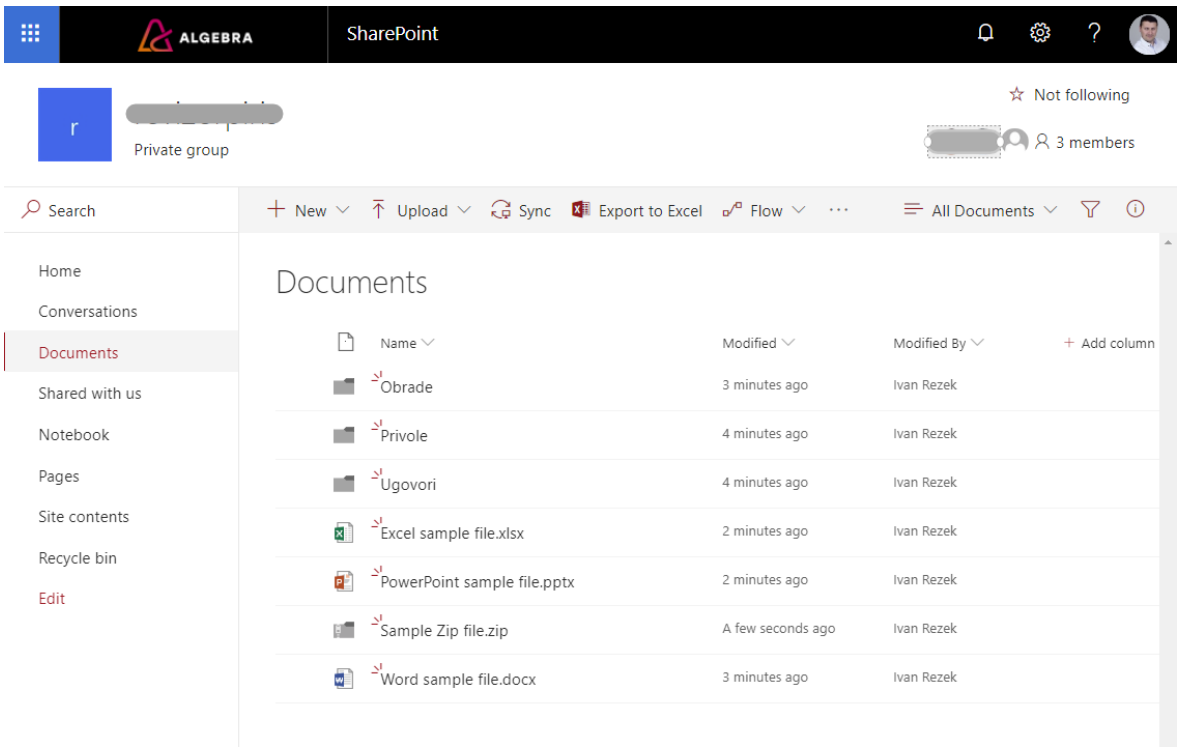
AD Group policy nam definira na što određena grupa ima prava. Članovi grupe mogu biti druge grupe ili korisnici, računala. Ostvarivanjem članstva grupe korisnik može ostvariti pravo pristupa aplikaciji kojoj do sada nije mogao ili datoteci. Grupe i članstva grupe su nam najbrži način da grupiramo ljude i delegiramo njihova prava. Dodjeljivanje prava po korisniku nikad nije dobra praksa jer u tom slučaju je vrlo teško ili skoro nemoguće pametno upravljati istim.

Naši konzultanti će procijeniti stanje organizacije u smislu da se analizira upravljanje grupama, da se napravi mala revizija prava grupa te da se uspostavi multifaktor autentikacija. Zatim prema željama organizacije će se raditi ili revizija servera na kojem se čuvaju podaci i dokumenti ili će se raditi revizija cloud usluge na kojoj imaju pohranu. Prijedlog će ići u smjeru cloud usluge SharePoint koja je Microsoftov proizvod dizajniran upravo kao sustav za pohranu i upravljanje dokumentima u cilju poboljšanja kolaboracije.

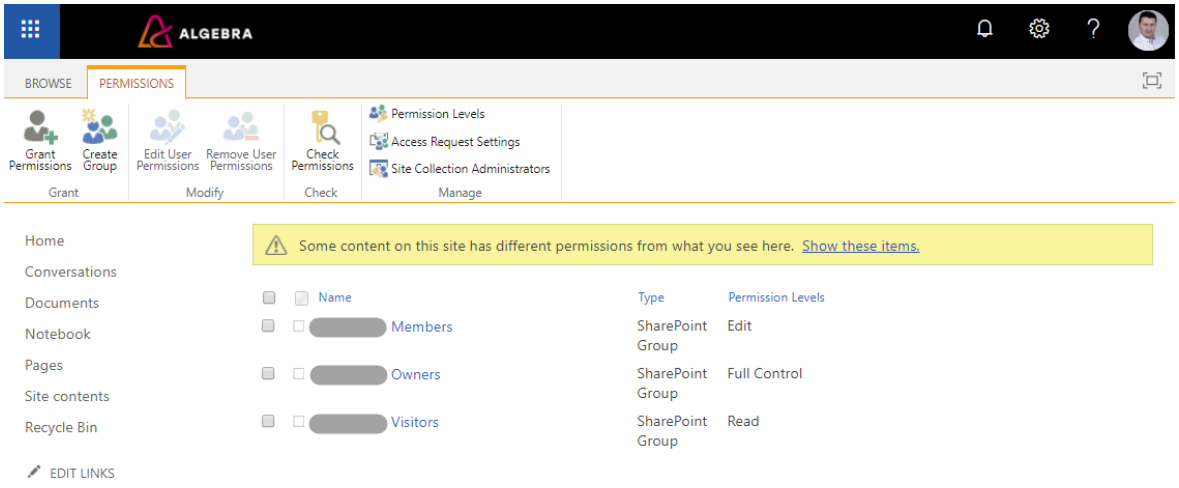
SharePoint nam omogućava upravljanje i razmjenu dokumentima unutar organizacije, a preko postavljenih i definiranih sigurnosnih politika reguliramo tko ima pristup. Također, možemo definirati i način rukovanja dokumentom, može li se samo čitati ili je dozvoljena i izmjena i brisanje. Alat omogućuje i definiranje radnih pravila (engl. *Workflow*) kojima možemo automatizirati procese. Upravo tu dobrobit možemo koristiti ako korisnik želi izmjenu ili brisanje iz sustava. Naši konzultanti, ako definiramo ugovorom, mogu postaviti osnovna pravila, definirati workfowove, radne mape i dati smjernice za upravljanje cijelom platformom. SharePoint ima upravljanje grupama prema svojoj internoj strukturi pa je

[25]Izvor:https://blog.lastpass.com/2017/05/announcing-cloud-backup-for-lastpass-authenticator-easier-multifactor-security-for-everyone.html/

potrebno još dodatno na samom alatu definirati pravila ako želimo ograničiti pristupe i po njegovim grupama.

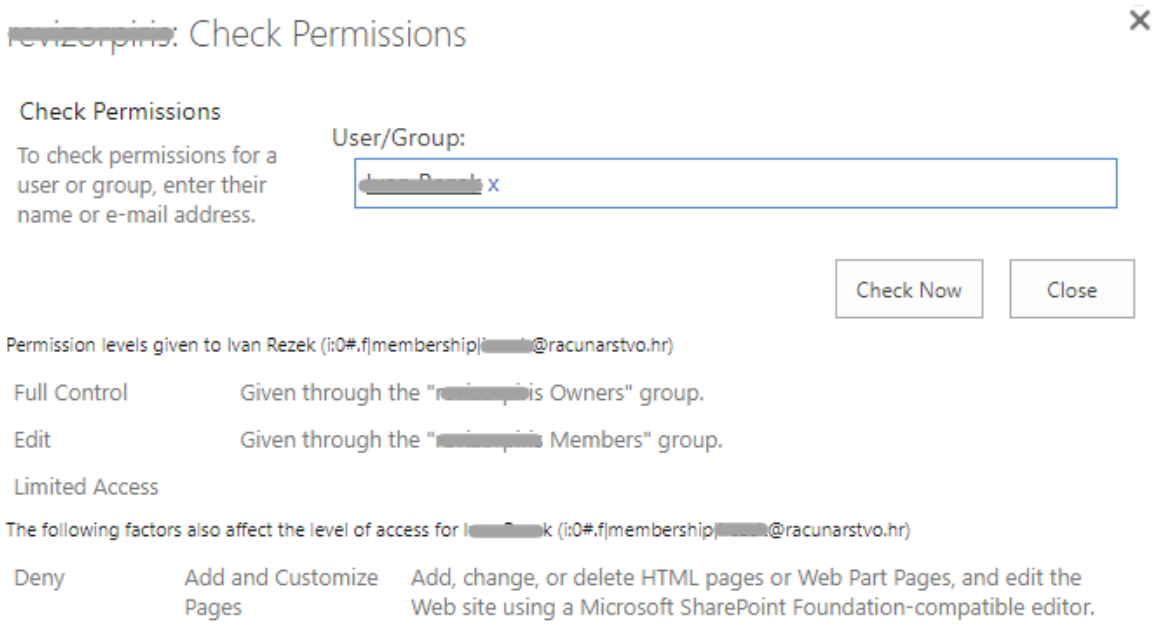


Slika 4.5 Prikaz SharePoint sučelja za pohranu i upravljanje dokumentima[26]



Slika 4.6 Prikaz SharePoint sučelja za upravljanje grupama i dodavanje članstva[27]

[26] Izvor: https://liveracunarstvo.sharepoint.com, 25. siječanj 2019.
[27] Izvor: https://liveracunarstvo.sharepoint.com, 25. siječanj 2019.



Slika 4.7 Prikaz provjere prava koje korisnik ostvaruje kroz članstvo grupe na SharePointu[28]

Osim mogućnosti generiranja workfowa na SharePointu, mi možemo generirati određene akcije nad dokumentom kao što automatizirane zadatke koristeći Microsoft Flow. Microsoft Flow je cloud workflow service koji automatizira akcije unutar dijeljenih aplikacija i servisa. Primjer bi bio dodjeljivanje potpisa za autorizaciju obrade. Korisnik postavi dokument u mapu, a time se okida flow, koji zahtjeva da voditelj obrade pročita taj dokument i dodjeli potpis odobrenja. Tako voditelj obrade dobiva poruku na svoj mobilni uređaj i može digitalno dodijeliti potpis. Po završetku potpisa izvršitelj obrade dobiva email da je odobreno ili odbijeno.

4.2.2. Moderne tehnike rada s podacima u bazi podataka

Naša baza podataka koju praznu isporučujemo korisniku bazira se na SQL Server 2016 instanci. Kako bismo podatke zaštitili da se u aplikacijama ne prikazuju za sve korisnike isto, u smislu ako netko iz odjela za unapređenje djelatnika ide pogledati njegov profil, taj isti ne mora vidjeti njegov OIB ili njegov broj tekućeg računa. Taj podatak je bitan za

[28] Izvor: https://liveracunarstvo.sharepoint.com, 25. siječanj 2019.

financije. Upravo tu nam na snagu stupa dinamičko maskiranje podataka (engl. *Dynamic Data Masking*, skraćeno DDM)[29].

DDM pomaže spriječiti nedozvoljen pristup osjetljivim podacima omogućavajući da sami odaberemo koju količinu osjetljivog podatka ćemo otkriti, a da to ima minimalan ili nikakav utjecaj na aplikacijski sloj. DDM radi tako da prilikom čitanja podatka, taj isti podatak maskira na samom SQL serveru, te takav odlazi u aplikaciju koja ga konzumira. Originalno stanje podatka se ne mijenja, on ostaje zapisan u bazi podataka, nepromijenjen.[30]

Ovo je Microsoftovo rješenje implementirano u SQL server od verzije 2016. DDL nam pruža na osnovi pravila pristupa definiranih u bazi podataka mogućnost da vidimo cijeli, samo dio ili da uopće ne vidimo podatak nego samo maskiranu vrijednost. Dostupnost ove funkcionalnosti se može ostvariti koristeći SQL Server ili samo Azure SQL Database.

Tablica 4.1 Primjer prikaza podataka bez maskiranja, s maskiranjem i djelomičnim maskiranjem

Ime	Prezime	IBAN
Marko	Markić	HR1723600001101234565
Krešo	Krešić	XXXXXXXXXXXXXXXXXXXXX
Ante	Antić	HR172360000XXXXXXX4565

Definiranje DDL se provodi tako da se identificiraju kolone u tablicama unutar baze podataka na koje želimo primijeniti DDL. SQL server dolazi sa četiri predefinirana tipa maskiranja. To su:

1. Default – potpuno maskiranje podatka
2. Email – metoda koja maskira email na način aXXX@XXX.com
3. Random – koristi se za nasumično maskiranje numeričkih vrijednosti tako da nasumično promjeni brojeve unutar brojčane vrijednosti
4. Custom string – način na koji možemo djelomično maskirati podatak s vrijednošću kojom odaberemo

[29] Izvor: https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-2017, 2. veljača 2019.
[30] Izvor: https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-2017, 2. veljača 2019.

DDL se može implementirati na postojeću kolonu u tablici ili se može definirati prilikom kreiranja kolone i tablice. Update vrijednosti u maskiranoj koloni neće biti narušen. Da bi pojedini korisnik mogao pročitati vrijednosti u toj koloni on mora imati „UNMASK“ razinu prava za tu kolonu.

```
CREATE TABLE Korisnik
(ID int IDENTITY PRIMARY KEY,
 Ime nvarchar(50) NOT NULL,
 Prezime nvarchar(100) NOT NULL,
 Email nvarchar(100) MASKED WITH (FUNCTION = 'email()') NULL)

INSERT INTO Korisnik (Ime, Prezime, Email) VALUES
('Željko', 'Željkić', 'ZZeljkic@demo.eu'),
('Branko', 'Brankić', 'BBrankic@demo.eu')
```

Kôd 4.1 Primjer kreiranja tablice s maskiranjem email kolone i ubacivanjem podataka

Kada smo definirali tablicu i ubacili podatke možemo napraviti upit na nju s razinom korisnika koji nema prava „UNMASK“. Radimo jednostavan upit `Select * From Korisnik` s time dobivamo rezultat s maskiranom kolonom za email.

```
1     Željko      Željkić     ZXXXXXX@XXXX.eu
2     Branko      Brankić     BXXXXXX@XXXX.eu
```

Kôd 4.2 Primjer rezultata s maskiranom e mail kolonom

Ako smo zaboravili prilikom kreiranja tablice dodati maskiranje kolone ili želimo izmijeniti postojeću tablicu napraviti ćemo izmjenu na tablici i željenoj koloni.

```
ALTER TABLE Korisnik
ALTER COLUMN Prezime nvarchar(50) MASKED WITH (FUNCTION =
'default()');
```

Kôd 4.3 Primjer dodavanja DDL-a na postojeću kolonu

Sada kada bismo napravili upit `Select * From Korisnik` dobili bismo dvije maskirane kolone.

```
1     Željko      XXXXXX      ZXXXXXX@XXXX.eu
2     Branko      XXXXXXX     BXXXXXX@XXXX.eu
```

Kôd 4.3 Primjer rezultata s maskiranom e mail kolonom

No ako bismo dodijelili prava korisniku da čita maskirane kolone, rezultat bi rezultirao prikazom čistih podataka.

```
GRANT UNMASK TO Operater;
EXECUTE AS USER = 'Operater';
SELECT * FROM Korisnik;
```

Kôd 4.4 Primjer dodavanja UNMASK prava korisniku Operater

Upitom Kôd 4.4 dodijelili smo korisniku prava i napravili čitanje podataka i rezultat nam sada izgleda upravo onakav kakav je zapisan inicijalno u bazi podataka. Pravo „UNMASK“ se može i oduzeti pa tako ako korisnik ide u drugi odjel, ima druge zadatke imat će i drugačiji pogled na podatke. No isto tako ako iz prakse vidimo da podatak ne treba više maskirati može se DDL s kolone ukloniti bez da se utječe na originalni podatak. Ovom funkcionalnošću čuvamo integritet podatka i njegovu sigurnost.

Još jedna razina sigurnosti se može postići koristeći stalnu enkripciju (engl. Always Encrypted)[31]. Stalna enkripcija je funkcionalnost SQL-a da koristeći certifikate u bazu podataka pohranjuje kriptirani podatak. Ta razina zaštite razdvaja aplikacijski sloj i podatkovni sloj tako da možemo bazu podataka dati trećoj strani na održavanje, a svi podaci koji su u njoj toj trećoj strani su u potpunosti beskorisni jer pravi vlasnik podataka je zapravo netko tko drži aplikacijski sloj i ima privatni ključ koji služi za dekriptiranje podataka. Brojevi kreditne kartice su idealan primjer podatka koji nikada nitko osim ovlaštene osobe ne bismo vidjeti, a u kontekstu GDPR-a ako pohranjujemo i podatke kao što su OIB, adresa, broj telefona dovodimo se do novog rizika da netko može pustiti bazu ili ukrasti podatke. Kada su kriptirani rizik od curenja podataka je minimaliziran.

Ova tehnologija se bazira na enkripciji kolona. U kriptiranju sudjeluju dva ključa. Glavni ključ kolone (engl. Column Master key) i enkripcijski ključ kolone (engl. Column Encryption key). Ključ za enkripciju podatka se pohranjuje na mjesto koje će slati podatke, obično je to aplikacijski sloj, a glavni ključ kolone je pohranjen u bazi podataka. S glavnim ključem kolone se generiraju ključevi za enkripciju kolone.

Naši konzultanti su upoznati sa navedenim tehnikama i mogu dati prijedloge implementacije, no samu implementaciju ako organizacija pristane na nju će raditi SQL razvojni inženjeri.

---

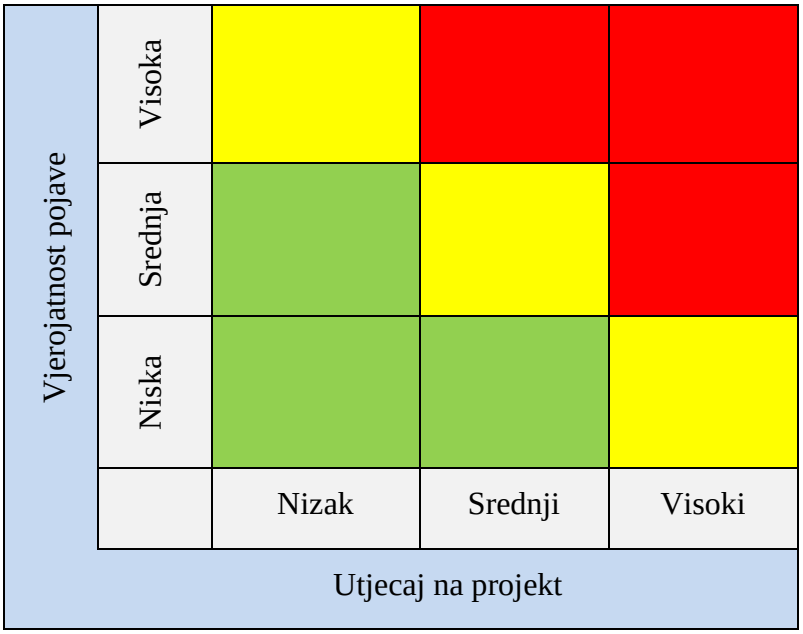
[31] https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017, 2. veljača 2019.

4.3. Rizici

Rizik je svaki neplanirani događaj koji može imati pozitivan ili negativan utjecaj na našu uslugu, može se pojaviti bilo kada i na njegovu pojavu nemamo direktan utjecaj. Zbog toga provodimo analizu rizika prilikom svakog ciklusa jer moramo prepoznati i upravljati s rizicima koji prijete dostupnosti i integritetu naše usluge.

Analizom rizika pokušavamo predvidjeti što više rizika te ih klasificirati. Također nije dovoljno rizike samo prepoznati, nego rizicima moramo upravljati tako da definiramo dokumente o upravljanju rizicima koji će sadržavati opis rizika, kakav utjecaj na našu uslugu oni imaju, predvidjeti moguća rješenja i postupanja te odraditi proračun za svako rješenja.

Tablica 4.2 Prikaz klasifikacije rizika



Zavisno od prepoznatog rizika prijedlog će biti prilagođen najboljem i najadekvatnijem rješenju. Sama procjena i analiza rizika će se izvoditi za svaku organizaciju posebno zbog različitosti organizacija u veličini, procesima, području djelovanja i odlukama uprave poduzeća.

Jedan od primjera mogućih rizika je promjena zakona i regulativa. Rizik koji tada nastaje je neusklađenost organizacije sa zakonom. Takav rizik bi bio rizik niske kategorije po vjerojatnosti pojave, ali visoke po utjecaju na organizaciju. Rješenja bi mogla biti najmanje dva, a mogla bi se i kombinirati.

Prvo rješenje:

Prihvaćanje rizika. U slučaju pojave reagirati i kontaktirati pružatelja usluge. Rezultat je neusklađenost organizacije jedan duži period zavisno o brzini reakcije pružatelja usluge i veličini organizacije, postoji rizik i od financijske kazne.

Drugo rješenje:

Transfer rizika. Organizacija odluči da se ne brine oko ovog rizika i prebaci ga na nas. U SLA se definiraju načini na koji mi pratimo usklađenost organizacije i djelujemo po potrebi. Rezultat je usklađenost organizacije uz cijenu SLA ugovora. Odgovornost je na pružatelju usluge i on je SLA definiran i odgovoran za usklađenost organizacije.

Primjer rizika s fizičkim dokumentom:

Iz dosadašnjeg iskustva na radnim nalozima znali smo viđati broj telefona, adresu, ime i prezime, OIB. Što je u potpunosti nebitno da se proces izvrši. Dovoljan set da se odradi radni nalog bi bio identifikacijski broj radnog naloga i podaci o radnjama koje se moraju izvršiti. U proizvodnji se ne smije dogoditi da neki nalog zaostane, završi u otpadnim papirima ili dođe trećoj osobi u ruke. Ovo je vrlo malo vjerojatna situacija, ali zamislite da se radi o medicinskom dokumentu koji sadrži vaše podatke, a nekako izađe u javnost? Ovo se smatra teškom povredom osobnih podataka, pa upravo iz tog razloga mi dajemo preporuke da se dokumenti izmjene i da pristup osobnim podacima imaju samo osobe koje to stvarno trebaju imati. Tako smo izbjegli nepotrebno izlaganje riziku.

Primjer rizika s digitalnim dokumentom:

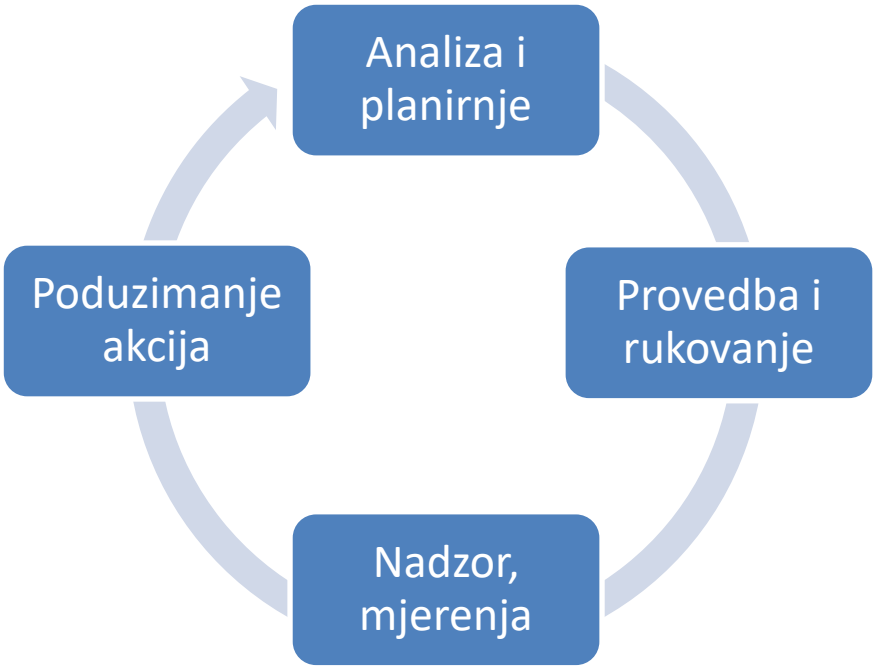
Dosta organizacija drži podatke na centralnom mjestu, no nema dobro implementirane sigurnosne politike pristupa, pa samim time se može dogoditi da administrativna djelatnica ili djelatnik klikne na poveznicu koja je ustvari Phishing[32] poveznica. Samim time ako su bili meta pristupni podaci za sigurnosni sustav treća strana ima pristup našem serveru s podacima. Implementiranjem multifaktor autentifikacije, sigurnosnih politika i Group policy možemo uvelike umanjiti ovaj rizik.

[32] Phishing je elektronička vrsta prijevare. Distribuira se najčešće elektroničkom poštom. Ona navodi korisnika na lažnu internet lokaciju koja je vrlo vjerna originalnoj da unese osobne podatke ili financijske podatke. Nakon što je osoba unijela podatke najčešće nije svjesna prijevare, a trećoj strani je dala upravo podatke koji su joj potrebni kako bi počinila štetu.

5. Rukovanje uslugom

Rukovanje uslugom je dio ITIL procesa koji nam govori o načinu kako mi rukovodimo cijelom uslugom nakon što je ona isporučena korisniku. U rukovanju ćemo objasniti kako kontroliramo pristup našoj usluzi, kako rukujemo incidentima i na koji način komuniciramo s našim korisnicima.

Prilikom izrade strategije napomenuli smo da ćemo se u fazi rukovođenja voditi normom ISO/IEC 20000-1:2011. Upravo ta norma definira da je za dobro rukovanje uslugom potrebno uspostaviti sustav upravljanja uslugom (engl. *Service management system*, skraćeno SMS). Kako bismo uspostavili SMS moramo dobro razumjeti zahtjeve i potrebe korisnika, uspostaviti način dokumentiranja te istim upravljati, dobro upravljati resursima bilo da su to ljudski resursi ili materijalni resursi. Upravo to će nam omogućiti da lakše rukovodimo implementiranom uslugom i možemo nuditi i sama poboljšanja te iste usluge.



Slika 5.5.1 Ciklus usluge upravljanja korisničkim podacima

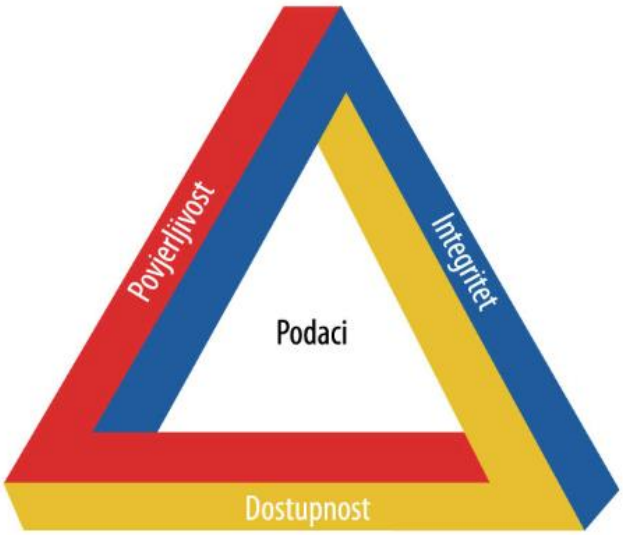
Ljudski resursi su naši IT stručnjaci, konzultanti, korisnička podrška. Da bismo uslugom rukovodili najkvalitetnije moguće uvijek se moramo pobrinuti da prilikom doticanja ili rada s ovom uslugom rade kvalificirani kadrovi. Ako se struktura naših kadrova bude mijenjala treba osigurati nove kadrove, obučiti ih i prenijeti im znanje.

Materijalni resursi su nam resursi aplikacije i baze podataka koje koristimo na našem Azure cloud servisu. Također materijalni resursi će biti i oni potrebni da bi konzultanti i IT stručnjaci mogli doći na lokaciju organizacijske jedinice i izvršavati svoje radne zadatke.

5.1. Upravljanje kontrolom pristupa

Naše programsko rješenje je jedinstveno za sve organizacije u koje je implementirana usluga. To znači da moramo upravljati kontrolom pristupa. Moramo se osigurati da određena organizacija ima pristup na svoj profil organizacije. Mora se posebnu pažnju posvetiti na praćenje tko se i kada prijavio u sustav te vidi li organizacija samo svoje podatke.

Cilj kontrole pristupa je poštivati načela informacijske sigurnosti i implementirati ih.



Slika 5.2 Prikaz načela informacijske sigurnosti[33]

Kako bismo što kvalitetnije upravljali kontrolom pristupa razvili smo sustav zapisivanja pristupa, pa tako jednostavnom pretragom zapisanih podataka možemo naići na nepravilnosti. Također smo na set zapisanih podataka implementirali algoritam pametnog učenja koji uči iz podataka prijava korisnika i što rade s podacima. Ako se očituje odstupanje od standardnog rada s podacima, sustav šalje rano upozorenje našim administratorima kako bi se pojedina aktivnost detaljno istražila.

[33] Izvor: https://blog.croz.net/blog/zastita-od-curenja-podataka/, 6. veljača 2019.

Kontrola pristupa, ako je došlo do narušavanja sigurnosti unutar neke organizacije koja koristi naše programsko rješenje, blokira se pristup u naše programsko rješenje.

5.2. Upravljanje incidentima

Kako bi kvalitetno upravljali uslugom moramo poznavati njene sve komponente, način na koji one djeluju i njihov status. Time smo omogućili prepoznavanje neželjenih događaja koji mogu rezultirati incidentima.

Incident je neplanirani prekid IT usluge ili smanjenje kvalitete IT usluge. Nedostatak u konfiguracijskoj stavci usluge koji još nije utjecao na uslugu se također smatra incidentom.[34]

Upravljanje događajima (engl. *Event management*) se bazira na praćenju događaja u usluzi, s ciljem poduzimanja određenih akcija da se spriječe incidenti. Praćenjem određenih dijelova usluge, možemo prepoznati potencijalne događaje koji će biti okidač da se poduzmu određene akcije s ciljem sprječavanja nastanka incidenta, koji može uzrokovati prekid usluge ili narušiti njenu dostupnost. Na ovaj način omogućujemo preventivno djelovanje i minimalizaciju incidenata.

Nepredviđene situacije se dešavaju svakodnevno u našim životima. Isto je i za očekivati da se može desiti i s našom uslugom. Sa stajališta naše usluge incidenti koji se mogu dogoditi su:

- Nedostupnost usluge
- Nepravovremeno reagiranje na promjene
- Pogreške prilikom usklađivanja
- Gubitak ili kompromitiranost podataka

Cilj upravljanja incidentima (engl. *Incident management*) je da po izbijanju incidenta uslugu što prije vratimo u stanje ispravnosti kako bi se minimalizirao utjecaj incidenta na korištenje usluge i na samu organizaciju. Želimo spriječiti eskalaciju incidenta pod svaku cijenu. Ako do incidenta dođe i on bude razriješen, pratit ćemo tijek izvođenja usluge kako bi se uvjerili da je sve u redu, prije nego kažemo da smo uspješno razriješili incident.

[34] Great Britain: Cabinet Office, ITIL 2011 Service Operation, TSO 2011

5.2.1. Nedostupnost usluge

Naša usluga se sastoji od više komponenata. Najpodložnija komponenta incidentu nedostupnosti usluge je naše programsko rješenje. Ranije smo naveli da se programsko rješenje sastoji od tri komponente (GUI, API i DAL), a sve tri komponente moraju imati dostupnost interneta. Uskraćivanjem pristupa internetu ili opterećujući poslužitelj s vrlo velikim brojem zahtjeva, naša usluga može postati nedostupna za korisnike koji joj žele pristupiti. Ako se onemogući pristup korisnicima programskom rješenju, naša usluga u tom danom trenutku nema svoju najbitniju komponentu, a to je sam upravljački mehanizam.

Uzroci tome mogu biti razni, ali generalno problemu pristupamo na tri različita načina.

Prvi način obuhvaća zaštite od distribuiranih napada uskrate usluge (engl. *Distributed Denial-of-service attack*, skraćeno DDoS)[35]. Naše programsko rješenje se nalazi u cloudu, točnije kao cloud pružatelj usluge koristimo Azure koji ima već predefinirane načine detekcije DDoS napada i reagiranje ako prepozna DDoS napad tako da preusmjeri promet kako bi naša aplikacija i dalje bila dostupna.

Drugi način naše programsko rješenje čuva od preopterećenosti i pada servera. Kako smo naveli da je programsko rješenje na Azure, tamo imamo podešen zrcalnu (engl. Mirror) instancu naše aplikacije. Azure infrastruktura se brine da pravilno distribuira zahtjeve. U slučaju pada jedne instance obavijesti naše inženjere o problemu i prebaci zahtjeve na drugu instancu.

Treći način zaštite je generiranje backup kopija baza i programskog rješenja. Backup baze provodit će se periodički dok backup programskog rješenja će izvoditi prilikom svake nadogradnje usluge. Nadogradnja usluge u IT svijetu često zna biti problem, pa ako se problem s novom nadogradnjom pojavio, korisnicima će biti vraćena stara verzija dok se nova ne popravi.

5.2.2. Nepravovremeno reagiranje na promjene

Zakon se ne mijenja često, ali s druge strane organizacije se mijenjaju mnogo češće. Rezultat tome je neusklađenost organizacije. Ako nismo pravovremeno reagirali na promjene nastale organizacija u kojoj je implementirana usluga može imati kobne financijske posljedice koje

[35] DDoS je informatički online napad generiranjem brojnih zahtjeva na određenu web lokaciju u isto vrijeme s ciljem da se sutav toliko optereti da postane nedostupan za normalno korištenje

se mogu odraziti i na nas. Ovoj problematici doskačemo tako da naša organizacija prati zakonske promjene, a promjene u organizaciji ili javlja organizacija sama ili se otkrivaju prilikom periodičkih pregleda usklađenosti.

5.2.3. Pogreške prilikom usklađivanja

Ljudski faktor je vrlo čest uzrok pogreški u radu. Krivo tumačenje zakona, pogrešno definiranje procesa, nepotpuno postavljanje sigurnosnih pravila ili pogreške prilikom tehničkih izvedbi mogu biti uzrok niza incidenata.

Kako bi se ljudski faktor minimalizirao, na implementaciji usluge uvijek će biti osposobljeni inženjeri i konzultanti s višegodišnjem iskustvom u IT poslovima. Naša organizacija će organizirati plan edukacija i certifikacija stručnjaka kako bi uvijek bili u korak s tehnologijom. Zakonske regulative će se prije primjene uvijek prodiskutirati na tri razine, pravnoj, procesnoj i tehničkoj kako bi se dobio dobar pogled na problematiku i moguće rješenje koje može nastati.

Sustavnim provjerama i mjerilima usluge već u prvom ciklusu imat ćemo uvid jesmo li napravili dobar posao ili su potrebne korekcije. Cilj je usklađivanje obaviti što kvalitetnije, a ne brže, jer kad su u pitanju osobni podaci, brže može vrlo lako značiti i skuplje po organizaciju u koju implementiramo uslugu, a s time i po našu organizaciju.

5.2.4. Gubitak ili kompromitiranost podataka

Kako bismo s naše stane utjecali da smanjimo gubitak podataka ili njihovu kompromitiranost, uvodimo razine pristupa i sigurnosne politike. No kako se znalo pokazati u IT svijetu, znalo se događati da poneki zaposlenik zbog nezadovoljstva namjerno počini kazneno djelo i prodaje ili samo objavi podatke koje se smatraju povjerljivim podacima, a tu se ubrajaju i osobni podaci. To je vrlo veliki teret i sramota za organizaciju jer se dosta teško može oprati obraz da mi nismo krivi nego netko drugi. Zakon jasno govori da će se takve stvari sankcionirati različito. To znači ako se desio ispad podataka, a podaci su u jasnom plain tekst formatu, kazne će biti rigorozne. No mi samo već predvidjeli Always Encrypted tehnologiju i u bazi podataka su najbitniji podaci kriptirani. Tako da ti podaci trećoj osobi neće koristiti, jer osoba nema ključ za pregled tih podataka koji ima aplikacija.

5.3. Korisnička podrška

Da bi olakšali komunikaciju s našim klijentima mi unutar vlastite organizacije, ako nemamo, moramo uspostaviti korisničku podršku (engl. *Service desk*). Komunikacija s klijentima obuhvaćat će reagiranje na incidente, pomoć korisnicima prilikom korištenja usluge te informiranje korisnika o promjenama unutar usluge. Komunikacije sa klijetima će se ostvarivati putem email poruka, poziva i video poziva.

Service desk će imati osnovni set procedura i pravila definiran koje mogu sami provjeriti i postupiti u skladu s njima. Također service desk je prvi koji analizira i klasificira problem te ga pokušava otkloniti prema setu pravila i procedura. Ako isti nije u moguće ukloniti, problem će unutar naše organizacije eskalirati voditeljima odjela koji su radili određen dio implementacije usluge.

Service desk je lice naše usluge i glavni komunikacijski kanal s korisnikom pa iz tog razloga prilikom edukacija djelatnika service deska o ovoj usluzi moramo posvetiti posebnu pažnju i nikako ih zaboraviti obavijestiti o mogućim promjenama koje implementiramo.

5.4. Upravljanje programskim rješenjem i IT problemima

Programsko rješenje koje smo razvili za potrebe upravljanja podacima unutar poslovnih procesa je naša briga i odgovornost. Kako programski tako sistemski. Odgovorni smo nadogradnje koje se tiču apstraktnog dijela programskog rješenja, razvijati prema najboljim praksama i metodama struke. Niti jedan dio kôda programskog rješenja ne smije biti isporučen korisnicima bez prethodnih iscrpnih testova i analiza. Nama je olakotna okolnost što promjene unutar aplikacije ćemo najčešće zahtijevati mi, a ne krajnji korisnik jer kao što smo spomenuli ranije mi pružamo jedinstvenu aplikaciju kao servis koji drugi koriste.

IT dio usluge zavisi o platformi na kojoj se nalazi i tako se naši Azure stručnjaci brinu da je usluga uvijek visoko dostupna, da se racionalno upravlja resursima u cloudu, te da pristup ostvaruju samo ovlaštene osobe.

6. Stalna poboljšavanja usluge

Kako se organizacije konstantno mijenjaju, postoji vrlo velika mogućnost da s vremenom naša usluga neće zadovoljavati početne kriterije koje smo zadali. Kako bi naša usluga ipak mogla zadovoljavati zadane kriterije, mi moramo raditi stalna poboljšanja usluge. U fazi stalnih poboljšavanja pozivat ćemo se na postavljene metrike i njihove rezultate kako bismo analizom tih rezultata uvidjeli na propuste ili moguće napretke i poboljšanja u našoj usluzi. Dakle, mi imamo viziju da će naša usluga postati prepoznata na tržištu po svojem jedinstvenom karakteru, a to je rad i djelovanje naših IT stručnjaka, konzultanata i pravnih savjetnika u procesu upravljanja korisničkim podacima u poslovnim procesima. Prepoznali smo da na tržištu postoji mnogo tvrtki koje nude savjetovanja i konzultacijske usluge, no mi ćemo ići taj dodatni korak dalje savjetom i djelovanjem.

Prilikom prvih implementacija zapravo ćemo spoznati koliko je svaki dio naše usluge primjenjiv na organizacije te ćemo iz iskustva implementacija uvidjeti koje dijelove naše usluge i na koji način moramo mijenjati. Ono što želimo postići je da našu uslugu što više napravimo generičkom kako bi bila što primjenjivija od organizacije do organizacije. Dobrobit koja iz tog proizlazi je manje utrošeno resursa naše organizacije. Posljedica te dobrobiti na organizacije u koje implementiramo uslugu je brža implementacija i naravno povoljnija cijena naše usluge.

Kako bismo postigli što kvalitetniju uslugu i učinili je primjenjivijom, poboljšanja ćemo raditi interno i eksterno. Interno podrazumijeva jačanje znanja naše organizacije, a eksterno znači poboljšanja na samoj usluzi koju pružamo prema organizacijama. Interna poboljšanja ćemo provoditi konstantno preko dijeljenja znanja i edukacija, bez da prethodno moramo čekati rezultate metrika, jer već iz iskustva znamo da moramo ulagati u stručne kadrove i konstantno ih educirati. Za eksterna poboljšanja vodit ćemo se prema postavljenim metrikama i rezultatima mjerenja određenih dijelova usluge.

Na kraju svakog ciklusa naše usluge, analizom metrika i spoznajama koje smo dobili iz same implementacije usluge, vidjet ćemo da li idemo u pravom smjeru i sukladno tome ćemo korigirati našu uslugu kako bi ostvarili našu viziju.

6.1. Interna poboljšanja

Interna poboljšanja su poboljšanja koja ćemo raditi mi unutar vlastite organizacije neovisno o zahtjevima organizacija ili vanjskim čimbenicima. Moramo se pobrinuti da na lokaciju kod klijenta uvijek dolazi najkompetentniji tim stručnjaka. Kompetentnost stručnjaka ćemo postići stalnim edukacijama te prijenosom znanja i iskustava u našem timu stručnjaka.

S ciljem poboljšanja razumijevanja zakona o zaštiti podataka i GDPR uredbe, unutar naše organizacije educirat ćemo naše konzultante i pravne savjetnike. Edukacije će se obavljati interno, prenoseći znanje s djelatnika na djelatnika i eksterno praćenjem promjena u zakonu, te sudjelovanjem na konferencijama i seminarima vezanim uz GDPR i sigurnost upravljanja i zaštite podataka. Također, naši IT stručnjaci će prolaziti edukacije vezane uz najnovije tehnologije i prakse u zaštiti podatka, radu s bazama podataka te izradi programskih rješenja.

Vrlo je važno napomenuti da sve incidente i pitanja koje je riješila naša korisnička podrška stvaraju određenu bazu znanja i da sa svakim riješenim incidentom znamo više, da bolje razumijemo problematiku, poslovne različitosti i posebnosti organizacija. Također sukladno iskustvima naših stručnjaka s terena, od implementacije do implementacije prilagodit ćemo naše procese usklađivanja. Iskustvom uvođenja usluge upravljanja korisničkim podacima u jednu organizaciju, naši stručnjaci će moći prilagoditi implementaciju usluge u drugim organizacijama kako bi je što brže i kvalitetnije odradili. Znanje i iskustvo koje naši stručnjaci steknu prilikom implementacija i sve novo s čime se susretnu, distribuirat će se na kraju implementacije unutar čitavog tima na završnom sastanku analize implementacije usluge.

6.2. Eksterna poboljšanja

Eksterna poboljšanja usluge tiču se samih organizacija i analize metrika koje smo dogovorili s organizacijama prilikom implementacije usluge upravljanja korisničkim podacima. Pratit ćemo postavljene metrike i nastojati razviti sustavni pristup rješavanju problema s ciljem povećanja primjenjivosti rješenja na sve organizacije, ne samo na jednu.

6.2.1. Poboljšanja zakonskog usklađivanja

Metrike zakonskog usklađivanja se odnose na analize anketa, analizu ispita te analizu dokumenta koje organizacija posjeduje. Ova analiza se provodi nakon provedenih mjerenja, što znači barem jednom godišnje.

Prilikom usklađivanja organizacije sa zakonom primijetili smo koje dokumente organizacija koristi, te koje sve dokumente organizacija treba posjedovati, a tiču se obrada osobnih podataka. Ako metrike pokazuju da postoje dokumenti koji nisu analizirani ili da je došlo do promjene u obradi ili procesu, a da to nije popraćeno potrebnom dokumentacijom, o tome ćemo obavijestiti DPO-a. Na temelju više ovakvih slučajeva razviti ćemo jedinstven pristup analizi i procedure obavještavanja organizacija i njihovih DPO-ova.

Analiza anketa svih sudionika obrada podataka ukazati će je li naš model edukacije korisnika bio dovoljno jasan. Ako rezultati nisu zadovoljavajući, raditi će se prilagodba programa. Također se može prilagoditi edukacijski program i ako se dogode značajne zakonske promjene, a koje su detektirane prilikom internih poboljšanja.

Godišnji GDPR ispit za DPO-a i voditelje obrada također će pokazati koliko oni kao odgovorni ljudi za osobne podatke shvaćaju svoje dužnosti i zadatke koje propisuje GDPR uredba. Ako rezultati svih sudionika nisu zadovoljavajući organizirati će se tečaj kako bi se ponovno cijeloj grupi objasnilo kako rukovati s podacima, a ako postoji mali broj korisnika koji nisu zadovoljili ispit, na temelju loše odgovorenih pitanja uputiti ćemo ih na adekvatnu literaturu. Iz iteracije u iteraciju vidjeti ćemo isplativosti i dobrobiti ispita, jer ne želimo pojedince dovoditi u stanje da se moraju brinuti o prolaska ispita. Želimo ih dovesti u stanje da se zapitaju radimo li nešto pogrešno, ukazati na moguću pogrešku i reći im kako to popraviti.

Cilj anketa i testova je povećati znanje DPO-a i korisnika o rukovanju osobnim podacima u poslovnim procesima, s ciljem poboljšavanja i ostvarenja što bolje usklađenosti sa zakonom i GDPR regulativom.

6.2.2. Poboljšanja procesnog usklađivanja

Procesna mjerenja usluge provodimo u suradnji s vodstvom organizacije, DPO-om i podacima koje prikupljamo od njih na godišnjoj bazi. Vodstvo organizacije se prilikom ovog mjerenja obvezuje dostaviti podatke koji su ažurni i točni, a to se odnosi na procese,

aktivnosti i zaposlenike. Konzultant će primarno razgovor odraditi s DPO-om organizacije te nasumičnim odabirom obrada će provjeriti ispravnost i dokumentiranost obrade i aktivnosti obrade. Provest će se i analiza promjena te jesu li unesene promjene evidentirane u programskom rješenju. U samom razgovoru dobiti ćemo i uvid koliko je organizaciji jednostavno ili komplicirano provoditi obrade i unositi ih u programsko rješenje. Sukladno tome možda će biti potrebno prilagoditi procesno usklađivanje i za buduće implementacije.

6.2.3. Poboljšanja tehničkog usklađivanja

Kako smo tehničke metrike podijelili na fizičke i digitalne tako ćemo iste i analizirati. U ugovoru smo definirali periodične kontrole koje ćemo provoditi s organizacijama. Uvijek krećemo od dokumenta preporuka koji su kreirali naši konzultanti na terenu. Ti dokumenti sadrže popis što treba implementirati, a što je opcionalno. Zavisno od fizičkih ili digitalnih, mjerenja se izvršavaju na drugi način.

Za fizička mjerenja, konzultant mora izaći na teren i uvidjeti jesu li preporuke implementirane. Prilikom svoga posjeta organizacijskoj jedinici provest će niz kratkih informativnih razgovora s djelatnicima organizacije, a u smislu anonimnog anketiranja da imamo uvid koliko su nam fizičke preinake koje smo preporučile uzrokovale problema u organizaciji ili su bile korak naprijed. Digitalna mjerenja kvalitete usluge ćemo mjeriti anonimnim anketama koje ćemo slati mailom kvartalno kao jednostavan link s nekoliko pitanja. Također, konzultant dok je na terenu će provjeriti pridržava li se organizacija i provodi li predložene sigurnosne politike i kontrole pristupa na svojim računalnim sustavima. Kao dodatna vrijednost izlaska na teren je iskustvo koje će konzultant dobiti iz razgovora s djelatnicima. Iz tih razgovora i kratkih pitanja moći ćemo saznati koliko smo problema tehničkom uskladbom riješili, a koliko smo novih potencijalno uzrokovali. Navedeno iskustvo ćemo iskoristiti za poboljšanje budućih tehničkih uskladbi.

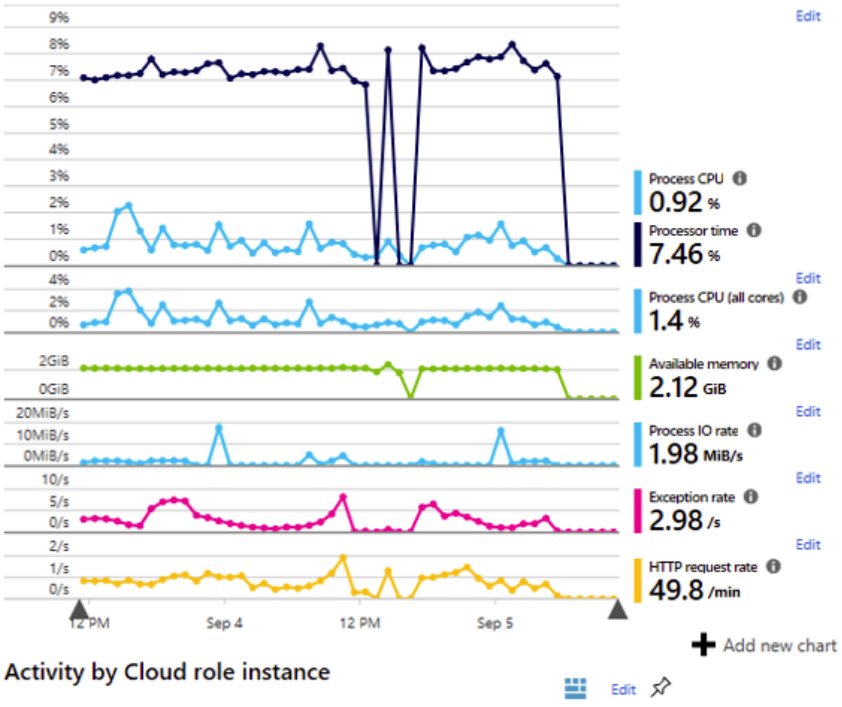
6.2.4. Poboljšanja programskog rješenja

U naše programsko rješenje implementirali smo Azure Application Insights kako bismo mogli pratiti metrike o performansama, dostupnosti i brzini izvođenja same aplikacije. Glavna ideja implementacije ove Azure usluge je kako bismo što bolje upravljali događajima unutar našeg programskog rješenja.

Slika 6.1 Prikaz dijela ciklusa razvijanja programskog rješenja[36]

Korištenjem ovog rješenja imamo mogućnost detektirati događaje koji utječu na naše programsko rješenje, analizirati ih te sukladno o kojim se događajima radi prijevremeno reagirati. Analizom podataka koje nam pruža Azure Application Insights možemo vrlo brzo doznati što se s našim programskim rješenjem događa. Na primjer, događaju li se greške prouzrokovane novim kodom koji je isporučen ili se pak radi o velikom broju zahtjeva na poslužitelj. Također možemo vidjeti trendove kada je promet u porastu pa unaprijed povećati resurse u to vrijeme kako bi programsko rješenje brže radilo.

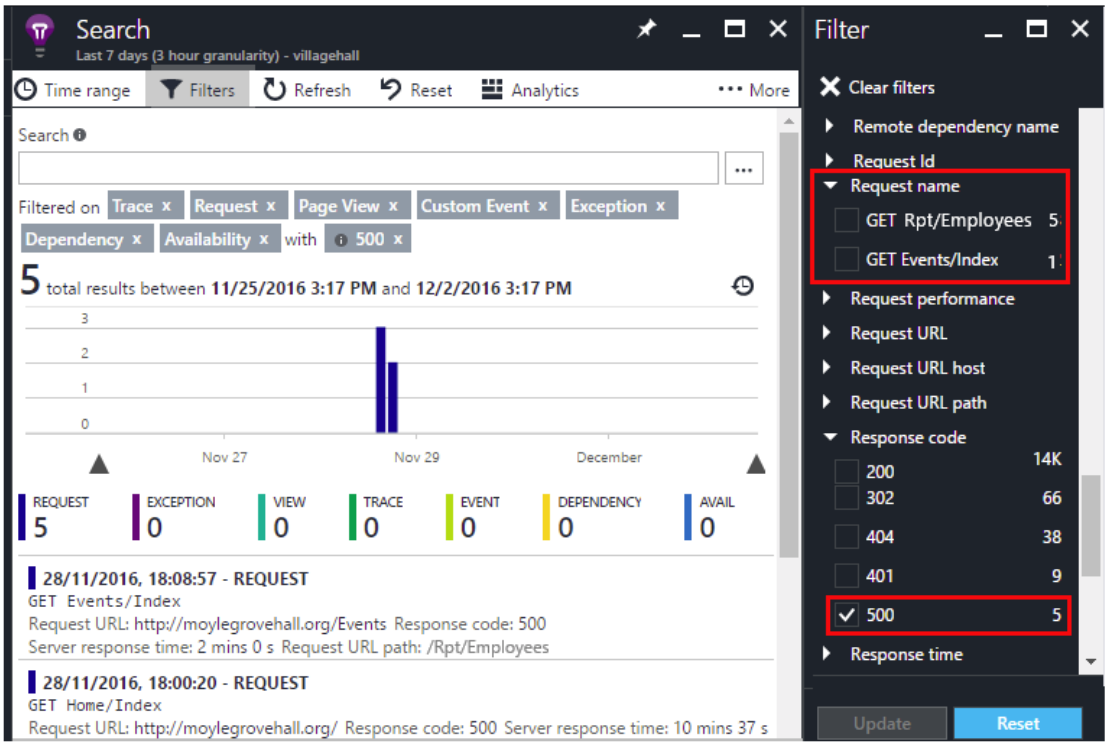
Dodatnu fleksibilnost koju pruža ova usluga je da se za određene metrike ili zahtjeve automatski obavještava korisnička podrška jednostavnom email porukom, dakle nema potrebe da naši IT stručnjaci redovito paze i gledaju što se s programskim rješenjem događa. Isto tako, ako je detektiran porast zahtjeva na aplikaciji, platforma sama nudi automatsko skaliranje infrastrukture tako da nam se dodjeli više radne memorije ili procesne moći.



Slika 6.2 Prikaz metrika u Azure Application Insightsu[37]

[36] Izvor: https://docs.microsoft.com/en-us/azure/azure-monitor/app/detect-triage-diagnose, 9. veljača 2019.
[37] Izvor : https://docs.microsoft.com/en-us/azure/azure-monitor/app/detect-triage-diagnose, 9. veljača 2019.

Slika 6.2 Prikaz metrika u Azure Application Insightsu pokazuje primjer kada je zabilježen nagli pad procesora, dakle Azure Application Insights je detektirao prestanak rada naše usluge u dva razdoblja. Sukladno detektiranom događaju možemo djelovati proaktivno i napraviti analizu prije nego što se problem počne češće događati i počne utjecati na dostupnost usluge. Potrebno je provesti analizu zahtjeva koji su stigli u to vrijeme na naš poslužitelj te koju su lokaciju na poslužitelju i s kojim parametrima ciljali. Bitno je za napomenuti kako Slika 3.2 prikazuje gdje se sve Azure Application Insights može implementirati, a kako mi imamo GUI i API odvojeno, za svaki možemo imati posebne analize. Time nam se povećava brzina analize jer jasno možemo vidjeti gdje npr. zahtjevi dugo čekaju na izvršenje s čime možemo odmah izolirati je li za spor odaziv kriv API ili GUI. Azure Application Insights nudi i mogućnost izvoza podataka kako bismo ih mogli nastaviti analizirati na nekoj drugoj platformi.



Slika 6.3 Prikaz analize zahtjeva na poslužitelj na Azure Application Insightsu[38]

Također analizom metrika možemo vidjeti koji dio našeg programskog rješenja je i koliko opterećen. Sukladno rezultatima analize možemo prepoznati na koje komponente možemo djelovati kako bismo ubrzali rad i smanjili odaziv na zahtjev korisnika. Korištenjem ovakvog alata možemo poboljšati korisničko iskustvo korištenja našeg programskog rješenja te

[38] Izvor: https://docs.microsoft.com/en-us/azure/azure-monitor/app/diagnostic-search

povećati njegovu dostupnost i smanjiti broj incidenata koji prijavljuju korisnici. Krajnji rezultat je da upravljamo događajima unutar našeg programskog rješenja, a ne da čekamo korisnika da nam prijavi incident. U ovom procesu upravljanja korisničkim podacima od iznimne je važnosti da djelujemo proaktivno, a ne reaktivno.

6.2.5. Prilagodbe potrebama organizaciji

Logično je pretpostaviti, a i za očekivati je, da se organizacije mijenjaju. Pod tim mislimo na veličinu organizacije, broj procesa, obrada i djelatnika kao i na broj organizacijskih jedinica. Naravno, organizacija može i uvesti nove proizvode, djelatnosti i poslovne funkcije pa čak i nove odjele. Isto tako može navedeno i mijenjati ili ukinuti. Dakle, organizacija je vrlo sklona promjenama, a kako smo već ranije naveli takvim promjenama, ako ih DPO dobro ne evidentira i ne provodi, organizacija rezultira neusklađenošću.

Našu uslugu možemo prilagoditi korisniku tako da definiranim ugovorima imamo periodične procjene organizacije, njenih procesa i evidentiranih obrada. Naše programsko rješenje nismo predvidjeli da se prilagođava organizaciji već zakonu.

Prilikom periodičnog pregleda ili na zahtjev organizacije napravit ćemo analize kako bismo dali preporuke organizaciji i pomogli joj da se vrati na pravi put, a to znači da bi ponovo bila usklađena sa zakonom.

6.3. Prilagodbe zakonskim okvirima

Zakonske prilagodbe su nama najzanimljivije prilagodbe zato što svoje rješenje za praćenje podataka o korisnicima pružamo svim organizacijama s kojima imamo definiran poslovni odnos. Naši pravni stručnjaci i savjetnici prate konstantno zakonske regulative i promjene te ako se desi promjena u zakonu koji se odnosi na upravljanje korisničkim podacima i zaštitu istih, dužni su navedene promjene prenijeti našim konzultantima kroz interne edukacije i prijenos znanja. Konzultanti tada rade opću analizu da utvrde utječe li ta promjena na procese unutar naše organizacije i našeg programskog rješenja. Ako primijete neke nesklade u procesima, aplikaciji ili načinima pohrane, interno će se sazvati sastanak i odraditi revizija pružene usluge. Paralelno s time, ako postoje neke promjene, iste će biti potrebno implementirati u naše rješenje. Prema korisnicima će ići obavijest o promjeni zakona i usluge te će se s korisnicima dogovoriti implementacija navedenih promjena. Oni koji nemaju definirane stavke u ugovorima dobiti će ponudu za izmjene. Sve promjene na našem

programskom riješenu ići će uz obavijest prema krajnjim korisnicima s datumom i vremenom od kada ta izmjena stupa na snagu. Isporuka nove verzije ići će prema svim korisnicima u isto vrijeme da se umanji količina posla koju je potrebno provesti prilikom nadogradnje.

6.4. Prilagodbe zahtjevima krajnjeg korisnika

Krajnji korisnik naše usluge je fizička osoba čijim podacima organizacija upravlja uz pomoć naše usluge i programskog rješenja koje je sastavni dio naše usluge. Direktan utjecaj na našu uslugu krajnji korisnik nema niti ga može ostvariti tako da on direktno traži promjene. Krajnji korisnik može, ako ima zahtjev, isti podnijeti organizaciji koja upravlja njegovim podacima i implementira našu uslugu. Organizacija je tada dužna evaluirati zahtjev korisnika i isti raspraviti sa svojim DPO. DPO je dužan prikupiti što više informacija i dokaza kako bi na temelju njih bio u mogućnosti kvalitetno procijeniti nastalu situaciju. Ako se uistinu ukaže na neke nedostatke ili propuste usluge, DPO organizacije tada treba kontaktirati svojeg konzultanta u našoj tvrtki.

Tada nam DPO organizacije iznosi problematiku s dokazima koje prikupio, a naši stručni kadrovi će analizirati problem i donijeti naše viđenje rješenja problema. Rješenje problema, ako isti postoji, ćemo pružiti prema potrebi savjetodavno prema organizaciji ili reaktivno tako da se implementiraju promjene u našoj usluzi, no cilj je da uslugu što manje prilagođavamo organizaciji, pa će rješenje koje ćemo ponuditi ići u smjeru primjenjivosti i na druge organizacije, koliko god je to moguće.

Zaključak

U današnje doba digitalizacije podaci imaju sve veću ulogu u postizanju poslovnih ciljeva. Sve je više tvrtki koje provode iscrpne analize nad podacima i iz njih prepoznaju trendove te prema trendovima usmjeravaju svoje marketinške akcije. Kao posljedica analiza podatka i marketinških kampanja pokazuje se narušavanje privatnosti fizičkih osoba. Vrlo često se radi ciljani marketing prema određenoj skupini ljudi koji bi taj proizvod kupili. U tome nema ništa loše sve dok se vi slažete da netko koristi vaše podatke. No iz osobnog iskustva, a i iz medija te iz poslovne okoline znam da se vrlo često narušava privatnost fizičke osobe.

Do nedavno postojao je zakon o zaštiti osobnih podataka, no pažnja i primjena koju je dobivao je bila vrlo mala. Europska unija je spoznala problem fizičke osobe i iskorištavanja osobnih podatka te je donijela uredbu o zaštiti osobnih podatka koja se odnosi na sve pravne i fizičke osobe u Europskoj uniji, s ciljem zaštite privatne osobe od zloupotrebe njezinih podataka. Sve članice EU su dužne primijeniti ovu uredbu.

Kako je ta uredba dobrobit za pojedinca tako je postala pravni i poslovni pritisak na organizaciju. Organizacije su prisiljene odraditi usklađivanje svojih poslovnih procesa s GDPR uredbom, te ako to isto ne odrade, prijete im velike financijske kazne. Što je organizacija veća, ima više poslovnih procesa i osobnih podatka korisnika s kojima rukovodi. Ja sam prepoznao poslovnu mogućnost kreiranja jedinstvene usluge upravljanja korisničkim podacima u poslovnim procesima koja bi na sustavan način olakšala usklađivanje organizacija s GDPR-om i pružila programsko rješenje kao alat s kojim bi se organizacijama olakšao sam proces rukovanja s podacima.

Ovu poslovnu priliku mnogi su protumačili samo kao konzultantske usluge, no ja sam u ovom radu opisao svoje viđenje usluge koja se ne bavi samo konzultiranjem i djelovanjem u organizaciji u koju će se usluga implementirati. Poučen iskustvom iz IT poslovnog svijeta, osmislio sam uslugu koja bi pružala konzultacije, provodila usklađivanja na pravnoj, procesnoj i tehničkoj razini tako da su u cijeli proces uključeni i drugi IT stručnjaci.

Prepoznao sam da većina organizacija misli da poštuju zakon ako samo za određen podatak daju papir na koji se fizička osoba potpiše da daje suglasnost odnosno privolu, te se nada da je sve u redu. To nije ni približno dovoljno. Potrebno je uskladiti organizaciju sa zakonom. No organizacija ne može postići usklađenost sa zakonom ako nismo proveli identifikaciju i analizu poslovnih procesa. A na kraju da bi se lakše pratilo tko, čemu, gdje i kada ima pristup

osmislio sam i opisao programsko rješenje. Za pohrane podataka i kontrole pristupa naglasak sam stavio na cloud usluge, a kao pružatelja usluga naveo sam Microsoft zbog dosadašnjeg iskustva u radu s njihovim programskim rješenjima.

Zaključio sam kako je bitno provesti sve tri uskladbe zajedno kao cjelinu, jer jedna drugu nadopunjava i jedna bez druge nije potpuna. Zaključio sam da upravo kako ćemo provoditi uskladbe, tako na našu uslugu djeluju i vanjski čimbenici koji pak imaju tendenciju i djelovanja jedan na drugoga. Svoju prepoznatu uslugu odlučio sam implementirati prema ITIL-ovom skupu dobrih praksi.

Programsko rješenje koje navodim kao alat u rukovanju s podacima, je web aplikacija s odijeljenim slojevima kako bi se povećala mogućnost nadogradnje ili promjene određenog dijela programskog rješenja bez utjecaja na drugi dio. Opisao sam načine komunikacije između slojeva programskog rješenja te kakve sigurnosne mehanizme smo implementirali da bi podatke s kojima naši korisnici rade, zaštitili od neželjenih i neplaniranih događaja.

Kako bi povećali kontrolu pristupa naveo sam uvođenje multifaktor autentikacije te objasnio njene dobrobiti. Dijelove tehničke uskladbe sam opisao kako i na koji način te upotrebom kojih tehnologija ćemo provoditi. Predložio sam u usluzi centralizaciju pohrane dokumenata na cloud servis SharePoint koji omogućava kontrolirani pristup dokumentima te dodatne mogućnosti u radu s dokumentima, kao što su workflowovi. Kako najviše iskustva imam s Microsoft platformom, svoje tehničke uskladbe bazirao sam na SQL Data Masking i Always Encrypted SQL tehnologiji kao dodatni faktor zaštite implementiran u našem programskom rješenju te kao opcija da se isto i prilikom tehničke uskladbe implementira kod korisnika, ako to korisnik bude želio i infrastruktura dozvoli.

Svoju uslugu sam predvidio kao mjerljivu, tako da sam predvidio načine na koje ću mjeriti pojedine komponente koji sačinjavaju uslugu. Predvidio sam upravljanje događajima i incidentima te sam objasnio važnost i koncept korisničke podrške, ne samo u kontekstu pružanja pomoći klijentu, već i kontekstu poboljšavanja usluge na način da se znanja stečena prilikom rješavanja incidenata prenesu na ostatak naše organizacije koja sudjeluje u procesu implementacije usluga. Dobrobit koja iz toga proizlazi je da se može na temelju iskustava smanjiti količina incidenata te ubrzati implementacija usluge u druge organizacije.

Objasnio sam da je vizija usluge biti prepoznat po pružanju konzultantskih usluga, ali i po djelovanju. Spomenute metrike koje su implementirane u usluzi pomoći će nam da našu uslugu možemo učiniti boljom, bržom i povoljnijom za naše korisnike. Cijela usluga je

zamišljena kao proces iz kojeg naša organizacija stalno uči i konstantno unaprjeđuje uslugu kako bi ostvarili što bolje korisničko iskustvo i organizacijama olakšali cijeli proces oko usklađivanja s GDPR-om.

Popis kratica

API	Application interface	Aplikacijsko sučelje
AD	Active Directory	Aktivni Direktorij
AAD	Azure Active Directory	Azure Aktivni Direktorij
BI	Business Inteligence	Poslovna inteligencija
DAL	Data Access Layer	Sloj pristupa podacima
DDL	Dynamic Data Masking	Dinamičko maskiranje podataka
DDoS	Distributed Denial-of-service attack	Distribuirani napad uskraćivanjem usluge
DPO	Data protection officer	Službenik za zaštitu osobnih podataka
CRM	Customer Relationship System	Sustavi upravljanja odnosa s kupcima
GDPR	General data protection regulation	Opća uredba o zaštiti podataka
GUI	Graphical user interface	Grafičko korisničko sučelje
HTTPS	Hyper text transfer protocol	Hiper tekstualni sigurnosni prijenosni protokol
ITIL	Information technology infrastructure library	Okvir infrastrukture informacijske tehnologije
JSON	JavaScript object notation	JavaScript objektna notacija
PDCA	Plan, Do, Check, Act	Planiranje, Provedba, Provjera, Djelovanje
SPA	Single page application	Jednostrana aplikacija
SAAS	Software as a service	Program kao usluga
SLA	Service level agreement	Sporazum o razini usluge
SMS	Service managment system	Sustav upravljanja uslugom
SQL	Structured Query Language	Strukturirani upitni jezik
QA	Software Quality Assurance Engineer	Inženjer kvalitete programskih rješenja

Popis slika

Slika 2.1 Primjer analize prekida ugovornog odnosa 13

Slika 2.2 Životni ciklus usluge prema ITIL-u 14

Slika 2.3 PDCA metodologija primjenjena na upravljanje uslugom..... 15

Slika 3.1 Prikaz utjecaja vanjskih čimbenika 18

Slika 3.2 Prikaz Azure Application insghts cloud rješenja 30

Slika 4.1 Prikaz analize procesa 33

Slika 4.2 Prikaz podjele procesne obrada 33

Slika 4.3 Prikaz sučelja Azure AD- User Profile 37

Slika 4.4 Primjer multifaktor notifikacije na android mobilnom uređaju 38

Slika 4.5 Prikaz SharePoint sučelja za pohranu i upravljanje dokumentima 39

Slika 4.6 Prikaz SharePoint sučelja za upravljanje grupama i dodavanje članstva..... 39

Slika 4.7 Prikaz provjere prava koje korisnik ostvaruje kroz članstvo grupe na SharePointu 40

Slika 5.5.1 Ciklus usluge upravljanja korisničkim podacima 46

Slika 5.2 Prikaz načela informacijske sigurnosti..... 47

Slika 6.1 Prikaz djela ciklusa razvijanja programskog rješenja 56

Slika 6.2 Prikaz metrika u Azure Application Insightsu 56

Slika 6.3 Prikaz analize zahtjeva na poslužitelj na Azure Application Insightsu..... 57

Popis tablica

Tablica 4.1 Primjer prikaza podataka bez maskiranja, sa maskiranjem i djelomičnim maskiranjem 41

Tablica 4.2 Prikaz klasifikacije rizika 44

Popis kôdova

Kôd 3.1 Primjer JSON objekta za prijenos podataka 24

Kôd 4.1 Primjer kreiranja tablice sa maskiranjem email kolone i ubacivanjem podataka.. 42

Kôd 4.2 Primjer rezultata sa maskiranom e mail kolonom 42

Kôd 4.3 Primjer dodavanja DDL-a na postojeću kolonu 42

Kôd 4.4 Primjer dodavanja UNMASK prava korisniku Operater 43

Literatura

[1] SLUŽBENI LIST EUROPSKE UNIJE, Uredba (EU) 2016/679 Europskog parlamenta i vijeća, EU, 2016

[2] CHAD RUSSEL, SHANE FULLER, GDPR for dummies, John Wiley & Sons, LTD, ISBN:9781119419266, West Sussex, 2017

[3] AHMAD, N., ZULKIFLI, M.S. *Systematic Approach to Successful Implementation of ITIL*, Procedia Computer Science 17 237 – 244, 2013

[4] ISO/IEC 20000-1:2011, https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en, 27. Siječanj 2019

[5] https://docs.microsoft.com/en-us/sql/relational-databases/security/security-center-for-sql-server-database-engine-and-azure-sql-database?view=sql-server-2017, 21. Siječanj 2019.

[6] https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017, 1. Veljače 2019.

[7] https://docs.microsoft.com/en-us/azure/active-directory/, 9. Veljače 2019.

[8] https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access, 9. Veljače 2019.

[9] HEARSUM, P. *Introduction to ITIL Service Lifecycle*, London: TSO; 2011, ISBN13: 9780113313099

[10] ITSMF UK, *An introductory overview of ITIL 2011*, London: TSO, ISBN:9780113313556, 2012

[11] GREAT BRITAIN: CABINET OFFICE, *ITIL 2011 Service Strategy*, Stationery Office, ISBN13: 9780113313044

[12] STATIONERY OFFICE, *ITIL 2011 Service Design*, TSO, ISBN13:9780113313112, 2011

[13] STATIONERY OFFICE, *ITIL 2011 Service Transition*, TSO, ISBN13:9780113313068, 2011

[14] GREAT BRITAIN: CABINET OFFICE, *ITIL 2011 Service Operation*, TSO, ISBN13:9780113313075, 2011

[15] INFORMATION RESOURCES MANAGMENT ASSOCIATION. *Business Inteligence: Concepts, Methodologies, Tools and Applications*, Liderpress TimPress, ISBN: 953-95472-1-0, USA 2016

[16] R. KELLY RAINER JR., CASEY G. CEGIELSKI, Introduction to information systems, Bussiness Science Reference, eISBN:9781466695634, USA, 2011

Prilog

Kao prilog prilažem CD s kompletnim završnim radom u izvornom formatu .docx i .pdf formatu.

ALGEBRA
VISOKO UČILIŠTE

UPRAVLJANJE KORISNIČKIM PODACIMA U POSLOVNIM PROCESIMA

Pristupnik: Ivan Rezek, 0321005486

Mentor: Renato Barišić, v. pred.