Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Maksic, Nikolija
Steinbråten, Anette

Anskaffelser av IT-løsninger - en casestudie

Bacheloroppgave i Digital Forretningsutvikling
Veileder: Torstein Elias Hjelle
Mai 2022

NTNU
Kunnskap for en bedre verden

Maksic, Nikolija
Steinbråten, Anette

Anskaffelser av IT-løsninger - en casestudie

Bacheloroppgave i Digital Forretningsutvikling
Veileder: Torstein Elias Hjelle
Mai 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU
Kunnskap for en bedre verden

Forord

Denne bacheloroppgaven er et resultat av en treårig utdanning i Digital forretningsutvikling ved Norges teknisk-naturvitenskaplige universitet i Trondheim. Oppgaven er skrevet ved Institutt for datateknologi og informatikk gjennom vårsemesteret 2022.

I studiets fjerde semester ble emnet DIFT2007 Informasjonssikkerhetsstyring introdusert, noe vi fant veldig interessant. Samtlige temaer i emnet virket spennende og vi ønsket derfor å tilegne oss bedre kunnskaper rundt temaene gjennom bacheloroppgaven.

Først vil vi takke vår motiverende og støttende oppgavestiller som har gitt oss god innsikt i virksomheten og deres systemer. Vi vil også takke for engasjementet, samarbeidet og veiledningen vi har fått i løpet av vårsemesteret. Samtidig vil vi rette en takk til vår hoved-informatør for deltakelse og hjelp med oppgaven. Dette har vært med på å forme bacheloroppgaven til en relevant og dagsaktuell oppgave, og har vært til stor hjelp.

Vi vil også takke vår veileder, Torstein Elias Løland Hjelle, for gode tilbakemeldinger, godt engasjement hjelp og støtte gjennom hele prosessen. Det har vært en svært spennende og lærerik oppgave, der vi har utnyttet læringsutbyttet fra studiet i tillegg til å tilegne oss ny kunnskap. Vi har fått en dypere forståelse for ulike utfordringer, rutiner og regelverk innenfor informasjonssikkerhet, samt anskaffelsesprosessen. Takk for støtten, gleden, motivasjonen, erfaringen, kunnskapsdelingen og de gode diskusjonene. Tusen takk for et meget godt samarbeid.

Trondheim, mai 2022

Anette Steinbråten og Nikolija Maksic

Sammendrag

På grunn av personvernforordningen (GDPR) som trådte i kraft i 2018 med den påfølgende Schrems II dommen som kom i 2020, har håndtering av personopplysninger blitt en stadig vanskeligere oppgave. Spesielt har håndteringen av digitale anskaffelser blitt en mer utfordrende prosess, da det både er vanskelig og tidkrevende å dokumentere at leverandørene oppfyller alle lovpålagte krav. Denne oppgaven går derfor i dybden på anskaffelsesprosessen for å se på typiske utfordringer som ofte dukker opp, og potensielle løsninger som skal hjelpe virksomheten i å sikre en god anskaffelsesprosess.

Dataene som er samlet, er hentet inn gjennom intervjuer fra et utvalg av ansatte i den valgte casevirksomheten. Forskningen baserer seg på hvordan dagens prosess ser ut, erfaringer fra ansatte og hva de selv syns er utfordrende. Dataene som ble hentet inn er diskutert opp mot relevant teori fra et bredt spekter av kilder for å komme med troverdige argumenter og en fornuftig konklusjon.

Resultatene fra studien har belyst flere utfordringer knyttet til anskaffelsesprosessen, og de fleste bunner ut i håndteringen av GDPR og Schrems II. For å forbedre prosessen er virksomheten nødt til å gjennomføre tiltak som skaper en enklere og raskere prosess, uten at det går på bekostning av kvaliteten. Dette vil bidra til at virksomenheten skaffer bedre kontroll over anskaffelsesprosessene, og samtidig styrke sikkerhetskulturen i virksomheten.

Abstract

Due to the new Privacy Regulation (GDPR) coming into force in 2018, followed by Schrems II in 2020, handling personal data has become difficult. In particular, the handling of digital procurement has become a more challenging process because it is both difficult and time-consuming to document that every supplier fulfills the mandatory requirements. Therefore, the thesis will focus on the procurement process, look at typical challenges that often arise, and potential solutions that will help the company ensure a good procurement process.

The collected data are obtained through interviews with employees in the selected company. The research is based on what the current process looks like, experiences from employees, and how they wish the process were. The collected data are discussed against relevant theories obtained from various sources to ensure valid arguments and a correct conclusion.

The results from our study have highlighted several challenges related to the procurement process, and most are based on handling GDPR and Schrems II. To improve the process, the company must implement specific measures to create a simpler and faster process without compromising quality. This process will help the company gain better control over the procurement processes and strengthen the safety culture in the company.

Innholdsfortegnelse

1. Innledning

I 2022 meldte Eurostat at over de siste seks årene har det vært en dobling av antall virksomheter som lagrer data i skyen (Gjessing, 2022). Hele 64% av norske virksomheter oppgir at de bruker diverse skytjenester i sin daglige drift. Dette er en del høyere enn det europeiske gjennomsnittet på 41%. Eurostat opplyser dessuten at over 70% av de som bruker skytjenester, bruker sofistikerte skytjenester til utvikling av programvare, lagring av data og drift av datasystemer (Gjessing, 2022).

På bakgrunn av den økte bruken av skytjenester har personvern blitt satt mer i fokus. Personvern handler om retten til å bestemme over egne personopplysninger og at alle har rett til et privatliv. Et resultat av dette er den nye loven GDPR som kom i 2018, og den påfølgende dommen Schrems II som kom i 2020. GDPR handler i hovedsak om behandling av persondata innenfor Europa, mens Schrems II handler om hvordan en skal forholde seg til overføring av personopplysninger utenfor Europa.

Deling og utnyttelse av data har ekspandert de siste årene og har blitt en viktig del av hverdagen. I takt med at virksomheter stadig tar i bruk flere eksterne tjenester og systemer, har kjeden av leverandører blitt både lenger og mer uoversiktlig. Det er vanskelig å finne og verifisere alle underleverandørene som er tilknyttet en enkelt virksomhet, og få ansatte har kjennskap til alle underleverandørene som er involverte i systemene deres (Telenor, 2021). Derfor har det blitt viktigere å få kontroll over alle tjenester som er tilknyttet en virksomhet, og dette blir gjort ved omfattende anskaffelsesprosesser.

De nye kravene har ført til en mer komplisert og tidkrevende anskaffelsesprosess. Virksomheter kan ikke lenger godta en ny leverandør uten å ha gjennomgått omfattende prosesser for å påse at leverandører etterlever lover og regler. Virksomheten må jobbe systematisk for å dokumentere enhver leverandør, uansett produkt eller tjeneste.

Denne bacheloroppgaven vil gå i dybden på anskaffelsesprosessen hos én valgt casevirksomhet, for å se på ulike utfordringer og potensielle tiltak for å bedre prosessen.

1.1 Problemstilling

Det er blitt mer vanlig å benytte seg av et økt antall leverandører til å levere diverse tjenester og systemer som trengs i en virksomhet (IKT Norge, 2018). Likevel er det få virksomheter som har gode rutiner på hvordan en anskaffelse skal gjennomføres, og det tyder på at det er enda færre som faktisk følger rutinene som er satt. Derfor er det viktig å få på plass en prosessbeskrivelse som etablerer rutiner og sikrer at prosessen blir gjennomført etter en gitt standard.

Ved anskaffelse av en ny leverandør er det viktig å ha en grundig gjennomgang av leverandøren sine rutiner og prosesser for å få et perspektiv på mulige utfordringer og risikoer i fremtiden. Leverandøren må forholde seg til regelverk og opprettholde en viss standard for at virksomheten selv kan stå inne for leverandøren. Virksomheten må ha avklart hvordan leverandøren skal benyttes, og hvordan dataene blir lagret gjennom deres

systemer. Med bakgrunn i stadig flere utfordringer knyttet til å utføre en anskaffelse har vi utformet en problemstilling som følger:

> *Hvordan kan en IT-virksomhet sikre en god prosess ved anskaffelse av nye IT-løsninger?*

Det er mange faktorer som kan bidra til å sikre en god prosess, og vi har derfor utarbeidet to forskningsspørsmål som skal hjelpe oss å svare på problemstillingen. Resultatet fra forskningsspørsmålene vil fungere som et hjelpemiddel for å trekke en konklusjon. Det skal bidra til å bryte ned problemstillingen i mer konkrete spørsmål som er enklere å svare på. Det første forskningsspørsmålet er:

> *Hvilke utfordringer vil en virksomhet typisk oppleve i forbindelse med anskaffelsesprosessen?*

For å svare på dette forskningsspørsmålet skal vi ta i bruk resultatene fra intervjurunden og knytte det opp mot aktuell teori. I intervjurunden hadde ansatte fra forskjellige avdelinger ulike oppfatninger om hva som var utfordrende for dem. Ved å gå nærmere inn på disse utfordringene vil det gi et helhetlig inntrykk av prosessen og hvordan den utføres i ulike deler av virksomheten i dag. Som en videreføring er det naturlig å se på hvordan casevirksomheten kan forbedre anskaffelsesprosessen, noe som leder til det andre forskningsspørsmålet:

> *Hvilke tiltak kan en virksomhet gjøre for å sikre vellykkede anskaffelsesprosesser?*

Ved å ta utgangspunkt i dagens utfordringer kan en se på potensielle tiltak som kan bidra til å forbedre anskaffelsesprosessen. Dette er en viktig prosess da konsekvensene av en mislykket anskaffelse kan bli kostbar og svekke verdiskapingen innad i virksomheten.

1.2 Avgrensninger

I denne oppgaven settes det fokus på utfordringer knyttet til anskaffelsesprosessen og hvilke tiltak som kan bedre dagens prosess. Casevirksomheten opplever særlig utfordringer knyttet til håndteringen av GDPR og Schrems II i anskaffelsesprosessen. Oppgaven er derfor vinklet mot anskaffelser av digitale tjenester og programvare, da det er disse type anskaffelser som i størst grad blir påvirket av GDPR og Schrems II hos casevirksomheten.

Oppgaven tar ikke for seg sikkerhetsbrudd og ulykker som er knyttet til angrep av leverandører som virksomheten bruker. Dette er fordi det er begrenset hvor mye virksomheten kan gjøre med trusler gjennom underleverandører. Et av de viktigste tiltakene som kan gjøres for å beskytte seg mot sikkerhetsbrudd gjennom leverandører er å ha en grundig anskaffelsesprosess (Telenor, 2021). Nettopp derfor er det så viktig å påse at underleverandørens sikkerhetssystemer blir grundig undersøkt før de blir godtatt og tatt i bruk. Utover dette kan ikke virksomheten gjøre veldig mye annet enn å godta risikoen ved anskaffelsen.

Selv om oppgaven tar utgangspunkt i casevirksomheten, så er dataene som er samlet inn generaliserbare for å ha gyldighet hos flere virksomheter og skape nytteverdi for utenforstående. Siden GDPR og Schrems II er gyldig i hele EU/EØS, vil utfordringene

knyttet til dette trolig oppstå i mange virksomheter. Det betyr at tiltakene kan være gyldige for flere virksomheter som ikke allerede er tilpasset de nye regelverkene godt nok.

Hensikten med problemstillingen er ikke å gi casevirksomheten et fasitsvar på hvordan de skal gjennomføre anskaffelsesprosessen sin. Det er ment som et verktøy for å belyse dagens utfordringer og komme med forslag som kan hjelpe med en bedre anskaffelsesprosess.

1.3 Oppgavens oppbygging

Bacheloroppgaven følger en klassisk oppgavestruktur og er delt inn i 6 kapitler. Kapittel 1 Innledning, gir innsikt i oppgavens problemstilling, avgrensing, bruksområde og casevirksomheten. Kapittel 2 Teorigrunnlag, beskriver teorigrunnlaget som problemstillingen er knyttet opp mot. Her er alt fra sentrale begreper til relevante temaer beskrevet. Videre er fremgangsmåten som oppgaven bygger på presentert i kapittel 3 Metode. Her vises det hvordan dataene er samlet inn og metodene som blir brukt for å analysere dataene. Kapittel 4 Resultat, inneholder resultatet fra forskningsprosessen. I denne delen er det gitt en beskrivelse av funnene i studiet, samt en analyse av de ulike funnene. Kapittel 5 Diskusjon, knytter resultatet opp mot den relevante teorien som er presentert i kapittel 2. Til slutt vil en oppsummering av hovedfunnene i oppgaven og videre forskning bli presentert i kapittel 6 Konklusjon.

1.4 Oppgavens nytteområde/bruksområde

Denne oppgaven fungerer veiledende for virksomheter i ulike bransjer som utfører anskaffelsesprosesser, og da spesielt digitale anskaffelser. Oppgaven presenterer ulike utfordringer som trolig flere virksomheter opplever ved anskaffelser. Som en videreføring vil det diskuteres diverse tiltak som virksomheten med fordel bør gjennomgå for å etablere en mest mulig sikker anskaffelsesprosess.

1.5 Casebeskrivelse

I denne oppgaven vil vi ta i bruk et fiktivt navn på casevirksomheten for å opprettholde deres anonymitet. Videre i oppgaven vil casevirksomheten bli omtalt som Datakonsulentene AS.

Datakonsulentene AS ble grunnlagt på 1980-tallet og har opparbeidet seg en lang erfaring innen systemutvikling og rådgiving. Virksomheten er i dag et nordisk IT-konsulentselskap som leverer digitale løsninger og tjenester til den offentlige og den private sektoren i Norden. De leder og bistår med digitaliseringsarbeid og bidrar med både rådgivning innen innovasjon og nye teknologiske løsninger, samt realisering nye innovasjonsprosjekter. Mange av prosjektene til Datakonsulentene AS har som formål å gjøre kundene mer effektive i de løsningene de allerede bruker, og bistår med rådgiving ved bruk av IT-løsninger. Virksomheten er en av de fremste ekspertene i markedet når det kommer til skyløsninger og kunstig intelligens i Norden. De omtaler seg selv som skyeksperter, og

tilbyr skyløsninger med banebrytende teknologiske muligheter som gir kundene sine enorme gevinster. De tilbyr dessuten tjenester inne skystrategi, systemutvikling, dataanalyse, brukeropplevelse og sikkerhet.

Virksomheten er representert av nærmere 300 ansatte, der omkring 200 jobber innenfor IT. Omtrent 85% av ansatte har en mastergrad, og resterende ansatte har en bachelorgrad eller en doktorgrad. De aller fleste ansatte kommer rett fra studie, og har gjerne vært innom virksomheten ved et «summer internship». Ansienniteten anses som høy, og det er flere i virksomheten som har 25-års jubileum dette tiåret.

Etter å ha besøkt kontorene til Datakonsulentene AS for å gjennomføre intervjuer fikk vi et godt inntrykk av virksomheten. Noe av det som skiller dem mest ut er den flate strukturen og hvor stor grad av selvstendighet ansatte fikk i arbeidet sitt. Alle kontorplassene var plassert i åpent landskap, og det var kun få ansatte med lederposisjoner som hadde faste plasser. Dette gjorde at det var kort vei opp til administrerende direktør, noe som skapte både åpenhet og et sterkt fellesskap mellom ansatte.

Det er flere grunner til at vi ønsket å skrive bacheloroppgaven sammen med Datakonsulentene AS. For det første ønsket vi å utfordre oss selv og bruke det vi har lært i tidligere emne til å løse reelle problemstillinger i markedet. Det var viktig for oss å skape en oppgave som faktisk gir nytteverdi for de vi samarbeider med og at vi kunne oppnå et faktisk resultat. For det andre ønsket vi oss et bedre innblikk i en bransje som vil være aktuell å jobbe i etter endt studieløp. Det vil dessuten gi oss muligheten til å etablere større faglig nettverk ved å bli kjent med flere i fagmiljøet. Ikke minst så er det en stor fordel å kunne hente ut informasjon fra virksomheten for å både få et teoretisk og et praktisk perspektiv på oppgaven.

Det var flere grunner til at også Datakonsulentene AS ønsket hjelp av oss for å utrede et større arbeid i form av en bacheloroppgave for seg. For det første er det en mulighet til å få inn ny kunnskap ved å gjennomføre prosjekter som ellers ikke ville blitt prioritert, men som likevel kan gi nytte for virksomheten. I tillegg vil vi som studenter, og ikke ansatte, gjerne ha et mer objektivt syn på virksomheten og gjøre det lettere å oppdage problemer og løsninger som virksomheten selv ikke ser. Dette er et arbeid som vil tilføre verdi for begge parter og danne nyskapende ideer og løsninger.

Det var dessuten et mål å skrive en bacheloroppgave som ville ha nytteverdi også for utenforstående. For å oppnå dette var det viktig å bygge opp oppgaven med fokus på et faglig perspektiv med en problemstilling som er relevant i dagens samfunn. Anskaffelsesprosesser er noe enhver virksomhet bedriver, og det vil derfor trolig være andre virksomheter enn Datakonsulentene AS som opplever at prosessen kan være utfordrende. Det har vært viktig å se på hvordan Datakonsulentene AS gjennomfører arbeid i praksis for å komme med praktiske eksempler og drøfte det i lys av relevant teori. På den måten reflekterer oppgaven en aktuell problemstilling som skal gi innsikt og opplyse om tematikken.

Informasjonssikkerhet er et tema som blir stadig viktigere for å sikre helhetlig styring og kontroll for alle virksomheter. Behandling av sensitiv informasjon er viktig for å sikre at virksomheter kan utføre sine daglige oppgaver og levere tjenestene sine, samt å nå mål og ønsket resultat. På bakgrunn av store endringer i regelverk de siste årene er det flere enn

Datakonsulentene AS som har sett seg nødt til å fokusere ytterligere på informasjonssikkerhet for å opprettholde kravene fra myndighetene. Dette er noe Datakonsulentene AS tar på alvor, og ønsker å bidra til et samfunn hvor det blir satt enda mer fokus på informasjonssikkerhet.

2. Teorigrunnlag

I dette kapittelet skal vi presentere relevant teorigrunnlag som er utgangspunktet for å besvare oppgavens problemstilling. Kapittelet tar for seg sentrale begreper og temaer, og gir leseren en grunnleggende forståelse for tematikken.

Under arbeidet med bacheloroppgaven var det nødvendig å danne et økt kunnskapsgrunnlag og det ble gjennomført et strukturert teorisøk. Formålet med teorisøket ee å finne data som kan støtte opp resultatet og som skal brukes til å besvare problemstilling. Teorisøkene har foregått kontinuerlig gjennom hele bacheloroppgaven og står sentralt for grunnlaget av konklusjonen. Vi har gjennomført systematiske søk på akademiske databaser som Oria og Google Scholar, samt brukt flere bøker som er tilgjengelige ved NTNUs biblioteker. Ettersom informasjonssikkerhet er et fagområde i stadig utvikling, har vi valgt å være kritiske til hvor gamle kildene er. Hovedvekten av litteraturen vi har basert oss på er publisert fra de siste 4 årene, altså fra 2018. Dette er for å sikre en tidsriktig og kvalitetssikret oppgave med et best mulig teorigrunnlag.

I dag finnes det begrenset med fagfellevurderte artikler knyttet til GDPR, og spesielt Schrems II. Hovedgrunnen til dette er at det er to nylige regulatoriske krav som det enda ikke er forsket for mye på. GDPR tråde i kraft i 2018 og har rukket å sette preg i samfunnet. Likevel er det begrenset med forskning og vitenskapelige artikler knyttet til GDPR og de langsiktige konsekvensene er enda ikke klare. Det er også fortsatt mye uklart rundt Schrems II, blant annet konsekvensene, og er en av grunnene til at det heller ikke har blitt forsket på i stor grad. Oppgaven har derfor ikke kunne basere seg på like mye på vitenskapelige artikler som er ønsket. Relevante artikler som har blitt benyttet i oppgaven er vurdert kritisk etter beste evne.

Vi har blant annet tatt i bruk fagbøkene «Digital sikkerhet - en innføring» av Håkon Bergsjø, Ronny Windvik og Lasse Overlier, «Akademisk skriving: for bachelor- og masterstudenter» av Busch og «Metode, dataanalyse og innsikt» av Ragnhild Silkoset, Ulf Henning Olsson og Geir Gripsrud. For å sikre kvaliteten har vi også tatt i bruk flere relevante fagbøker for å få en bedre forståelse, samt få en dypere forståelse av temaene. I motsetning til litteraturen på nett har vi ikke vært så kritiske på utgivelsesåret når det gjelder fagbøkene knyttet til metodekapittelet da metoderelaterte fagartikler ikke endres i like stor grad som teknologi og sikkerhet.

2.1 Sentrale begreper

I oppgaven videre vil det benyttes sentrale begreper innenfor temaet informasjonssikkerhet, og dette delkapittelet vil gi en grunnleggende forklaring til disse begrepene.

Anskaffelse – En aktivitet med formål om å dekke et behov for varer, tjenester eller bygg og anleggsarbeider (DFØ, 2021).

Anskaffelsesprosess – En prosessmodell for alle faser som skal gjennomføres i en anskaffelse. For eksempel avklare behov, gjennomgang av sikkerhetskontroller og signering av kontrakt (DFØ, 2021).

Personopplysninger – Opplysninger som er knyttet til en enkeltperson kalles personopplysninger. Eksempler på personopplysninger er navn, epost og fødselsnummer (Datatilsynet a., 2019).

Personvern – Handler om retten til et privatliv og retten til å bestemme over egne personopplysninger (Datatilsynet b., 2019).

Servicedesken - Ved en anskaffelse skal forespørselen gå gjennom Servicedesken, som er det formelle stedet hvor alle henvendelser angående nye anskaffelser skal gå gjennom.

Sikkerhet – En tilstand uten uønskede hendelser. Det kan være bevisste handlinger hvor noen med vilje ønsker å forårsake disse uønskede hendelsene. De kan også være ubevisste handlinger hvor noen gjør feil eller det skjer en ulykke som forårsaker en uønsket hendelse. (Bergsjø, Windvik, & Øverlier, 2020)

Skytjenester – En samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett (Datatilsynet a., 2018).

Tredjeland – Et land som ikke er en del av en bestemt avtale eller traktat. I denne oppgaven vil land omtalt som tredjeland være land utenfor EU/EØS (Nav, u.d.).

Underleverandører – Er en leverandør som utfører en del av det oppdraget som er avtalt mellom hovedleverandøren og kunde (Arbeidstilsynet, u.d.).

2.2 Sentrale temaer

I oppgaven videre vil det diskuteres rundt sentrale temaer som er viktige å forstå for å besvare problemstillingen. Dette delkapittelet vil dermed forklare betydningen til disse temaene og skal gi god nok grunnleggende forståelse for å forstå resultatene og diskusjonen.

2.2.1 Informasjonssikkerhet

Informasjonssikkerhet handler om hvordan organisasjoner innfører rutiner og prosesser for å sikre diverse informasjon. Informasjonssikkerhet bygger på tre viktige grunnsteiner, nemlig konfidensialitet, integritet og tilgjengelighet. Konfidensialitet handler om at informasjonen som er samlet inn ikke blir kjent for uvedkommende. Integritet handler om at informasjonen som blir lagret ikke blir endret utilsiktet eller av uvedkommende. Tilgjengelighet handler om at informasjonen til enhver tid er tilgjengelig for autoriserte ved behov (Datatilsynet b., 2018).

Hvilke sikkerhetstiltak som blir etablert for å sikre at informasjonen opprettholder både konfidensialitet, integritet og tilgjengelighet bør alltid formes etter virksomhetens egne hensikter. Dersom virksomheten skulle etablere for strenge sikkerhetstiltak kan det gå på bekostning av deres evne til å produsere produktene eller tjenestene sine. Da vil virksomheten komme i en situasjon hvor de kanskje er sikker, men ikke lønnsom (Bergsjø, Windvik, & Øverlier, 2020).

Informasjon i IKT-systemer og utenfor IKT-systemer, for eksempel dokumenter som er skrevet ut, faller under begrepet informasjonssikkerhet (Bergsjø, Windvik, & Øverlier, 2020). Finansielle opplysninger, personopplysninger, statshemmeligheter og forretningshemmeligheter er eksempler på informasjon en ønsker å verne. Personopplysninger blir blant annet vernet av lovverket GDPR, og er noe som virksomheten er nødt til å følge for å sikre informasjonssikkerhet.

2.2.2 GDPR

General Data Protection Regulation, GDPR, er EUs personvernforordning som ble innført i Norge i 2018, og gjelder per dags dato for alle land i EU og EØS (SuperOffice, u.d.). Selve roten i GDPR handler om å gi enkeltpersoner større mulighet til å styre personopplysninger som er registrert om dem. I dagens samfunn har menneskerettigheter blitt et stadig viktigere tema, og GDPR skal sikre at virksomheter i EU/EØS som samler inn og behandler data, gjør det i henhold til menneskerettighetene i forhold til personvern. I dag må virksomheter blant annet utdype hvorfor de ønsker å samle inn dataene, samt begrunne bruk av dataene for at det skal ses på som lovlig (Datatilsynet a, u.d.).

EUs personvernforordning ble også gjennomført i Norge, og gjør personvernforordningen til norsk lov som alle norske virksomheter må forholde seg til. Det gjelder for så vidt også alle virksomheter som selger og/eller lagrer personopplysninger om europeiske statsborgere, også virksomheter på andre kontinenter. For Datakonsulentene AS som opererer i business to business markedet (B2B) vil GDPR gjelde for alle enkeltpersoner som interagerer og/eller deler informasjon på vegne av virksomheten. Selv om kundene i et B2B-marked er andre virksomheter, vil det fortsatt være krav om å håndtere forretningene med hensyn på alle enkeltindivider (Regjeringen, 2019).

Formålet med GDPR er å gi brukeren større kontroll over ens personopplysninger, i tillegg at den sikrer at dataen er trygt beskyttet i hele Europa. Enkeltpersoner har dermed rett til å vite hvor dataene lagres, hvem som har tilgang til den og hvor lenge den skal være lagret etter artikkel nr 15. *Den registrertes rett til innsyn*. Brudd på GDPR straffes i dag med bøter på opptil 4% av virksomhetens globale omsetning eller 20 millioner euro, hvor det alternativet som utgjør den høyeste summen er gjeldende (Regjeringen, 2019). Bare i 2021 var det utsendt 412 bøter til virksomheter i Europa på grunn av brudd på GDPR, hvor 28 av dem tilhørte Norge. Dette setter Norge på femteplass over antall utsendte bøter i Europa. Totalt ble virksomhetene i Europa bøtelagt for over ti milliarder norske kroner, noe som er mer enn en femdobling fra året før (Nygård-Hansen, 2022).

I personopplysningsloven artikkel 30 er det lovfestet at det skal føres protokoller over behandlingsaktiviter av personopplysninger som utføres av virksomheten. GDPR protokollen inneholder informasjon om formålet ved databehandlingen, personopplysninger kategorisert etter innhold og hvem som har tilgang på personopplysningene. Status på GDPR protokollen gir et ærlig bilde på hvordan statusen hos virksomheten er (Bedrebedrift, u.d.).

Hovedårsaken til at GDPR ble lovfestet var fordi EU på begynnelsen av 2010-tallet innså at de ikke hadde noe eksisterende lovverk som var tilpasset den digitale hverdagen som oppsto (Sørebø, Fredriksen, Simnica, & Mollestad, 2021). Den økte digitalisering av

virksomheters systemer har ført til økt strøm av personopplysninger, økt risiko for opplysninger på avveie og et behov for sterkere styring av personvern. GDPR ble derfor utformet med et mål om å gi enkeltpersoner kontroll over informasjon som virksomheter og offentlige myndigheter registrerer. Det ble tjenesteleverandørens oppgave å tilrettelegge for at hver enkeltperson får tilstrekkelig informasjon om hvordan personopplysningene blir håndtert (Sørebø, Fredriksen, Simnica, & Mollestad, 2021).

Som en forløper til GDPR ble personverddirektivet vedtatt i 1995 av EU-kommisjonen. Målet var å samle de europeiske landene ved å skape et trygt og sikkert direktiv som skulle ivareta personvernet til befolkningen. Medlemslandene samarbeide for å sikre fysisk trygghet og frihet, for å gi enkeltpersoner muligheten til privatliv. EU-kommisjonen vedtok i 2016 at personverddirektivet var utdatert i forhold til den nye digitale virkeligheten med en enorm økning i registrering, bruk og spredning av personopplysninger. Dermed ble personverddirektivet fra 1995 erstattet med GDPR-forordningen for å håndtere utviklingen (Sørebø, Fredriksen, Simnica, & Mollestad, 2021).

Implementering av GDPR kan oppleves som både tidkrevende og ressurskrevende for virksomheter. Det skyldes at det krever mye administrativt arbeid som planlegging og etablering av systemer for registrering, bruk og spredning av personopplysninger. Videre må virksomheter reforhandle eksisterende databehandleravtaler for å påse at de etterlever kravene i GDPR. Det er blant annet viktig å skape et bevisst forhold til hva virksomheten egentlig trenger og hva som betraktes som relevant data for virksomheten. I tillegg skal dette gjøres i en allerede hektisk hverdag hvor de resterende arbeidsprosessene må fortsette som vanlig. Selv om det er tydelig at GDPR har gode intensjoner, så gjør kompleksiteten av innføringen det til en tidkrevende prosess å planlegge og utføre (Sørebø, Fredriksen, Simnica, & Mollestad, 2021).

GDPR har blant annet ført til økte kostnader ved anskaffelse av digitale systemer, spesielt for mindre virksomheter (Sørebø, Fredriksen, Simnica, & Mollestad, 2021). Det krever både bruk av ansattes arbeidstid, men det kommer også kostnader knyttet til innkjøp, lisenser, brukerstøtte og vedlikeholdsavtaler. For eksempel er det viktig å påse før innkjøp at den digitale løsningen har lagt til rette for riktig bruk av anonymisering og sletting i henhold til kravene i GDPR.

2.2.3 Schrems II

Schrems II er en dom nedfelt av European Data Protection Board (EDPB) i juli 2020. Avtalen er en rettslig avgjørelse som skal hindre overføring av personopplysninger til tredjepartsland, altså land utenfor EU/EØS. Overføring av personopplysninger til tredjeland er et problem på grunn av at personopplysningene forsvinner ut av den beskyttende boblen som GDPR har skapt (PWC, 21).

Dommen er oppkalt etter den østeriske juristen Max Schrems som klagde til det irske datatilsynet angående overføring av personopplysninger mellom Facebook i Irland og USA. Klagen kom som en konsekvens av at han ikke mente at personopplysningene ble ivaretatt i USA. Den første klagen ble sendt inn allerede i 2011, men ble oversett av domstolen. I ettertid skjedde det flere avsløringer angående USAs bruk av personopplysninger, deriblant

den mye omtalte Snowden lekkasjen. Dette fører til en ny klage til det irske datatilsynet, som denne gangen blir tatt mer på alvor. Det irske datatilsynet sender saken videre til høyesterett, som videre sender saken til EU-domstolen. Dette førte til slutt fram til Schrems II dommen som ble vedtatt i 2020 (Fossen, 2021).

Hvis en skal flytte over personopplysninger utenfor EU, og da spesielt USA, så må det gjennomføres en risikovurdering og kartlegge hvilke opplysninger som vurderes (Fossen, 2021). Dette må vurderes opp mot overvåkningslovverkene som finnes i det landet en ønsker å flytte dataene til. Her er et viktig poeng at det skal gjøres en objektiv vurdering for sannsynlighet for overvåkning. Det betyr at dersom en sender data over til USA, så må en regne med at det blir overvåket (Fossen, 2021). Det er med på å vurdere hvilke tiltak en kan gjøre for å sikre at en opprettholder dommen.

USA og EU hadde tidligere en avtale som het Privacy Shield som åpnet for at en kunne overføre personopplysninger til USA, men denne avtalen ble kjent som ugyldig etter Schrems II dommen. EDPBs konklusjon om at Privacy Shield ble kjent ugyldig ettersom de mente at overføringen av data til USA ikke var tilstrekkelig for å sikre europeerens rettigheter knyttet til personvern (Gjessing, 2022).

I USA kan FBI og etterretningstjenester be om å få tilgang til dataene fra datasentrene og selskapene da de har hjemmel til det i amerikansk overvåknings lovgivning. Amerikanske myndigheter kan kreve data utlevert uten at en varsler de det omhandler. Det kan drives mye etterregning i det stille i USA, og dette ble godtatt etter terrorangrepet 11. September 2001 (Rossen & Jørgenrud, 2014). EU og EØS ser på dette som problematisk, Da personvernet i USA ikke blir like godt vernet som i Europa. I motsetning til USA har en rett til å vite hvor dataen om seg selv lagres og bruke.

I dag må en ha særskilt grunnlag for å overføre personopplysninger til tredjeland, i tillegg må behandlingsansvarlig oppfylle tilleggskravene EU-domstolen har satt. Det særkilte grunnlaget baserer seg på dokumentene «Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data og «Recommendations on the European Essential Guarantees for surveillance measures» og omhandler hvilke vurderinger en må sette seg inn I, og hvordan en skal vurdere lancets overvåkningslover. Disse to dokumentene forteller også virksomheten hvordan en skal gå fram i prosessen (Datatilsynet, 2021). I dag gjelder kun Schrems II for virksomheter, og ikke privatpersoner.

Ved for eksempel SaaS-løsninger er det anbefalt at alt av prosessering bør skje i EU. Med en gang leverandøren har et morselskap i USA vil det bli utfordrende. Det skyldes overvåkningslover som krever at etterretningstjenestene kan hente ut informasjon fra datterselskapene i EU gjennom morselskapene USA (Fossen, 2021).

2.2.4 SaaS-løsning

Software as a Service (Saas), programvare som tjeneste, er en programvaremodell som innebærer at sluttbrukeren får tilgang til programvare via en nettleser på internett, i stedet for at programvaren må lastes ned og lagres lokalt på datamaskinen (Datatilsynet a., 2018). Typiske SaaS-løsninger kan være e-post, kalender og Office-verktøy. Virksomheten

tar i bruk en løsning som er koblet til via en nettleser som eies, lagres og administreres eksternt av en leverandør. Spesielt de siste fem årene har denne formen for programvare blitt populær på grunn av et stadig raskere og mer stabilt internett som klarer å håndtere den enorme datamengden som kreves (Turner, 2020). I tillegg tilbyr enkelte SaaS-løsninger et eget «frakoblet modus» som tillater grunnleggende funksjonalitet uten å være tilkoblet internett. Bruken av SaaS-løsninger har dessuten vokst på grunn av fordeler som tilgjengelighet og kompatibilitet. Ofte er alt en trenger å gjøre for å ta i bruk programvaren å registrere seg som abonnement for tjenesten og så får en tilgang via nettleseren.

2.2.5 ISO27001

Det er utfordrende å utvikle en standardiserte former for risikostyring for å håndtere de regulatoriske kravene i GDPR og Schrems II. Dette skyldes blant annet at det som er beskrevet ofte er tvetydig og vanskelig å forstå, selv for sikkerhetseksperter (Beckers, Heisel, Solhaug, & Stølen, 2013). Det gjør det til en tidkrevende prosess å sette seg inn i alle de nødvendige oppgavene for å gjøre dem forståelige å arbeide med. Dermed har Den internasjonale standardiseringsorganisasjonen (ISO) og Den internasjonale elektrotekniske kommisjonen (IEC) danner et system som skal gi en global standardisering innen informasjonssikkerhet. En av disse standardene er ISO 27001.

ISO27001 er i dag en av de mest kjente sikkerhetsstandardene, og flere virksomheter ønsker seg denne sertifiseringen i dag. Det er en global ledelsesstandard som blir brukt over hele verden, og blir i dag omtalt som en internasjonal kravstandard (Standard Norge, 2022). Standarden stiller krav som en virksomhet bør ta stilling til, og som vil hjelpe en virksomhet med å sette opp et ordentlig ledelsessystem for informasjonssikkerhet. Standarden fokuserer på risiko og strategi, identifisere det, og lage en plan for hvilke tiltak en skal gjøre for å redusere ulike risikoer, i tillegg avdekke sårbarheter (DNV, u.d.). Formålet med sertifiseringen er å ivareta virksomhetens informasjonsverdier, i tillegg stiller sertifiseringen krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av ledelsessystem for informasjonssikkerhet (Kiwa, u.d.). En virksomhet som er ISO 27001 sertifisert viser kundene, potensielle kunder og leverandører at en tar sensitiv og konfidensiell informasjon på alvor, i tillegg til at virksomheten tar cybersikkerhet alvorlig (DNV, u.d.).

ISO 27001 sertifisering er gyldig i tre år, gitt at styringssystemet som virksomheten tar i bruk oppfyller alle ISO 27001 kravene. Virksomheten må gjennomføre oppfølgings revisjoner hvert år etter at en er sertifisert (Kiwa, u.d.).

Innføring av ISO 27001 kommer som et resultat av den stadig digitale utviklingen som setter nye krav for hvordan sikkerhet skal håndteres. Å bli ISO-sertifisert er en viktig del av arbeidet med å opprettholde sikkerheten i en virksomhet, likevel krever det en innsats for å få dette inn i deres daglige arbeid (Vejseli & Hedberg, 2016). Ved å innføre ISO 27001 kan ansatte bli mer oppmerksomme på sikkerhet og skapte tryggere måter å utføre arbeid på. Dette er med på å påvirke ansattes arbeid og rutiner og utforme en organisasjonskultur med økt fokus på sikkerhet. (Vejseli & Hedberg, 2016).

Det er flere virksomheter som stiller krav til samarbeidspartnere, leverandører og underleverandører om at de kan dokumentere at de har kontroll på deres interne prosesser. Det finnes flere fordeler ved å være ISO 27001 sertifisert. Kontroll på interne prosesser og på informasjonsflyten reduserer risikoen for at konfidensiell informasjon om kunder og seg selv havner på avveie. En annen fordel ved ISO27001 sertifiseringen er at virksomheten fremstår som mer troverdig overfor kunder, ansatte og samarbeidspartnere når det gjelder informasjonssikkerhet, i tillegg til at en styrker sin posisjon i markedet. En sterk markedsposisjon kan bidra til at en virksomhet vinner flere private og offentlige oppdrag, som regel ender opp i langvarige samarbeid (Vejseli & Hedberg, 2016).

2.2.6 Organisasjonskultur

Begrepet kultur har flere definisjoner, og brukes i ulike sammenhenger med ulike betydninger. En bruker gjerne begrepet i forbindelsene med tanke, kommunikasjons- og atferdsmønstre hos mennesker (Schackt, 2019). Organisasjonskultur kjennetegnes ved normene, verdiene og virkelighetsoppfatningen i virksomheten, og blir utviklet av ledelsen og ansatte over lengre tid. Normer defineres som uskrevne regler og lover, og er gjerne knyttet til ulike situasjoner. En kan se på normer som aksepterte regler innad i en virksomhet, typiske eksempler på normer er hvordan en skal kommunisere med andre eller hva kleskoden i virksomheten er. Verdier er noe en ansatt ønsker å oppnå i virksomheten (Jacobsen & Thorsvik, 2019). Organisasjonskultur er et begrep som har fått mer oppmerksomhet de siste tiårene. Det er flere forskere som i dag mener at organisasjonskultur er en viktig faktor for suksess. For å forstå hvordan virksomheten fungerer er det nødvendig å sette seg inn i og forstå organisasjonskulturen til virksomheten(Fey & Birkinshaw, 2005).

Det er viktig med en god balanse for å oppnå en god organisasjonskultur. I dag er det HR-avdelingen og ledelsen som i størst grad kan påvirke organisasjonskulturen ved selektiv rekruttering. Selektiv rekruttering går ut på at HR og ledelsen setter sammen ansatte med riktig bakgrunn, tankegang og verdisett, samt at de oppfyller kompetansekravene for stillingen de har eller søker på ((Bang, 2020). Tillit og kommunikasjon mellom ledelsen og ansatte er viktig for å oppnå en god organisasjonskultur. Det er viktig at ansatte er informert om bedriftens målsetninger og verdier, slik en vet hva en skal jobbe og strekker seg etter.

Organisasjonskultur skaper sterk følelse av fellesskap, tilhørighet, fremmer samarbeid og koordinering, i tillegg til å motivere ansatte. Organisasjonskulturen påvirker ansattes handlingsmønstre i virksomheten. Kulturen i virksomheten påvirker ikke kun hvordan en skal kommunisere eller hva en skal ha på seg, den påvirker også holdningen og bruken av digitale løsninger i dag.

2.2.6.1 Sikkerhetskultur

Sikkerhetskultur har det siste tiåret fått mer oppmerksomhet, og blir sett på som en del av organisasjonskulturen (Safetec, u.d.). Det finnes flere definisjoner på sikkerhetskultur, men et fellestrekk er at det handler om å beskytte digitale verdier fra ulike former for trusler

rettet mot innebygde sårbarheter (Bergsjø, Windvik, & Øverlier, 2020). Hvordan ansatte i virksomheten velger å handle i ulike sikkerhetsrelaterte situasjoner danner en form for sikkerhetskultur. Ansatte i ulike virksomheter vil gjerne håndtere sikkerhet forskjellig ut ifra hvordan virksomheten har lært dem opp til å takle ulike situasjoner.

Nasjonal sikkerhetsmyndighet definerer en god sikkerhetskultur som et sett med verdier som deles av ansatte i en virksomhet, og som er med på å påvirke deres tanker og forventninger til sikkerhet. For å ha en god sikkerhetskultur, samt ivareta kulturen som virksomheten allerede har, er det viktig at ledelsen motiverer ansatte til å tenke på sikkerhet. Sikkerhetskultur kan bli sett på som et sett med verktøy for å etterleve retningslinjene satt i virksomheten. Det er viktig å arbeide systematisk med sikkerhetskulturen, slik at ansatte forstår sammenhengen mellom de teknologiske og organisatoriske faktorene som påvirker virksomhetens sikkerhet (Nasjonal Sikkerhetsmyndighet, 2020). En god sikkerhetskultur er viktig i virksomheter som behandler sensitive personopplysninger og verdier i store mengder, og som tar i bruk en rekke programmer og tjenester. Ansatte som ikke tar sikkerhetskulturen på alvor kan medføre at virksomheten blir utsatt for store sikkerhetsinnbrudd, ulykker og bøter.

2.2.6.2 Digital kultur

I likhet med sikkerhetskultur er digital kultur et begrep som faller inn under organisasjonskulturen. Digital kultur kjennetegnes ved fire kjerneverdier: åpenhet, hastighet, innvirkning og autonomi (Bouwman, Van Den Hooff, Van De Wijngaert, & Van Dijk, 2005). Åpenhet handler om at ansatte ikke skal sitte på informasjon selv, men at en skal dele informasjon, råd og kunnskap med kollegaer i virksomheten. En skal benytte flere kilder for å tilegne seg ny kunnskap på. I dag lever vi i en verden der teknologien stadig endres og utvikles, det er dermed viktig at virksomheter utvikler seg i takt med teknologien. Prinsippet autonomi handler om at ledelsen skal tillate ansatte å utføre arbeidsoppgaven på måter de selv ønsker, fremfor å be dem følge de strukturelle formene. Innvirkning handler om at ansatte ønsker å påvirke virksomheten ved å ta i bruk flere gode teknologiske tjenester, i tillegg til å tenke nytt. Ved at en ansatte tenker nytt og bidrar med sine ideer vil det bidra til at virksomheten henger med den teknologiske utviklingen. Fokus på hvordan teknologien og mennesket samspiller sammen er viktig, da det kan ha store konsekvenser for organisasjonskulturen (Hartl, 2019). Det kan medføre til at ansatte leverer dårligere kvalitet på arbeidet som utføres, motivasjonen og effektivitet blir dårligere.

I dag utvikles nye tjenester og programmer i rekordfart, noe som medfører at utvalget av tjenester og programmer er enormt. Dette medfører til at ansatte har utallige valgmuligheter når det gjelder hjelpetjenester for å utføre arbeidsoppgavene. En god organisasjonskultur med fokus på sikkerhetskultur er derfor helt sentralt for virksomheter da det kan medføre store negative konsekvenser for virksomheten.

3. Metode

Metodekapittelet beskriver valget av forskningsmetodene som er benyttet i arbeidet med bacheloroppgaven og er ment for å sikre oppgavens validitet og pålitelighet (Gripsrud, Olsson, & Silkoset, 2021). En metode er en planmessig fremgangsmåte og beskriver innsamlingen av dataene, hvilke datatyper som er hentet inn og hvordan dataene har blitt analysert (Tranøy K. E., 2019). Kapittelet vil først presentere utviklingen av problemstillingen, og vil videre gå inn på de metodiske tilnærmingene som har blitt tatt i bruk.

Videre i dette kapittelet er det gitt en beskrivelse av valgene vi har tatt når det gjelder valg av forskningsdesign og vitenskapsteoretisk utgangspunkt. De ulike formene for forskningsdesign vil bli presentert, i tillegg kan en lese om hvorfor vi har valgt de bestemte metodene. Videre i metodekapittelet gis det en beskrivelse av innsamlingsprosessen og det forklares hvordan dataene har blitt analysert. Til slutt avsluttes metodekapittelet med en diskusjon av kvaliteten til forskningsmetodene, og deres styrker og svakheter.

3.1 Utvikling av problemstilling

I november 2021 hadde vi vårt første møte med Datakonsulentene AS, hvor vi møtte Chief Executive Officer, Cheif Information Officier og Head Of Security. Vi presenterte temaet informasjonssikkerhet, som vi så på som et innholdsrikt og dagsaktuelt tema. Vi ble raskt enige om at dette var et interessant for begge parter å lære mer om. Etter det første møte sendte vi inn ulike problemstillinger innenfor tema informasjonssikkerhet som vi syntes var interessante og som vi ønsket å lære mer om. Kartlegging av oppgaven og dens innhold ble utviklet gradvis i tråd med problemstillingen.

I januar startet arbeidet med å snevre inn problemstillingen mot et tema innen informasjonssikkerhet, da problemstillingen fra november var for generell. Vi leste teori, forskning og empiri rundt temaet informasjonssikkerhet innenfor flere underkategorier som personvern, trusselprofilering, sikkerhetskultur og risikoanalyse. Etter hvert ble det klart at sikkerhet ved anskaffelser av IT-systemer var et aktuelt tema som Datakonsulentene AS hadde opplevd noen utfordringer ved. Sammen utarbeidet vi en oppgave, som omhandlet hvordan en virksomhet kan sikre en god prosess ved anskaffelser av IT-løsninger. Det resulterte i problemstillingen som ble presentert i delkapittel 1.1 Problemstilling.

3.2 Valg av vitenskapsteoretisk utgangspunkt

Valg av metode og analyse bygger videre på det vitenskapelige utgangspunktet. To helt sentrale begreper når vi snakker om valg av vitenskapsteoretisk utgangspunkt er hermeneutisk og positivistisk tilnærming. Hermeneutisk tilnærming representer at det ikke kan avdekkes en objektiv verden, med andre ord en fortolkningsbasert tilnærming. I motsetning til hermeneutisk tilnærming går positivistisk tilnærming ut på at en kan avdekke en objektiv verden (Busch, 2021). Vi ønsket subjektive meninger, fordi det ikke finnes et objektivt fasitsvar på problemstillingen i dag. Derfor har vi tatt utgangspunkt i en

hermeneutisk tilnærming for å tilegne oss subjektive meninger til forskningsprosessen. Til slutt skal svarene reflekteres opp imot den relevante teorien i kapittel 2 Teori for å besvare problemstillingen.

Videre blir vitenskapelige argumenter delt inn i induktiv og deduktiv forskning (Wrålsen & Berntsen, 2022). Den induktive konklusjonen tar i bruk data fra den fysiske verden om tidligere hendelser, altså tar den utgangspunkt i casevirksomheten og forskningsarenaen. Dermed kan en si at den induktive modellen tar utgangspunkt i empirien for å komme fram til et endelig svar på en problemstilling. En bruker en induktiv metode for å forsøke å forstå en situasjon. Den induktive konklusjonen baserer sin konklusjon på sannsynlighet, da en ikke har noen forventninger. I motsetning til den induktive modellen tar den deduktive modellen i bruk logikk for å trekke konklusjoner sammen, altså ved bruk av eksisterende teori (Wrålsen & Berntsen, 2022). Som nevnt tidligere er informasjonssikkerhet et tema vi har en del kunnskap om, noe som førte til at vi hadde en del forventninger til empirien intervjuene ville gi oss før selve forskningsprosessen hadde startet. På den andre siden hadde vi ingen hypoteser vi ønsket å teste opp mot resultatet. Dermed vil denne oppgaven ta utgangspunktet i det som kalles en abdukitv modell, som er en blanding av induktiv og deduktiv metode med et preg av den induktive modellen (Busch, 2021).

3.3 Forskningsdesign

3.3.1 Valg av forskningsdesign

En beskrivelse av analyseprosessen en trenger for å løse problemstillingen kalles forskningsdesign. Forskningsdesign handler om hvordan en skal innhente dataene som er aktuelle, og hvordan den skal analyseres. Forskningsdesign blir delt inn i tre hovedtyper, og valget av design avhenger av hvor mye kunnskap en har om området, kjennskapen en har til teoretiske studier og hvilken hensikt som ligger bak for å analysere og utdype sammenhengen. Forskningsdesign deles inn i eksplorativt design, deskriptivt design og kausalt design (Gripsrud, Olsson, & Silkoset, 2021).

Eksplorativt design benytter sekundærdata og litteraturstudier i stor grad. Formålet med eksplorativt design er å forstå, tolke og få en bedre oversikt over det som har blitt analysert og undersøkt. Dybdeintervjuer og fokusgrupper er to sentrale teknikker som brukes for datainnsamling. Når en har en grunnleggende forståelse av temaet og problemstillingen som skal undersøkes, brukes det som kalles deskriptivt design. Denne type forskningsdesign benytter store representative utvalg for datainnsamling, og tar i bruk teknikkene; spørreskjemaer, observasjoner og dagbokmetoden. Når en skal undersøke nye årsaksforklaringer, tar en i brukt kausalt design. Denne type forskningsdesign egner seg best når en skal finne ut hvilke variabler som påvirker hverandre (Gripsrud, Olsson, & Silkoset, 2021).

Denne oppgaven kunne både ha fulgt et eksplorativt og et deskriptivt design, da vi har tilegnet oss grunnleggende kunnskap om informasjonssikkerhet gjennom studiet. I tillegg til at denne oppgaven er preget av tolkning og analyse av dataene vi har skaffet oss gjennom forskningsprosessen. Vi ønsker å gå i dybden på rutinen og prosessen ved anskaffelser av nye IT-løsninger for å få en bedre forståelse, i tillegg til å levere et godt resultat. Dermed vil

det være hensiktsmessig å benytte seg av dybdeintervjuer fremfor spørreundersøkelser, altså vil oppgaven følge et eksplorativt design.

3.3.2 Ekstensivt eller intensivt design

Det som kjennetegner et ekstensivt design er at en samler inn data fra flere respondenter, gjerne ved hjelp av spørreundersøkelser. Intensivt design kjennetegnes ved at en samler inn data fra et fåtall respondenter, og en tar gjerne i bruk dybdeintervjuer og fokusgrupper (Busch, 2021). I delkapittelet 3.1.1 Valg av forskningsdesign ble det nevnt at vi ønsket å gå i dybden på anskaffelsesprosessen for å få bedre forståelse. På bakgrunn av valget om å benytte et eksplorativt design, der vi benytter dybdeintervjuer for innsamling av data har vi valgt å ta i bruk et intensivt design. Et intensivt design vil gi oss et dypere innblikk i hvordan anskaffelsesprosessen er i dag.

3.3.3 Kvantitative og kvalitative data

Innsamling av kvantitative og kvalitative data henger sammen med valget mellom ekstensivt og intensivt design. Kvalitative data egner seg godt når en velger et intensivt design, da det er få respondenter og komplekse sammenhenger (Busch, 2021). Etter en diskusjon med oppgavestiller og veileder, kom vi raskt frem til at vi ønsket å gjennomføre en undersøkelse med intensivt design, da vi ønsket å gå i dybden på temaet.

For å få den innsikten vi ønsker har vi gått for individuelle dybdeintervjuer som er semistrukturerte. Semistrukturerte intervjuer kjennetegnes ved at de er mer eller mindre standardiserte, men at intervjueren har muligheten til å legge til forklaringer, endre ordlyden og komme med reformuleringer av spørsmålet (Gripsrud, Olsson, & Silkoset, 2021). Vi ønsket at respondentene skulle få flere av de samme spørsmålene, i tillegg ønsket vi å ha muligheten til å utforske nye temaer som dukket opp underveis i intervjuene. Hensikten med dybdeintervjuene var å få et bedre innblikk i dagens anskaffelsesprosess og dens utforming, samt få innspill til hvordan vi kan lage en prosessbeskrivelse som skal sikre den fremtidige anskaffelsesprosessen. Ettersom dybdeintervjuer har vært en tidkrevende prosess har vi jobbet sammen med vår oppgavestiller om å finne aktuelle ansatte i virksomheten for å få mest mulig relevant informasjon fra dem som vi kan bruke i analysedelen av oppgaven.

3.3.4 Tidsperspektiv

Det ble gjennomført tverrsnittsundersøkelser som går ut på at en samler inn alle dataene på et tidspunkt (Torvik, 2011). Intervjuene ble gjennomført i en periode som strakk seg over flere sammenhengende dager, og vi kan dermed konkludere med at dette er en tverrsnittsundersøkelse. Bacheloroppgaven skrives på ett semester, og det medførte til at vi ikke hadde muligheten til å analysere revideringer og utviklingen av anskaffelsesprosessen.

En langsgående undersøkelse kunne også blitt gjennomført hvor intervjuene gjennomføres på ulike tidspunkt over en lengre periode for å gi bedre innblikk i mulige endringer i anskaffelsesprosessen (Torvik, 2011).

3.4 Datainnsamling

I denne delen av metodekapittelet vil vi presentere den valgte metoden for datainnsamling, hvilke datakilder vi har tatt i bruk og valg av variabler. Vi vil også se på arbeidet før, under og etter datainnsamlingsprosessen. I delkapittel 3.3.3 Kvantitative og kvalitative data konkluderte vi med at vi ønsket å gå for en kvalitativ metode for å gå i dybden av anskaffelsesprosessen av IT-løsninger. Det finnes flere ulike kvalitative måter å samle inn data som også var aktuelle for oppgaven, for eksempel observasjoner, individuelle intervjuer, gruppeintervjuer og innsamling av dokumentdata (Busch, 2021).

I delkapittelet 3.3.3 Kvantitative og kvalitative data besluttet vi at vi ønsket semistrukturerte intervjuer til datainnsamlingen. Arbeidet med utformingen av intervjuguiden var en omfattende prosess som blant annet baserte seg på dokumentene som vi fikk tilgang til. For å få tilgang til dokumentene måtte vi skrive under på en taushetserklæring som sikret at vi ikke skulle misbruke informasjonen som ble hentet ut fra Datakonsulentene AS. Taushetserklæringen er en avtale som presiserer at informasjonen vi hentet ut skulle holdes hemmelig for å sikre at konfidensiell informasjon ikke ble spredd. På bakgrunn av virksomhetens nåværende dokumenter og konsultasjon med både veileder og oppgavestiller, ble intervjuguiden utformet. Signeringen av taushetserklæringen satte noen begrensninger for oss og vår oppgave, da det blant annet førte til at vi ikke fikk muligheten til å forske i flere virksomheter. Dokumentene vi fikk tilgang til fra Datakonsulentene AS måtte holdes hemmelig, og det førte til at vi ikke kunne sammenligne dem med andre virksomheters dokumenter. Vi følte også på at taushetserklæringen satte noen begrensninger i kapittel 4 Resultat, som blir diskutert i delkapittel 6.2 Refleksjon rundt oppgavens begrensninger.

3.4.1 Datagrunnlag fra casevirksomheten

Tidlig i informasjonsinnhentingsfasen fikk vi tilgang til kvalitetshåndboken som beskrev ulike prosesser, dokumentene knyttet til anskaffelsesprosessen og ISO dokumentene til Datakonsulentene AS. Disse ble delt for at vi skulle få mulighet til å lese gjennom de relevante dokumentene og gi oss et bedre bilde av anskaffelsesprosessen og hvordan rutinene i virksomheten faktisk er. Dokumentene er lagret på en digital plattform hvor alle ansatte har hver sin bruker med ulike rettigheter til de ulike dokumentene. Det var en tydelig oversikt over hvem som hadde skrevet de ulike dokumentene og når de sist var oppdatert.

De digitale dokumentene var sortert etter tema med flere underkategorier. Vi forholdt oss stort sett til dokumentene under temaet «virksomhetens prosesser», i underkategorien «anskaffelse». Inne på dette området kunne vi lese om anskaffelser av ulike varer, tjenester og ekstern kompetanse. Dette gjaldt alt fra grunnleggende informasjon som formål, omfang og ansvar, men også hvordan prosessene ble aktivert, risikovurderingen og

godkjennelsen av leverandører ble gjennomført. Vi fikk også tilgang til allerede godkjente leverandører i de ulike kategoriene, tidligere leverandører og leverandører en ikke lenger ønsker å bruke. Alle leverandører tilknyttet Datakonsulentene AS skal ligge i listen med et tilhørende utfylt skjema som viser hvorfor eller hvorfor ikke leverandøren brukes.

3.4.2 Analyse av datagrunnlaget fra casevirksomheten

Som nevnt tidligere i kapittelet, så skrev vi under en taushetserklæring, som omhandlet at konfidensiell informasjon ikke skulle bli delt med andre. Dokumentene vi fikk tilgang til ble lagret på en digital plattform, hvor vi ikke hadde muligheten til å markere eller kommentere ulike deler av dokumentene. Vi tenkte først å skrive ut de mest relevante dokumentene, for å så deretter markere ulike deler med ulike farger. Dette ble ikke gjort da risikoen for å miste eller etterlate seg et dokument er stor. Vi endte derfor opp med å lagre den viktigste informasjon fra dokumentene i vår egen lukkede mappe på Teams, med de resterende bachelordokumentene våre. NTNU har i dag en databehandleravtale med Office 365, og dette var hovedgrunnen til at vi tok i bruk Teams fremfor andre tekstbehandlingsverktøy. Vi ønsket å ta i bruk et verktøy som skulle sikre våre og virksomhetens personopplysninger, samt opprettholde GDPR lovverket.

Informasjonen vi oppfattet som viktigst og mest relevant ble brukt til å utforme intervjuguiden. Det var viktig å sette seg inn i prosessene deres, slik at en kunne få mest mulig ut av intervjuene som kom senere. Vi ønsket ikke å bruke tid på intervjuene til å hente ut teoretisk informasjon om prosessene som allerede fantes i dokumentene deres og ville heller fokusere på hvordan prosessene ble utført i praksis. Forarbeidet var til stor hjelp for å spisse intervjuene inn på det temaet vi ønsket. Vi opplevde dessuten at intervjuene ble av bedre kvalitet da vi var trygge på temaet og ga uttrykk for å ha god kjennskap til prosessene.

3.4.3 Tillatelse før gjennomføring av intervjuer

Før intervjuene var det helt sentralt at intervjuobjektene skrev under på et samtykkeerklæringsskjema. Samtaletykkeerklæringen har blitt vurdert og godkjent av Norsk Senter for Forskningsdata (NSD). NSD har klare retningslinjer for hvordan dataene skal lagres og oppbevares, opprettholdelse av anonymiteten til virksomheten, i tillegg til hvordan en skal håndtere de innsamlede dataene ved endt prosjekt. Det var viktig for å få avklart hvem som er ansvarlig for å avklare hvorfor intervjuobjektet får spørsmål om å delta og hva det innebærer å delta, samt presentere respondentenes rettigheter og opplyse hva som skjer med dataene etter prosjekts slutt. Samtykkeskjemaet ble utdelt av programansvarlig ved studiet vårt og er en standard mal som ble revidert for å knytte den opp mot vår bacheloroppgave. Vi ønsket dessuten å ta opptak av intervjuene og la inn et avsnitt med informasjon om hvor dataene ble lagret og hvor lenge. Før samtaleskjemaet ble sendt til respondentene ble det først godkjent av vår veileder.

Se vedlegg 2 for Informasjonsskriv fra NSD.

Ved gjennomføring av intervjuer var det sentralt å ivareta integriteten til intervjuobjektene, både under selve intervjuet og i etterkant, samt når resultatene skal presenteres og fortolkes (Fangen, Kvalitativ metode, 2015). Ved å ta i bruk samtykkeskjema ville det sørge for at de etiske prinsippene som er nevnt over ble oppfylt, i tillegg til at konfidensialiteten ble overholdt.

3.4.4 Gjennomføring av individuelle semistrukturerte intervjuer

Formålet med de individuelle semistrukturerte intervjuene var å få et innblikk i hvordan dagens anskaffelsesprosess av IT-løsninger fungerer og ansattes personlige erfaringer knyttet til prosessen. I tillegg ønsket vi å høre om de hadde opplevd mangler eller svakheter ved dagens prosess, og om de hadde forslag til forbedringer ved prosessen.

Intervjuguiden som ble utarbeidet ble sett på som en veiledende mal, og inneholdt spørsmål knyttet til dagens anskaffelsesprosess. Vi var svært opptatte av at intervjuguiden ikke skulle inneholde ja/nei spørsmål, da vi ønsket å gjøre det lettere for respondentene å utdype svarene sine. Det ble dessuten mer naturlig å stille oppfølgingsspørsmål dersom vi ønsket å gå i dybden på et tema respondenten inkluderte i svaret.

Se vedlegg 1 for Intervjuguide.

I forkant av intervjuene mottok intervjuobjektene en e-post med informasjon om intervjuet som inkludertehovedformålet med intervjuet, i tillegg hvilke rettigheter de hadde i forhold til intervjuet. Det ble også sendt ut et samtaletykkeskjema for å få godkjennelse til å gjennomføre intervjuene, samt å ta opp intervjuene med lydopptak. Her ble det blant annet opplyst at lydopptakene og annen informasjon om intervjuobjektene skal slettes innen 01.06.2022. Flesteparten av intervjuene ble gjennomført fysisk på kontorene til Datakonsulentene AS, mens resterende ble gjennomført digitalt. Blant informasjonen som ble sendt ut til respondentene ble ikke intervjuguiden lagt ved. Dette var et bevisst valg da vi ønsket at respondentene ikke skulle forberede seg med mulige svar, men heller få en åpen og mer reflektert samtale.

Totalt ble det gjennomført 10 intervjuer, der de ulike respondentene hadde ulike stillinger i virksomheten. Vi snakket med ansatte i svært ulike stillinger som alle hadde ulike syn på anskaffelsesprosessen. For eksempel vil ansatte som arbeider med økonomi ha mer fokus på det økonomiske aspektet av prosessen, IT-avdelingen har mer fokus på det tekniske og sikkerhetsmessige, mens konsulentene var mer opptatt av å ha gjennomførbare løsninger som ikke tar for mye tid. Alle har et forhold til anskaffelsesprosessen, men hadde på svært ulike perspektiver. Det var nyttig for å gi oss et helhetlig perspektiv fra alle avdelingene i virksomheten. Vi var opptatte av at alle avdelingene skulle få sagt sitt for å gi en følelse av at vi lyttet til alle sidene. Dessuten ga det oss et godt bilde på hva hver avdeling fokuserte på og hva de så på som en utfordring ved dagens prosess. Respondentene fikk de samme spørsmål, men enkelte fikk oppfølgingsspørsmål som var tilpasset deres svar. Intervjuene hadde en varighet på 45- 50 min.

Intervjuet ble startet med en presentasjon av oss og vår oppgave, før vi fortalte mer om problemstillingen og formålet med intervjuet. Videre fikk intervjuobjektet muligheten til å presentere seg og gi oss grunnleggende informasjon om seg selv. Her ble vi bedre kjent

med vedkommende, og vi fikk informasjon om deres rolle i virksomheten og deres erfaring. Etter en intro av intervjuobjektet gikk vi videre til å anvende intervjuguiden til å snakke om anskaffelsesprosessen.

Videre ønsket vi å høre om kriteriene og utfordringene knyttet til anskaffelsesprosessen, og hva de selv mente var en utfordring og ikke hva bedriften så på som en utfordring. Vi var spente på å se om vi fikk ulike svar med tanke på at vi intervjuet ansatte i ulike avdelinger. Som en videreføring fortsatte vi med spørsmål som omhandlet potensielle mangler, forbedringer og endringer. Her fikk intervjuobjektene mulighet til å utdype mer om sine personlige erfaringer, og hvordan vi kunne være med på å utforme en bedre rutine for anskaffelse av IT-løsninger. Videre ønsket vi å høre hva ledelsen gjorde for å motivere ansatte for å tenke på sikkerhet, i tillegg til motivasjonsspørsmålene ønsket vi å høre hva ansatte mente var hovedpoenget med instruksen. Helt til slutt fikk hvert intervjuobjekt et åpent spørsmål der de kunne tilføre noe dersom de ønsket det.

For å beholde intervjuobjektenes anonymitet vil det ikke bli laget en oversikt med bakgrunnsinformasjon om hver enkel respondent. Dette er viktig for å ikke kunne koble noen av svarene til en spesifikk informant. Videre i oppgaven vil alle bli omtalt som informant.

3.4.5 Analyse av intervju

Under gjennomføringen av intervjuene var det ingenting som ble notert, dette var et bevisst valg fra vår side. Vi ønsket å ha fokus på respondenten for å gjøre dem mest mulig trygge og skape en naturlig samtale, samt ha muligheten til å stille gode oppfølgingsspørsmål. Etter at intervjuene var gjennomført ble intervjuene transkribert ved hjelp av opptakene for å få mest mulig utbytte av alt som ble sagt. Det ble tatt opp flere viktige perspektiver under intervjuene og vi ville forsikre oss om at alle sine meninger ble husket på i resultatet. Transkribering viste seg å være en tidkrevende prosess, men fordelen ved å ta opptak var at en hadde muligheten til å høre opptaket i ønsket hastighet flere ganger. I tillegg hadde vi muligheten til å spole frem og tilbake.

Etter transkriberingen var det flere sider med tekst, og for å gjøre det mest mulig oversiktlig valgte vi å sortere informasjon vi mente var viktig og relevant i forhold til den daværende problemstillingen. Vi tok i bruk fargene grønn, gul og rød for å markere viktigheten på svarene til respondentene, og dette gjorde vi hver for oss før vi tok en felles gjennomgang av det vi mente var viktigst og mest relevant. Ettersom det var flere innfallsvinkler fra intervjuene prøvde vi å sortere informasjon basert på avdeling før vi sorterte de i kategoriene anskaffelsesprosessen, utfordringer og forbedringer.

Vi tok i bruk denne analysemetoden da det ga god oversikt over datagrunnlaget som ble samlet inn. For å få mest mulig ut av intervjuene var vi nødt til å filtrere ut relevant informasjon fra dokumentene.

3.4.6 Behandling av data

Dokumentene med informasjon som omhandlet respondentene og virksomheten ble oppbevart i en lukket mappe på Microsoft Teams. Mappen er lukket, noe som begrenser hvem som har tilgang. I vårt tilfelle var det kun vi, vår veileder fra NTNU og hovedinformatør fra Datakonsulentene AS. Microsoft Teams ble tatt i bruk fordi NTNU tilbyr alle studentene sine Office 365, noe som gir tilgang til verktøy for tekstbehandling, skylagring og samhandlingstjenester.

Lydopptakene ble tatt opp via Google Meets, og ble lagret i en mappe som Datakonsulentene AS administrerte. Vi tok i bruk Google Meets framfor Teams for lagring av lydopptakene da Datakonsulentene AS hadde egen databehandleravtale med Google. Virksomheten kunne tenke seg dette fordi de ville at alle samtalene skulle lagres et sted de selv følte seg komfortable med. Det var opprinnelig tenkt å ta lydopptak med en båndtaker, men dette følte de at ikke var et sikkert verktøy da den fort kan mistes eller stjeles. Lydopptakene ble derfor tatt opp gjennom Datakonsulentene AS sine verktøy og ble direkte lagret i en mappe på fillagringstjeneste deres. Denne mappen var det kun vi og vår hovedinformatør som hadde tilgang til.

3.5 Troverdighet og gyldighet av funnene

Kvaliteten i arbeidet skal sikres av den vitenskapelige metoden, og er med på å sikre troverdigheten til oppgavens resultat. Malterud (2003) presenterer fire krav til vitenskapelighet, og disse kravene kan både benyttes for kvantitative og kvalitative metoder. Kravene Malterud presenterer forkortes til logisk og troverdig (Wrålsen & Berntsen, 2022). I tillegg er disse kravene til hjelp for å stille spørsmål om kunnskapens rekkevidde, begrensning og mening (Malterud, 2003). Tor Busch derimot trekker frem tre forhold han mener er sentrale når en skal si noe om oppgavens kvalitet. De tre forholdene er pålitelighet, gyldighet og overførbarhet. Punktene til Malterud og Busch er relativt like, Malterud sine punkt går litt mer i dybden når det gjelder kritisk tenkning.

Det første punktet Busch presenterer er pålitelighet og handler om å måle kvaliteten, og om en kan stole på dataen. Oppgaven vår er basert på data fra dokumentdata vi har fått fra virksomheten og intervjuene. I likhet med Busch sitt krav så har Malterud også et krav som går på validitet, gyldighet og pålitelighet. Ingen kunnskap er allmenngyldige. Dette beskriver hva det er en egentlig har funnet ut. Validitet kan deles inn i intern validitet og ekstern validitet. Intern validitet handler om hva som er sant, mens ekstern validitet handler om overførbarheten av resultatet. For å sikre påliteligheten ble intervjuet basert på datagrunnlaget fra virksomheten. Før hvert eneste intervjuet forsikret vi informantene om at intervjuet ble anonymisert og at de ikke vil bli oppgitt ved navn eller stilling i oppgaven. Det ble i hovedsak gjort for å skape en trygg stemning i rommet, slik at informantene kunne svare mest mulig ærlig.

Malterud har inkludert gyldighet inn i kravet validitet, mens Busch har gyldighet som et eget krav. Gyldighet handler om i hvilken grad dataene som vi har samlet inn og analysert er gyldig for oppgavens problemstilling. En svakhet ved kvalitative metoder er at de kan være upresise i formuleringen av spørsmål. Vi informerte intervjuobjektet om at hvis det var noe

de lurte på, noe som var uklart eller at de ønsket en annen formulering så var det bare å spørre. I likhet så stilte vi spørsmål tilbake der vi var usikre, og der det oppsto misforståelser.

Det neste kravet til Malterud innen vitenskapelighet er systematisk kritisk refleksjon. Systematisk kritisk refleksjon handler om ens resultater er gjenbrukbare. Det er sentralt at kunnskap deles med andre, da det bidrar til kritisk refleksjon, og da gjerne fra andre synsvinkler. En skal ikke sitte på alt av kunnskap selv. Graden av vitenskapelighet kan ikke måles, det handler om selvkritisk håndtering av kunnskap (Hamberg, Johansson et al.1994, Mays og Pope 1995). Det er viktig at forskerne gir leseren innsikt i de betingelsene som kunnskapen er utviklet under, og blir gjerne omtalt som intersubjektivitet (Malterud, Kvalitative forskningsmetoder for medisin og helsefag, 2017).Busch definerer kravet som overførbarhet, og handler om oppgavens resultater kan overføres til andre lignende situasjoner (Busch, 2021). Med tanke på at oppgaven er skrevet med grunnlag i en casevirksomhet er det ikke sikkert alle funnene er like overførbare. Likevel er anskaffelsesprosessen noe enhver virksomhet bedriver, og det vil trolig være en grad av overførbarhet i resultatet.

Det neste kravet Malterud presenterer er relevans. Kravet forteller om hva resultatene og funnene kan brukes til og ikke. I tillegg er det fokus på hvorfor en velger å se på det arbeidet som relevant. Malterud legger også vekt på at det skal være noe nytt eller unikt for kunnskapsutviklingen, originalitet med andre ord. En kan ha oppfylt kravet om systematisk kritisk refleksjon og validitet, er det ikke gitt at det leder frem til vitenskapelig kunnskap.

Helt til slutt presenterer Malterud refleksivitet, som handler om hvordan forskningsprosessen har preget funn og konklusjoner. Skjevhet, fordomsfullhet, subjektivitet og objektivitet er ulike faktorer som kan påvirke oppgavens funn og konklusjoner (Wrålsen & Berntsen, 2022). Det finnes ikke et fasitsvar, og det er dermed viktig at en viser leseren hvorfor det en har kommet frem til er det som er mest aktuelt. I tillegg er det viktig at en viser leseren at en er kritisk til sitt eget verk (Malterud, Kvalitative forskningsmetoder for medisin og helsefag, 2017).

3.5.1 Kritisk refleksjon og svakheter ved metoden

Ved enhver metode er det også svake sider som en må ta hensyn til når en trekker en konklusjon ut ifra resultatet. Det er derfor viktig å være kritisk til sin egen oppgave og være tydelig på de svakhetene som kan forekomme. På den måten blir resultatet mer troverdig (Wrålsen & Berntsen, 2022).

3.5.1.1 Tverrsnittsundersøkelser

I kapittel 3.2.4 Tidsperspektiv ble det presentert at undersøkelsen vår er gjennomført som en tverrsnittsundersøkelse. En svakhet ved tverrsnittsundersøkelser er at en ikke får muligheten til å se på utviklingen slik som en langtidsundersøkelse ville gitt mulighet til. Ved å følge utviklingen av dagens sikkerhetskrav og standarder ville det ha gitt oss et bedre bilde over rutiner og utfordringer knyttet til anskaffelsesprosessen. I dag er Schrems II svært relevant når det gjelder lagring av persondata i tredjeland. Schrems II dommen som

kom i 2020 har fortsatt en del uklare konsekvenser. Om vi derimot hadde hatt en langtidsundersøkelse ville vi fått muligheten til å følge Schrems II dommen og dens utvikling i større grad, og forhåpentligvis fått klarere retningslinjer.

I løpet av 2022 kommer det helt nye krav for ISO27001, noe som fører til at virksomheten må endre deler av anskaffelsesprosessen for å oppfylle disse kravene. Kravene for ISO27001 har siden 2013 vært relativt like, men med dagens teknologiske utvikling og nye lover så er det mye som må endres på. Dersom vi hadde hatt mulighet til å utføre en langtidsundersøkelse ville vi fått enda bedre innsikt i hvordan sikkerhetsavdelingen hos Datakonsulentene AS jobber med å opprettholde sikkerheten og sikre en god anskaffelsesprosess.

3.5.1.2 Intervju

Det finnes en del utfordringer som er knyttet til bruken av intervju som informasjonsgrunnlag. Den første utfordringen kan ses på som en svakhet er at det foreligger en risiko ved at intervjuobjekt tolker spørsmål ulikt. Intervjurunden tok for seg ansatte med forskjellige bakgrunner. Enkelte er godt kjent med fagbegreper innen sikkerhet mens andre ikke er det. Dette kan medføre at ansatte ikke skjønner helt hva en blir spurt om og oppfatter spørsmålet ulikt. Dette kan føre til at ansatte fra ulike avdelinger svarer på noe helt annet enn det som er intensjonen. Sikkerhet er dessuten et tema som er sensitivt for mange og kan medføre at intervjuobjektet kan velge å svare uærlig. Det kan være en risiko for at ansatte velger å fremstille seg selv på en mer positiv måte enn en kanskje er. Ved å benytte semistrukturerte intervjuer har vi prøvd å skape en naturlig samtale hvor respondentene føler seg komfortable til å snakke åpent og fritt. Dersom vi har sett at intervjuobjektene har vært usikre, har vi prøvd å endre på spørsmålet og forklare grundigere hva vi spør etter.

En annen svakhet ved intervju er at det ikke var noen grense på hvor lenge intervjuobjektet kunne svare. Dette fikk vi oppleve på noen av de første intervjuene vi hadde, hvor intervjuobjektet først svarte på spørsmålet, før de snakket seg videre inn på et annet tema. I de neste intervjuene stilte vi ikke fullt så åpne spørsmål, da vi ønsket mer konkrete svar. Dersom noen av svarene var spennende så fulgte vi opp med oppfølgingsspørsmål for å grave oss inn på temaet. Vi opplevde også å måtte bryte inn og styre intervjuet i riktig retning i enkelte situasjoner, noe som gikk lettere etter hvert.

I analyseprosessen la vi merke til at vi gikk litt for bredt ut når det gjelder anskaffelsesprosessen, det var flere av intervjuobjektene som begynte å snakke om anskaffelser som ikke gjaldt IT-løsninger, men heller anskaffelser av kontorrekvisita og renholdsbyråer. Det førte til litt ekstra arbeid, men det førte også til at vi fikk et bedre helhetlig bilde av anskaffelsesprosessen og hvor nøye en fulgte anskaffelsesprosessen slavisk.

Det er også verdt å nevne at vi brukte en uke på å besøke casevirksomheten og gjennomføre intervjurunden. Det kunne vært en fordel brukt lengre tid på besøk hos casevirksomheten for å få et mer helhetlig inntrykk av virksomheten. Da kunne oppgaven basert seg på hva som ble sagt også utenfor intervjuene, noe som kunne gitt dypere innsikt

i virksomheten. Grunnen til at vi var så lite på kontorene var i hovedsak på grunn av Covid-19, men også at kontorene befant seg i en annen by enn vi studerer i.

3.5.1.3 Forsket på en casevirksomhet

Det finnes ikke et fasitsvar på hvordan en anskaffelsesprosess skal utøves. I denne oppgaven har vi kun forsket på én virksomhet, der vi har satt oss inn hvordan deres anskaffelsesprosess er i dag, og hvilke utfordringer de står ovenfor. Resultatet vårt vil være preget av at vi ikke har hatt muligheten til å se på anskaffelsesprosessen utenfor casevirksomheten. Dermed vil oppgaven bære preg av å hovedsakelig basere seg på casevirksomheten, fremfor å få et bredere spekter fra flere virksomheter.

Når det kommer til digitale anskaffelser så er alle virksomheter i EU/EØS pålagt å følge de regulatoriske kravene i GDPR og Schrems II. Med andre ord vil utfordringene knyttet til GDPR og Schrems II trolig også oppstå i andre virksomheter. Med andre ord vil flere av utfordringene som Datakonsulentene AS opplever trolig også være utfordringer som andre virksomheter opplever. Likevel kunne det vært en fordel og undersøkt anskaffelsesprosessen hos flere virksomheter for å sikre et resultat med bedre overførbarhet. På den måten kunne vi sett på hvordan ulike virksomheter håndterer kravene ulikt og fått en bedre idé om hva som fungerer best.

4. Resultat

I dette kapittelet vil vi presentere funnene som ble gjort gjennom studien samt analysene som vi har kommet frem til. Kapittelet vil begynne med å gi en beskrivelse av dagens anskaffelsesprosess ved å vise hvordan prosessen gjennomføres hos Datakonsulentene AS. Videre vil kapittelet ta for seg ulike utfordringer ved anskaffelsesprosessen som har kommet frem gjennom intervjurunden. Dette inkluderer i hovedsak utfordringer knyttet til bruken av SaaS-løsninger, for dårlig intern kompetanse i virksomheten og lang godkjennelsestid for nye anskaffelser.

4.1 Dagens anskaffelsesprosess

Datakonsulentene AS har i dag et omfattende system som skal bidra til å sikre en god anskaffelsesprosess. Prosessen er beskrevet i et skriftlig dokument som alle ansatte i virksomheten skal ha tilgang til. En anskaffelsesprosess skal settes i gang når det oppstår et behov i en organisasjonsenhet, avdeling eller i et prosjekt. Etter at IT og sikkerhetsavdelingen har godkjent eller avvist anskaffelsen, er det viktig å laste opp dokumentasjonen om leverandøren og anskaffelsen på deres digitale plattform.

Formålet med å ha en så omfattende anskaffelsesprosess er å sikre at varer og tjenester blir anskaffet i henhold til fastsatte spesifikasjoner. Denne rutinen skal sikre at varer leveres til riktig tid og pris ved bevisst oppfølging av leverandørene. Her er det viktig å presisere at denne prosessen også omhandler produkter og tjenester som er gratis. Dette er spesielt viktig i forhold til systemer og tjenester som skal behandle personopplysninger hvor det er viktig at kravene til informasjonssikkerhet og personvern ivaretas.

Anskaffelsesprosessen omfatter alle avdelingene i virksomheten, og gjelder alle typer varer og tjenester. Ved endring av leverandør skal den ansvarlige i Datakonsulentene AS gjøre en ny vurdering og ta stilling til det nye leverandørvalget. Det er økonomidirektøren som har det overordnede ansvaret for å påse at denne rutinen følges, og vedlikeholde prosessen.

4.1.1 Kriterier for ulike anskaffelsestyper

For alle anskaffelsene som gjøres i Datakonsulentene AS skal valg av leverandør dokumenteres ut ifra gitte minimumskriterier. Kriteriene avhenger av hvilke typer anskaffelse det dreier seg om. Anskaffelsene deles inn i tre kategorier. Den første kategorien er *ikke kritiske anskaffelser*. Det er anskaffelser som ikke har stor påvirkning på virksomheten og kan for eksempel være kontorrekvisita, bøker og tidsskrifter. Den andre kategorien er *viktig infrastruktur og tjenester,* som er anskaffelser som er nødvendig for at virksomheten skal fungere. Dette kan være innkjøp av software, konsulentinnkjøp til intern bruk og IT-systemer som SaaS-løsninger. Den tredje og siste kategorien er *underleveranser*, det er anskaffelser som er en del av Datakonsulentene AS sine leveranser. Dette kan være software for videresalg til kunde eller konsulentinnkjøp som underleverandør.

Ved valg av en ny leverandør skal de ulike kriteriene dokumenteres og beskrive hvordan leverandøren har blitt evaluert mot kriteriene. De leverandørene som blir godkjente skal legges inn i en liste, blant andre godkjente leverandører. I dokumentet står det at organisasjonen selv skal bestemme og anvende kriterier for evaluering, utvelgelse, overvåking av prestasjon og fornyet evaluering av eksterne leverandører. I tillegg skal det oppbevares dokumentert informasjon for disse aktivitetene og alle nødvendige tiltak som følger av evalueringene.

4.1.2 Risikovurdering

Ved enhver anskaffelse skal det gjennomføres en grundig risikovurdering av informasjonssikkerhet, personvernhensyn, lisensbestemmelser og avtalevilkår ved anskaffelse av ny software, systemer eller tjenester. I denne prosessen skal både jurist, personvernansvarlig og sikkerhetsansvarlig delta i vurderingen.

Ved anskaffelser hvor personopplysninger blir behandlet så er det viktig at informasjonssikkerheten ivaretas. Sikkerhetsansvarlig skal i samråd med de aktuelle avdelingene vurdere om kravene oppfylles eller ikke. En leverandør oppfyller informasjonssikkerhets kriteriene dersom de har ISO 27001 sertifisering. Virksomheter som er sertifisert, oppfyller automatisk kravene og trenger ikke gjennomgå en ny vurdering.

I anskaffelsesprosesser hvor persondata blir brukt er det viktig å ta hensyn til personvern og påse at den opprettholdes. Selskapets personvernansvarlig skal delta i en vurdering sammen med aktuelle avdelinger og definere disse kravene:

- Beskrive prosessen
- Beskrive formål(ene) med behandlingen av personopplysninger
- Beskrive kategorier av personopplysninger som vil bli behandlet
- Beskrive det rettslige grunnlaget for behandlingen, altså «behandlingsgrunnlaget»
- Gjennomføre en første vurdering av behandlingen
- Dersom leverandøren skal behandle personopplysninger må det inngås en databehandleravtale
- Vurdering av informasjonssikkerhet og tilgangskontroll
- Redegjørelse for overføring av data. Dersom persondata skal overføres utenfor EU/EØS må overføringen sikres med særlige garantier
- Redegjøre for sletterutiner i løsningen
- En risikovurdering av behandlingen
- Vurdere behov for endringer i rutiner og retningslinjer som resultat av risikovurdering i henhold til risikovurdering med hensyn til personvern
- Vurdere personvernkonsekvenser. Må også vurdere om det er behov for å gjennomføre en vurdering og dokumentere vurderingen

- Dersom risikoen anses for å være høyere enn kategorien «lav», må mulige avhjelpende tiltak vurderes

Basert på punktene som ble listet opp, skal et utkast til endelig beslutning legges frem til administrerende direktør eller den som blir utpekt som ansvarlig. På den måten kan de ansvarlige ta en avgjørelse på om behandlingen av personopplysninger kan iverksettes. Etter gjennomført risikovurdering av personvern og de potensielle konsekvensene ved bruk av den eksterne aktøren, skal det bestemmes om virksomheten ønsker å benytte seg av leverandøren. Dersom virksomheten godtar risikoen og ønsker å benytte seg av leverandøren, så skal det inngås en databehandleravtale med leverandøren.

Ved anskaffelse av tjenester eller systemer som innebærer behandling av personopplysninger må behandlingsprotokollen oppdateres. Systemeier må registrere eller oppdatere systemet slik at dokumenteringen blir riktig i henhold til personvern for å sikre at behandlingsprotokollen vedlikeholdes med riktig informasjon. Ved endret bruk av tjenestene eller systemene, eller endrede vilkår for disse, må behandlingsprotokollen oppdateres. Systemeier er ansvarlig for å melde inn endringen til Servicedesken for personvern.

Selve anskaffelsesprosessen foregår hovedsakelig i to trinn. Først skal leverandøren godkjennes, og deretter kan innkjøpet foretas. Som nevnt tidligere skal alle godkjente leverandører legges inn i en liste med eksisterende godkjente leverandører med tilhørende evaluering. Ikke godkjente leverandører skal legges inn i en egen liste med begrunnelser, som for eksempel på grunn av manglende sikkerhetskrav eller miljømessige årsaker. Det er også en egen liste for tidligere leverandører som ikke lenger er i bruk, men som kan tas i bruk igjen senere uten å måtte gjennomføre en full evaluering på nytt.

4.1.3 Kvalitetshåndboken

Kvalitetshåndboken til Datakonsulentene AS er et styringssystem som skal kontrollere og effektivisere nøkkelområdene i virksomheten slik at kundene er fornøyde med tjenestene som blir levert og hvordan de blir levert. Det er viktig for virksomheten å levere sine tjenester med riktig kvalitet og ha en høy leveringsdyktighet. Kvalitetshåndboken har flere formål, som å:

- Utføre prosesser på en enhetlig, effektiv og etterprøvbar måte
- Synliggjøre prosessene for enkel gjenfinning, analyse og kontinuerlig forbedring
- Samle styrende dokumentasjon på ett sted slik at den er lett å finne
- Støtte ansattes roller i deres daglige arbeide. Det skal være enkelt å finne støtte til hvordan oppgaver skal utføres ved sjekklister, maler osv.
- Gjøre det enkelt å dele relevante deler av styringssystemet for å dokumentere systemutviklings- og leveransemetodikk
- Gjøre det enkelt å dele relevante deler av styringssystemet når (potensielle) kunder etterspør dokumentasjon av kvalitetssystemet

- Dokumentere at en har et fungerende kvalitetssystem på nivå med ISO9001

Kvalitetshåndboken skal inneholde styrende informasjon om hvordan Datakonsulentene AS sine ansatte skal utføre sine arbeidsoppgaver. Dette inkluderer flere verktøy som skal gjøre det enklere for ansatte å vite hvordan de skal utføre ulike arbeidsoppgaver etter virksomhetens retningslinjer. Det er også verdt å nevne at alle dokumenter skal tilpasses virksomhetens størrelse og type aktiviteter, prosessenes kompleksitet samt deres samspill og personalets kompetanse. En slik oversikt sørger for at virksomhetsstrategien går i samme retning som alle andre instanser.

4.1.4 Testperiode

Ansatte har ofte mulighet til å teste ut digitale programmer og tjenester gratis ved bruk av en prøveperiode for å se om de ønsker å ta det i bruk. I denne fasen får ansatte per dags dato opprette en bruker med jobbmailen uten å informere IT og sikkerhetsavdelingen. Det er i dag ingen retningslinjer for hva som er lov og ikke lov å oppgi av sensitiv informasjon når en tester ulike systemer og programmer. Flere av ansatte var usikre når vi forhørte oss om hvilken mail som var lov å teste med, om det var ens jobb mail eller ens private mail, og hvilken informasjon en kunne teste med. Dette er med på å skape en del problemer for virksomheten.

Det første utfordringen handler om ukjente anskaffelser ansatte gjør. En ansatt kan når som helst kan be om at alt av informasjon om en selv skal slettes og fjernes fra de ulike systemene og programmene som en har brukt. Dette problemet er knyttet opp mot GDPR og innsynsretten, og vil diskuteres i delkapittel 5.4 GDPR og Schrems II.

Den andre utfordringen bygger på mangel på informasjon rundt testperioden. I anskaffelsesdokumentene til Datakonsulentene AS var ikke testperioden definert. Det finnes ingen informasjon om hvor lenge denne fasen varer, om det er en uke, en måned eller et kvartal. Utfordringen ved å ikke ha en definert testperiode, vil medføre at ansatte tolker tidsperioden ulikt. Etter intervjuene med IT og sikkerhetsavdelingen oppfattet vi at utfordringen gjerne oppstår når testperioden strekker seg over en lenger periode, og når ansatte tar det i bruk så mye at det til slutt blir en vane. En ansatt som er fornøyd med et program eller en tjeneste anbefaler det gjerne videre til sine kollegaer, som igjen anbefaler det til andre. Dette medfører at ansatte ikke lenger tenker over at de faktisk tar i bruk nye leverandører som skal meldes inn via servicedesken. IT og sikkerhetsavdelingen kan vurdere om de nye leverandørene følger regelverkene, og om de har ulike sertifiseringer. Konsekvensene av dette vil bli diskutert i kapittel 5.4 GDPR og Schrems II.

4.1.5 Godkjennelse av leverandører

Ved en anskaffelse skal forespørselen gå gjennom Servicedesken, som er det formelle stedet hvor alle henvendelser angående en ny anskaffelse skal gå gjennom. Her skal alle ansatte i Datakonsulentene AS sende inn henvendelser angående nye produkter eller tjenester som er ønsket. Dette er et viktig ledd i anskaffelsesprosessen fordi det opplyser virksomheten om et behov fra ansatte.

I mindre tilfeller blir henvendelsen tatt opp hos lederen for den representative avdelingen som henvendelsen kom fra. Dette er fordi søknaden må godkjennes hos lederen som har ansvar for budsjettet for den representative avdelingen. Eksempler på slike avdelinger kan være sikkerhetsavdelingen, markedsføringsavdelingen eller regnskapsavdelingen. I større tilfeller som gjelder hele virksomheten vil henvendelsen tas opp i ledergruppen som må finne plass i budsjettet sitt.

Dersom henvendelsen skulle bli godkjent og virksomheten godtar de økonomiske kostnadene, så er det neste steget å se på det juridiske. Hvor stor denne jobben er, avhenger av størrelsen på anskaffelsen. Virksomhetens jurister eller innleide jurister vil gå gjennom en avtale for å komme til enighet med den nye leverandøren. Er det snakk om digitale produkter eller tjenester vil også sikkerhetsavdelingen trekkes inn for å opprettholde sikkerheten. Eksempelvis vil det være naturlig å se på hvor dataene blir lagret, for å sikre at en oppfyller de regulatoriske kravene i GDPR og Schrems II. Dersom dette også går som planlagt, vil virksomheten begynne å ta i bruk det nye produktet eller tjenesten. Det er viktig å presisere at dette er et helt generelt overblikk over hvordan anskaffelsesprosessen ser ut i praksis. Ut ifra hva slags anskaffelse det er, vil det komme andre punkter som også må utføres i anskaffelsesprosessen.

4.2 SaaS-løsninger

Etter intervjurunden var det tydelig at en av de største utfordringene med anskaffelser er knyttet til SaaS-løsninger. Spesielt de siste fem årene har virksomheten økt bruken denne formen for programvare. Den teknologiske utvikling medført at internett har blitt raskere og mer stabilt, slik at nettbaserte løsninger klarer å håndtere den enorme datamengden som kreves. Det er flere fordeler med SaaS-løsninger som gjør hverdagen til ansatte hos Datakonsulentene AS enklere og mer fleksibel. Noen av de viktigste grunnene er smarte løsninger og brukervennlige grensesnitt. Likevel er det en del utfordringer som en må ta hensyn til for å sikre at bruken forblir sikker og innenfor lovverket. Det er her de store utfordringene som ble adressert av intervjuobjektene ligger.

4.2.1 Fordeler ved SaaS-løsninger

En av de viktigste fordelene for Datakonsulentene AS er at SaaS-løsninger gir tilgang til avanserte programmer uten å måtte kjøpe, installere, oppdatere eller vedlikeholde maskinvare, mellomvare eller programvare. SaaS-løsninger blir ofte brukt ved mangel på ressurser til å kjøpe, distribuere og styre de nødvendige programvarene selv, eller om en ikke ønsker å prioritere driften av disse verktøyene selv. Selv om Datakonsulentene AS er et mellomstort konsulentfirma så har de ikke økonomi eller ressurser til å lage egen programvare for alt de trenger. Det er dessuten ofte mulighet til å skalere verktøyet etter bruksnivået, noe som sikrer at virksomheter kun betaler for de funksjonene de faktisk trenger og bruker. Dette gjør SaaS-løsninger økonomisk gunstig for Datakonsulentene AS som ville brukt mye ressurser på å lage noe eget, og gir dem heller mulighet til å fokusere på kjerneoppgavene sine.

SaaS-løsninger gjør det enklere for ansatte hos Datakonsulentene AS å arbeide fra ulike lokasjoner, nettopp fordi løsningene er tilgjengelige over internett og en kan få tilgang fra enhver internett-tilkoblet enhet. Virksomheten trenger blant annet ikke å fundere på hvordan applikasjonen skal kjøre på ulike enheter, fordi tjenesteleverandøren allerede har gjort den jobben. Dataene blir dessuten lagret på nett i en sky. Skulle en være uheldig å miste dataene som er lagret lokalt på datamaskinen, så vil SaaS-løsningen ha lagret alle dataene i skyen. Dette gjør at Datakonsulentene AS kan legge ansvaret for bruk, lagring og vedlikehold til tjenesteleverandøren. Likevel er det verdt å nevne at Datakonsulentene AS med fordel bør ha en form for back-up dersom noe skulle skje med tjenesteleverandøren. SaaS-løsninger kan spare Datakonsulentene AS for mye arbeid, gitt at avtalene blir opprettholdt.

4.2.2 Ulemper ved SaaS-løsninger

Dessverre er det også en del utfordringer ved bruk av SaaS-løsninger, noen som helt klart Datakonsulentene AS har fått kjenne på. Noen av utfordringene knyttet til SaaS-løsninger handler om at en er avhengig av internett for å få tilgang på dataene, at dårlig internettforbindelse fører til dårlig ytelse, eller svikt i leverandørens systemer som fører til at en ikke får tilgang til dataene sine. Dette er imidlertid en utfordring som ikke har påvirket dem i for stor grad. Det som virkelig er en utfordring for Datakonsulentene AS handler om sikkerhet og det å forsikre seg om at løsningene en tar i bruk opprettholder de regulatoriske kravene som GDPR og Schrems II.

Etter intervjuene med ansatte i Datakonsulentene AS har det kommet frem at en stor utfordring er å ha kontroll på alle SaaS-løsningene som blir brukt i virksomheten. En sak er SaaS-løsninger som virksomheten har lisens på og betaler faste utgifter i måneden for, men en annen sak er alle de «gratis» SaaS-løsningene hvor det ikke blir betalt en fast månedssum for lisenser. En kan omtale den som «gratis» i hermetegn fordi de som regel blir finansiert på en annen måte enn direkte betaling, som reklameplass eller bruk av data som legges igjen etter bruk. Dette oppleves som en stor utfordring da virksomheten er helt avhengig av at de ansatte melder ifra om bruken av disse systemene, noe som har vist seg å ikke alltid skje.

Spesielt «gratis» SaaS-løsninger har flere utfordringer som gjentatte ganger ble nevnt av intervjuobjektene. En av hovedutfordringene er at det er så utrolig enkelt å ta i bruk en gratis løsning. Det er som oftest bare å skrive inn en mail-adresse og trykke godta på betingelsene, også er en klar til å ta i bruk løsningen. Dette er også en form for anskaffelse, da ansatte i virksomheten velger å ta i bruk nye løsninger. Dessverre er det ofte slik at en ikke leser vilkårsbetingelsene og blar rett forbi uten å gi det en tanke før de trykker «godkjenn». På den måten blir mail-adressen til Datakonsulentene AS registrert hos en tjeneste uten at noen vet hvilke vilkår de har sagt seg enige i. Dette er spesielt utfordrende da enkeltpersoner godtar vilkårene på vegne av hele virksomheten, noe som i verste fall kan resultere i at en bryter lovgivninger og ender opp med bøter fra Datatilsynet.

Et annet velkjent problem ligger ved styring av identiteter og hvem som skal ha tilgang til sensitiv data hos en ekstern part. Ved bruk av et system kan det være greit nok å holde styringen på hvem som har tilgang til hva, men når det går over til å være titalls, om ikke

hundretalls av SaaS-løsninger å holde styr på er det fort at noen glipper. Spesielt ved «gratis» løsninger er det ofte en utfordring at en ikke kan prioritere hvem som skal ha tilgang til ulik data. Dette er som regel ikke et problem da gratis-løsninger som regel ikke skal håndtere sensitiv informasjon. Likevel er det viktig å kunne velge hvem som skal ha tilgang til ulike områder.

Et problem som kanskje er større er å ha kontroll på hvem som har tilgang til tjenester som er i bruk. IT og sikkerhetsavdelingen har egne rutiner for å oppheve tilgang til epost og bedriftsnettverket sentralt. Derimot må tjenestene som er i bruk utenfor IT og sikkerhetsavdelingen stole på at administrator fjerner tilgangen på hver enkelt SaaS-løsning manuelt selv. Dette problemet ble avslørt i et intervju, hvor det viste seg at et kodedelingsprogram som ofte blir benyttet av konsulenter på oppdrag, hadde flere tidligere ansatte registrert med tilgang til alle dataene. Dette er noe som absolutt ikke burde forekomme og kan gjøre virksomheten svært sårbar, spesielt med sensitiv data som egen kode. Når en ansatt forlater virksomheten er det viktig at de mister tilgangen til alle dataene som kun ansatte skal ha tilgang på. Dette blir ganske enkelt løst ved at administratoren fjerner de tidligere ansatte fra organisasjonen. Her er det viktig å ta med seg at selv om løsningen er nokså enkel, så er det å oppdage problemet som var utfordringen.

Det å ha kontroll på alle tjenester hvor vedkommende bør fjernes er vanskelig, spesielt i programmer som virksomheten ikke engang vet at er i bruk. Alle programmer som ansatte registrerer seg i fortsetter å eksistere selv etter at en har sluttet å bruke programmet. En må selv aktivt inn på profilen og slette brukeren, som ofte blir glemt av virksomheten. Dette har vist seg å være en spesielt stor utfordring med gratis tjenester hvor ansatte trenger et enkelt verktøy for å gjennomføre en enkel oppgave, men ikke varsler ifra at de tar i bruk programmet. Selv om det kun er et engangstilfelle så vil fortsatt brukeren eksistere helt frem til noen sletter den. På den måten har Datakonsulentene AS oppdaget at de har registrerte brukere på en tjeneste som de ikke visste eksisterte. En utfordring som ble adressert her var at tjenester som opprinnelig er gratis kan endre forretningsmodell og kreve betaling for tjenestene sine. Selv om det ikke har oppstått noen uheldige situasjoner hvor en tjenesteleverandør begynner å kreve penger fra Datakonsulentene AS, så er det noe de ønsker å fortsette å være oppmerksomme på og unngå at skjer.

Selv om SaaS-løsninger skal gjøre det enklere for brukere å få tilgang på tjenester, så øker kompleksiteten raskt med antall tjenester. Hver SaaS-løsning trenger mail og passord for å registrere en bruker, og passord har vist seg å være en utfordring. De ulike tjenestene har gjerne ulike passordregler og ulike utløpstider, i tillegg til at en helst ikke skal bruke det samme passordet flere steder. Dette kan skape utfordringer ved at ansatte er nødt til å huske, administrere og tilbakestille passordene sine. Det er en bekymring spesielt sikkerhetsavdelingen har, fordi de vet at ansatte fort kan bli lei alle passordene og ender opp med å bruke enkle passord eller bruke samme passord flere steder gjentatte ganger. Datakonsulentene AS har blant annet opplevd at ansatte har skrevet ned passordene sine på en lapp. Dette blir et stadig større problem da ansatte gjerne bruker en god del forskjellige tjenester og må håndtere mange passord i arbeidshverdagen.

Alle disse utfordringene er tett knyttet opp mot de regulatoriske kravene i GDPR og Schrems II. Disse to regulatoriske kravene er spesielt sentrale da de er grunnsteinene i den

omfattende prosessen som må gjennomføres ved anskaffelser. Før disse regelverkene kom var det ikke så strenge krav til hvordan en anskaffelse skulle være. Nå derimot, har det blitt veldig mye strengere og det er en stor jobb å håndtere alle SaaS-løsningene som brukes. Dette vil diskuteres videre i delkapittel 5.2 Håndtering av SaaS-løsninger.

4.3 Kunnskapsmangel

Etter intervjurunden kom det frem at ikke alle ansatte føler seg trygge på at de faktisk kan regelverket rundt anskaffelsesprosessen til tross for at de skal ha fått opplæring ved ansettelse. Dette gjelder både Datakonsulentene AS sine interne regler i virksomheten, og de nasjonale og internasjonale krave som GDPR og Schrems II. Respondentene hadde god kjennskap til GDPR, men færre hadde hørt om det den litt nyere dommen Schrems II.

4.3.1 Intern kommunikasjon

En nyansatt skal ved ansettelse gjennomgå ganske mye nytt og mye informasjon vil trolig falle bort i den store mengden med informasjon. En bør ha en god innføring ved ansettelse og det oppfyller Datakonsulentene AS ved ansettelsesrutingene sine. Det er blant annet vanlig å gjennomføre en intensivuke hvor nyansatte skal få tilstrekkelig informasjon om alt en trenger å vite. Likevel oppleves det at de med fordel bli flinkere på å ta opp igjen kunnskap som blir formidlet ved anskaffelse også senere i arbeidstiden.

Datakonsulentene AS har blant annet en egen fagdag noen få ganger i året hvor de gjennomfører flere korte foredrag med hensikt å gi ansatte faglig kunnskap. Disse fagdagene har hatt svært stort spekter av temaer tidligere, og det er ingen grenser for hva de kan inneholde. Under intervjuene kom det innspill fra et intervjuobjekt om at de sikkert burde brukt dager som dette for å gi en påminnelse og informere om nye endringer som omhandler anskaffelsesprosessen. Enten om det gjelder virksomhetens interne prosesser og hvorfor de er så viktige å følge, eller kanskje lære mer om de store regulatoriske kravene som påvirker prosessene som GDPR og Schrems II. Som Datakonsulentene AS har merket tidligere, så kan en liten påminnelse kan gi store resultater i ansattes bevissthet og dermed deres handlinger.

Tidligere har Datakonsulentene AS gjennomført større seminarer om viktige temaer som håndtering av bestikkelse eller trakassering på arbeidsplassen. Virksomheten har gjennomført slike seminarer da kunnskapsmangel ofte er en kilde til at ansatte gjør feil, og tilføring av kunnskap vil kunne avverge uheldige situasjoner hvor en ansatt gjør feil uten å selv være klar over det. Flere av intervjuobjektene nevner dette som en mulighet for å belyse viktige temaer som anskaffelsesprosessen. Likevel er det ressurskrevende å skulle arrangere store seminarer for alle viktige temaer som ansatte bør vite mer om. Derfor har Datakonsulentene AS allerede begynt å utvikle ideen om bruk av e-læringssystemer. De er i en prosess nå hvor de ser på mulighetene for å skaffe seg et slikt system som kan gjøre det enklere å ha opplæring av ansatte innenfor flere viktige fagfelt for virksomheten. Dette vil bli et verktøy hvor Datakonsulentene AS enkelt kan spre informasjon blant sine ansatte og gi dem en oppfriskning innenfor de viktigste temaene. Ved å bruke tid på et e-læringskurs

vil det kunne gi ansatte et større forhold til anskaffelser og forhåpentligvis gjøre dem tryggere på prosessene.

Et annet kommunikasjonsverktøy som blir hyppig brukt for å formidle kunnskap er meldingsappen «Slack». Der finnes det ulike kanaler som ansatte kan være en del av, og følge med på det de selv ønsker. På de ulike kanalene kan ansatte diskutere ulike prosjekter eller arbeidsoppgaver, men en kan også kontakte enkeltpersoner for mer private samtaler. En av kanalene er obligatoriske for alle ansatte å være en del av da viktig informasjon som absolutt alle ansatte må få med seg det som blir delt. Det ble foreslått i intervjurunden å bruke en slik form for kanal for å dele mer informasjon og gjøre ansatte mer oppmerksomme. Flere var positive til forslaget og tror at en liten grad av bevisstgjøring kan gjøre stor forskjell. Likevel ble det presisert av informantene at det er viktig å finne en riktig balansegang for hvor mye informasjon som sendes ut til ansatte. Slik som det fungerer i dag, så sendes det ikke ut informasjon altfor ofte. Det resulterer i at ansatte faktisk setter seg inn i det som blir sendt. Hvis mengden informasjon øker vil det fort kunne ødelegge den gode kulturen ved at flere ansatte ikke vil ta seg tid til å lese alt av viktig informasjon som kommer.

Det ble presentert at Datakonsulentene AS har eget nyhetsbrev som blir sendt ut til ansatte hver uke. Her står det diverse informasjon som virksomheten tror kan være interessant for flere ansatte å lese om, men det er ikke obligatorisk. Dette er også en god måte å dele viktig informasjon uten å overbelaste nyhetsvarslingene på Slack. Virksomheten opplever at flere ansatte tar seg tid til å se over nyhetsbrevet. Derfor kan også dette være et verktøy for å spre informasjon om anskaffelsesprosessen for å gjøre ansatte mere bevisste rundt det hele. Som vi skal gå nærmere inn på senere, vil også endringer i ulike regulatoriske krav som GDPR eller endringer i ISO27001 standarden være informasjon som kan være verdt å dele. Men igjen er det viktig å ikke overdrive informasjonen som sendes ut slik at det blir oppfattet som spennende og interessant, i stedet for overveldende og uinteressant.

4.3.2 Kvalitetshåndboken

Datakonsulentene AS har en egen kvalitetshåndbok som skal bidra med å sikre god kvalitet på forskjellig type arbeid, blant annet anskaffelsesprosessen. En stor utfordring med kvalitetshåndboken er at den begynner å bli så omfattende, at det er vanskelig å forholde seg til alt av informasjon som er lagret på den digitale plattformen deres. Selv om den blir hyppig brukt på enkelte områder, så oppleves det at ansatte er mindre kjent med å bruke den med hensyn til anskaffelsesprosessen. Intervjuobjektene forteller at det er mye tekst og det er ikke noe en går inn for å lese «for moro skyld». De gangene en tar i bruk kvalitetshåndboken er det som regel fordi en vet akkurat hvor en skal og vet akkurat hvilken informasjon en leter etter. Utover dette oppleves kvalitetshåndboken som noe uoversiktlig da fåtall har oversikt over alt som ligger ute og hvordan en kan bruke denne informasjonen.

Som nevnt i delkapittel 4.1.1 Kriterier for ulike anskaffelsestyper, skal det være relativt lett for ansatte å finne informasjon om alle godkjente og ikke godkjente leverandører, da alt står oppført på egne sider i kvalitetshåndboken. Likevel røper flere av intervjuobjektene at de ikke har vært inne på siden og heller ikke tatt den i bruk. Når ansatte trenger et

program, vet de ikke alltid hva de er på utkikk etter, og da blir ofte Google brukt som hjelpemiddel for å finne det en trenger. Der er det enkelt og ved hjelp av få tasteklikk kommer det uendelig mange forslag på søket. En så bra søkemotor har ikke kvalitetshåndboken. For å ta i bruk søkemotoren inne i kvalitetshåndboken er en avhengig av at ansatte vet hva de er på utkikk etter, noe de som oftest ikke er. Selv ansatte i IT- og sikkerhetsavdelingen omtaler søkemotoren som vanskelig og at det krever at du vet det nøyaktige søkeordet som trengs.

En spesiell utfordring som kan oppstå, som også har oppstått tidligere, er at ansatte tar i bruk en tjeneste de finner på internett, samtidig som Datakonsulentene AS har en tilsvarende betalende tjeneste som er godkjent og egentlig er ment å bruke. Dette er upraktisk da Datakonsulentene AS kanskje allerede har tatt seg bryet med å godkjenne en leverandør og inngått avtale med dem, og så velger ansatte å ta i bruk andre løsninger hvor dette kanskje ikke er tilfellet. Da vil ansatte fort ende opp med en løsning som ikke er dokumentert, og gjerne et dårligere tilbud enn de kunne fått fra den allerede godkjente leverandøren. Dette er lite kostnadseffektivt og bør naturlig helst unngås. Det er dessuten et problem da Datakonsulentene AS ønsker å ha tilhørende dokumentasjon for alle programmer og tjenester som er i bruk innad i virksomheten. Dette er nemlig et av kravene i kvalitetshåndboken som skal sikre at virksomheten blant annet opprettholder GDPR og Schrems II.

4.4 Tidsbruk ved godkjenning av nye programmer og tjenester

Selve anskaffelsesprosessen blir omtalt som en utfordrende prosess av flere respondenter, mye på grunn av den lange ventetiden. Ettersom hvor stor anskaffelsen er, så kan det ta opptil et halvt år fra det sendes inn som et ønske til Servicedesken til det blir godkjent og offisielt kan tas i bruk i virksomheten. Dette er i enkelte tilfeller alt for lang tid og kan føre til at ansatte velger å ta i bruk verktøy som ikke er godkjente. Det er flere grunner til at denne prosessen ofte blir strukket utover en lengre tidsperiode, og konsekvensene kan i verste fall være brutale for Datakonsulentene AS.

Det er en utfordring at ingen avdelinger ønsker å påta seg kostnadene for anskaffelsen. Alle avdelinger har hvert sitt interne budsjett som skal dekke de nødvendige kostnadene som avdelingen har behov for. En anskaffelse vil fylle opp en del av en avdelings budsjett, og naturlig nok er det ingen som ønsker et mindre budsjett enn de allerede har. Derfor oppstår det en evig sirkel hvor ulike avdelinger mener at en annen avdeling må påta seg kostnadene av ulike grunner. På denne måten stopper hele prosessen opp og en ender opp med å ikke komme seg videre i prosessen. Flere av respondentene nevner dette som en vesentlig årsak til at prosessen strekkes ut over lengre tid.

Dersom avdelingene til slutt blir enige om hvem som skal påta seg kostnadene og budsjettet blir godkjent, så oppstår det en ny utfordring i forhold til hvem som skal være ansvarlig for det nye systemet. Den som er ansvarlig vil få nye arbeidsoppgaver som omhandler bruken og behandling av systemet. En type betalingsmodell som ofte blir brukt på digitale løsninger er betalende lisenser etter antall brukere, altså at en betaler jevnlig for antallet brukere av systemet. Spørsmålet som ofte oppstår da er hvem det er som skal få rettighetene til å bruke systemet og hvem det er som skal disponere lisensene blant de

ansatte i bedriften. Det er vanskelig å bestemme hvilke ansatte som har mer bruk for et system enn andre, og det er ingen gøy oppgave å gi avslag til kollegaer som ønsker seg en lisens. En respondent omtaler oppgaven som utfordrende da det er vanskelig å prioritere kollegaer og venner opp mot hverandre, spesielt når det er flere som har gode grunner.

En annen årsak til at godkjennelsesperioden strekker seg over et lenger tidsrom er fordi underleverandørene ikke oppgir tilstrekkelig informasjon slik at Datakonsulentene AS kan ta en beslutning angående anskaffelsen. Det skyldes ofte at underleverandørene av ulike årsaker ikke ønsker å dele for mye informasjon om prosessene sine. Dette fører til at de som er ansvarlige for å gjennomgå og godkjenne avtalen må gjennomgå lange samtaler med underleverandøren for å hente ut tilstrekkelig informasjon for å kunne ta en avgjørelse om anskaffelsen. Denne informasjonen trenger Datakonsulentene AS for å dokumentere selve anskaffelsen og påse at underleverandøren oppfyller gitte lovpålagte regelverk som GDPR. For eksempel må de forsikre seg om at underleverandøren lagrer personopplysninger i henhold til loven. En informant som arbeider mye med å godkjenne underleverandører sier at det sjeldent er underleverandører som bryter lovverket og at de som regel ønsker å hemmeligholde informasjon for sin egen sikkerhet skyld. Uansett går dette i strid med kravene Datakonsulentene AS stiller til sine underleverandører, og de kan ikke godkjenne en leverandør før de får tilstrekkelig informasjon til dokumenteringsprosessen sin.

5. Diskusjon

I denne delen av oppgaven skal vi redegjøre for de ulike funnene som er gjort og se på hva de betyr i sammenheng med etablert teori og praksis. Kapittelet vil diskutere hvordan funnene påvirker virksomheten, og vil først ta for seg utfordringen med ulike ansattes oppfatninger av en anskaffelse og hvordan det kan by på juridiske utfordringer for Datakonsulentene AS. Videre vil kapittelet ta for seg utfordringene knyttet spesifikt opp mot bruken av nettbaserte skyløsninger og hvordan virksomheten bør forholde seg til disse. I tillegg til å diskutere viktigheten av riktig opplæring og hvordan dette kan gjøre ansatte trygge på valgene sine. Til slutt skal kapittelet ta for seg utfordringene som oppstår rundt GDPR og Schrems II ved dagens anskaffelsesprosess.

5.1 Dagens status

Dagens anskaffelsesprosess er formet etter ISO27001 standarden som skal være med å sikre at virksomheten oppfyller de lovpålagte kravene fra GDPR og de rettslige avgjørelsene basert på Schrems II. Det er viktig å presisere at GDPR bare stiller overordnende krav til behandling av personopplysninger for å ivareta personvernet, mens ISO 27001 er en veiledning til hvordan virksomheter kan sette opp funksjoner og prosesser for å etterleve GDPR-kravene (Standard Norge, 2022). ISO 27001 standarden skal altså hjelpe Datakonsulentene AS med å dokumentere overholdelse av lover om databeskyttelse som for eksempel GDPR. Selv om standarden er utrolig nyttig i arbeidet med å overholde lovverket, har det også medført omfattende arbeid med anskaffelsesprosessen.

5.1.1 Hva er en anskaffelse?

Etter intervjurunden fikk vi et inntrykk av at ansatte definerer en anskaffelse ulikt, noen tenker på en anskaffelse ved at en tar i bruk et helt nytt program mens andre definerer en anskaffelse som noe en skaffer seg. Det kan være alt fra tilleggspakker i Google som kun påvirker en selv til store systemer som påvirker flere avdelinger. Etter intervjuene sitter vi igjen med at flere ansatte er usikre på om det finnes retningslinjer for hvordan en skal ta i bruk tjenester som er gratis på nett. Om en for eksempel skal ta i bruk jobbmailen eller om en skal ta i bruk sin private mail, og hvilken informasjon en skal og ikke skal dele. I tillegg er det flere av ansatte som er usikre på om de trenger å informere IT og sikkerhetsavdelingen når de ønsker å teste et nytt produkt, og når en ønsker å anskaffe noe som kun påvirker en selv. I dokumentene til Datakonsulentene AS er ikke en anskaffelse definert, det en ansatte kan finne om en anskaffelse er at anskaffelsesprosessen også gjelder for produkter og tjenester som er gratis. Så det store spørsmålet ansatte og vi kan stille oss er;

«Hva faller under en anskaffelse?»

For det første, finnes ikke informasjon om hva som kan ses på som en anskaffelse og hva en er pliktig til å melde inn til IT og sikkerhetsavdeling per dags dato. Derfor vil veksten av anskaffelser ansatte gjør som IT og sikkerhetsavdeling ikke har kontroll over å vokse.

Ansatte vil fortsette i samme takt som i dag ved å ta i bruk nye tjenester, tilleggspakker og programmer som hjelper dem med å utføre arbeidsoppgavene. Dette vil føre til at IT og sikkerhetsavdelingen ikke har kontroll på hvilke programmer som brukes, hvem som bruker de, hva slags informasjon som blir lagret og hvor den blir lagret. Det største problemet knyttet til dette omhandler Schrems II og norsk lovgiving. Ved at Datakonsulentene AS ikke har kontroll på om personopplysninger blir sendt ut av Europa kan det by på store konsekvenser, og risikoen for å bli bøtelagt er betydelig større.

Et steg i riktig retning er å sørge for å skape en god organisasjonskultur som setter fokus på sikkerhet, i tillegg til å skape en god sikkerhetskultur. Autonomi er et av prinsippene som kjennetegner digital kultur og handler om at ansatte skal få lov til å utføre arbeidsoppgaven sin på måter de er komfortable med fremfor å følge strukturelle former og regler. Dagens situasjon tillater at ansatte finner nye programmer og tjenester de ønsker å teste for å se om de ønsker å ta de i bruk. Når en ønsker å ta i bruk et nytt system må en som nevnt tidligere melde inn hvilket program eller tjeneste en ønsker å ta bruk, slik at IT og sikkerhetsavdelingen kan ta en titt på leverandørene, lagring og behandlingen av dataene. Den friheten ansatte får når de selv får muligheten til å finne ulike hjelpeverktøy som bidrar til å løse arbeidsoppgavene, er med på å styrke organisasjonskulturen i virksomheten. Ansattes valgfrie handlingsrom er med på å styrke ansattes motivasjon, som igjen bidrar til effektivisering av oppgaver og økt verdiskapning. Det største problemet i dag er at ansatte ikke melder inn programmene og tjenestene de bruker til IT og serviceavdelingen. Prosessen fra en sender inn en forespørsel til en mottar et svar om hvorvidt en kan eller ikke kan ta det i bruk tar opptil et halvt år i dag. Det er flere av ansatte som synes dette er frustrerende, og i flere situasjoner tar en bare i bruk mindre programmer og tjenester uten å tenke seg om at en er pliktig til å melde det inn til IT og sikkerhetsavdelingen. Noen av ansatte uttrykket misnøye med hele anskaffelsesprosessen. De mente at den bare satte stopper for arbeidsoppgavene.

I intervjuene med ansatte fra IT og sikkerhetsavdelingen har vi fått vite at de ønsker at alle typer program og tjeneste som er i bruk av en ansatt skal sendes inn via servicedesken. Dette handler rett og slett om at IT og sikkerhetsavdelingen ønsker å ha kontroll på alle programmer som blir tatt i bruk. Kontroll over programmer og tjenester vil medføre at IT og sikkerhetsavdelingen vil kunne jobbe systematisk å avdekke hvilke risikoer en står ovenfor når en tar i bruk det programmet, og hvordan virksomheten skal beskytte seg på en best mulig måte. I tillegg ønsker avdelingen å ha oversikt i tilfelle leverandører eller underleverandører av de som leverer og/eller leverer den tjenesten, lisensen eller programmet blir utsatt for et angrep. Ved at IT og sikkerhetsavdelingen ikke har kontroll i dag, kan det medføre at det er noen av leverandørene eller underleverandørene til programmer som enkelte ansatte bruker som svekker virksomhetens sikkerhet/motstandsdyktighet mot angrep.

Det finnes i dag ikke et fasitsvar på hvordan ting i forbindelse med anskaffelsesprosessen skal gjøres, men heller anbefalinger på hvordan en virksomhet bør gjennomføre en anskaffelsesprosess. Definisjonen av en anskaffelse fra nett i dag er veldig vid da den inkluderer både varer, bygg, anleggsarbeid og tjenester (DFØ, 2021). Den sier heller ingenting om gratis tjenester på nett. I Datakonsulentene AS vil det første være å definere hva som omfatter en anskaffelse

Er en anskaffelse en tilleggspakke i VScode eller er en anskaffelse det å ta i bruk et nytt program som omfatter flere?

I tillegg til opplæring vil det være helt sentralt å få på plass en klar definisjon av en anskaffelse, en oppdatering av anskaffelsesdokumentet, samt opplyse ansatte. Datakonsulentene AS burde prioritere å utforme noen retningslinjer på hva som er lov og ikke, samt unntakstilfeller. Et oppslagsverk vil gi ansatte større trygghet for hva de kan gjøre, som igjen vil gjøre dem tryggere på de valgene de tar. Ansatte bør også opplyses om lovverket og konsekvensene ved lagring av personopplysninger utenfor Europa. Bevissthet hos ansatte vil medføre at flere vil være mer konsekvente ved å laste ned og ta i bruk programmer og tilleggspakker. Bevisstgjøringen burde gi kunnskap om hvorfor en må ta anskaffelser seriøst, samt kunnskap om konsekvensene og hva som kan skje med opplysningen som lagres. Dette vil medføre at flere melder inn til IT og sikkerhetsavdelingen om hvilke programmer og tjenester de ønsker å ta i bruk.

5.1.2 Håndtering av testperioden

I likhet med anskaffelsesprosessen bør testperioden defineres i anskaffelsesdokumentene, samt bør Datakonsulentene AS opprette retningslinjer på hvordan en skal teste tjenester og programmer, og loggføre testperioden. Bedre rutiner rundt testperioden vil redusere risikoen rundt sikkerhetsbrudd, ulykker og bøter. I delkapittel 4.1.2 Testperiode presenterte vi at ansatte har muligheten til å teste ulike programmer og tjenester, og at en i dag ikke må opplyse IT og sikkerhetsavdelingen om hvilke programmer og tjenester en tester. Dette medfører null kontroll over hva som blir lagret og hvor informasjon blir lagret.

Det vil være hensiktsmessig for Datakonsulentene AS å definere retningslinjer for hvordan testperioden skal se ut og hva en skal melde inn. Retningslinjer blir i dag definert som anbefalinger en bør følge for å utføre en bestemt handling. Ved å definere retningslinjene til testperioden vil ansatte i Datakonsulentene AS oppfatte det som noe en bør følge. Ved at flere ansatte følger retningslinjene vil det bli en del av kulturen og ansatte utfører rutinene uten å egentlig tenke over det. Nyansatte i virksomheten vil dessuten få et inntrykk av at en skal følge retningslinjene for å tilpasse seg kulturen i virksomheten. Når flere av de ansatte er innforstått med hvorfor en må følge retningslinjene og hva konsekvensene er, vil en ta med seg de erfaringene videre og dele de med sine kollegaer. Åpenhet blant ansatte bidrar til et bedre samarbeid. Forskningen Fey og Birkinshaw har gjennomført er basert på selskaper i Storbritannia og Sverige. De konkluderer med at åpenhet medfører at en tar i bruk nye metoder og fremmer nye forslag, bidrar til en høyere presentasjon når det gjelder den teknologiske utviklingen. Ved at ansatte deler kunnskap og ved at terskelen for å spørre sine kollegaer er lav, vil også effektiviteten økte. En ansatt vil i tillegg tilegne seg mer kunnskap, og en vil være åpen for nye metoder å arbeide på, samt komme med nye innovative ideer. Dette vil styrke sikkerhetskulturen, fordi flere vil få en bedre forståelse og kunnskap om informasjonssikkerhet, men også styrke organisasjonskulturen ved at det er et fellesskap med et godt miljø (Fey & Birkinshaw, 2005).

Det vil være nødvendig å definere lengden på en testperiode, da det i dag er veldig usikkert blant ansatte på hvor lenge denne perioden er. Videre vil det være sentralt å opplyse

ansatte hva en skal gjøre etter testperioden er ferdig. Dersom en ansatt ikke ser seg fornøyd med programmer eller tjenesten og dens funksjoner vil det være nødvendig å opplyse IT og sikkerhetsavdelingen at en har testet dette og at en ønsker å slette alt av informasjon som er lagret der. Hvis det viser seg at en ansatt er fornøyd vil det være viktig at en sender inn en forespørsel via servicedesken, slik at IT og sikkerhetsavdelingen kan ta en grundigere titt på programmet eller tjenesten, og se hvor dataene blir lagret, samt ta en grundig sjekk av underleverandører. Her er det også viktig at den ansatte forteller avdelingslederen om at en ser behovet for den funksjonaliteten, samt IT og sikkerhetsavdelingen hvorfor en ønsker å ta det i bruk, og hva en har lagret i testperioden. Dette vil medføre at IT og sikkerhetsavdelingen får bedre kontroll over programmer og tjenester ansatte tester uten at det oppfattes som overvåkning.

Etter intervjurunden ser vi at rutinen rundt testperioden klart kan forbedres. Dagens håndtering av testperioden medfører utfordringer knyttet til GDPR og Schrems II vil diskuteres videre i delkapittel 5.4 GDPR og Schrems II.

5.1.3 Håndtering av tidsbruk

Det er ingen tvil om at GDPR har ført til mer arbeid for anskaffelsesprosessen. Ved en anskaffelse er det Datakonsulentene AS sitt ansvar å påse at underleverandøren oppfyller kravene i henhold til GDPR. I tilfeller hvor Datakonsulentene AS inngår avtaler med underleverandører innenfor EU/EØS må de i tillegg undersøke om denne leverandøren bruker underleverandører utenfor EU/EØS (PWC, 2020). Datakonsulentene AS må dessuten dokumentere bruken av slike underleverandører og påse at de oppfyller minstekravene for behandling av personopplysninger. Dette er tidkrevende arbeid som gjør at anskaffelser både tar lengre tid og er mer kompliserte enn tidligere.

Som nevnt er det en utfordring at underleverandører ikke gir nok informasjon til å kunne godkjenne dem med en gang. Dessverre er hvor behjelpelige potensielle underleverandører er, er svært vanskelig å gjøre noe med da det ligger utenfor Datakonsulentene AS sin kontroll. Dette gjør det vanskelig å finne tidsbesparende tiltak som kan bedre prosessen. Så lenge Datakonsulentene AS har kontroll på hva de trenger å vite og har gode rutiner for å hente ut slik informasjon, så ligger det meste på leverandøren og hvor enkelt det er å få tilstrekkelig informasjon fra dem. Det er tross alt ikke lett for underleverandørene å finne en balanse hvor de deler nok informasjon om sine interne prosesser uten at det går utover sin egen sikkerhet.

At godkjenningsprosessen i dag kan ta flere måneder er alt for lang tid og er noe som helt klart bør reduseres. Dersom IT og sikkerhetsavdelingen skulle klare å få ned tiden fra flere måneder til bare noen uker, eller kanskje til og med noen dager, så vil det utgjøre en stor forskjell. Øvrige ansatte vil kunne få økt motivasjon til å faktisk sende inn ønsker til servicedesken nettopp fordi de vet at de får raskt svar. Raske godkjenningsprosesser vil dessuten gjøre det enklere for ansatte å utføre jobben sin da de verktøyene de trenger er raskt tilgjengelige. En raskere godkjenningsprosess vil dessuten være med på å raskere fylle opp listene med godkjente og ikke godkjente leverandører, slik at virksomheten får et stort repertoar av tjenester som allerede er vurdert og eventuelt godkjent. Det vil gjøre det

enklere for øvrige ansatte å finne tjenester som kanskje allerede er godkjente og passer til den arbeidsoppgaven som den trengs til.

Det er dessverre ingen enkel oppskrift som kan følges for å gjøre at godkjennelsesprosessen tar mindre tid. Det er en omfattende prosess hvor det er viktig at det gjøres en grundig vurdering fordi konsekvensene av slurv vil kunne bli fatale. For å korte ned tidsbruken kan det være en ide å lage et bedre system der kriterier i risikovurderingen kan godkjennes på et overordnet nivå. På den måten vil det bli lettere å godkjenne enkelte kriterier på en rask måte, samtidig som det blir tydeligere hvilke kriterier som stilles. Det vil eksempelvis gjøre at alle tjenester med informasjon til et gitt sensitivitetsnivå kan behandles direkte i systemer uten en altfor omfattende prosess. Samtidig vil tjenester som møter et gitt sensitivitetsnivå behandlers nøye. Dermed vil de tjenestene med høy sensitivitet få mer oppmerksomhet, mens de mindre sensitive får mindre oppmerksomhet. Dette vil forhåpentligvis resultere i en raskere prosess hvor IT og sikkerhetsavdelingen kan ha enda mer fokus på det som virkelig er viktig samtidig som tidsbruken går ned for alle typer godkjenningsprosesser av lavere sensitivitet

5.2 Håndtering av SaaS-løsninger

Som nevnt i delkapittel 4.2.1 Fordeler ved SaaS-løsninger, er det en rekke fordeler med SaaS-løsninger som gjør at Datakonsulentene AS kan utføre arbeidsoppgaver på en helt annen måte enn tidligere. Fordelene anses som større enn ulempene, og fører derfor til at virksomheten velger å bruke det til svært mange ulike aktiviteter. Dette gjelder imidlertid bare hvis Datakonsulentene AS bruker SaaS-løsningene i henhold til lovgivninger og de rettslige avgjørelsene som GDPR og Schrems II. Skulle virksomheten ta i bruk SaaS-løsninger som ikke er i henhold til lovverket vil det kunne gi betydelige bøter som vil gå hardt utover økonomien i virksomheten.

For Datakonsulentene AS er det spesielt utfordrende å håndtere SaaS-løsninger fordi det finnes en del utfordringer knyttet til lovverk rundt bruken av dem. En kjent forretningsmodell for SaaS-løsninger er at brukere enkelt kan opprette en bruker og få tilgang til primitive versjoner uten å måtte betale for det. En spesiell utfordring knyttet til dette er at du som oftest mister eierskap til data som legges igjen på siden. Skulle programmet brukes til å dele sensitive data vil Datakonsulentene AS miste eierskap til dataene de sender, noe virksomheten naturligvis bør unngå. For å hindre at slike situasjoner oppstår er det viktig at ansatte er klar over hva de registrerer knyttet til jobb-mailen sin, og ikke minst hvilke data de gjør tilgjengelig. Det er stor forskjell på å sende sensitiv data gjennom en underleverandør med en gjennomarbeidet avtale enn en vilkårlig tjeneste som er funnet på internett.

Det finnes uendelige SaaS-løsninger på internett som enkelt kan tas i bruk av hvem som helst. For å unngå at ansatte går i en felle er det viktig å sørge for at de er oppmerksomme på problemstillingen og kan ta bevisste valg. Igjen er det viktig å være bevisst på hva en anskaffelse er og regelverket rundt bruken. For å gjøre det enda tydeligere hva som er lov og ikke så vil det være lurt av Datakonsulentene AS å innføre tydelige retningslinjer for hvordan anskaffelsesprosesser skal gjennomføres.

Spesielt ved bruk av SaaS-løsninger må det komme på plass et tydeligere regelverk for hvordan bruken av dem skal håndteres.

> *Når skal det være greit å ta i bruk en ny tjeneste for å teste den ut og når skal det ikke være lov? Hvilke data kan en benytte seg av til testingen og hva skal en holde seg langt unna? Hvor lang tid kan det gå før en må sende inn ønsker om bruk videre til servicedesken slik at IT og sikkerhetsavdelingen kan ta en fullstendig gjennomgang av tjenesten?*

Her vil det være lurt å sette en klar tidsfrist for hvor lenge en ansatt kan teste en SaaS-løsning og gi tydelige retningslinjer for bruken i testperioden. Det må blant annet tydeliggjøres at en ikke kan behandle persondata i testperioden, og dersom det skulle være ønskelig må det avklares med IT og sikkerhetsavdelingen først. Det er også viktig å sette tydelige retningslinjer for hva som skal skje dersom en finner ut at en ikke ønsker å bruke tjenesten videre. Dette er viktig fordi en har opprettet en bruker som er tilknyttet til virksomheten, og dersom den ikke skal brukes mer så er den nødt til å aktivt slettes.

SaaS-løsninger er noe som har kommet for å bli, og da er det viktig å være tidlig ute med å definere retningslinjer for anvendelsen. Dette gjelder for så vidt også alle andre nye trender som skulle dukke opp i fremtiden som etter hvert vil kreve sine egne retningslinjer. Det bør aldri være uklart for ansatte hvordan de skal takle ulike situasjoner, og dersom det skulle oppleves bør en legge retningslinjer for det som skulle dukke opp. I likhet med testperioden er det viktig at Datakonsulentene AS implementerer og opprettholder gode rutiner når det kommer til SaaS-løsninger. Det er viktig at ledelsen og IT og sikkerhetsavdelingen skaper en forståelse hos ansatte, og at de motiverer dem til å tenke på sikkerhet. Dersom ansatte er bevisste på hva som forventes av dem, vil de ta mer ansvar for handlingene sine, i tillegg til å danne en bredere forståelse for de ulike sikkerhetstiltakene. Tiltakene bidrar til at medarbeiderne tenker mer på å ivareta sikkerheten når de finner og tar i bruk nye systemer, og dette er med på å styrke sikkerhetskulturen innad i virksomheten (Nasjonal Sikkerhetsmyndighet b., 2020).

5.3 Opplæring

For å forbedre anskaffelsesprosessen vil det være viktig å tilegne ansatte hos Datakonsulentene AS kunnskap om prosessen og gjøre dem trygge på hva den innebærer. Virksomheten har i dag flere prosesser for å sikre at dette skjer på best mulig måte.

5.3.1 Opplæring av interne prosesser

Som nevnt tidligere i delkapittel 4.3.1 Intern kommunikasjon har Datakonsulentene AS en opplæringsperiode når de ansetter nye i virksomheten sin. Her blir alt av viktig informasjon presentert slik at en nyansatt skal ha tilstrekkelig kunnskap for å arbeide hos Datakonsulentene AS. Likevel kan det tenkes at det ikke er tilstrekkelig å opplyse ansatte kun én gang helt i startfasen av ansettelsen, da det er fort at mye rett og slett blir glemt etter hvert. Selv ansatte som har vært i virksomheten i over 20 år kan med fordel ha en

form for oppfriskning utover årene for å sikre at det ikke går i glemmeboken. Ut ifra hva som er hensiktsmessig kan en mulighet være å ha en fast tidsperiode mellom hver gang ansatte skal ha sett gjennom dokumentene angående anskaffelser. Dette er dessuten lurt da dokumentene stadig revideres.

En viktig faktor for kontinuerlig læring er gode systemer for opplæring. Tidligere har Datakonsulentene AS arrangert større seminarer hvor viktige temaer blir presentert for en større folkemengde. Dette er trolig et bra tiltak, men krever en del ressurser for å gjennomføre. Derfor har virksomheten begynt arbeidet med å skaffe seg et e-læringssystem for å enklere kunne nå ut til flere ansatte med relevant og forståelig informasjon. For at disse metodene skal bli en suksess er det viktig å sette fokus på god systemkvalitet som sikrer god brukervennlighet, intuitive funksjoner og kort svartid, samt godt faglig innhold som er både pålitelig og relevant (Frøkedal & Juliussen, 2012). Utover det rent tekniske og teoretiske er Datakonsulentene AS helt avhengige av at ansatte er åpne for å ta i bruk et digitalt læringsverktøy, og ikke minst at de har kunnskap nok til det. Dette vil trolig ikke være den største utfordringen for Datakonsulentene AS da de allerede er digitaliserte, samt bidrar det til en økt akseptanse for å ta i bruk nye digitale løsninger.

For å spre informasjon vil det også være en fordel å bruke de verktøyene som Datakonsulentene AS allerede har i bruk. Meldingsverktøy og nyhetsbrev er ypperlige digitale plattformer for å spre kunnskap. Virksomheten har stort fokus på å ha god intern kommunikasjon, men kan helt klart utnytte plattformene enda mer. Som nevnt er det ikke alle ansatte som har kontroll på hvilke leverandører som er godkjente, noe som kan kommuniseres ved bruk av slike verktøy. Likevel er det viktig å presisere at virksomheten ikke må bruke det for hyppig heller. Det optimale er å finne en balanse hvor virksomheten kan spre mest mulig informasjon uten at ansatte faller fra og lar være å få det med seg. Dette er en vanskelig balansegang da virksomheten ønsker å sende ut mest mulig informasjon til ansatte for å holde dem informerte, men dersom det blir for mye ender ansatte heller opp med la være å lese eller overser viktig informasjon. Hvor denne balansegangen ligger er forskjellig for ulike virksomheter og det er viktig å finne en balansegang som fungerer for seg.

5.3.2 Opplæring i informasjonssikkerhet

Selv om ansatte hos Datakonsulentene AS har gode kunnskaper om hvordan en skal gjennomføre ulike interne prosesser, så er det også viktig å ha en grunnleggende forståelse for informasjonssikkerhet. Selv om virksomheten har gode sikkerhetstiltak, er ikke det alltid nok. Ansatte må ha kunnskap om hvorfor en har så mange forskjellige prosesser og regler som må følges. På den måten skapes en helhetlig god sikkerhetskultur som vil ha et konstant fokus på å gjennomføre arbeidsoppgaver på en trygg og sikker måte.

Informasjonssikkerhet er et tema en aldri blir utlært. Den digitale verdenen er i stadig endring, og det som var bra for noen måneder siden er kanskje ikke godt nok i dag. En må hele tiden følge med på utviklingen og helst ligge litt i forkant for å beskytte seg mot ulike trusler som kan komme. En undersøkelse fra NorSIS viser at 77% av ansatte selv mener at de får bedre kompetanse etter opplæring i informasjonssikkerhet, mye på grunn av at en blir mer bevisst i valgene sine (NorSIS, 2016). Eksempelvis er det flere med opplæring i

informasjonssikkerhet som undersøker om et nettsted er trygt eller bruker forskjellige passord på ulike plattformer. Dette viser at bevissthet rundt informasjonssikkerhet er viktig for å sikre at ansatte tar gode valg både privat og på jobb.

Bevissthet rundt informasjonssikkerhet er dessuten viktig for å skape en helhetlig god sikkerhetskultur innad i virksomheten. Virksomhetens sikkerhetskultur er den delen av kulturen som retter seg mot sikkerheten og deres evne til å styre sikkerhet (Bergsjø, Windvik, & Øverlier, 2020). Sikkerhetskultur er et viktig verktøy for å effektivisere og etterleve regler og krav, og handler om å beskytte digitale verdier fra ulike former for trusler. Ved å bygge opp en kultur med sterk bevissthet rundt informasjonssikkerhet vil det kunne skape større forståelse for de omfattende prosessene som IT og sikkerhetsavdelingen må utføre, samt bevissthet for hvorfor de må utføres. Ved å sikre at ansatte har god kompetanse om sikkerhet vil det skape større tillit til at ansatte melder ifra om bruken av nye tjenester og forholder seg til de reglene som er satt av IT og sikkerhetsavdelingen. Det skaper også en tillit til at IT og sikkerhetsavdelingen gjør et nødvendig arbeid som blir respektert av øvrige ansatte. Dette vil igjen skape et bedre fellesskap mellom alle ansatte som igjen styrker organisasjonskulturen i virksomheten.

Digitalisering er en ønsket utvikling for de fleste virksomheter og den teknologiske utviklingen virker nærmest uunngåelig (Bergsjø, Windvik, & Øverlier, 2020). Der er derfor viktig å sikre at enhver ansatt har god kompetanse om informasjonssikkerhet, som igjen vil gjøre ansatte tryggere i valgene de tar. Tryggheten vil bidra til at ansatte vil dele kompetanse og erfaringer mellom seg, og skaper en kunnskapsdelende kultur. Åpenhet er en av de fire kjerneverdiene som kjennetegner digital kultur, og er en verdi av stor betydning for å styrke fellesskapet og skape en god kultur i virksomheten. Åpenhet bidrar til å sikre bedre kompetanse og en god kultur hvor ansatte føler seg komfortable rundt kollegaene sine uten å føle på et press. Kompetansen bidrar med sikkerhetskulturen innad i virksomheten, og god sikkerhetskultur styrker også selve organisasjonskulturen.

5.3.3 Opplæring av GDPR og Schrems II

Selv om GDPR og Schrems II byr på nye utfordringer og ekstra arbeid for virksomheten, så åpner det også opp for helt nye muligheter. Det er viktig som virksomhet å vise at enkeltpersoners personvern verdsettes og være åpne om hvordan de bruker informasjon som samles inn, samt utvikle gode metoder for å håndtere og sikre dataene. Dette vil gi både ansatte, kunder og andre større tillit til virksomheten (SuperOffice, u.d.). Dette er blant annet viktig for å sikre seg dyktige ansatte som ønsker å bidra med å skape en dyktig virksomhet som tar personvern på alvor. Det er også viktig for å tilegne seg lojale kunder med stor tiltro til virksomheten som ser at virksomheten etterstreber å oppfylle mer enn de absolutte minstekravene satt av lovverkene. Ikke minst vil et slikt omdømme spre seg utover og bidra til å sette en standard for hvordan virksomheter bør behandle personopplysninger og andre sensitive data i samfunnet.

5.4 GDPR og Schrems II

5.4.1 Utfordringer med GDPR

Som nevnt tidligere er GDPR en lov i EU kalt personvernforordningen, som ble vedtatt i 2018. Siden den gang har Datakonsulentene AS satt mye mer fokus på riktig behandling av personvernopplysninger for å oppfylle de nye kravene som stilles. Selve roten i GDPR handler om å gi enkeltpersoner større mulighet til å styre personopplysninger som er registrert om dem (Datatilsynet a, u.d.). Det er ingen tvil om at GDPR har bidratt til at landene i EU/EØS har satt personvernfordringen på toppen av prioriteringslistene, noe som har styrket personvernet i hele Europa (PWC, 2020). Likevel har GDPR medført utfordringer for flere enn bare Datakonsulentene AS, og virksomheten lever hele tiden i frykt for å gjøre noe galt og pådra seg betydelige bøter.

Det virker som flere opplever at GDPR bare handler om IT, noe som er langt fra tilfellet. Personvernforordningen har omfattende konsekvenser for hele virksomheten, inkludert aktiviteter som håndteringen av salgsaktiviteter og markedsføringsaktiviteter. For å illustrere dette må det blant annet gis eget separat samtykke for ulike markedsføringsaktiviteter. Det betyr at Datakonsulentene AS må kunne bevise at enkeltpersoner har samtykket å motta nyhetsbrev. Et annet viktig poeng er at samtykket må gis ved at det foretas en aktiv handling, som betyr at en ikke kan ha forhåndsavkryssede bokser, men at brukerne aktivt må trykke «godkjenn» selv (SuperOffice, u.d.). Regler som dette har ført til at virksomheten har sett seg nødt til å arbeide annerledes enn tidligere.

Hvorfor må Datakonsulentene AS ta GDPR på alvor?

Delkapittel 4.1.2 Testperiode konkluderte med at testing av ulike programmer og tjenester som IT og sikkerhetsavdelingen ikke visste om ville skape problemer da virksomheten ikke har kontroll. Dette vil stride imot GDPR protokollen, da virksomheten ikke vil kunne dokumentere hvor personopplysningene er lagret og hvilke andre opplysninger som er lagret. Det at en virksomhet ikke vil kunne klare å dokumentere hvor opplysningene er lagret og hvilke opplysninger som er lagret vil defineres som er sikkerhetsbrudd ifølge Lov om behandling av personopplysninger artikkel 4 nr. 12:

> *«… brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet»*.

Brudd på GDPR kan i dag straffes med bøter på opptil 20 millioner euro eller 4% av virksomhetens globale omsetning (Hagene, 2018). Slike sikkerhetsbrudd vil påvirke virksomheten økonomisk, men vil også sette virksomheten i et dårlig lys. Dette kan medføre til at flere leverandører og kunder blir skremt og velger å avslutte dagens avtaler og samarbeid. Det vil også kunne gå utover ansettelsesprosessen ved at personer ikke ønsker å jobbe i en virksomhet hvor det er påvist at de ikke arbeider etter loven. Det kan også hende at flere av ansatte velger å forlate virksomheten på bakgrunn av skandalen. Håndteringen av bruddet/avviket vil dessuten kunne påvirke om Datakonsulentene AS vil kunne beholde ISO27001 sertifiseringen ved den neste revisjonen.

5.4.2 Utfordringer med Schrems II

Schrems II er i dag en dagsaktuell dom som stadig blir omtalt i mediene og i jobbsammenheng. Som nevnt i delkapittel 2.2.3 Schrems II ble dommen nedfelt i 2020, og det medfører en del utfordringer. I dag er de praktiske konsekvensene uklare, og dette medfører uklarhet i hvordan dommen og konsekvensene vil påvirke virksomheten. Anskaffelser og bruken av skyløsninger vil i fremtiden bli påvirket, men i hvilken grad er usikkert. Skytjenester er et begrep som omfatter Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS), og i hovedsak er de eksterne serverparkene lokalisert utenfor Norge. Det skaper utfordringer ved at en virksomhet må sørge for at lagringen av data i serverparkene er i samsvar med lovgivningen i Norge.

Dette byr også på utfordringer for Datakonsulentene AS. I et av intervjuene som ble gjennomført fikk vi vite at det nylig er avslørt at det er tatt i bruk omkring 400 SaaS-løsninger i virksomheten som IT og sikkerhetsavdelingen ikke hadde kunnskap om. Flere intervjuobjekter var enige om at dette var et skremmende høyt tall som helt klart må reduseres. I de aller fleste ukjente anskaffelsene har ansatte hos Datakonsulentene AS i stor grad gjennomført anskaffelser av tilleggspakker til programmerings programmene. Dette er anskaffelser der en ikke lagrer personopplysninger, og som ikke vil medføre noen konsekvenser når det gjelder Schrems II og annen norsk lovgiving.

Det er derimot de større anskaffelsene som kan by på utfordringer og større konsekvenser for virksomheten. Under det ene intervjuet ble det opplyst at det var en avdeling som hadde tatt i bruk et system for å sende ut interne nyhetsbrev til ansatte. Her ble informasjon om ansatte lagt inn i en database slik at den kunne hente ut igjen på et senere tidspunkt. Dette ble ikke meldt ifra til IT og sikkerhetsavdelingen før avdelingen hadde møtt på et problem med systemet. Avdelingen hadde brukt dette systemet omtrent et helt år uten å opplyse IT og driftsavdelingen. De hadde ikke sjekket om hvor dataene ble lagret, hvilken data som ble lagret og om det i det hele tatt var greit å ta det i bruk. Dette kunne ha ført til store konsekvenser dersom det hadde vist seg at dataene hadde blitt lagret i et tredjeparts land, og at datatilsynet hadde kommet til virksomheten og bedt dem om innsyn i leverandørene deres. I denne situasjonen ville ikke Datakonsulentene AS hatt muligheten til å redegjøre for hvilke programmer og tjenester de bruker da de ikke har en oversikt over dem alle, noe som kunne ha medført til betydelige bøter.

En annen utfordring knyttet til Schrems II er at det er en stor andel av ansatte hos Datakonsulentene AS som ikke har noe kjennskap til Schrems II og hva det innebærer. Dette ble oppdaget gjennom intervjurundene som ble gjennomført, og flere av ansatte presiserte at de heller ikke hadde blitt informert om det på Slack, fagdager eller nyhetsbrev. Noe av grunnen skyldes trolig at det fortsatt er relativt nytt og at det fortsatt er uklart i fagmiljøet hva Schrems II faktisk utgjør. Lite bekjentskap til Schrems II hos ansatte kan føre til at de ikke er klar over de mulige konsekvensene som kan oppstå når en tar i bruk et program eller en tjeneste som lagrer sensitiv persondata i tredjepartsland. Dette kan føre til store konsekvenser for virksomheten.

6. Konklusjon

I denne bacheloroppgaven har vi gått i dybden på anskaffelsesprosessen hos Datakonsulentene AS og sett på diverse utfordringer og potensielle tiltak for å bedre prosessen. Videre i dette kapittelet vil vi besvare problemstillingen med de tilhørende forskningsspørsmålene. Det vil også drøftes potensiell videre forskning og se på fremtidige problemstillinger knyttet til temaet. Til slutt vil det reflekteres rundt oppgavens begrensninger og hva vi eventuelt kunne gjort annerledes.

6.1 Besvare problemstillingen

For å besvare problemstillingen har vi tatt for oss de to forskningsspørsmålene som problemstillingen bygger på. Det første forskningsspørsmålet er:

> *Hvilke utfordringer vil en virksomhet typisk oppleve i forbindelse med anskaffelsesprosessen?*

Det har vist seg å være mange ulike utfordringer knyttet til anskaffelsesprosessen som gjør det vanskelig å sikre en god prosess for Datakonsulentene AS. Spesielt GDPR og Schrems II har vist seg å være røttene til de største utfordringene på grunn av flere nye retningslinjer som virksomheten er nødt til å etterleve for å unngå betydelige bøter.

Utfordringene knyttet til GDPR og Schrems II medfører at dagens anskaffelsesprosess har blitt mer omfattende, fordi det stilles helt nye krav til hvordan prosessen må utføres. Det er blant annet satt nye krav til dokumentering av anskaffelsesprosessen som har vist seg å være tidkrevende å etterleve. Dette har gjort ansatte utålmodige og Datakonsulentene AS har spesielt opplevd utfordringer knyttet til at ansatte tar i bruk gratis tjenester uten at de er godkjent av IT og sikkerhetsavdelingen.

Spesielt anskaffelser av SaaS-løsninger har vist seg å være utfordrende da det er enkelt for hvem som helst å ta i bruk løsninger i virksomhetens navn, uten at virksomheten selv har kontroll over det. Her er det spesielt utfordringer knyttet til håndtering av dataene som blir lagret, hvem som har tilganger, og fjerning av tjenester som ikke lenger er i bruk. Igjen kan en se at GDPR og Schrems II ligger til grunn for utfordringene.

En annen utfordring handler om at ansatte ikke har god nok kontroll på hva en anskaffelse faktisk er og hvordan prosessene skal gjennomføres. Ansatte føler seg ikke trygge på regelverkene, verken de interne reglene i virksomheten, eller de nasjonale og internasjonale regelverkene. Selv om det er dokumenter tilgjengelig så er det for mye tekst til at ansatte faktisk tar seg tid til å lese det, med mindre de absolutt må. Selv ansatte i IT og sikkerhetsavdelingen synes det er vanskelig å forstå alle reglene knyttet til GDPR og den faktiske betydningen av Schrems II.

Selv om det er en del utfordringer knyttet til anskaffelsesprosessen er det også flere mulige tiltak for å bedre prosessen. Det andre forskningsspørsmålet skal svare på det:

> *Hvilke tiltak kan en virksomhet gjøre for å sikre vellykkede anskaffelsesprosesser?*

Med tanke på at GDPR og Schrems II er røttene til de fleste utfordringene knyttet til anskaffelsesprosessen er det også naturlig å gjøre tiltak knyttet til dem. Først og fremst er Datakonsulentene AS nødt til å definere tydeligere retningslinjer. Spesielt bruken av gratis tjenester og programvarer bør få retningslinjer om hva som faktisk kan prøves ut, hvilke datatyper som kan brukes i prøveperioden og når virksomheten må varsles om bruken. På den måten vil ansatte ha klare retningslinjer for hva de må forholde seg til og konkrete oppgaver de er nødt til å utføre i denne prosessen. Som nevnt vil IT og sikkerhetsavdelingen ha full kontroll på absolutt alle programmer og tjenester som brukes i virksomheten, og retningslinjene må gjenspeile dette kravet.

Det er ikke nok å lage nye retningslinjer hvis ansatte ikke har kunnskap om dem. Kunnskapen er i dag for lav blant ansatte og det bør tas tak i. Enten ved bruk av mindre påminnelser ved nyhetsbrev eller meldingsapplikasjoner, eller større tiltak som fagdager og bruken av e-læringssystemer. Ansatte er nødt til å få opplæring i de interne retningslinjene for å kunne følge dem. Det vil dessuten være en fordel å gi ansatte økt kompetanse om GDPR og Schrems II for å bedre forstå hvorfor det er så viktig at de følger retningslinjene som er satt.

For at tydeligere retningslinjer og økt kompetanse skal hjelpe er det også viktig at selve godkjennelsesprosessen reduseres tidsmessig. Dagens prosess kan ta flere måneder, og er nødt til å reduseres til få uker, eller til og med noen dager. På denne måten vil det være større sannsynlighet for at ansatte blir motiverte til å følge de nye retningslinjene, nettopp fordi de får raske svar og ikke føler i like stor grad at godkjennelsesprosessen hindrer dem i å utføre arbeidet sitt. Forhåpentligvis blir det en gjensidig forbedring hvor ansatte følger opp retningslinjene med sine nye kunnskaper, mens IT og sikkerhetsavdelingen gjør forbedringer for å gjøre hele anskaffelsesprosessene lettere og kortere.

For å oppsummere utfordringene og potensielle tiltak kan vi svare på problemstillingen:

> *Hvordan kan en IT-virksomhet sikre en god prosess ved anskaffelse av nye IT-løsninger?*

Det finnes ikke et fasitsvar på hvordan en anskaffelsesprosess skal se ut, men det finnes tiltak som skal sikre at prosessen blir gjennomført best mulig. Vi vil anbefale enhver virksomhet å følge ISO 27001 standarden for å sørge for god dokumentering av prosessen for å sikre at en så langt det lar seg gjøre oppfyller GDPR og Schrems II. Selv om dagens prosess er for tidkrevende og ansatte ikke har nok kunnskap om hva den innebærer, er det viktig å få hele virksomheten på samme side i prosessen. På den måten kan en avverge at en anskaffelse skulle blitt rapportert samtidig som kostbare konsekvensene som følger brudd på GDPR og Schrems II unngås. Det er viktig å styrke sikkerhetskulturen innad i virksomheten, og skape et fellesskap som har de samme intensjonene, målene og motivene.

6.2 Videre forskning

Som nevnt finnes ikke noe enkelt fasitsvar på hvordan en anskaffelsesprosess bør se ut. Digital teknologi er i konstant utvikling, noe som betyr at digitale anskaffelser også vil være

i konstant utvikling. For Datakonsulentene AS vil det derfor være naturlig å kontinuerlig arbeide med å utvikle anskaffelsesprosessen for å optimalisere den i forhold til dagens situasjon.

Allerede i dag vet vi at anskaffelsesprosessen kan endre seg på bakgrunn av varsling om endringer i ISO27001 sertifiseringen. Datakonsulentene AS avslørte at de har fått varsel om store endringer i 2023, noe som de blir nødt til å tilpasse seg for å fortsette å ha sertifiseringen. Tidligere har det kommet mindre endringer mellom hvert år, men denne gangen skulle det komme noen vesentlige endringer som vil kreve at Datakonsulentene AS må gjennomføre endringer i rutinene de har nå. Dette er helt klart en spennende utfordring som kunne være interessant å følge med på.

Det er heller ikke til å legge skjul på at Schrems II er et spennende område hvor det er mye å hente fra. Hva betyr Schrems II for en virksomhet, og hva er egentlig konsekvensene av dommen? Dette er fortsatt veldig uklart og mange virksomheter, inkludert Datakonsulentene AS, syns dette er et vanskelig tema. Det kan med fordel gjøres grundigere analyser for å gi bedre forståelse om hva Schrems II egentlig er, hvordan virksomheter skal forholde seg til dommen, og hvordan de kan unngå lovbrudd.

Ettersom Privacy Shield avtalen ikke ble lovlig etter Schrems II dommen diskuteres det i dag om det skal opprettes andre avtaler mellom Europa og USA, som skal gjøre det mulig å lagre persondata lovlig i USA. Den 25.mars 2022 ble avtalen «Trans-Atlantic-Data Privacy» presentert. Denne avtalen vil muliggjøre og legge til rette for at virksomheter i Europa kan lagre personopplysninger i USA, i forbehold om at virksomheten i USA er sertifiserte og har særskilte forpliktelser. Avtalen skal sikre beskyttelsesnivået på personopplysningene når de blir overført og lagret i USA. Avtalen er kun presentert, og i dag er det kun en enighet om at avtalen er nødvendig da flere virksomheter er avhengige av amerikanske skytjenester som har datasentre i USA (Datatilsynet, 2022). Diskusjonen om detaljene i Trans-Atlantic-Data Privacy diskuteres og konkretiserer i disse dager. Det vil derfor være gunstig å forske videre på hvordan dette vil påvirke Datakonsulentene AS, og om dette fører til at ansatte i større grad kan ta i bruk SaaS løsninger utenom å sende inn henvendelser ved hjelp av servicedesken.

Som nevnt i delkapittel 3.4.1 har vi kun forsket på én casevirksomhet, og basert denne oppgaven på informasjon vi har hentet ut fra Datakonsulentene AS. For videre forskning vil det være gunstig å forske på flere virksomheter. I første omgang vil det være naturlig å sammenligne IT virksomheter og deres anskaffelsesprosesser opp mot hverandre før en sammenligner virksomheter i ulike bransjer.

6.3 Refleksjon rundt oppgavens begrensninger

En bacheloroppgave er begrenset til et semester, noe som medfører at det er begrenset hvor mye oppgaven kan ta for seg. Det er derfor viktig å påpeke at det er flere aspekter ved oppgaven som kunne blitt gjort annerledes, men som har blitt nedprioritert på grunn av begrensningene.

Oppgaven har valgt å fokusere hovedsakelig på GDPR og Schrems II, samt hvilke utfordringer disse har medført i anskaffelsesprosessen. Dette er ikke fordi det ikke finnes andre utfordringer knyttet til anskaffelsesprosessen, men det er fordi disse utfordringene er mest dagsaktuelle for virksomheten. Andre utfordringer som kontraktshåndtering og rekrutteringsprosessen er oppgaver som også byr på enkelte utfordringer i anskaffelsesprosessen, men oppleves ikke som like viktige da det er utfordringer som har eksistert i lang tid, og allerede har fått tiltak som skal gjøre det lettere å håndtere.

Det er flere aspekter som har ledet opp til GDPR og Schrems II. Det er en lang historie bak som kunne vært interessant å diskutere. Likevel velger vi å ikke gjøre det fordi det ikke er relevant for å besvare problemstillingen.

Bruken av sitater er fraværende i oppgaven, og det blir heller ikke spesifisert hvilke ansatte som har blitt intervjuet og hvem som har sagt hva. Bakgrunnen for dette er at det skal være umulig å oppdage hvilke intervjuobjekter som har sagt hva. Selv ikke ansatte i Datakonsulentene AS skal kunne identifisere svarene fra intervjuobjektene. Derfor har vi valgt å ikke kommentere hvilke stillinger de ulike intervjuobjektene har, selv om det kunne gitt bedre innsikt i resultatene. Det var forskjell på svarene til intervjuobjektene som jobber med sikkerhet til daglig og ansatte som ikke jobber med det. Det kunne vært interessant å gå i dybden på disse forskjellene, men det ble altså ikke gjort for å sikre at svarene ikke kunne spores tilbake.

I delkapittel 3.5.1 Kritisk refleksjon og svakheter ved metode er oppgavens fremgangsmåte diskutert. Blant annet tar oppgaven kun for seg en tverrsnittsundersøkelse, noe som hindrer oppgaven i å få et større tidsperspektiv. Dette blir begrunnet med at bacheloroppgaven er tidsbegrenset og at det ikke er tid til en langtidsundersøkelse. Videre er bruken av intervjuer som informasjonskilde diskutert. Likevel gir informasjonen som er hentet inn ved bruk av intervjuer en økt dybde i svarene, samt bedre innblikk i ansattes meninger, holdninger og tankesett (NDLA, 2019).

En anskaffelsesprosess er individuell for hver virksomhet og det vil være utfordrende å konkludere på et generelt grunnlag. Ved å kun forske hos en virksomhet vil det endelige resultatet være tilpasset Datakonsulentene AS, noe som kan føre til at ikke alle resultatene er like overførbare for andre virksomheter. Ved å benytte flere virksomheter i forskningen ville oppgaven fått bredere innsikt rundt problematikken. På tross av dette er det flere likheter. Det er aktuelt for enhver virksomhet å opprettholde regulatoriske kravene i GDPR og Schrems II, samt se om deres anskaffelsesprosesser oppfyller kravene som stilles. Selv om resultatet bærer preg av å basere seg på én casevirksomhet, vil konklusjonen være nyttig for mange andre også.

7. Bibliografi

Arbeidstilsynet. (u.d.). *§ 3. Definisjoner* . Hentet fra arbeidstilsynet.no: https://www.arbeidstilsynet.no/regelverk/forskrifter/forskrift-om-informasjons--og-paseplikt-mv/1/3/ (Hentet 15.02.2022)

Bang, H. (2020). *Organisasjonskultur.* Universitetsforlaget.

Beckers, K., Heisel, M., Solhaug, B., & Stølen, K. (2013). *ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System.* SINTEF.

Bedrebedrift. (u.d.). *GDPR: Hva er en behandlingsprotokoll (artikkel 30)?* Hentet fra Bedrebedrift.no: https://www.bedrebedrift.no/blog/gdpr-for-sma-bedrifter-steg-1 (Hentet 23.02.2022)

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). *Digital Sikkhert - en innføring.* Universitetsforlaget.

Bouwman, H., Van Den Hooff, B., Van De Wijngaert, L., & Van Dijk, J. (2005). *Information & Communication Technology in Organizations.* SAGE Publications .

Busch, T. (2021). *Akademisk skriving for bachelor- og masterstudenter.*

Datatilsynet. (2021). *Tillegskrav*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/tilleggskrav-til-overforingsgrunnlag-schrems-ii/ (Hentet 29.03.2022)

Datatilsynet. (2022). *Enighet om overføring av personopplysninger til USA*. Hentet fra Datatilsynet: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/enighet-om-overforing-av-personopplysninger-til-usa/ (Hentet 29.02.2022)

Datatilsynet a. (u.d.). *Virksomhetes plikter*. Hentet fra datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/ (Hentet 19.04.2022)

Datatilsynet a. (2018). *Skytjenester*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/ (Hentet 20.04.2022)

Datatilsynet a. (2019). *Hva er en personopplysning?* Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/ (Hentet 17.02.2022)

Datatilsynet b. (2018). *Iverksette styringssystem for informasjonssikkerhet*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/ (Hentet 28.02.2022)

Datatilsynet b. (2019). *Hva er personvern?* Hentet fra Datatilsytnet.no: https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/ (Hentet 16.02.2022)

DFØ. (2021, Desember 09). *Anskaffelsesordbok.* Hentet fra Anskaffelser.no: https://anskaffelser.no/ofte-stilte-sporsmal-om-anskaffelser/anskaffelsesordbok#anskaffelse (Hentet 10.02.2022)

DNV. (u.d.). *ISO/IEC 27701 - ledelsessystem for personverninformasjon*. Hentet fra Dnv.no: https://www.dnv.no/services/iso-iec-27701-ledelsessystem-for-personverninformasjon-213123?fbclid=IwAR21gJRMyaREQIzJARBWTo2CYw0ibM2JX8jk7VIg--6BP5Yyg1IY8_p8ZvQ (Hentet 02.03.2022)

Fangen, K. (2015). *Kvalitativ metode*. Hentet fra Den nasjonale forskningsetiske komiteene: https://www.forskningsetikk.no/ressurser/fbib/metoder/kvalitativ-metode/

Fey, C. F., & Birkinshaw, J. (2005, august 1.). Journal of Management. *External Sources of Knowlede, Governance mode, and R&D Peformance*, ss. 597-621.

Fossen, E. A. (2021). *Veien fram til Schrems II*. Hentet fra Kantega: https://www.youtube.com/watch?v=UBw28hwqgGQ (Hentet 05.05.2022)

Frøkedal, Ø. V., & Juliussen, T. A. (2012). *Kritiske suksessfaktorer ved bruk av e-læring i private bedrifter. En casestudie fra Aker Solutions.* Universitet i Agder.

Gjessing, M. (2022). *Varsler massivt tilsyn med bruk av skytjenester i offentlig sektor*. Hentet fra Digi.no: https://www.digi.no/artikler/varsler-massivt-tilsyn-med-bruk-av-skytjenester-i-offentlig-sektor/517398 (Hentet 01.03.2022)

Gripsrud, G., Olsson, U. H., & Silkoset, R. (2021). *Metode, dataanalyse og innsikt.* Cappelen damm akademisk.

Hagene, E. (2018). *Konsekvenser av databrudd*. Hentet fra frontcore.no: https://frontcore.no/blogg/konsekvenser-databrudd-gdpr/ (Hentet

Hamberg K, Johansson E, Lindgren G, Westman G(1994) *Scientific rigour in qualitative research – examples from a study of womens`s health in family practice,* Fam Pract

Hartl, E. (2019). *A Characterization of Culture Change in the Context of Digital Transformation.* LMU Munich.

IKT Norge. (2018). *Knekk i kompetanse får konsekvenser*. Hentet fra IKT Norge: https://www.ikt-norge.no/kommentar/knekk-kompetanse-far-konsekvenser/ (Hentet 27.04.2022)

Jacobsen, D. I., & Thorsvik, J. (2019). *Hvordan organisasjoner fungerer*. Fagbokforlaget.

Kiwa. (u.d.). *ISO 27001 - Sertifisering for informasjonssikkerhet*. Hentet fra Kiwa.no: https://www.kiwa.com/no/no/tjenester/iso-27001-sertifisering-for-informasjonssikkerhet/ (Hentet 24.02.2022)

Malterud, K. (2011). *Kvalitative metoder i medisinsk forskning* . Oslo: Universitetsforlaget AS.

Malterud, K. (2017). *Kvalitative forskningsmetoder for medisin og helsefag.* Universitetsforlaget.

Mays N, Pope C (2006) *Qualitative research: Observational methods in health care settings*, Blackwell

Nasjonal Sikkerhetsmyndighet. (2020). *Grunnprinsipper for personellsikkerhet*. Hentet fra nsm.no: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/ (Hentet 21.04.2022)

Nav. (u.d.). *Tredjeland*. Hentet fra Datakatalogen: https://data.nav.no/begrep/BEGREP (Hentet 05.05.2022)

NDLA. (2019). *Kvantitative og kvalitative metoder*. Hentet fra NDLA: https://ndla.no/nb/subject:1:f18ad41e-d9c3-4428-8cb6-5eb852e45082/topic:1:7df2950d-3af9-462e-b27f-cf3df147eaa3/topic:1:f189e9b6-222c-4d31-adc4-d7bc74149e03/resource:f2a118d4-d382-4476-ac4a-8906bba2f736 (Hentet 04.03.2022)

NHO. (u.d.). *Hva er personvernforordningen (GDPR)?* Hentet fra nho.no: https://arbinn.nho.no/forretningsdrift/personvern/personopplysningsverktoy/personvernforordningen/ (Hentet 14.02.2022)

NorSIS. (2016). *Virker opplæring i informasjonssikkerhet?* Hentet fra Norsis.no: https://norsis.no/virker-opplaering-informasjonssikkerhet/ (Hentet 31.03.2022)

Nygård-Hansen, H.-P. (2022). *Over ti milliarder kroner i GDPR-bøter i 2021 og Amazon og Meta viser vei*. Hentet fra Kampanje.com: https://kampanje.com/tech-design/2022/01/--over-ti-milliarder-kroner-i-gdpr-boter-i-2021-og-amazon-og-meta-viser-vei/ (Hentet 22.04.2022)

PWC. (2020). *Dommen etter to år med GDPR*. Hentet fra pwc.no: https://www.pwc.no/no/pwc-aktuelt/dommen-etter-to-ar-med-gdpr.html (Hentet 06.04.2022)

PWC. (21). *Schrems II: Slik håndterer din bedrift de nye kravene*. Hentet fra pwc.no: https://www.pwc.no/no/pwc-aktuelt/schrems-ii-overfore-personopplysninger-til-usa-uten-a-bryte-loven.html (Hentet 06.04.2022)

Regjeringen. (2019). *Ny personopplysninslov*. Hentet fra Regjeringen.no: regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/ (Hentet 14.02.2022)

Rossen, E., & Jørgenrud, M. B. (2014). *Kunne datalagring stoppet «9/11»?* Hentet fra Digi.no: https://www.digi.no/artikler/kunne-datalagring-stoppet-9-11/288086 (Hentet 22.02.2022)

Safetec. (u.d.). *Sikkerhetskultur*. Hentet fra Safetech.no: https://www.safetec.no/tjenester/risk-management/sikkerhetskultur/ (Hentet 18.02.2022)

Schackt, J. (2019). *Kultur*. Hentet fra snl.no: https://snl.no/kultur (Hentet 27.04.2022)

Standard Norge. (2022). *NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav*. Hentet fra standard.no: https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/ (Hentet 04.05.2022)

SuperOffice. (u.d.). *Hva er GDPR, og hva betyr det for din bedrift?* Hentet fra SuperOffice.no: https://www.superoffice.no/ressurser/artikler/hva-er-gdpr/ (17.02.2022)

Sørebø, Ø., Fredriksen, J., Simnica, F., & Mollestad, H. J. (2021). *EUs personvernforordning (GDPR) - Utfordringer ved implementering i HRM-sammenheng.* Praktisk økonomi & finans.

Telenor. (2021). *Valgene vi tar Digital Sikkerhet 2021*. Telenor.

Torvik, K. (2011). *Kvantitativ metode.* Hentet fra https://ogbedreskalvibli.files.wordpress.com/2011/03/kvantitative-metoder.pdf (Hentet 02.03.2022)

Tranøy, K. (2019 , Mars). *SNL*. Hentet fra Store norske leksikon : https://snl.no/metode#:~:text=Metode%20er%20en%20planmessig%20fremgangsm%C3%A5te,grunnet%20p%C3%A5%20regler%20og%20prinsipper (Hentet 01.03.2022)

Tranøy, K. E. (2019). *Metode.* Hentet fra snl.no: https://snl.no/metode#:~:text=Metode%20er%20en%20planmessig%20fremgangsm%C3%A5te,grunnet%20p%C3%A5%20regler%20og%20prinsipper (21.03.2022)

Turner, B. (2020). *What is SaaS? Everything you need to know about Software as a Service*. Hentet fra techradar.com: https://www.techradar.com/news/what-is-saas (Hentet 04.02.2022)

Vejseli, A., & Hedberg, S. (2016). *Hinder och möjligheter med införandet av ISO 27001 - En undersökning på en medelstor organisation.* Linneuniversitetet, Institutionen för informatik.

Wrålsen, A., & Berntsen, K. E. (2022). *Vitenskaplighet i BA-oppgaven.* Institutt for datateknologi og informatikk.

8. Vedlegg

8.1 Intervjuguide

Presentasjons del

Presentasjon av oss selv:

- Navn
- Kommer fra NTNU
  - Studie: Digital Forretningsutvikling

Før oppstart:

- Skrevet under taushetserklæring
  - Virksomheten er anonymisert
- Gå gjennom informasjonsskriv og innhente skriftlig samtykke til:
  - Deltagelse
  - Lydopptak

Presentasjon av oppgaven og formålet med datainnsamlingen:

- Skriver en bacheloroppgave om informasjonssikkerhet
- Knyttet til anskaffelser av digitale løsninger

Introduksjon av oppgaven

«Oppgaven handler om hvordan en IT-virksomhet som Datakonsulentene AS på best mulig måte kan sikre en god anskaffelsesprosess av nye IT-løsninger. Vi vil gjerne høre mer om hvilke utfordringer du opplever i forbindelse med anskaffelsesprosessen, og gjerne forslag til hva som kunne vært bedre. Vi ønsker å se på hvilke rutiner som bør være på plass og hvordan kan de være med på å sikre at anskaffelses prosessene blir gjennomført på en best mulig måte.

En anskaffelse handler om når virksomheten skaffer seg et nytt produkt eller tjeneste. For eksempel hvis Datakonsulentene AS bestemmer seg for om de vil ta i bruk et nytt meldingsprogram, så må de gjennom fastsatte rutine før de kan begynne å ta det i bruk. Man må blant annet se på hvor dataene lagres, for eksempel se om de blir lagret i EU eller i USA, og påse at de opprettholder kravene til GDPR.
Vi har fått tilgang til kvalitetshåndboken til Datakonsulentene AS og sett igjennom en del av dokumentene deres. Det virker som at intensjonene er bra og at dere har en god løsning på papiret. Likevel har vi fått beskjed om at systemet kan bli bedre og det må bli tydeligere hvordan det skal brukes og i hvilke situasjoner det skal brukes.»

Spørsmålsdel

Intro:

- Hva heter du?
- Hvor gammel er du?
- Hva er din stilling?
- Hva er din rolle? Erfaring? Bakgrunn?
- Hvor lenge har du vært ansatt?
- Har du hatt noen andre roller tidligere? Eller hvordan kom du til denne stillingen?

Generell bruk:

- Hvordan bestemmer dere om dere skal ta i bruk et nytt system?
  - Vurderer dere systemet opp mot annet?
- Hva gjør dere i dag for å sikre en god ibrukstakelses prosess?
- Hvordan pleier en ibrukstakelses prosess å se ut hos Datakonsulentene AS?
  - Følger dere faktisk manualen? (Slavisk eller løst)
- Hvor mange pleier å være med i prosessen ved ny anskaffelse?
- Hvem er det som har sisteordet i prosessen ved ny anskaffelse? Og hvorfor?

Utfordringer og kriterier:

- Hva ser dere på som en utfordring ved bruk av underleverandører?
- Har dere noen gang gått på en «smell»?
  - Hvis ja, hvordan her dere håndtert det?
- Hvilke kriterier har dere til underleverandører?
  - Vet du at dere har ISO 27001?
  - Vet du hva ISO 27001 er?
  - Vet du hvorfor dere bruker ISO 27001?

Personlige oppfatninger:

- Har du selv vært med i en anskaffelsesprosess hvor dere har brukt dagens instrukser?
  - Hvis ja, fortell hvordan det opplevdes
- Føler du at det er noen mangler eller svakheter med metoden dere bruker i dag?
- Kan du fortelle om noe du syns er utfordrende med dagens prosess?
- Hva mener du kunne blitt gjort annerledes i denne prosessen?
  - Forslag til endringer i instruksene?
- Hva mener du er det viktigste å gjøre for å sikre en god anskaffelsesprosess?
  - Hvilke kriterier er viktigst å oppfylle?

Ledelsen og instrukser:

- Gjør ledelsen tiltak for å motivere dere til å tenke på sikkerhet i anskaffelsesprosessen?
- Hva oppfatter du som hovedpoenget med fremgangsmåten?
- Forstår du innholdet og vet du hvordan du eventuelt tar det i bruk?
- Har du noen gang blir oppfordret til å lese gjennom instruksen til anskaffelsesprosessen (flere ganger)?
    - Eventuelt i hvilken sammenheng.
- Vet du hvem du kan prate med dersom det er noen spørsmål til instruksen?

Engangsspørsmål til sikkerhetsansvarlig:

- Når ble guiden for anskaffelser laget?
- Hvordan var prosessen før dere laget en egen guide for anskaffelse?
- Hvorfor lagde dere en guide?
- Hvorfor ofte oppdateres guiden?
- Hvor lang tid tar en slik prosess?
- Hva opplever du som sikkerhetsansvarlig som den største utfordringen?
- Hva skulle du ønske ansatte var flinkere til?

Avslutning:

- Er det noe mer du ønsker å si før båndopptakeren slåes av?
- Er det noen andre du mener vi burde ta kontakt med?
- Minne om rettigheter jfr. samtykkeskjema.
- Runde av på en positiv måte. Takk for bidraget.

8.2 Samtaletykkeskjema

Vil du delta i forskningsprosjektet

«Digital forretningsutvikling»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kunne studere anvendelse av IT og hvordan dette kan skape gevinster for virksomheten. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Denne oppgaven er en bacheloroppgave i studiet Bachelor i Digital forretningsutvikling ved Institutt for datateknologi og informatikk NTNU, og vil forsøke å belyse et tema tilhørende den overordnede problemstillingen om hvordan anvendelse av IT på ulike måte kan skape gevinster for virksomheten.

Hvem er ansvarlig for forskningsprosjektet?
NTNU er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
I samråd sammen med vår veileder Steve Kawandami fant vi ut at du er en interessant og en aktuell person, og kan være en viktig informasjonskilde. Vi har valgt ut 10 personer med ulike stillinger, men som likevel er veldig relevante når det gjelder anskaffelsesprosessen. Vi håper at du ønsker å dele dine erfaringer og din kunnskap sammen med oss, slik at vi får til å lage et best mulig produkt for dere

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du blir intervjuet. Det vil ta deg ca. 45 minutter. Intervjuet inneholder spørsmål om dagens ansakffelsprosses og hvordan vi evt. kan forbedre denne prosessen. Dine svar fra intervjuet vil bli tatt opp med bånd, og slettet innen 01.06.2022

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- *Ved behandlingsansvarlig institusjon vil prosjektgruppe og veileder ha tilgang.*
- *Lydopptak ved intervjuer vil lagres på sikret nettverk/digital plattform der NTNU har databehandleravtale*

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 1.6.2022. *Personopplysninger og lydopptak slettes ved prosjektslutt.*

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- NTNU ved Leif Erik Opland (leif.e.opland@ntnu.no).
- Vårt personvernombud: Thomas Helgesen.
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Torstein Hjelle — *Anette Steinbråten & Nikolija Maksic*

Veileder — Bachelorstudenter

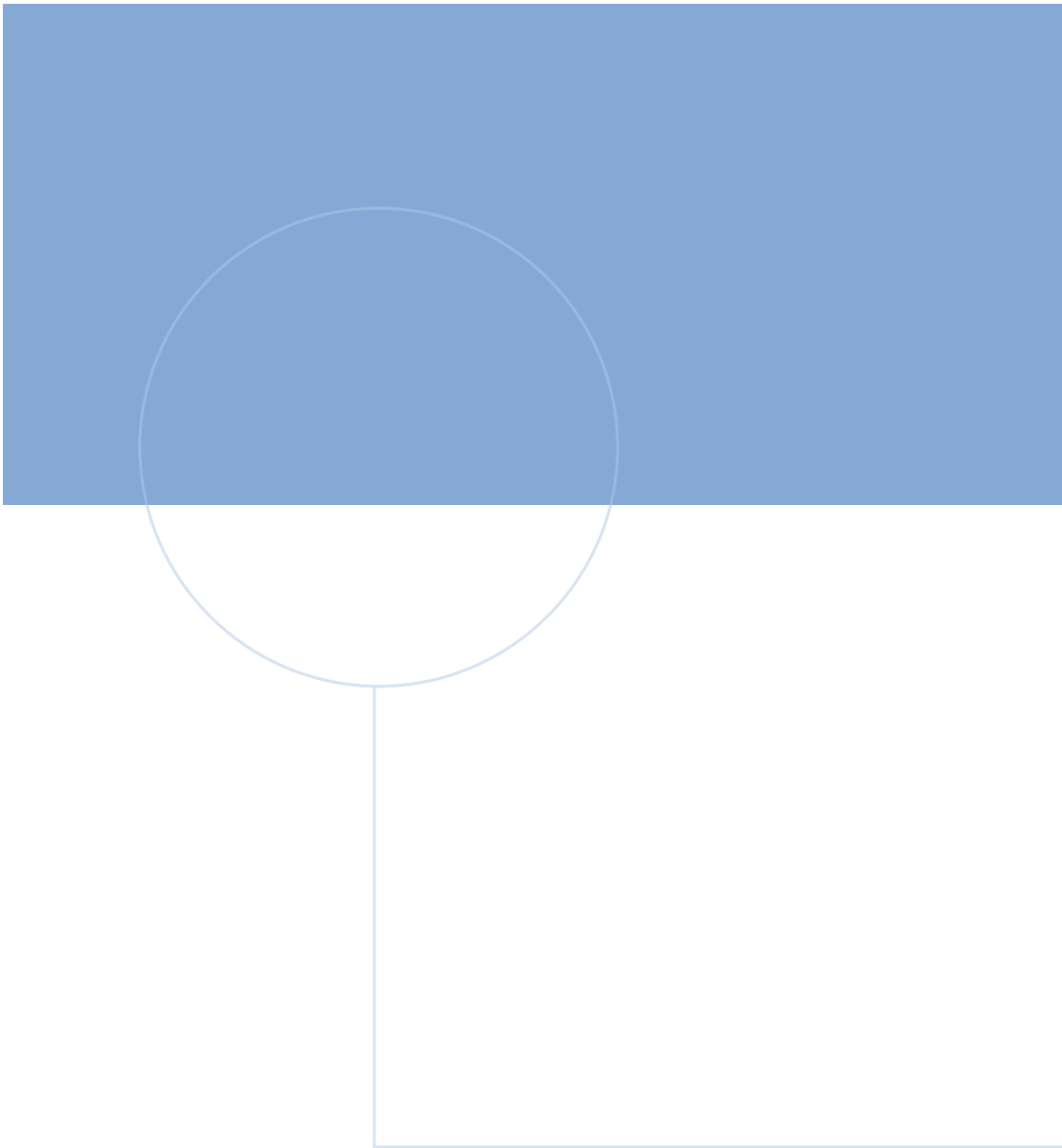
Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Digital forretningsutvikling*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju med lydopptak

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet 1.6.2022

(Signert av prosjektdeltaker, dato)



NTNU

Kunnskap for en bedre verden