Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2021 Åpen / ~~Konfidensiell~~
Forfatter: Camilla Smedhaug	
Fagansvarlig: Sissel H. Jore **Veileder:** Sissel H. Jore	
Tittel på masteroppgaven: Er sikkerhetskulturen god nok? - En kvalitativ studie av sikkerhetskulturen i Bergen kommune **Engelsk tittel:** Is the safety culture good enough? - A qualitative study of the safety culture in Bergen municipality	
Studiepoeng: 30	
Emneord: Digital sikkerhet, Bergen kommune, digitalisering, personopplysninger, personvern, informasjonssikkerhet, kultur, sikkerhetskultur, safety og security, forsvarlig håndtering	Sidetall: 85 + vedlegg/annet: 105 Stavanger, 14 juni 2021

Er sikkerhetskulturen god nok?

- En kvalitativ studie av sikkerhetskulturen i Bergen kommune

Universitetet i Stavanger

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Juni 2021

Camilla Smedhaug

FORORD

Denne oppgaven markerer slutten på mastergradsutdanningen innen samfunnssikkerhet, og videre slutten på fem år som student ved Universitet i Stavanger. Oppgaveskrivingen har vært en lang og krevende prosess, men også en spennende og lærerik erfaring jeg ikke ville vært foruten. Kunnskapen jeg har tilegnet meg gjennom masterstudiet har gjort meg godt rustet for veien ut i arbeidslivet, som jeg gleder meg enormt til å ta fatt på!

Jeg vil først og fremst starte med å takke professor og veileder, Sissel H. Jore, ved Universitetet i Stavanger. Tusen takk for konstruktive tilbakemeldinger, gode innspill og veiledningen jeg har fått under oppgaveskrivingen.

En stor takk går også til informantene fra Bergen kommune, som i en travel arbeidshverdag har tatt seg tid til å stille opp på intervjuer. Uten dere hadde ikke oppgaven blitt det samme! Takk for åpenheten, og takk for at jeg fikk låne litt av tiden deres.

Jeg vil også rette en stor takk til medstudenter, venner og familie. Takk for tålmodigheten, oppmuntringen og motivasjonen det siste halve året. Dere har alle vært en uvurderlig støtte. En spesielt stor takk går til mamma og pappa. Takk for alt dere gjør for meg, takk for all støtte og takk for at dere siden studiestart har oppmuntret og presset meg til å fullføre.

Stavanger, 14 juni 2021

Camilla Smedhaug

SAMMENDRAG

Hverdagen vår blir stadig mer digital, og gjør at det stilles nye krav til aktører som forvalter og håndterer sensitiv informasjon om oss. Som innbygger skal vi være trygge på at kommunen tilrettelegger for en forsvarlig håndtering av personopplysninger, og videre at håndteringen følger lovverket, gjeldende rutiner og retningslinjer. Hva skjer når en kommune ikke klarer å ivareta dette ansvaret og tilliten som den er tillagt? I praksis vet vi som innbygger lite om hvordan dette arbeidet foregår. Hvordan jobber kommunen med ivaretakelsen av personopplysninger for å sikre personvernet? Hvordan kan vi som innbygger være trygg på at kommunen gjør den jobben de er pålagt? Finnes det et bedre utgangspunkt som i høyere grad kan sikre våre personopplysninger?

Denne oppgaven er en studie av hvordan Bergen kommune jobber med sikkerhetskultur og hvorvidt denne danner et godt utgangspunkt for arbeidet kommunen gjør tilknyttet personopplysninger og personvern. De siste fire årene har kommunen stått i sentrum av to hendelser som innebærer alvorlige overtredelser i håndtering av personopplysninger. Hendelsene viste hvor sårbare slike opplysninger kan være, og hvor alvorlig mangelfull håndtering kan være for innbyggerne. Oppgaven sin problemstilling lyder dermed som følger: *«Hvordan kan Bergen kommune sitt arbeid med sikkerhetskultur tilrettelegge for forsvarlig håndtering av personopplysninger?*

Oppgaven har en kvalitativ tilnærming hvor dokumenter og intervjuer danner datagrunnlaget. Det er gjennomført kvalitative innholdsanalyser av flere kommunale dokumenter, i tillegg til at det er gjennomført seks kvalitative intervjuer med informanter fra Bergen kommune. Det teoretiske rammeverket inkluderer teori om kultur og subkultur, organisasjonskultur, kultur i sammenheng med safety og security, og sikkerhetskultur.

Resultater fra studien viser at Bergen kommune har en aktiv tilnærming til sikkerhetskultur og jobber med å forankre denne i hele organisasjonen. Dette setter et godt utgangspunkt for håndtering av personopplysninger, og kommunen viser videre en evne til å «tenke utenfor boksen». Likevel er det svakheter med kommunens arbeid; kompetanse, manglende avviksrapportering og dårlig ledelsesforankring kan svekke sikkerhetskulturens formål, og dermed lede til mangelfull håndtering av personopplysninger.

Studiens konklusjon er at kommunen har dannet et godt grunnlag for arbeidet videre med en sikkerhetskultur som tilrettelegger for god håndtering av personopplysninger. Likevel har kommunen fortsatt arbeid som gjenstår og utfordringer som må håndteres. Slik kan hendelsene kommunen var involvert i fra 2018 til 2019 ha vært en viktig påminnelse om at en sikkerhetskultur som tilstrekkelig legger til rette for at ansatte skal forsvarlig kunne håndtere personopplysninger, behøver økt fokus i kommunal sektor.

Liste over forkortelser

Forkortelser	Forklaring
API	Avdeling for personvern og informasjonssikkerhet
FD	Forsvarsdepartementet
Digdir	Digitaliseringsdirektoratet
GDPR	General Data Protection Regulation
HRO	High Reliability Organization
IKT	Informasjons-og kommunikasjonsteknologi
JBD	Justis-og beredskapsdepartementet
KD	Kunnskapsdepartementet
KMD	Kommunal-og moderniseringsdepartementet
Meld. St.	Meldinger til Stortinget
NSD	Norsk senter for forskningsdata
NSM	Nasjonal sikkerhetsmyndighet
ROS	Risiko-og sårbarhet

Oversikt over figurer

Oversikt over tabeller

Liste over definisjoner

Digitalisering: Innebærer «... det å legge til rette for generalisering av digital informasjon samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi» (Dvergsdal, 2019).

Informasjonssikkerhet: Ivaretakelse av alle former for informasjon og følgelig sikre at dens konfidensialitet, integritet eller tilgjengelighet ikke brytes (Digdir, u.å.-a).

Kultur: Et «fellesskap av ideer, verdier og normer som en gruppe mennesker deler, og som de prøver å overføre til den neste generasjonen» (Bergsjø et al., 2020, s. 34).

Personopplysninger: Enhver opplysning som direkte kan knyttes til, eller brukes for å identifisere et individ (Datatilsynet, 2019b)

Personvern: Ethvert menneskets rett til privatliv, familieliv, sitt hjem og sin kommunikasjon, samt retten til å råde over egne personopplysninger (Datatilsynet, 2019c).

Risiko: Refererer til den todimensjonale kombinasjonen av hendelser/konsekvenser og tilhørende usikkerheter (vil hendelsene inntreffe, hva blir konsekvensene) (Aven & Renn, 2010, s. 2).

Safety: Frihet fra fare og skade. Knyttes til handlinger gjort uten en ondsinnet hensikt, som for eksempel uhell, feil og ulykker (Smith & Brooks, 2013, s. 9).

Security: Farer tilknyttet rasjonelle mennesker med en ondsinnet hensikt, som for eksempel sabotasje eller terrorisme (Ale, 2009, s. 12).

Sikkerhetskultur: «The product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures» (ACSNI, 1993, i Antonsen, 2009b, s. 16).

Sårbarhet: «Sårbarhet er manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon eller hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden» (Njå et al., 2020, s. 52).

Tillit: Tillit kan beskrives som «En tilstand der man aksepterer sårbarheter basert på positive forventninger til intensjonen til en annen» (Engen et al., 2016).

Usikkerhet: «I *fortid* handler usikkerhet om hva som har blitt observert, gjenkjent, fortolket og gitt en underliggende forståelse. I *fremtiden* handler usikkerhet om hva som vil skje. I fremtiden eksisterer usikkerhet, men denne usikkerheten kan ikke reduseres eller måles» (Njå, 2020, s. 49).

Uønsket hendelse: «Hendelse eller tilstand som kan medføre skade på mennesker, miljø, materiell eller annen form for økonomisk tap» (NS 5814, ISO 14 001: 1996, i Vatnelid, 2018, s. 124).

Innholdsfortegnelse

1. Introduksjon

1.1 Presentasjon av tema

«Vi har fått et skikkelig varsku. Systemene som skal sikre informasjonssikkerhet og personvern er ikke gode nok» (Jansen, 2019). Dette sa Trine Skei Grande i 2019 om Vigilo-saken hvor Bergen kommune stod i sentrum av en skandale som sendte sjokkbølger gjennom kommune-Norge. Under implementeringen av den nye kommunikasjonsløsningen, Vigilo, ble personopplysninger til flere familier tilgjengeliggjort for andre som ikke skulle hatt tilgang. Flere familier opplevde at en tidligere samboer uten foreldrerett fikk innsyn i personlige opplysninger. For en annen mor ble opplysningene gjort synlig for en voldelig ekssamboer som familien var skjermet fra, ved å bo på hemmelig adresse (Jansen et al., 2020). Saken fikk av denne grunn særdeles stor oppmerksomhet i det norske mediebildet.

I mars 2020 startet Bergen kommune en omfattende utbedring av sine digitale systemer, referert til som Helhetlig Gjennomgang. Gjennomgangen avdekket en rekke kritiske mangler, særlig knyttet til informasjonssikkerhet og personvern. I tråd med dette ble manglende kompetanse, manglende kapasitet og et økt fokus på sikkerhetskultur trukket frem som særlige viktige forbedringspunkt for kommunen (Bergen kommune, 2020b, s. 7). Som oppgavens teorikapittel gjør rede for, blir det stadig viktigere for organisasjoner å ha en helhetlig tilnærming til sikkerhet som favner om alle ansatte. Særlig i arbeidet med digitalisering og det å ivareta digitale personopplysninger har dette utpekt seg som viktig, grunnet opplysningenes sårbarhet i en digital kontekst.

Ifølge Meld. St. 38 er det i dag høye forventninger knyttet til digitale tjenester. Tjenestene skal være robuste, motstå trusler, forsøk på misbruk, feil i utstyr og menneskelig svikt (Meld. St. 38 (2016-2017), s. 14). Meld. St. 38 formidler videre at en vellykket digitalisering forutsetter at personvernet ivaretas på en tilfredsstillende måte. Rollen som aktør og forvalter av personopplysninger blir dermed viktig fremover. «Det hviler et ansvar på de som samler og behandler personopplysninger, for å sikre at disse dataene ikke blir misbrukt eller kommer på avveie» (Meld. St. 38 (2016-2017), s. 15). Tillit til aktører som forvalter slike opplysninger, blir dernest en forutsetning for en vellykket digitalisering av samfunnet.

Å styre potensielle risikoer ved hjelp av ledelse og styring, opplæring, informasjon og sikkerhetskultur kan, ifølge Aven et al. (2004), være en løsning på utfordringer som kommunen

i dag møter i tilknytning til digitalisering og ivaretakelse av personvern (Aven et al., 2004, s. 32). En sikkerhetskultur utpeker seg som særlig viktig i dette arbeidet, da den:

> [...] defineres som et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet. Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, kan virksomheten skape en god sikkerhetskultur (NSM, u.å,).

I tråd med sitatet fra Trine Skei Grande, kan det derfor stilles spørsmål til hvorvidt det er systemene kommunen benytter er for dårlig, eller om det er kommunens forståelse for, og arbeid med sikkerhetskultur som hadde skyld i Vigilo-saken. Oppgavens formål er dermed å undersøke hvordan Bergen kommune jobber med sikkerhetskultur for å tilrettelegge for sikker og forsvarlig håndtering av innbyggernes digitale personopplysninger.

1.2 Bakgrunn for valg av tema

1.2.1 Digitalisering i Bergen kommune

Å være digitalisert, innebærer «... det å legge til rette for generalisering av digital informasjon samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi» (Dvergsdal, 2019). Offentlig sektor har de siste årene vært preget av et overveiende fokus på å digitalisere, med mål om å skape brukervennlige og effektive tjenester for innbyggerne (Meld.St. 27 (2015-2016), s. 11). Digitalisering forstås dermed ikke bare som en metode for å skape effektive og nyttige tjenester i samfunnet, men også som en forutsetning for å opprettholde Bergen kommune sin status som relevant samfunnsaktør.

Arbeidet rundt digitalisering har således ført til en rekke endringer og omstruktureringer i kommunen. I tråd med dette må ansatte i kommunen forholde seg til nye regler, rutiner og retningslinjer som kan lede til komplekse og utfordrende arbeidshverdager. Dette kan knyttes særlig opp til betydningen av informasjonssikkerhet og personvern, et fagområde som kontinuerlig er i endring. For å takle de utfordringene som digitaliseringen medbringer, kan kommunen ha nytte av en felles forståelse tilknyttet hva ansattes arbeidsoppgaver og ansvarsområde er, og som sørger for at arbeidet gjøres i tråd med kommunens mål og verdier.

1.2.2 Utfordringer med digitaliseringen

Offentlig sektor er en av de sektorene som sysselsetter flest mennesker i Norge. Bare i Bergen kommune er det ca. 19 000 ansatte som jobber fast (Bergen kommune, u.å.). Å digitalisere en sektor av denne størrelsen er dermed et stort og omfattende prosjekt, som ikke vært foruten utfordringer. Hva er digitalisert nok? Stilles det like krav for alle seksjonene i offentlig sektor? Hvem har ansvaret for innbyggernes digitale sikkerhet? Hvordan sørger kommunen for at ansatte jobber etter gjeldende regler og retningslinjer? Hvem har skyld dersom det skjer brudd i personvern og informasjonssikkerhet?

Andre utfordringer retter seg særlig mot manglende kompetanse, som pekt på av KMD i digitaliseringsstrategien for offentlig sektor (KMD, 2019a, s. 26), men også av Bergen kommune selv i etterkant av Helhetlig Gjennomgang. Dette kan også kobles til den raske utviklingen av teknologiske systemer.

1.2.3 Personvernets rolle i kommunen

Økt fokus på personvern og ivaretakelse av dette har vokst frem som et viktig fokusområde i offentlig sektor. I 2018 ble GDPR innført, og den nye Personopplysningsloven vedtatt. Hensikten var å sørge for at aktører tilstrekkelig skulle lyktes med å sikre menneskers privatliv, personopplysninger og videre stille krav til aktører som behandler slike opplysninger. Som rettsdisiplin er personvern forholdsvis ungt, men har i kjølevannet av den teknologiske utviklingen vokst frem som et særegent og viktig samfunnsområde (Wessel-Aas & Ødegaard, 2018, s. 19). Den teknologiske utviklingen har også ledet til at personopplysninger som regel omtales i en digital kontekst i dag.

Innførelsen av GDPR og den nye loven om personopplysninger i 2018 førte til at flere aktører var tvunget til å omstrukturere arbeidet med å sikre personopplysninger. I tråd med den teknologiske utviklingen blir arbeidet med å sikre slike opplysninger stadig mer komplekst og krevende. Teknologiske systemer og verktøy krever kunnskap, og riktig bruk forutsetter at ansatte har den kunnskapen som kreves for å håndtere systemene. Samtidig er det viktig at store aktører, som Bergen kommune, evner å følge utviklingen for å ikke miste sin rolle som samfunnsaktør. I dagens samfunn kan kommunens rolle dermed beskrives som et paradoks. På den ene siden kreves det at kommunen følger den teknologiske utviklingen og digitaliserer, samtidig som regelverk og retningslinjer for å håndtere personopplysninger i lys av

digitaliseringen gjør arbeidet mer komplekst. Bergsjø et al (2020) formidler at det er ikke teknologien i seg selv som truer personvernet, det er bruken av den (Bergsjø et al., 2020, s. 88).

For aktører som Bergen kommune, blir det dermed viktig å være innforstått med ansvaret kommunen har ovenfor innbyggerne knyttet til personvern, hva bruk av digitale systemer og verktøy kan medføre i form av sårbarheter, risikoer og konsekvenser.

1.2.4 Eksempler på brudd på personvern og informasjonssikkerhet i kommunen

Fra Vigilo ble valgt som leverandør i slutten av 2018 og frem til systemet ble stengt høsten 2019, har flere avgjørelser tilknyttet prosjektet vært utsatt for kritikk. Særlig kritisert er arbeidet som ble gjort i forbindelse med innlesing av persondata (personopplysninger) om barn med tilhørende familieforhold. Kort tid etter den første innlesningen ble det rapportert tilbake fra foresatte om klare brudd på personvernet. Kommunen foretok justeringer i arbeidet, men fortsatte innlesingen utover høsten 2019 (Jansen et al., 2020). Ikke før i oktober trakk kommunen i nødbremsen og stengte ned Vigilo. Etter en gjennomgang av saken trakk Seksjon for Internkontroll frem dårlig prosjektledelse, manglende oppfølging, manglende kompetanse og dårlig avviksrapportering som grunner til hvorfor prosjektet mislyktes (Seksjon for internkontroll, 2019).

Et år før Vigilo-saken utspilte seg, stod Bergen kommune i sentrum av en annen hendelse som også reiste en rekke spørsmål til den digitale sikkerheten i kommunen og arbeidet ivaretakelsen av innbyggernes personopplysninger. En datakyndig barneskoleelev fant et sikkerhetshull på en av kommunens nettsider, hvor personopplysninger om ca. 30 000 elever og lærere i grunnskolen i Bergen lå tilgjengelig (NTB & Nilsen, 2018). Da det første varselet til kommunen og skoleledelsen ikke ble fulgt opp, valgte eleven å sende ut en e-post i rektors navn, hvor kommunens systemer og IKT-sikkerhet ble kritisert og latterliggjort. Kommunen svarte med å sende politiet på døren til eleven, og beslagla elevens datautstyr. Politiet registrerte også en anmeldelse på gutten fra kommunen, men denne ble senere trukket (Opheim, 2018).

For hendelsen fikk Bergen kommune en bot på 1.6 millioner kroner (Datatilsynet, 2019a), og for Vigilo-saken ble kommunen ilagt en bot på 3 millioner kroner (Datatilsynet, 2020).

1.3 Litteraturgjennomgang

Det finnes flere publikasjoner som tar for seg hvordan offentlig sektor skal arbeide mot en mer digital hverdag, hva som kreves for å nå dette målet og hvordan lover og regelverk skal ivaretas i dette arbeidet. Dette kan sees i sammenheng med en økende etterspørsel og interesse for å bruke digitale løsninger i offentlig sektor, samt nye utfordringer og problemstillinger som oppstår i tilknytning til digitaliseringsarbeidet.

Digital agenda for Norge

En transformasjon av den norske IKT-politikken ble presentert i «Digital agenda for Norge» (Meld.St. 27 (2015-2016)). Formålet med Meld. St. var å belyse utfordringer offentlig sektor og næringsliv stod ovenfor vedrørende produktivitet, omstilling og effektivisering rundt digitalisering. Målet var en samlet og brukervennlig forvaltning, hvor verdiskapning og deltakelse for alle stod i sentrum. Bakgrunnen for meldingen var ambisjonen om «å fornye, forenkle og forbedre offentlig sektor, samtidig som innbyggere og næringsliv har forventninger om en enklere hverdag» (Meld.St. 27 (2015-2016), s. 11).

Digitaliseringsstrategi for offentlig sektor 2019-2025

Formålet med den nye digitaliseringsstrategien var å videreføre arbeidet som ble startet av «Digital agenda for Norge», og de to rapportene har av den grunn samme målsetning. Dette skal nås ved å effektivisere hvordan ressursene brukes i offentlige virksomheter og samtidig tilrettelegge for å øke produktiviteten i samfunnet (KMD, 2019a, s. 3). Digitaliseringsstrategien peker også på nye utfordringer knyttet til digitaliseringen av offentlig sektor, og trekker frem betydningen av arbeid med informasjonssikkerhet og personvern. Rapporten går noe inn på viktigheten av digital sikkerhet, men sier så lite om rollen dette kan ha i arbeidet med digitalisering i for eksempel kommunene i Norge.

Nasjonal strategi for digital sikkerhet

I strategidokumentet utgitt i 2019 vektlegges betydningen av digital sikkerhet, og det understrekes at dette vil være et område regjeringen fremover vil prioritere høyt (JBD & FD, 2019). Med rapporten ønsker regjeringen å oppnå et felles grunnlag for forståelse og håndtering av utfordringer knyttet til digitalisering og sikkerhet i offentlig sektor. Videre henvender rapporten seg særlig til privat-og kommunal sektor, noe tidligere rapporter ikke har gjort (JBD & FD, 2019, s. I).

Nasjonal strategi for digital sikkerhetskompetanse

Dokumentet fungerer som en utdypelse og komplettering av «Nasjonal strategi for digital sikkerhet». Regjeringen fremhever betydningen av kompetanseområdet, og beskriver digital sikkerhetskompetanse som et prioritert område. «En forutsetning for trygg bruk av IKT er tilstrekkelig digital sikkerhetskompetanse på alle samfunnsnivåer [...]» (JBD & KD, 2019, s. 3). Rapporten formidler at digitale ferdigheter i dagens samfunn er grunnleggende, og bør betraktes på lik linje med lesing, skriving og regning (JBD & KD, 2019, s. 4 og 7).

Undersøkelser gjort av NSM viste et klart forbedringspotensial blant flere virksomheter vedrørende sikkerhetsbevissthet og sikkerhetskompetanse. Videre viste undersøkelsene at virksomheter ikke prioriterer arbeid som omfatter sikkerhet som en total del av styringen og at «Ledelsen vet derfor heller ikke hvilken risiko de tar på vegne av virksomheten» (NSM, 2017 s. 19).

IKT-sikkerhetskompetanse i arbeidslivet: behov og tilbud

Rapporten er en studie rettet mot å undersøke behovet for, og tilgang til IKT-sikkerhetskompetanse på alle samfunnsnivåer i Norge. Basert på to delstudier konkluderer rapporten med at innen en ti-års periode vil det foreligge en mangel på rundt 15 000 personer med tilstrekkelig IKT-sikkerhetskompetanse som dekker markedets etterspørsel (Mark et al., 2017, s. 7). Antall studenter som fullfører høyere utdanning innenfor fagfeltet har de siste årene økt, men rapporten kan ikke svare på hvorvidt dette vil være nok til å dekke inn den forventede etterspørselen fremover (Mark et al., 2017, s. 8).

De overnevnte publikasjonene tar for seg det svært relevante arbeidet med digitalisering av offentlig sektor i Norge. Publikasjonene viser til planlagte mål for digitalisering av offentlig sektor og strategier for å nå disse. Litteraturen som henvender seg til kommunal sektor oppleves som manglende, da særlig publikasjoner som tar for seg arbeidet med å sikre tilstrekkelig personvern og setter dette i kontekst med betydningen av sikkerhetskultur.
Dette ble således avgjørende i valg av tema og problemstilling.

1.4 Presentasjon av problemstilling

I tråd med hvordan sikkerhetskultur defineres av NSM, har oppgaven som formål å trekke linjer mellom dette og arbeidet Bergen kommune skal gjøre med å ivareta innbyggernes

personopplysninger på en trygg og forsvarlig måte. For å undersøke om kommunens arbeid er i tråd med de forventinger og retningslinjer som stilles, er det således behov for å gå i dybden på kommunen som organisasjon.

For å belyse oppgavens tema har jeg undersøkt flere faglige områder i kommunen, som er relevant for det å skape en sikkerhetskultur. Jeg har synliggjort arbeidet kommunen gjør med digitalisering og trukket frem utfordringer med denne. Videre er personvern og ivaretakelse av personopplysninger i kommunen undersøkt, og det skal trekkes linjer mellom dette og hvordan en sikkerhetskultur kan tilrettelegge for håndtering av personopplysninger. For å skape en dybde rundt hvordan kommunen tilnærmer seg sikkerhetskultur er skal det følgelig undersøkes hvorvidt kommunens arbeid med risiko og sårbarheter er av betydning for kulturutformingen. Arbeid med personopplysninger blir stadig mer komplekst og utfordrende, og det er derav nødvendig at kommunen klarer å ivareta de oppgavene og ansvaret de er tillagt. Problemstillingen lyder dermed som følger:

«Hvordan kan Bergen kommune sitt arbeid med sikkerhetskultur tilrettelegge for forsvarlig håndtering av digitale personopplysninger?»

For å kunne forstå hvordan kommunen arbeider med dette, er det tillagt tre forskningsspørsmål med hensikt å gi forskningen mer dybde. Forskningsspørsmålene vil belyse hvordan kommunen arbeider med sikkerhetskultur, hva kommunen anser som forsvarlig håndtering av personopplysninger, hvilken tilnærming til sikkerhet kommunens sikkerhetskultur har og hvorvidt kommunen er tjent med denne tilnærmingen. Sammen vil dette danne et grunnlag for å besvare oppgavens problemstilling. De tre forskningsspørsmålene er følgende:

1. **Hvordan jobber Bergen kommune med sikkerhetskultur i forhold til personvern?**
2. **Hva kjennetegner en sikker og forsvarlig håndtering av digitale personopplysninger ifølge Bergen kommune?**
3. **Hvilken tilnærming til sikkerhet danner det beste utgangspunktet for håndtering av personopplysninger?**

1.5 Avgrensning

Problemstillingen er utformet på bakgrunn av hendelsene kommunen var en del av i henholdsvis 2018 og 2019, da de innebærer tydelige brudd på retningslinjer og lovverk knyttet til håndtering av personopplysninger. Hendelsene skal ikke undersøkes videre, men er inkludert for å insinuere aktuelle problemstillinger som kan forekomme fremover, og viser dermed betydningen av arbeidet med sikkerhetskultur i en organisasjon og særlig blant en relevant samfunnsaktør, som Bergen kommune.

Flere av systemene Bergen kommune bruker er svært tekniske og består av mange komponenter. Å vurdere kommunens digitale systemer faller dermed utenfor oppgavens formål, og egen kunnskap. I den grad det henvises til kommunens digitale systemer gjelder dette kommunens kvalitetssystem, BkKvalitet, som blant annet brukes av ansatte for å gjøre ROS-analyser og melde inn avvik. Vurderingen av kommunens sikkerhetskultur vil således ikke inkludere en vurdering av systemene i seg selv, men bruken av dem vil inngå som en naturlig del av arbeidshverdagen til ansatte, og kan videre være aktuell å inkludere som en del av sikkerhetskulturen.

Hvordan kommunen arbeider for å etterleve sikkerhetskulturen utover i organisasjonen, undersøkes ikke. Oppgaven er begrenset til å undersøke hvordan ansatte tilknyttet til prosjekter, API og Samfunnssikkerhetenes hus forstår og tolker sikkerhetskultur i kommunen, og hvorvidt arbeidet tilknyttet personopplysninger og personvern har en sammenheng med denne.

1.5.1 Empirisk avgrensing

Oppgaven er begrenset til en kvalitativ innholdsanalyse av kommunale dokumenter, samt seks kvalitative intervjuer av ansatte i Bergen kommune. Dette betyr at oppgavens resultater ikke kan generaliseres på lik linje med resultater gjort av kvantitative undersøkelser. Dersom samtlige ansatte i kommunen blir intervjuet om oppgavens tema og alle relevante kommunale dokumenter belyses, er det dermed sannsynlig at dette kan formidle et annet resultat enn det som presenteres i denne oppgaven.

Datagrunnlaget er også begrenset i forhold til oppgavens tema. Sikkerhetskultur og dens innvirkning på arbeid tilknyttet digitalisering og personvern er bare et av mange områder som

kan undersøkes i kommunen. Risikobildet er stort og komplekst, og kommune-Norge står av den grunn ovenfor en rekke trusler som fremover kan påvirke arbeidet kommunen gjør.
En del av datagrunnlaget er også begrenset til informantenes egen oppfattelse og forståelse av arbeidet kommunen gjør i praksis. Dette er videre drøftet i delkapittel 3.6.2 (Metodiske styrker og svakheter).

1.6 Oppgavens struktur

Fokusområde	
1: Innledning	Presentasjon av tema og bakgrunn for oppgaven. Videre vil oppgavens problemstilling med tilhørende forskningsspørsmål presenteres. Avslutningsvis vil avgrensinger knyttet til oppgavens omfang, samt empiriske avgrensninger presenteres.
2: Teoretisk grunnlag	Kapittelet vil innledningsvis ta for seg relevant terminologiforståelse tilknyttet enkelte begreper som er av betydning for oppgaven. Videre vil teori knyttet til kultur, subkultur og organisasjonskultur presenteres, før teori om sikkerhetskultur gjøres rede for.
3: Metode	Gjør rede for metodiske valg knyttet til oppgaven. Metodisk tilnærming skal redegjøres for, metode for innsamling av data skal forklares, og dette skal videre drøftes opp mot kvalitetspremissene for *trustworthiness*. Avslutningsvis skal metodiske styrker og svakheter gjennomgås, samt etiske vurderinger knyttet til innhenting og vurdering av data.
4: Empiriske funn	Empiriske funn blir systematisk gjort rede for, og kategorisert etter forskningsspørsmål og tematisk relevans.
5: Analyse og drøfting	Empiriske funn skal analyseres og drøftes opp mot oppgavens teoretiske grunnlag. Analysen og drøftingen vil således kunne besvare oppgavens tre forskningsspørsmål.
6: Konklusjon	Oppgavens siste del vil oppsummere viktige funn og konklusjoner tilknyttet forskningsspørsmålene. Samlet vil dette gi en konklusjon på oppgavens problemstilling. Avslutningsvis skal det gjøres rede for forslag til videre forskning.

7: Referanseliste	Kapittelet viser en litteraturliste over referanser brukt i oppgaven.
Vedlegg	Oversikt over vedlegg brukt i oppgaven

Tabell 1: Oppgavens struktur

2. Teoretisk grunnlag

Det følgende kapittelet vil danne det teoretiske rammeverket for oppgaven. Første delkapittel vil ta for seg terminologiforståelse, en utdypende definisjon av særlig relevante begrep for oppgaven. Videre vil de ulike teoriene som brukes i oppgaven presenteres, herunder teori om safety og security, teori om kultur, subkultur og organisasjonskultur, samt teori knyttet til sikkerhetskultur.

De ulike teoriene i kombinasjon med terminologiforståelsen vil således gi en indikasjon rundt de ulike konseptene for oppgaven, og vil dermed være praktisk for å forstå oppgavens forskningsspørsmål, hvordan oppgavens funn blir presentert, og videre hvordan funnene analyseres og drøftes.

2.1 Terminologiforståelse

Personopplysninger og personvern

En personopplysning er enhver opplysning eller vurdering som kan knyttes til, og brukes for å identifisere en enkeltperson. Herunder faller opplysninger som for eksempel navn, adresse, telefonnummer, fødselsnummer, bilder (dersom personer kan gjenkjennes), lydopptak, e-postadresse og IP-adresse (Datatilsynet, 2019b: Bergen kommune, 2021b, s. 7: Seksjon for internkontroll, 2019, s. 10). Det skilles mellom personopplysninger, og det Datatilsynet beskriver om særlige kategorier av personopplysninger. Dette gjelder opplysninger som blant annet etnisk opprinnelse, religion, politisk oppfatning og seksuell legning (Datatilsynet, 2019b).

Personvern beskriver et hvert menneskets rett til privatliv. «Som enkeltmenneske har du derfor på en privat sfære som du selv kontrollerer, hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker» (Datatilsynet, 2019c). Som menneske har du altså en rett til å kunne bestemme og råde over egne personopplysninger, informasjon om hvem som forvalter slike opplysninger og hva formålet med bruken av opplysningene er (KMD, 2019b). Denne rettigheten ble ytterligere styrket i etterkant av innføringen av GDPR i 2018 (Datatilsynet,

2019c). KMD formidler blant annet at innenfor personvern står «[...] det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred sentralt» (KMD, 2019b).

Informasjonssikkerhet

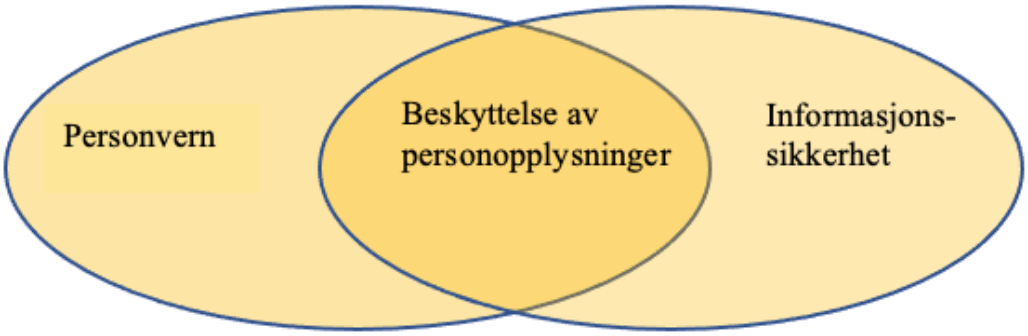
I organisatorisk sammenheng knyttes stadig personvern til informasjonssikkerhet. Ifølge Digdir handler informasjonssikkerhet om å sikre alle former for informasjon. Dette innebærer at informasjon:

- «ikke blir kjent for uvedkommende (**konfidensialitet**)»
- «ikke blir endret utilsiktet eller av uvedkommende (**integritet**)»
- «er tilgjengelig ved behov (**tilgjengelighet**)» (Digdir, u.å.-a).

Dette fremkommer også i «Reglement for informasjonssikkerhet og personvern», som formidler at informasjonssikkerhet skal ivareta og beskytte alle former for informasjon, og sikre at den ikke bryter med prinsippene for konfidensialitet, integritet og tilgjengelighet (Bergen kommune, 2020c, s. 6). Det formidles videre av Digdir, at informasjonssikkerhet brukes synonymt med digital sikkerhet, cybersikkerhet og IKT-sikkerhet (Digdir, u.å.-b).

Som organisasjon og forvalter av personopplysninger er det dermed svært viktig at Bergen kommune klarer å sikre de opplysningene (som forvaltes). Ifølge Digdir kan dette med fordel kan gjøres ved å identifisere hvilke risikoer som kan være en trussel for personopplysningene og videre vurdere hvilke tiltak som kan iverksettes for å redusere de ulike risikoene (Digdir, u.å.-b). Således blir arbeidet med å skape en kultur i organisasjonen viktig for å ivareta det ansvaret og forventingene som stilles til samfunnsaktører.

I denne oppgaven vil informasjonssikkerhet forstås som et naturlig forlenget ledd i arbeidet Bergen kommune gjør med å sikre innbyggernes personopplysninger og personvern som vist til i figuren under.



Figur 1: Forholdet mellom personvern og informasjonssikkerhet

(Bergen kommune, 2020c, s. 6)

Risiko

Ifølge Aven & Renn (2010) finnes det ikke én akseptert definisjon av risiko, og begrepet brukes av den grunn ulikt på tvers av fagdisipliner.

Njå et al. (2020) definerer risiko som «... et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall» (Njå et al., 2020, s. 46). Risiko handler således om en vurdering, og innenfor sikkerhetsfaget knyttes denne vurderingen til verdier, menneskeliv, omdømme, økonomi eller klima, og omtales som risikovurderinger eller ROS-analyser. Forfatterne vektlegger også usikkerhet i forbindelse med risiko. Tilstedeværelsen av usikkerhet gjør det umulig å forberede, planlegge eller konsekvensvurdere alle faktorer tilknyttet risikoer, og det er således viktig at dette blir tatt høyde for i arbeidet med risiko (Njå et al., 2020, s. 47).

Engen et al (2016) formidler at «risiko er produktet av sannsynlighet og konsekvens» (Engen et al., 2016, s. 78). Aven & Renn (2010) beskriver risiko som «Risk is equal to the two-dimensional combination of events/consequences and associated uncertainties (will the events occur, what will be the consequences) (Aven & Renn, 2010, s. 2). I likhet med Njå et al (2020) sin definisjon, inkluderer Aven & Renn (2010) usikkerhet som faktor, i motsetning til definisjonen presentert av Engen et al. (2016). Rosa (1998) definerer risiko som «Risk is a situation or event where something of human value (includinghumans themselves) is at stake and where the outcome is uncertain» (Rosa, 1998, s. 28). Her kan det også trekkes linjer til Aven & Renn (2010) sin definisjon, samtidig som Rosa (1998) trekker frem verdier i form av *hva* som står på spill.

I oppgaven forstås risiko i forbindelse med kommunens arbeid mot å forhindre at personopplysninger kommer på avveie og brudd i informasjonssikkerheten. Hvordan kommunen forholder seg til risiko og arbeid med å vurdere risikoer vil også være relevant å undersøke i tilknytning til kommunens arbeid med å forme en sikkerhetskultur.

Sårbarhet

«I praksis er sårbarhet vanskelig å måle i en organisasjon fordi definisjoner av begrepet ikke retter seg mot størrelser eller målbare dimensjoner» (Njå et al., 2020, s. 52). Sårbarhet blir dermed et begrep som ikke nødvendigvis aktivt brukes i organisasjoners arbeid, ifølge Njå et al. (2020). Forfatterne har valgt å definere det som «Sårbarhet er manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon eller hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden» (Njå et al., 2020, s. 52).

Engen et al. (2016) definerer sårbarhet som «[...] et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse» (Engen et al., 2016, s. 47). Forfatterne utdyper videre hva som tillegges en teknologisk sårbarhet og beskriver dette som en «[...] egenskap ved systemet som gjør at det mangler evnen til å gjenopprette funksjonaliteten hvis det blir utsatt for ytre påkjenninger» (Engen et al., 2016, s. 47).

Videre i oppgaven vil sårbarheter brukes for å beskrive ansattes egen oppfatning i forhold til hva som gjør kommunen sårbar i lys av den teknologiske utviklingen, og hvorvidt dette kan ha en innvirkning på hvordan kommunen håndterer og tilnærmer seg personopplysninger og personvern. Identifiserte sårbarheter vil således alltid være preget av en grad av usikkerhet, men arbeidet med å identifisere sårbarheter og planlegge for håndtering er likevel viktig i et helhetlig sikkerhetsarbeid. Knyttet til personvern og informasjonssikkerhet kan sårbarheter for eksempel være hendelser eller faktorer som truer opplysningenes konfidensialitet, integritet og tilgjengelighet.

2.2 Kultur

2.2.1 Hva er kultur?

Litteraturen viser til ulike definisjoner av, og forståelse for hva som menes med kultur. Det finnes dog ikke én akseptert definisjon i litteraturen, og begrepet brukes ulikt på tvers av fagdisipliner. Kultur kan innenfor samfunnsvitenskap beskrives som et «...fellesskap av ideer,

verdier og normer som en gruppe mennesker deler, og som de prøver å overføre til den neste generasjonen» (Bergsjø et al., 2020, s. 34).

Schein & Schein formidler at:

> The culture of a group can be defined as the accumulated shared learning of that group as it solves its problems of external adaption and internal integration; which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, feel, and behave in relation to those problems (Schein & Schein, 2017, s. 6).

Ved å vektlegge fellesskap, læring, persepsjon og verdier kan vi dermed forstå at ulike grupper i samfunnet skiller seg fra hverandre, men også at de innehar grunnleggende likheter. Slik er kultur en svært viktig del av ulike land og nasjoner, og fungerer således som et lim som binder innbyggerne sammen (Bergsjø et al., 2020, s. 34).

Engen et al. (2016) trekker frem en noe annen forståelse for kultur når begrepet knyttes til sikkerhet. «I kultur betraktes sikkerhet som delte tankemønstre og de administrative strukturene og ressursene som er knyttet til og støtter utviklingen av organisasjoners og systemers intelligens og forestillingsevne knyttet til farer og trusler» (Engen et al., 2016, s. 157). Her vektlegger forfatterne både organisasjoners forestillingsevne, men også de ulike systemene som inngår i en organisasjon. Sistnevnte blir således sentral når kommunen som organisasjon skal undersøkes videre. I lys av digitaliseringen kan kommunen beskrives som mer enn en organisasjon bestående av verdier, læring og holdninger. Kommunen består også av digitale systemer og verktøy som aktivt inngår som en del av arbeidshverdagen til ansatte. Dette må det følgelig tas høyde for.

Dette understøttes av Bergsjø et al. (2020) som definerer det forfatterne refererer til som *digital sikkerhetskultur*, nemlig «[...] de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier» (Bergsjø et al., 2020, s. 36). I en arbeidshverdag hvor ansatte i kommunen nærmest er totalt avhengig av digitale systemer og verktøy, kan det være viktig å trekke frem at digitale verdier også bør vektlegges når en kultur skal utformes.

I lys av oppgavens problemstilling og forskningsspørsmål blir det således nødvendig å vektlegge en forståelse av kultur som også griper om det materielle i en organisasjon, som digitale systemer og verktøy, og ikke bare det immaterielle som normer, holdninger og verdier. Det vil følgelig være nødvendig å definere hvorvidt Bergen kommune arbeider mot en egen kultur, eller mot en subkultur. Hvordan kulturen i Bergen kommune defineres og forstås av ansatte og kommunen selv, vil ha betydning for arbeidet som gjøres videre. Defineres den som en egen kultur er det rimelig å anta at arbeidet med å forstå, forbedre og implementere i høyere grad vil vektlegges og etterfølges, enn om den defineres som en subkultur.

2.2.2 Subkultur

Kulturer er som nevnt ovenfor sjeldent definert eksplisitt. Kulturelle verdier forstås og tolkes på ulike måter, og utvikler seg videre i *subkulturer,* hvor personlige faktorer som for eksempel interesser, kjønn og geografi spiller inn (Bergsjø et al., 2020, s. 35). Maanen & Barley (1983) beskriver subkulturer som ulike grupper som står ovenfor forskjellige problemer i samfunnet. I et forsøk på å takle eller overvinne problemene, utvikler gruppene forskjellige løsninger og fordeler seg dermed i ulike grupperinger (Maanen & Barley, 1983, s. 3).

Sander (2019) definerer subkultur på følgende måte «En begrenset kulturell gruppe som lever sammen som et identifiserbart segment innenfor et større og mer komplekst samfunn» (Sander, 2019). Dette samsvarer hva Martin (1992) formidler om subkulturer. Martin beskriver subkultur som en gruppe som ønsker å skape et sammenhengende meningssystem eller gi klare løsninger på problemer som en gruppe mennesker deler. Ifølge forfatteren gjør dermed subkultur en uforståelig kompleksitet om til en kompleksitet som er mer forståelig for en gruppe mennesker (Martin, 1992, s. 153).

Maanen & Barley (1983) formidler også en definisjon på hva som menes med en subkultur innad i en organisasjon. Ifølge forfatterne er dette en undergruppe av organisasjonens medlemmer som interagerer med hverandre regelmessig, som identifiserer seg selv som en distinkt gruppe i organisasjonen, som deler et sett med problemer som defineres som felles for alle, og som rutinemessig iverksetter tiltak på grunnlag av kollektive forståelser som er unike for den gruppen (Maanen & Barley, 1983, s. 12).

2.2.3 Organisasjonskultur

Ikke før i 1980 ble organisasjonskultur benyttet for å beskrive de felles normene, verdiene og virkelighetsoppfatningene som ansatte i en organisasjon deler (Sagberg, 2020). Det er i litteraturen diskutert hvorvidt sikkerhetskultur skal defineres som en egen kultur, eller om det er en subkultur som har utviklet seg fra organisasjonskultur. For å skape en bedre forståelse av hva sikkerhetskultur er, og hvordan vi kan forstå kulturen i Bergen kommune, er det derfor nødvendig og kort gjøre rede for hva som menes med organisasjonskultur.

Edgar Schein (1992) presenterte i 1992 en kjent definisjon på organisasjonskultur ved å beskrive den som «The way we do things around here» (Schein, 1992, s. 8-9). Ifølge Hopkins (2006) har alle organisasjoner en kultur (eller en rekke subkulturer), som har en innvirkning på sikkerhet (Hopkins, 2006, s. 876).

Trice & Beyer (1993) sin definisjon av organisasjonskultur sier «Organizational cultures, like other cultures, develop as groups struggle to make sense of and cope with their worlds» (Trice & Beyer, 1993, s. 4). Forfatterne forstår videre organisasjonskultur som et felles system av ideer, meninger og symboler som i fellesskap former kulturen.

James Reason skiller i «Managing the Risks of Organizational Accidents» mellom nasjonale og organisatoriske kulturer. Reason argumenterer for at nasjonale kulturer oppstår på bakgrunn av felles verdier og at organisatorisk kultur oppstår som et resultat av delt praksis mellom ansatte i en organisasjon (Reason, 1997, s. 192). Det er følgelig den organisatoriske forståelsen Reason følger videre i sin teori om sikkerhetskultur.

Oppsummert forstås dermed organisasjonskultur som et sett av felles verdier, meninger, normer, ideer og virkelighetsoppfatninger som deles av medlemmer av en organisasjon. I tråd med definisjonene og redegjørelsen for subkulturer redegjort for i delkapittelet over, vil sikkerhetskultur videre i denne oppgaven tolkes som en egen kultur, og ikke en subkultur som har utviklet seg fra organisasjonskulturen. Dette fordi ingen av de overnevnte definisjonene retter seg særlig mot sikkerhet. Videre samsvarer det med Maanen & Barley sin definisjon av subkultur i en organisatorisk sammenheng, som vektlegger at medlemmer identifiserer seg selv som en distinkt gruppe i organisasjonen. Sikkerhetskultur er følgelig en kultur en hel organisasjon bør etterstrebe, og ikke bare en gruppe av den.

2.3 Kultur i safety og security

Safety og security representerer to ulike tilnærminger til sikkerhet, og assosieres blant annet med frihet fra trusler og skader (Jore, 2020, s. 44). Innen sikkerhetsfaget skiller begrepene tradisjonelt sett mellom farer uten en ondsinnet hensikt (safety) og farer tilknyttet rasjonelle mennesker med en ondsinnet hensikt (security) (Jore, 2020, s. 43). Engen et al. (2016) formidler at de to tilnærmingene til sikkerhet skiller mellom «[...] sikkerhet som tilstand og sikkerhet som følelse» (Engen et al., 2016, s. 26).

Ifølge Smith & Brooks (2013) handler safety om frihet fra fare og skade. Forfatterne formidler videre at fordi security ikke er tilstrekkelig definert, mangler det litteratur og forskning som kan utvikle feltet videre (Smith & Brooks, 2013, s. 2). Security kan likevel defineres i henhold til konteksten den brukes i. Dette samsvarer med Ale (2009) som skiller mellom de to ved å assosiere safety til uhell og ulykker, mens security favner om handlinger gjort med en ondsinnet hensikt, som sabotasje og terrorisme (Ale, 2009, s. 12).

Omfanget av hendelser som faller under security er tidvis kompleks at det normalt sett ville vært vanskelig for en organisasjon og håndtere den alene. Slike hendelser forekommer også sjeldent og med lav frekvens. Spørsmålet blir da hvorvidt en organisasjon skal bruke tid og ressurser på en kultur som sikrer håndtering av slike hendelser, på lik linje med kulturen vi finner innenfor safety (Jore, 2020, s. 45).

Litteratur innen safety viser til at menneskelig hensikt jevnt kan knyttet til ulykker. Det er derfor nødvendig at organisasjoner evner å skape robuste løsninger som i og for seg tar høyde for at individer *kan* avvike fra standard prosedyrer og retningslinjer med vilje (Jore, 2020, s. 44). Dette påpeker også Jore ved å formidle at innenfor safety finnes det rasjonelle aktører som med vilje unngår å bruke riktig utstyr eller på andre måter tar snarveier som letter egen arbeidssituasjon (Jore, 2020, s. 45).

På grunnlag av dette assosieres tradisjonell sikkerhetskultur med safety. I tråd med definisjonene av kultur presenter ovenfor, favner tilnærmingen til sikkerhetskultur derfor i stor grad til det immaterielle aspektene ved kultur. Samtidig kan teknologiske systemer og digitale verktøy være sårbar ovenfor ansatte som bevisst velger å ta de enkle utveiene, i stedet for å gjøre arbeidet skikkelig, som formidlet av Jore (2020). Teknologi og digitale systemer har vist seg å være svært sårbare dersom feil begås, og det kan derfor være nødvendig å i større grad

etterstrebe en kultur som fokuserer på barrierer, konsekvensredusering og tilsiktede feil i større grad enn hva det gjøres nå.

Malcomson (2009) argumenterer for at det ikke eksisterer en akseptert definisjon av sikkerhetskultur. Av denne grunn finnes det heller ikke en akseptert metode for å måle sikkerhetskultur i en organisasjon på (Malcomson, 2009, i Jore, 2016, s. 471). I en rekke fagmiljøer er det gjort forsøk på å overføre de grunnleggende prinsippene for safety til security med et holistisk perspektiv, men fordi forskjellige sektorer er organisert og fungerer ulikt, har dette vært utfordrende å gjennomføre i praksis (Reniers et al., 2011, s. 1242).

Reiners et al. (2011) sitt argument går dog imot hva Kongsvik et al. (2018) formidler. Ifølge forfatterne er digitaliseringen av arbeidslivet er et eksempel på at de to tilnærmingene er i ferd med å vokse sammen (Kongsvik et al., 2018, s. 279). Avanserte systemer med kritiske funksjoner kan gjøre organisasjoner attraktive for angrep, hacking ol. (security), samtidig som systemene kan være sårbare for uskyldige feil og ulykker internt i organisasjonen (safety). Forfatterne formidler videre at dette skaper en arbeidshverdag hvor truslene og risikokildene ikke kan fjernes, og arbeidet med å «[...] bygge konsekvensreduserende barrierer og motstandskraft blir de viktigste virkemidlene» (Kongsvik et al., 2018, s. 280). Antonsen (2009a) ser en økende oppfatning av at den teknologiske og formelle organisasjonsstrukturen i en arbeidspraksis kan påvirke sikkerhet vel mye som den kulturelle konteksten (Antonsen, 2009a, s. 118).

Dette samsvarer med hva Kriaa et al (2015) formidler, om at safety og security kan ikke beskrives som gjensidig utelukkende, fordi de deler en rekke likheter. De fungerer således som to ulike tilnærming til sikkerhet, som gir gjensidig støtte til hverandre (Kriaa et al., 2015, s. 161). Dette fremkommer også i Jore (2020), som sier at safety og security bør forstås uavhengig av hverandre, men i praksis bør ikke de to tilnærmes ulikt (Jore, 2020, s. 43).

Dermed faller den tradisjonelle oppfattelsen av sikkerhetskultur utenfor den arbeidshverdagen til flere organisasjoner i dag, fordi den favner ikke i stor nok grad om de materielle aspektene ved kultur. I lys av definisjonene av kultur presentert ovenfor samt hvordan kultur oppfattes innenfor safety og security, kan det grunnleggende bruken av kultur som begrep videre problematiseres. Ifølge Antonsen (2009a) kan ikke kulturens innvirkning på sikkerhet kun

belyse kulturelle (immaterielle) aspekter alene. Antonsen formidler videre at et mer helhetlig perspektiv er nødvendig, som blant annet innebærer å legge vekt på samspillet mellom kulturelle (ideelle og uformelle), strukturelle (formelle regler og forskrifter) samt interaksjonelle (sosialt samspill) aspekter av arbeidet (Antonsen, 2009a, s. 118).

Denne oppgaven skal undersøke hvordan Bergen kommune kan arbeide med sikkerhetskultur for å tilrettelegge for forsvarlig håndtering av personopplysninger. I lys av dette vil det være naturlig å bruke teorier som favner om den tradisjonelle sikkerhetskulturen, samtidig som bruken av denne også kan problematiseres, særlig i tilknytning til safety og security. Digitalisering i og av offentlig sektor kan reise problemstillinger hvor det kan være nødvendig å tilnærme seg en sikkerhetskultur som favner om både safety og security som to likeverdige deler av sikkerhetskultur.

2.4 Sikkerhetskultur

Innenfor safety-tilnærmingen til sikkerhet argumenteres det for at sikkerhetskultur er noe som kan identifiseres i alle organisasjoner, og den kan beskrives som svak eller sterk, positiv eller negativ. Andre forskere mener at kun organisasjoner som har et overveiende fokus på sikkerhet, kan sies å ha en sikkerhetskultur (Jore, 2016, s. 470).

Sikkerhetskultur har vokst frem som en viktig del av flere virksomheters tilnærming til sikkerhet, særlig i etterkant av Tsjernobyl-ulykken i 1986. Til tross for dette, er det fortsatt usikkerhet knyttet til hva sikkerhetskultur og konseptet rundt det betyr, som Malcomson (2009) argumenterer for. Dette sier også Engen et al. (2016), som trekker frem at sikkerhetskultur består av mange ulike definisjoner og perspektiver. Forfatterne formidler videre at sikkerhetskulturen som vokste frem i etterkant av Tsjernobyl-ulykken har vært utsatt for kritikk fordi den reduserer kultur til noe en organisasjon har, og ikke noe en organisasjon er. Kritikken har således gått ut på at en organisasjon sin kultur ikke kan «[...] reduseres til observerbar atferd og individuelle opplevelser» (Engen et al., 2016, s. 157-158). Kultur er dermed mer omfattende og komplekst enn som så. Antonsen (2009a) formidler at Tsjernobyl-ulykken viste at de immaterielle aspektene (kulturelle og organisatoriske) ved høyteknologiske systemer kan vise seg å ha svært omfattende konsekvenser (Antonsen, 2009a, s. 119).

2.4.1 Hva menes med en sikkerhetskultur

James Reason (1997) argumenterer for at sikkerhetskultur er noe som kan utformes sosialt ved å identifisere og fabrikkere dens essensielle komponenter og deretter samle den i en felles fungerende enhet. En sikkerhetskultur er dermed ikke noe som oppstår av seg selv fra den organisatoriske ekvivalenten til en ulykke, den oppstår gradvis fra en systematisk og vedvarende implementering og anvendelse av godt utformede tiltak (Reason, 1997, s. 192). En god sikkerhetskultur er således en prosess med fokus på kollektiv og systematisk læring, samt en enighet om felles mål og verdier på alle nivå i organisasjonen. Reason definerer således sikkerhetskultur på følgende måte, «Shared values and beliefs that interact with an organization´s structures and control systems to produce behavioural norms» (Reason, 1997, s. 192).

Antonsen (2009b) viser til en definisjon som er mye brukt innen kjernekraftindustrien, som definerer sikkerhetskultur på følgende måte:

> The product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures (ACSNI, 1993, i Antonsen, 2009b, s. 16).

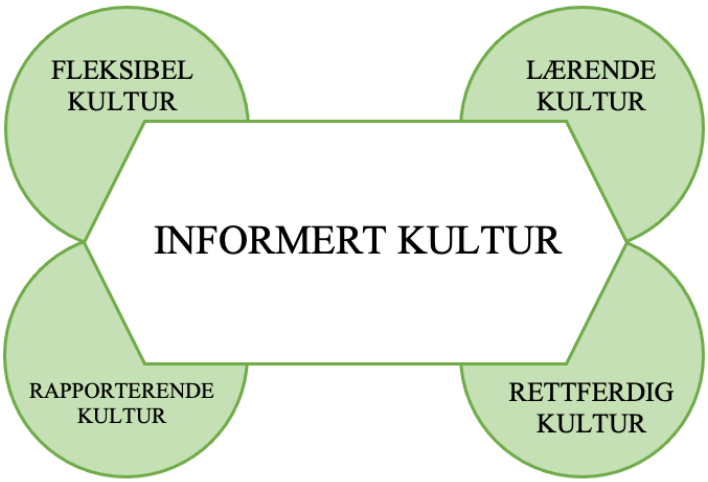
Begge definisjonene deler betydningen av delte verdier, holdninger og oppførsel i sikkerhetskultur. Antonsen (2009b) sin definisjon går dog mer i dybden på hva som menes med sikkerhet, og trekker videre frem forebyggende tiltak som en viktig del av sikkerhetskulturen.

I sin teori om sikkerhetskultur, problematiserer Reason (1997) hvorvidt sikkerhetskultur er noe en organisasjon *er*, eller om det er noe en organisasjon *har*. Selv tar han utgangspunkt i sistnevnte, og begrunner dette med hvordan ledelsen i en organisasjon kan, dersom ønskelig, påvirke eller endre sikkerhetskulturen ved å introdusere nye tiltak eller mål for organisasjonen (Reason, 1997, s. 192). Ifølge Reason tilsvarer en god sikkerhetskultur derfor en helhetlig informert kultur. På denne måten kan vi forstå hans definisjon av sikkerhetskultur i lys av det funksjonalistiske perspektivet, som formidler at sikkerhetskultur er avgjørende for en

organisasjon sin måloppnåelse, og manglende måloppnåelse kan således knyttes til dysfunksjonelle kulturer, ifølge Kongsvik et al. (Kongsvik et al., 2018, s. 222).

For å oppnå en informert kultur kreves det et sikkerhetsinformasjonssystem som samler inn, analyserer og formidler informasjon fra ulykker og nestenulykker, samt fra regelmessige kontroller av det operative systemet. En informert kultur er en kultur hvor de som administrerer og driver systemet har oppdatert kunnskap om menneskelige, tekniske, organisatoriske og miljømessige faktorer som setter premisser for sikkerheten til systemet (Reason, 1997, s. 194-195). Dette oppnås ved å tilrettelegge for en rapporterende kultur, en rettferdig kultur, en fleksibel kultur og en lærende kultur.

Weick & Sutcliffe (2007) omtaler de fire premissene for informert kultur som subkulturer, som sammen utgjør en organisasjonskultur. Forfatterne gjør rede for hvordan de ulike subkulturene sammen utgjør en «mindful» organisasjon (Weick & Sutcliffe, 2007, s. 5). Begrepet «mindfulness» brukes ofte i forbindelse med HRO-tankegangen og sier noe om arbeidet organisasjonen gjør for sikre at uønskede hendelser ikke forekommer i organisasjonen.



Figur 2: Sikkerhetskultur

(Reason, 1997: Weick & Sutcliffe, 2007)

En rapporterende kultur

For å oppnå pålitelige sikkerhetssystemer, er en organisasjon avhengig av ansatte som 1) arbeider nær ulykker og nesten-ulykker, og 2) at disse ansatte er villig til å rapportere inn egne feil, hendelser hvor det kunne ha gått galt og andre former for avvik (Reason, 1997, s. 195). Et overordnet fokus på å rapportere og undersøke selv de minste feil ved et system, samsvarer med

hvordan en HRO systematisk tilnærmer seg feil og nesten-feil, ifølge Weick & Sutcliffe (Weick & Sutcliffe, 2007, s. 3).

Det kan i utgangspunktet være en utfordring å overtale ansatte til å rapportere ulykker og nesten-ulykker, spesielt når dette kan innebære å gå i dybden på egne feil. Som mennesker er det naturlig å reagere ulikt på feil, men det å innrømme dem faller ikke like naturlig. En annen grunn til at ulykker og nesten-ulykker ikke rapporteres er ledelsens reaksjon (Reason, 1997, s. 196). Samtidig kan kollegiale forhold også ha en innvirkende faktor, og et ønske om å ikke sette verken kolleger eller seg selv i fare. Andre forhold som kan fraråde ansatte fra rapportere hendelser kan være ekstra arbeid, generell skepsis, et ønske om å glemme at hendelsen i det hele tatt hendte, mangel på tillit og frykt for konsekvenser (Reason, 1997, s. 196).

Arbeidet med å tilrettelegge for god håndtering av rapporteringer om ulykker og nesten-ulykker er derfor viktig. Reason presenterer fem punkt som innvirker på hvorvidt en organisasjon tilrettelegger for tilfredsstillende rapportering (Reason, 1997, s. 197):

1. Ansatte må beskyttes mot disiplinære handlinger- så langt dette er praktisk mulig
2. Ansatte må kunne rapportere anonymt og/eller rapportene må tilrettelegge for at ansatte ikke kan identifiseres.
3. De som samler inn og analyserer rapportene må være en uavhengig gruppe eller avdeling og det må kunne skilles mellom denne og dem som har myndighet til å iverksette disiplinære handlinger og ilegge sanksjoner.
4. Tilbakemeldingene på rapportene må være effektive, tilgjengelig og forståelig for rapporteringssamfunnet
5. Det må være enkelt å formulere rapporten.

Fokuset hos organisasjonen som bygger en rapporterende kultur må dermed være å generere tillit, samt skape et miljø hvor det er akseptabelt å melde inn om feil og avvik. En avgjørende faktor på hvordan dette oppfattes er hvordan ledelsen håndterer feil og avvik (Reason, 1997, s. 198). Urimelig straff og konsekvenser kan svekke ansattes tillit og vilje til å rapportere. Ledelsen skal derfor fokusere på sikkerhet og tillit blant de ansatte, og ikke på straff, konsekvenser og sanksjoner. Weick & Sutcliffe oppfordrer også til at ansatte belønnes for å innrømme feil (Weick & Sutcliffe, 2007, s. 3). Dette kan skape et bedre utgangspunkt for å bygge en kultur hvor ansatte føler seg komfortabel med å rapportere ulykker og nesten-ulykker.

En rettferdig kultur

En rapporterende kultur er som nevnt avhengig av hvordan straff og sanksjoner håndteres fra ledelsens side i en organisasjon. For å bygge en rettferdig kultur er det viktig å finne en balanse mellom en ikke-skyld-kultur og en rent straffegivende kultur (Reason, 1997, s. 195). En organisasjon som ikke evner å irettesette individer etter deres handlinger er hverken gjennomførbart eller ønskelig. Samtidig må organisasjonen være observant på å ikke i for stor grad straffe ansatte for hver minste feil og uhell, da dette vil være uakseptabelt blant ansatte. En rettferdig kultur som tydeliggjør hvor grensen mellom akseptabel og uakseptabel oppførsel er dermed ideelt (Reason, 1997, s. 205).

Reason (1997) fremhever tre punkter som beskriver hvordan ansatte handler (Reason, 1997, s. 205).

1. En intensjon som beskriver et mål og hvilke handlinger som er nødvendig for å nå dette målet.
2. Handlingene utløst av denne intensjonen.
3. Konsekvensen av valgte handlinger.

Det må altså kunne skilles mellom handlinger som er utført med en intensjon om å skade, og mellom handlinger som ledet til ulykke på bakgrunn av en eller flere uskyldige feil (Reason, 1997, s. 205). Her fremkommer et tydelig skille mellom safety og security-tilnærmingen innen sikkerhetstenking. Dersom en handling er gjort med en ondsinnet hensikt (intensjon om å skade) faller den under security-tilnærmingen. Da Reason sin teori om sikkerhetskultur retter seg mot safety-tilnærmingen, gjøres det følgelig ikke rede for hvilke konsekvenser som følger handlinger som faller under security.

En fleksibel kultur

Fleksibilitet kan referere til tilbøyelighet, tilpasningsevne eller smidighet (Nilstun, 2018). Organisatorisk fleksibilitet handler dermed om en organisasjons evne til å effektivt tilpasse seg skiftende krav. En fleksibel kultur tilrettelegger for at forandringer raskt håndteres, samtidig som det ikke er mye rom for prøving-og-feiling (Reason, 1997, s. 213-214). Dette gjør at organisasjoner som etterstreber er fleksibel kultur arbeider med en tilnærmet kronisk uro, og som aktivt leter etter feil eller avvik i systemene. Ideen er at jo bedre forberedt et system er på feil eller avvik, desto enklere blir håndteringen, og konsekvensene kan minske i alvorlighetsgrad. Weick & Sutcliffe beskriver dette som en forpliktelse til å hele tiden jobbe

med å bygge en resilient organisasjon («commitment to resilience») (Weick & Sutcliffe, 2007, s. 3). Resiliens betyr at systemer er tilpasningsdyktig ovenfor endringer. Ifølge Njå et al. (2020) forstås dette som en organisasjon som utelukkende fokuserer på god praksis, og som har gått vekk fra å fokusere på svikt, mangler og uønskede hendelser (Njå et al., 2020, s. 53).

Når situasjoner må håndteres, vektlegger Reason viktigheten av kompetanse. Dette betyr at valg og avgjørelser vedrørende situasjonen som skal håndteres, må tas av den eller de som innehar best kompetanse (Reason, 1997, s. 216). Weick & Sutcliffe (2007) mener ansatte bør oppfordres til å dele kunnskap og lærdom i etterkant av kriser. På denne måten kan de ansatte som helhet nærme seg en felles forståelse for hva som er nødvendig å gjøre dersom et system utsettes for stress eller belastning (Weick & Sutcliffe, 2007, s. 3).

Reason formidler videre betydningen av hvordan kommunikasjon og samarbeid bidrar til å skape en kultur hvor teamarbeid er verdsatt og aktivt brukes. En organisasjons evne til å bytte fra en byråkratisk, sentralisert styringsmetode til en mer desentralisert profesjonell styringsmetode fremgår dermed som en viktig faktor for å håndtere perioder med høyt tempo og stress, og videre sikre en organisasjons pålitelighet (Reason, 1997, s. 216). Ofte besitter enkelte ansatte eksplisitt kompetanse eller en dyp situasjonsforståelse for situasjoner som må løses. Weick & Sutcliffe oppfordrer organisasjoner til å se vekk fra den hierarkiske ordningen, og la ansatte med det beste utgangspunktet få ta de viktige beslutningene (Weick & Sutcliffe, 2007, s. 4). Når organisasjonen vender tilbake i normaltilstand, vil også autoriteten sømløst falle tilbake til sin byråkratiske, flate form (Reason, 1997, s. 216).

En lærende kultur

Ifølge Reason er en lærende kultur den enkleste å konstruere, men den vanskeligste å få til i praksis. En lærende kultur vektlegger observering ved å være oppmerksom og ha øye for detaljer, reflektere ved å analysere og rapportere, skape ved å planlegge og utvikle, samt handling ved implementering eller testing (Reason, 1997, s. 218). En lærende kultur aksepterer at det begås feil, så lenge ansatte rapporterer feil og er åpen om dette. Et godt tillitsforhold mellom ansatte og ledelsen setter her et viktig premiss for organisasjonens evne til å få et læringsutbytte av hendelsen (Reason, 1997, s. 218).

Weick & Sutcliffe påpeker at i HRO-er foreligger det ofte uenighet på tvers av de ulike nivåene i organisasjonen. Dersom det for eksempel ikke foreligger enighet mellom ledelse og

førstelinjen av arbeidere, er dette et problem som kan hindre arbeidet med organisasjonens «mindfulness» og derunder svekke den lærende kulturen (Weick & Sutcliffe, 2007, s. 4).

Samtidig må organisasjonen være kritisk til eget arbeid, og proaktivt søke etter mangler eller avvik som kan ramme den eksisterende praksisen. Dette gjør at organisasjonen kan komme i forkant av hendelser, og kan dermed ha forberedt endringer eller tiltak for hvordan en gitt hendelse kan håndteres (Reason, 1997, s. 218).

Læring er også viktig i etterkant av en hendelse. Da dette er en oppgave som i stor grad tilfaller en organisasjons ledelse, er det dermed viktig at ledere selv er villige til å trekke lærdom fra hendelsen og deretter formidle denne kunnskapen til øvrige ansatte (Engen et al., 2016, s. 301). Videre formidler forfatterne det har over tid blitt tilgjengelig mye informasjon og erfaringer fra hendelser som har rammet organisasjoner «[...] og forvaltningen kan bli bedre til fullt ut å trekke lærdom av hverdagserfaringer [...]» (Engen et al., 2016, s. 319). Reason (1997) gjengir Peter Senge, som skrev følgende «learning disabilities are tragic in children, but they are fatal in organizations» (Reason, 1997, s. 219). For at læringen skal manifestere seg på et organisatorisk nivå, må resultatene implementeres som en naturlig del av ansattes mentale kunnskapsbase (Njå et al., 2020, s. 430).

3. Metode

Formålet med dette kapittelet er å beskrive oppgavens forskningsprosess fra begynnelse til slutt. Metodiske valg vil gjøres rede for, og det vil videre drøftes om valgt tilknyttet metoden kan ha påvirket oppgavens kvalitet. Dernest vil etiske vurderinger tatt i forbindelse med innsamling av data drøftes. Samlet vil dette tydeliggjøre hvorfor valgt metode gir det beste utgangspunktet for å belyse oppgavens tema, samt svare på problemstilling og tilhørende forskningsspørsmål.

3.1 Forskningsdesign

Studien ble gjennomført i perioden mellom januar og juni 2021. Formålet med oppgaven er å få innblikk i hvordan Bergen kommune arbeider med sikkerhetskultur, og hvordan dette arbeidet kan virke inn på kommunens behandling og arbeid med digitale personopplysninger. Andre områder som er relevant å belyse i dette arbeidet er hvordan kommunen arbeider med risiko og risikoanalyser, sårbarheter, kompetanse og digitalisering. Utgangspunktet for

oppgaven er valgt problemstilling *«Hvordan kan Bergen kommune sitt arbeid med sikkerhetskultur tilrettelegge for forsvarlig håndtering av digitale personopplysninger?»*. Ifølge Grønmo beskriver en problemstilling «... avstanden mellom det vi vet, og det vi ønsker å vite» (Grønmo, 2016, s. 443).

For å undersøke problemstillingen og svare på tilhørende forskningsspørsmål, kreves det data. Data beskrives som «... informasjon som er bearbeidet, systematisert og registrert i en bestemt form og med sikte på bestemte analyser» (Grønmo, 2016, s. 434). Det skilles mellom data som er kvalitativ og kvantitativ. Uttrykkes i form av mengdetermer kan den beskrives som kvantitativ. Uttrykkes dataen derimot som tekst, defineres den som kvalitativ (Grønmo, 2016, s. 440 og 265). Dataen som danner det empiriske grunnlaget for oppgaven, er kvalitativ og består av dokumenter og intervjuer.

En kvalitativ tilnærming er hensiktsmessig når det fra før ikke foreligger mye kunnskap eller data på området som skal studeres. Ved en kvalitativ tilnærming går forsker i dybden på et valgt forskningsområde, hvor målet er å gi mening til sosiale fenomener som individer selv opplever og er en del av. Metoden egner seg dermed godt når sikkerhetskultur i Bergen kommune skal undersøkes fordi det ikke foreligger mye empiriske data på kommunens arbeid med dette. Sikkerhetskultur forstås således som et sosialt fenomen, da det er noe ansatte i kommunen må forholde seg til i det daglige arbeidet. I studier med en kvalitativ tilnærming kan datainnsamling og analyse av dataen foregå parallelt. Dette gir en fleksibel forskningsprosess, hvor innsamling og analyse alene ikke kan skilles ut som egne faser i forskningen (Grønmo, 2016, s. 265).

For forskningsprosjekter som bruker kvantitative data eksisterer det en rekke standardiserte statistiske teknikker for analyser. Dette er dog ikke tilfellet når kvalitative data skal analyseres, som i denne oppgaven. Kvalitative data er normalt sett uttrykt i form av tekst, og analyseres ved hjelp av generelle strategier. Formålet med kvalitative studier er således ikke å generalisere, men å gå i dybden på et sosialt fenomen og generere mer forståelse rundt dette (Grønmo, 2016, s. 295).

Litteraturgjennomgangen viste til en rekke dokumenter som i og for seg omhandler digitalisering, utfordringer med digitalisering, hvordan sikre tilstrekkelig personvern og digital sikkerhetskultur. Rapporter som henvender seg til kommunal sektor og tar opp verdien og betydningen av å ha en sikkerhetskultur, er manglende. For å hente ut relevant informasjon ble

det derfor metodisk nødvendig for meg å kombinere kvalitativ innholdsanalyse med kvalitative intervjuer.

Datainnsamling ble gjort mellom februar og mai 2021. Å kombinere kvalitativ innholdsanalyse og intervjuer gir anledning til å undersøke hvorvidt kommunen arbeider og selv forstår kultur og sikkerhetskulturarbeidet. Intervjuene gir informasjon om hvordan ansatte i kommunen oppfatter dette arbeidet. Dette gir meg et godt grunnlag for å si noe om hvordan sikkerhetskulturen i kommunen og arbeidet med personvern, belyst både fra ansatte og kommunen som organisasjon.

Oppgaveløpet er presentert i tabellen under, og er inkludert for å vise den omfattende forskningsprosessen.

Måned	**Hva ble gjort**	**Formål**	**Oppnådd resultat**
Januar	Problemstilling og tilhørende forskningsspørsmål rettet mot digital sikkerhet i kommunal sektor ble skissert sammen med en skisse av innledning og bakgrunn for valg av tema. Tok deretter kontakt med Bergen kommune angående et samarbeid knyttet til valg av potensielle informanter og dokumenter relevant for oppgaven.	Hensikten var å tidlig danne seg et reelt bilde av hva oppgaven skulle handle om, dens målsetninger og begrensninger, samt forsikre meg om at Bergen kommune var interessert i et samarbeid.	Opprettet kontakt med kommunen, og fikk bekreftet at de hadde interesse av å være en del av oppgaven. Så at bredden på oppgaven var for stor, og fikk hjelp av veileder til å snevre den mer inn. Fikk tildelt ny veileder i slutten av måneden.

Februar	Ytterligere samtaler med min kontaktperson i kommunen angående potensielle informanter. Fikk tilsendt dokumenter som kunne være relevant å bruke videre i innholdsanalysen. På bakgrunn av dokumentene ble intervjuguide utarbeidet. Oppgavens teorikapittel ble skissert samtidig som intervjuguiden ble skrevet.	Tidlig få på plass forslag til informanter, for å igangsette prosessen med intervjuer så snart som mulig. Ved å aktivt bruke dokumentene som referansepunkt når intervjuguiden skulle utformes, gjorde at jeg fikk god oversikt over hva som var nødvendig å spørre informantene om. Ønsket også at det teoretiske rammeverket i stor grad skulle være ferdig før intervjuene ble gjennomført.	Fikk oversikt over hvilke dokumenter som skulle inngå i den kvalitative innholdsanalysen, og hentet også frem andre dokumenter. Oppgavens teorikapittel viste seg å være noe gjentagende vedrørende valg av teorier, og en del ble derfor kuttet bort. Fikk anbefalt fra veileder å se etter andre relevante teoretiske perspektiver, og gjorde dette.
Mars	Fikk tilbakemelding på intervjuguide fra veileder, og søkte om godkjenning for å gjennomføre intervjuene hos NSD. Jeg tok deretter kontakt med min kontaktperson i kommunen og etterspurte oversikt over informanter. Teori om safety og security ble supplert inn i teorikapittelet.	Ønsket å gjennomføre alle intervjuene før påske, men så at det ble vanskelig å få til. Suppleringen av teoretiske perspektiver endret noe av fokuset i oppgaven, men ikke i stor grad. Ønsket også rask godkjenning fra NSD så intervjuene kunne gjennomføres så snart som mulig.	Fikk godkjenning fra NSD en uke ut i mars, og var dermed klar for å gjennomføre intervjuer. I påvente av svar fra kontaktperson angående informanter ble metode-kapittelet formulert. Fikk etter hvert kartlagt de to første informantene, og avtalte videre intervjutidspunkt. Båndopptaker ble kjøpt.
April	Fortsatte å skrive på de innledende kapitlene for å utdype tema og problemstilling. Teori-og metodekapittelet ble ferdigstilt. Gjennomførte fire kvalitative intervjuer med informanter fra kommunen. Transkribering ble gjennomført etter hvert intervju, og deretter sendt til informantene for godkjenning. Startet på empirikapittelet.	Hadde som mål å få ferdig de innledende kapitlene i forkant av intervjuene, da intervjuprosessen ble igangsatt noe sent i oppgaveløpet. Dette sikret også at jeg fikk veiledning på de innledende kapitlene, og mulighet for å rette opp i tilbakemeldinger på dette.	Transkriberingen fra de første intervjuene gjorde det naturlig å begynne på empirikapittelet. Funnene fra innholdsanalysen og intervjuene ga et omfattende datagrunnlag, men det ble likevel et godt samspill mellom de to metodene etter at rådata ble kodet.

Mai	Hadde ytterlige to intervjuer av informanter fra kommunen, som også ble transkribert og sendt for godkjenning. Skrev empirikapittelet samtidig som jeg startet på analyse og drøfting. Da intervjuene fulgte det samme grunnleggende oppsettet, var det enkelt å føre resultatene fra de to siste intervjuene inn i empirien.	All datainnsamlingen sikret at empirikapittelet ble ferdig, og det ble derfor naturlig å legge fokus på analyse og drøfting samt starte på en konklusjon på oppgavens problemstilling.	Etter veiledning på de innledende kapitlene ble noe justert for å sikre en bedre flyt og forståelse av tema-og problemstilling. Var dels usikker på hvorvidt funnene belyste hva problemstillingen faktisk spurte etter, og så videre behovet for å moderere forskningsspørsmålene noe.
Juni	Arbeidet med en helhetlig flyt og rød tråd i teksten. Dobbeltsjekket at referanser var ført inn korrekt og la til bildetekst under hver figur og tabell. Skrev konklusjon, sammendrag og forord. Korrigerte også noe på oppgavens empirikapittel etter tilbakemelding fra veileder.	Teksten ble justert for å sikre en rød tråd gjennom hele oppgaven. Skrivefeil og tekstflyt ble rettet opp i for å sikre at oppgaven ikke har noen uklarheter.	Oppgaven ble omsider levert 14 juni.

Tabell 2: Oversikt over fremdrift i oppgaven

3.2 Forskningsstrategi

En forskningsstrategi representerer en måte å tilnærme seg et tankesett på, og det skilles mellom fire ulike forskningsstrategier (Danermark, 2002, s. 79). I denne oppgaven gjør problemstillingen og forskningsspørsmålenes formulering at abduksjon som forskningsstrategi er hensiktsmessig å bruke. Ifølge Dey (2004) utgjør en abduktiv forskningsstrategi at utgangspunktet for forskningen er et teoretisk rammeverk som empiriske observasjoner blir tolket i tråd med. Sammen kan dette lede forsker til ny kunnskap på området som undersøkes (Dey, 2004, s. 91). Formålet med denne oppgaven er å undersøke hvorvidt arbeidet kommunen gjør med å tilrettelegge for håndtering av personopplysninger kan beskrives og omtales som en kultur, herunder sikkerhetskultur. Empiriske data skal således tolkes og drøftes opp mot teorier knyttet til kultur og sikkerhetskultur. Kommunens tilnærming til sikkerhet skal også vurderes etter teori om safety og security.

Danemark et al., (2002) sin redegjørelse for hva som menes med abduksjon samsvarer i stor grad med Dey (2004) sin. Ifølge Danermark går den abduktive forskningsstrategien ut på at 1) den tar utgangspunkt i en empirisk hendelse eller fenomen, som 2) kan knyttes til et teoretisk rammeverk og som således 3) leder forsker til en ny antakelse om eller forståelse for hendelsen eller fenomenet (Danermark, 2002, s. 90: Dey, 2004, s. 91). Med dette forstås arbeidet kommunen gjør med å skape en kultur som et fenomen. Fenomenet tolkes videre i tråd med det teoretiske rammeverket presentert ovenfor, og kan således lede til nye antakelser eller forståelse, noe som samsvarer med hva Dey (2004) formidler.

Samlet vil oppgaven fokusere på å trekke linjer og finne sammenhenger mellom fenomener som er begrenset til nåtiden. Forskningen kan dermed kategoriseres som et kryss-seksjonellt studie, ifølge Blaikie & Priest (Blaikie & Priest, 2019, s. 198). Kunnskap knyttet til kommunens arbeid med sikkerhetskultur fremkommer som mangelfull, og det har dermed vært en målsetning gjennom hele studien å generere mer kunnskap på dette området. I tråd med dette er oppgaven preget av et eksplorerende forskningsdesign og ifølge Jacobsen vil oppgavens formål dermed være å utdype sosiale fenomener som er preget av manglende kunnskap (Jacobsen, 2005, s. 61).

3.3 Kvalitativ innholdsanalyse

Kvalitativ innholdsanalyse er ideelt å bruke som metode når det foreligger et behov for å samle inn mengder med data som fremstilles som tekst, og som har hensikt om å gi dybdekunnskap om fenomenet som undersøkes. Dokumenter utgjør én hovedtype av samfunnsvitenskapelige kilde, av totalt tre, ifølge Grønmo (Grønmo, 2016, s. 435). Dokumenter som brukes i en kvalitativ innholdsanalyse kan være store og omfattende, og det er således viktig å kategorisere dem etter nødvendighet, og utarbeide en systematisk tilnærming for å hente ut relevant data. Det er denne prosessen som utgjør grunnstrukturen i en innholdsanalyse, ifølge Grønmo (Grønmo, 2016, s. 134-135). Målet er å identifisere relevant informasjon om det eller de sosiale forholdene som undersøkes, herunder Bergen kommune, avgrenset til sikkerhetskultur, personvern og hvordan kommunen arbeidet med dette. Innholdsanalysen har derfor tatt sikte på å hente ut informasjon som særlig belyser relevante tema, og informasjon vurdert til å være mindre relevant er derfor utelatt.

Ved å systematisk hente ut data fra dokumenter, kan det trekkes linjer mellom sammenhenger som dernest kan skape et mønster som belyser det oppgaven undersøker. En fordel med å bruke

kvalitativ innholdsanalyse som metode, er at dokumentinnsamling og analyse kan foregå parallelt. Dette gir en fleksibel forskningsprosess, og forsker en unik anledning til å få oversikt over hvilke dokumenter som er nødvendig for å best kunne gjennomføre. Prosessen med å samle inn og analysere dokumenter kan være krevende, og det er viktig at jeg som forsker er innforstått med å gjøre justeringer og endringer underveis i oppgaveløpet (Grønmo, 2016, s. 175).

I forkant av en innholdsanalyse er det viktig å utarbeide en klar målsetning med studien, hva som skal undersøkes og hensikten med datainnsamlingen. En annen oppgave som må gjøres i forkant er å finne dokumentene som skal brukes i analysen (Grønmo, 2016, s. 176). Det skilles mellom flere ulike metoder for å identifisere og hente inn dokumentene som skal analyseres. I denne oppgaven er det brukt en metode som Grønmo (2016) omtaler som en snøballmetode. Dette innebærer at utvalgte dokumenter settes som utgangspunkt for datainnsamlingen. Disse dokumentene kan lede meg til andre dokumenter som er relevant for analysen, og så videre (Grønmo, 2004, s. 187). Jeg fikk tilsendt en rekke dokumenter fra min kontaktperson i Bergen kommune, som jeg dernest bruke videre i arbeidet med å samle inn relevant dokumentasjon.

Når den kvalitative innholdsanalysen skal gjennomføres, er det viktig at jeg som forsker kan foreta kildekritiske og kontekstuelle vurderinger av tekstene. Å være kildekritisk betyr å kunne vurdere de ulike dokumentenes tilgjengelighet, relevans og troverdighet. De kontekstuelle vurderingene omhandler det å vurdere teksten i sammenheng med dens
opphav, og dernest vurdere hvorvidt den er autentisk og om innholdet kan beskrives som troverdig (Grønmo, 2016, s. 177-178). Dataen som hentes ut fra de kommunale dokumentene er prosesserte data. Dette betyr at datagrunnlaget består av data og informasjon som er samlet inn og behandlet av andre. Dokumentene som inngår i analysen i denne oppgaven er kommunale, og ligger derfor tilgjengelig på Bergen kommunes nettsider, eller per forespørsel. Figuren under gjør rede for dokumentene, deres fokusområde og hvilken relevans de har for oppgaven.

Dokument	**Beskrivelse**	**Relevans for oppgaven**
Digitalisering og innovasjon i Bergen kommune 2017-2020	Planen fungerer som et hjelpemiddel for kommunen, og skal medvirke til at kommunen når de	Belyser kommunens arbeid med digitalisering fra 2017 og frem til 2020.

	digitaliseringsmålene som er satt nasjonalt.	
Digitaliseringsstrategi Bergen kommune 2021-2025	Kommunens gjeldende digitaliseringsstrategi. Beskriver kommunen sitt arbeid med digitalisering og relevante områder rundt dette, herunder ivaretakelse av personopplysninger, sikkerhetskultur og andre fokusområder i kommunen.	Strategien formidler hvordan kommunen skal tilnærme seg relevante områder knyttet til digitalisering nå og fremover. Belyser også områder hvor personvern og digitalisering er relevante, og redegjør videre for hvordan kommunen skal arbeide med dette fremover mot 2025.
Gjennomgang av avvik i kommunikasjonsløsning (Vigilo)	Internkontrollrapport utarbeidet i etterkant av Vigilo-saken i Bergen kommune høsten 2019.	Belyser kommunens arbeid med Vigilo-saken fra 2019, og trekker frem svakheter med prosjektarbeidet, og formidler videre hva som tilsynelatende gikk galt med innførelsen av systemet.
Reglement for digitalisering og IKT	Presenterer gjeldende reglement og retningslinjer for digitalisering og IKT i kommunen.	Relevant for å få informasjon om regelverket og retningslinjer knyttet til digitalisering og IKT i kommunen, og hvorvidt dette etterleves.
Reglement for personvern og informasjonssikkerhet	Presenterer gjeldende reglement og retningslinjer for personvern og informasjonssikkerhet i kommunen.	Relevant for å innhente informasjon om gjeldende regelverk og retningslinjer knyttet til kommunens arbeid med personvern og informasjonssikkerhet og hvorvidt dette etterleves.
Forvaltningsrevisjon: Bergen kommune (informasjonssikkerhet)	Forvaltningsrevisjonens formål var å undersøke hvorvidt kommunens styringssystem etterlever de regler og retningslinjer som stilles til informasjonssikkerhet. Forvaltningsrevisjonen er gjennomført av Deloitte på vegne av kommunen.	Belyser kommunens arbeid med informasjonssikkerhet og personvern de siste årene (en lignende forvaltningsrevisjon ble gjennomført i 2014). Trekker frem flere interessante resultater særlig tilknyttet informasjon, kunnskap og avvikshåndtering i kommunen.

Temaplan for informasjonssikkerhet og personvern 2021-2025	Hensikten med temaplanen er å tilrettelegge for at kommunen i større grad kan lykkes med arbeidet tilknyttet det å sikre informasjonssikkerhet og personvern i kommunen.	Belyser kommunens aktive tilnærming til personvern og informasjonssikkerhet, og etterstreber en helhetlig forståelse for dette blant alle ansatte i kommunen.
Byrådssak /20: *Avslutning av helhetlig gjennomgang personvern og informasjonssikkerhet og overføring av ansvar for videre oppfølging til ordinær virksomhet*	Byrådssaken oppsummerer gjennomgangen kommunen har hatt av digitale systemer som benyttes i kommunen. Hovedfunn fra gjennomgangen legges frem, og videre målsetningen utarbeides.	Helhetlig Gjennomgang var en stor del av arbeidet kommunen gjorde i 2020 for å bedre kommunens eget arbeid tilknyttet regelverk og rutiner for kommunens systemer i lys av personvern og informasjonssikkerhet.
Bergen ROS 2014	ROS-analysen viser til et overordnet risiko-bilde av kommunen gjeldende fra 2014 og frem til revidert utgave kom ut i 2020.	Belyser kommunens tidligere arbeid med helhetlig risiko og ROS-analyser. Gir videre informasjon om hvordan kommunen anser brudd i IKT-og/eller informasjonssikkerhet som en trussel for innbyggere og kommunen selv.
Bergen ROS 2020	ROS-analysen er den gjeldende for kommunen. Tegner et overordnet bilde av risikoer og sårbarheter i kommunen fra 2020 og fremover.	Belyser kommunens nåværende arbeid med helhetlig risiko og ROS-analyser. Gir videre informasjon om hvordan kommunen anser brudd i IKT-og/eller informasjonssikkerhet som en trussel for innbyggere og kommunen selv.

Tabell 3: Dokumenter brukt i kvalitativ innholdsanalyse

3.4 Kvalitativt intervju

For å undersøke oppgavens tema og problemstilling er det nødvendig å supplere informasjonsgrunnlaget fra den kvalitative innholdsanalysen. Ved å intervjue ansatte fra kommunen, skapes det en dypere forståelse for arbeidet kommunen gjør. Dette vil gi meg mer inngående kunnskap om hvordan kommunen *konkret* jobber ifølge ansatte, og ikke bare hvordan det er *tiltenkt* at kommunen skal jobbe, slik det fremkommer av innholdsanalysen.

I tråd med den kvalitative innholdsanalysen beskrevet ovenfor, vil intervjuene også ha et kvalitativt utgangspunkt. På denne måten vil data generert fra intervjuene brukes for å belyse funnene fra den kvalitative innholdsanalysen. Datagrunnlaget som intervjuene danner, kan defineres som rådata, som er et ubehandlet datamateriale. Dette er videre behandlet og kategorisert slik at den er hensiktsmessig å bruke for analyse i oppgaven.

Det finnes flere ulike måter et kvalitativt intervju kan gjennomføres på. Grønmo (2016) fremhever uformelle intervjuer som et eksempel på en tilnærming. I denne oppgaven har jeg tatt utgangspunkt i å intervjue ansatte i Bergen kommune for å nærmere undersøke hvordan kommunen arbeider. Dette samsvarer med Grønmo sin definisjon av uformelle intervjuer, som sier at «[...] forsker stiller spørsmål til respondentene om de forholdene som skal studeres...» (Grønmo, 2016, s. 167). Grønmo formidler at et uformelt intervju kun inneholder en oversikt over temaer som skal gjennomgås i intervjuet (Grønmo, 2016, s. 167), noe som ikke tilstrekkelig dekker intervjuprosessene gjennomført i denne oppgaven. Intervjuprosessen må av denne grunn utdypes videre.

Blaikie & Priest (2019) gir en lignende beskrivelse som nevnt ovenfor, men omtaler intervjumetoden som et semi-strukturert intervju. Forfatterne påpeker at intervjumetoden er godt egnet for å hente inn data innenfor kvalitativ forskning (Blaikie & Priest, 2019, s. 202). Forskjellen mellom de to er hvor utarbeidet og strukturert intervjuguiden er. Grønmo (2016) formidler at den normalt sett består av relevante temaer som skal gjennomgås, mens Blaikie & Priest (2019) legger til grunn at flere relevante spørsmål også kan inkluderes. Dette samsvarer med det Kvale (2015) beskriver som et semistrukturert intervju hvor intervjuguiden inneholder «[...] en oversikt over emner som skal dekkes, og forslag til spørsmål» (Kvale, 2015, s. 162).

På denne måten forstås intervjuene dermed som kvalitative, og av en semistrukturert karakter. I intervjuene vektlegger jeg informantenes egne beskrivelser, oppfatninger, meninger og fortolkninger vedrørende kommunens arbeid med å skape en sikkerhetskultur som sikrer at ansatte tilstrekkelig ivaretar personopplysninger og personvern. Dette samsvarer med hva Kvale (2015) formidler, hvor «[...] det er intervjuerens skjønn og taktfullhet som er avgjørende for hvor nær han [intervjuer] vil holde seg til guiden [...]» (Kvale, 2015, s. 162).

3.4.1 Utvalg av informanter og utforming av intervjuguide

Før intervjuguiden utformes, må jeg ha en klar formening om hvem som kan være hensiktsmessig å bruke som informant. Det må i tillegg vurderes hvor mange informanter som skal inkluderes, for å best kunne tilstrekkelig belyse oppgavens tema. Samtidig må jeg være observant på å ikke inkludere for mange informanter, da dette kan lede til mye overflødig og unødvendig informasjon om temaet.

Ved valg av informanter, var det åpenbart at det ville være behov for å intervjue ansatte i Bergen kommune. På denne måten ville jeg få inngående kunnskap om hvordan kommunen arbeider med sikkerhetskultur, digitalisering og personvern. Grønmo (2016) bruker begrepet respondent, og beskriver dette som et individ som responderer på spørsmål stilt ved for eksempel en strukturert utspørring (Grønmo, 2016, s. 444). I oppgaven brukes begrepet informant, men med samme forståelse som hva Grønmo formidler.

I samarbeid med min kontaktperson i Bergen kommune ble det derfor utarbeidet en oversikt over hvilken stilling og ansvarsoppgaver det var ønskelig at informantene hadde. Grønmo referer til en slik utvelgelsesprosess som et strategisk utvalg, og omtaler det som et «Utvalg som bygger på systematiske vurderinger av hvilke enheter som ut fra teoretiske og analytiske formål er mest relevante og mest interessante å inkludere i en bestemt studie» (Grønmo, 2016, s. 445).

En intervjuguide beskrives av Grønmo som en skisse av hvordan et uformelt intervju skal gjennomføres. Skissen inneholder en tematisk oversikt over hva intervjuobjektet kan vente seg å bli spurt om (Grønmo, 2016, s. 438). Således fungerer en intervjuguide som en oversikt over aktuelle temaer som skal gjennomgås i løpet av intervjuet. I tråd med Kvale (2015) og Blaikie & Priest (2019) sine definisjoner av et semi-strukturert intervju, ble det i tillegg ført opp spørsmål under hvert tema.

Før en intervjuguide utformes må det foreligge en oversikt over hva målsetningen med intervjuet er, og ut ifra denne skal relevante tema skisseres. Grønmo (2016) beskriver dette som å vurdere informasjonsbehovet for oppgaven (Grønmo, 2016, s. 168). I denne oppgaven består intervjuguiden av seks temaer, i tillegg til noen få spørsmål som kartlegger informantenes bakgrunn. Temaene som inngår i intervjuguiden, er: digitalisering, kompetanse og kultur,

personvern, sårbarheter og (avslutningsvis) noen spørsmål om hvordan kommunens arbeid kan tenkes å være fremover i tid.

En oversikt over informantene er presentert i tabell 4.

Informant	**Stilling**	**Rolle/ansvarsområde**
Informant A	Rådgiver, avdeling for personvern og informasjonssikkerhet	Utpreget rolle innen informasjonssikkerhet. Bistå i faglige vurderinger inn i risiko-og sårbarhetsanalyser, prosjekter og kravstillinger
Informant B	Personvernombud og avdelingsleder personvern og informasjonssikkerhet	Arbeidsoppgaver forankret i personvernforordningen. Operativt tildelte oppgaver fra IKT-sikkerhetsansvarlig vedrørende informasjonssikkerhet
Informant C	Prosjektleder/Rådgiver	Leder for ulike prosjekt innad i kommunen innenfor forskjellige byrådsavdelinger
Informant D	Rådgiver/Samvirkekoordinator	Del av det nye samvirkesenteret. Rådgiver for bystyrets kontor. Betjene, støtte og hjelpe i deres sikkerhetsarbeid.
Informant E	Spesialrådgiver/Prosjektleder	Leder for ulike prosjekt innad i kommunen innenfor forskjellige byrådsavdelinger
Informant F	Anonym	Anonym

Tabell 4: Oversikt over informanter, stilling og ansvarsområde

3.4.2 Gjennomføring av intervjuer

Intervjuene ble gjennomført i april og mai. Dette sikret at store deler av oppgavens innledende kapitler var ferdigstilt. Samtidig ga det meg tid til å hente frem de empiriske resultatene, og videre drøfte dem opp mot det teoretiske rammeverket for oppgaven.

I forkant av intervjuene hadde informantene signert en samtykkeerklæring og lest gjennom et informasjonsskriv. Dette sikret at informantene fikk informasjon om hensikten med intervjuene, samt oversikt over temaene som ville bli tatt opp under intervjuet. I tillegg fikk informantene informasjon om deres rettigheter, hvordan opplysninger om dem ville brukes samt informasjon vedrørende tilbaketrekking av samtykke. I samtykkeerklæringen ble det også informert om at informantene kunne være anonyme, dersom de ønsket dette. En av oppgavens seks informanter ønsket å være anonym (Informant F).

Intervjuene ble gjennomført digitalt over Microsoft Teams. Økt bruk og avhengighet av digitale løsninger som Microsoft Teams og Zoom i arbeids-og studenthverdagen kan beskrives som en positiv erfaring i lys av dagens pandemisituasjon. At intervjuene ble gjennomført digitalt skal derfor ikke ha noen innvirkning på informantenes åpenhet eller respons. Det ble satt av halvannen time til hvert intervju. Som informert om på forhånd ble også intervjuene tatt opp ved bruk av en båndopptaker, og ble i etterkant transkribert og sendt til informantene for godkjenning. Informantene ble også intervjuet enkeltvis. På denne måten sikret jeg informantenes egne vurderinger og refleksjoner rundt de spørsmålene som ble stilt, uten påvirkning fra andre.

3.5 Hvordan analyseres datagrunnlaget

Råmaterialet med data vil ikke i sin helhet anvendes i oppgaven. Datagrunnlaget må behandles, og som forsker er det viktig å trekke ut sentrale funn fra datagrunnlaget. Ifølge Grønmo «... finnes det ingen standardiserte analyseteknikker som kan benyttes til analyser av kvalitative data» (Grønmo, 2016, s. 265), og det er dermed opp til hver enkelt forsker å avgjøre hvilken metode som er mest hensiktsmessig å benytte for å generere et best mulig resultat.

Kvalitative data foreligger som regel i form av tekst (Grønmo, 2016, s. 265), noe som også er tilfelle i denne oppgaven. For å enkelt kunne trekke ut viktige funn fra datamaterialet, er det kodet. Formålet er det Grønmo beskriver som «[...] å avdekke generelle eller typiske mønstre i materialet» (Grønmo, 2016, s. 266). Dette innebærer at jeg som forsker leser gjennom og studerer råmaterialet, med den hensikt å finne sammenhenger, motsetninger og danne meg et inntrykk av generelle tendenser. Et kvalitativt datagrunnlag er som regel omfattende og det kan derfor være vanskelig å få oversikt over. Ved å kode datamaterialet vil tekstenes innhold sammensettes og gjøres mer oversiktlig (Grønmo, 2016, s. 266).

I kvalitative studier brukes koder som en beskrivelse på et større utsnitt av en tekst. I praksis kan for eksempel et gitt stikkord beskrive et bestemt tema, aktør, hendelse eller relasjon (Grønmo, 2016, s. 267). Det skilles mellom *deskriptive koder, fortolkende koder* og *forklarende koder* avhengig av hva formålet er. I denne oppgaven vil deskriptive koder sette utgangspunktet for kodingen, da de vil være et uttrykk for «[...] karakteristikker av det faktiske og eksplisitte innholdet i teksten» (Grønmo, 2016, s. 267).

I det første steget av koding er empirien førende for hva som vektlegges. Ved å ta utgangspunkt i fortolkende koder vil prosessen, ifølge Grønmo, kunne «[...] være åpen nok til å kunne oppdage uforutsette og overraskende empiriske fenomener, mønstre og sammenhenger» (Grønmo, 2016, s. 268). I det videre arbeidet med koding av datamaterialet vil også problemstillingen med tilhørende forskningsspørsmål være viktige retningslinjer for hvordan teksten forstås og karakteriseres.

Kodene for datamaterialet, samsvarer med oppgavens intervjuguide. Således vil ord som *digitalisering, personvern, sikkerhetskultur, avvik, risiko-og risikoanalyser, sårbarheter, kompetanse, læring* og *fremtiden* aktivt brukes for å kode datamaterialet og derav oppdage generelle mønstre og avklare meningsinnholdet i datagrunnlaget (Grønmo, 2016, s. 268). Sammen vil de ulike kodene skape ulike kategorier som vil danne grunnlaget de empiriske resultatene. Disse skal videre benyttes for å belyse oppgavens tema og problemstilling.

3.6 Studiens kvalitet

Valgt forskningsmetode er egen oppfatning og formening om hva som best vil egne seg som metodisk tilnærming. Som forsker er det viktig å ha et ærlig og kritisk blikk gjennomgående i forskningsløpet for å sikre studiens kvalitet, troverdighet og resultater. I dette delkapittelet skal jeg derfor gjøre rede for og argumentere for oppgavens kvalitet, styrker og svakheter. Avslutningsvis vil etiske vurderinger drøftes.

3.6.1 Betingelser for trustworthiness

Begreper som validitet, reliabilitet og generalisering er vanlig å henvise til innenfor forskningsfeltet, men knytter seg særlig til det kvantitative forskningsfeltet. Dette gjør således at bruk av dem kan problematiseres innenfor kvalitativ forskning. Ifølge Grønmo har dette

sammenheng med at kvalitative studier har mer ustrukturerte forskningsmetoder, som i denne oppgaven henviser til det fleksible forskningsopplegget en kvalitativ innholdsanalyse og kvalitative intervjuer gir (Grønmo, 2016, s. 248-249). Av denne grunn skal oppgavens kvalitet heller vurderes opp mot de fire betingelsene som ifølge Guba (1981) samles under begrepet *trustworthiness*. Forfatteren presenterer de fire betingelsene som kriterier for å bedømme kvaliteten av studier som bruker en kvalitativ tilnærming for å undersøke relasjoner, mennesker, kultur og samfunnsformer (Sommerfelt, 2015). Guba (1981) beskriver denne forskningstilnærmingen som *naturalistic inquiry paradigm*, og stiller således bedre kriterier for å måle kvaliteten på studier enn hva de tradisjonelle metodene for validitet og reliabilitet gjør (Guba, 1981, s. 75).

De fire prinsippene for trustworthiness presenteres som følgende:

Aspekt med begrepene	Tradisjonelle vitenskapelige begrep	Naturalistisk begrep
Sannhetsverdi	Intern validitet	Troverdighet
Anvendbarhet	Ekstern validitet / generalisering	Overførbarhet
Konsistens	Reliabilitet	Pålitelighet
Nøytralitet	Objektivitet	Bekreftbarhet

Tabell 5: Betingelser for Trustworthiness

(Guba, 1981, s. 75)

Troverdighet

Troverdighet handler om å måle forskningens sannhetsverdi, hvorvidt det kan etableres tillit til den sannheten som funnene fra undersøkelsen presenterer, og sammenhengen undersøkelsen ble gjort i (Guba, 1981, s. 79). For å gjøre dette må funn og tolkninger prøves opp mot de ulike kildene for å teste deres troverdighet. I denne oppgaven forstås dette ved å se på sammenhengen mellom funnene presentert i den kvalitative innholdsanalysen, og funnene fra intervjuene som er gjennomført. Samsvarer de ulike datakildene? Fremkommer det særlige forskjeller? Samsvarer hensikten med undersøkelsen med de datakildene og resultatene som oppgaven legger frem?

Dette betyr at dersom oppgavens funn har en klar sammenheng med det oppgaven har som hensikt å studere, kan datamaterialet sies å ha være troverdig. Digitalisering, personvern, sikkerhetskultur, sårbarheter og risikoarbeid har fungert som kategorier for å systematisere

datagrunnlaget. For at dette skal kunne beskrives som troverdig, må det således kunne trekkes linjer mellom dette og hensikten med oppgaven, som er å undersøke hvordan kommunens arbeid med sikkerhetskultur kan tilrettelegge for forsvarlig håndtering av personopplysninger. Samsvarer dette kan oppgaven således kunne beskrives som å være troverdig.

Overførbarhet

Ifølge Guba (1981) kan vitenskapelige funn vanskelig generaliseres, fordi fenomenene som undersøkes er for tett knyttet til både tiden og konteksten de undersøkes i (Guba, 1981, s. 80). Forfatteren trekker likevel frem at overførbarhet kan forekomme mellom to sammenhenger, basert på likheter mellom dem. Dette forutsetter kunnskap om overførings-og mottakssammenhenger, og sier videre at dersom det finnes likhet mellom to sammenhenger kan det være rimelig å anta at foreløpige funn for kontekst A, også kan være gjeldende for kontekst B. Overførbarhet handler således ikke om å generalisere funn i sin helhet, men å utarbeide arbeidshypoteser som kan være overførbar mellom ulike kontekster avhengig av likhet mellom de ulike kontekstene (Guba, 1981, s. 81).

I denne oppgaven skal jeg undersøke Bergen kommune, ved hjelp av å intervjue ansatte og hente ut informasjon fra kommunale dokumenter. Bergen kommune er en av Norges største kommuner, og sysselsetter svært mange mennesker. I tråd med hva som formidles angående overførbarhet, kan det dermed argumenteres for at resultatene i denne oppgaven kan representere den helhetlige forståelsen ansatte i kommunen har for kultur, for sikkerhet og personvern. Ifølge Guba må det gjøres empiriske undersøkelser før en sammenheng mellom to kontekster kan etableres og defineres som like (Guba, 1981, s. 81). Dette vil også være nødvendig å gjøre før oppgavens resultater kan sies å være gjeldene for hele Bergen kommune. Samtidig kan den kvalitative innholdsanalysen trekkes frem som en styrke, da dokumentene som er en del av den kvalitative innholdsanalysen gjelder for hele kommunen, og ikke et begrenset utvalgt. En begrensning kan knyttes til informantene, som kun representerer et fåtall ansatte i en kommune som sysselsetter ca. 19 000 mennesker.

Pålitelighet

Guba (1981) formidler videre at det er vanskeligere å forholde seg til pålitelig forskning innen den kvalitative forskningstilnærmingen, fordi dataene kan hele tiden variere og endre seg. Således handler ikke pålitelighet om uforanderlighet i data, men en sporbar varians. Dersom

endringer kan forklares og redegjøres for, kan data og resultater likevel være pålitelig. Den sporbare variansen kan tilskrives kilder, feil, virkelighetsskifter og lignende. Aspektet rundt pålitelighet handler om konsistens, og tolkes derfor som hvorvidt data kan fremstå som pålitelig i lys av sporbare, forklarlige endringer i datamateriale og resultater (Guba, 1981, s. 81).

Oppgavens data og resultater er begrenset til Bergen kommune, men har som formål å være overførbar til andre kommuner. Med dette menes at forskningsmetode, intervjuguide, empiriske data og teoretisk grunnlag skal kunne gjøre studien mulig å gjenta, men forsker må være observant på at datagrunnlag og videre resultater kan avvike fra det som presenteres her. Dette gjelder særlig knyttet til å ha informanter som kilder. Informantene vil være preget av egne holdninger, verdier, normer og formening om hvordan kommunen jobber. Dette kan bety at det personlige forholdet en ansatt har til kommunen, uavhengig om dette er godt eller dårlig, kan prege svarene som ble gitt under intervjuene og således påvirke datamaterialet. Ved å være observant på slike forklarlige og sporbare endringer, kan det forskningen likevel sies å være pålitelig.

Bekreftbarhet

Bekreftbarhet handler om hvorvidt funnene kan tolkes som er resultat av respondenter, datagrunnlaget og undersøkelsens formål, uten at den er påvirket av forskers egne motiver, interesser, perspektiver og partiskhet (Guba, 1981, s. 80). Guba vektlegger videre at nøytralitetsbyrden er forskjøvet fra den som undersøker, til dataene. Således handler det ikke om hvilken metode som brukes for å hente inn data, da den kan være vanskelig å bedømme innen kvalitativ forskning med hensikt å studere mennesker, relasjoner og kultur. Dette handler om bekreftbarheten til de produserte dataene (Guba, 1981, s. 80-81).

Som forsker er det viktig å etterstrebe resultater som er upåvirket av egne meninger, holdninger og verdier. Ved å benytte dokumenter som kilde, unngår jeg kontrolleffekter og reaktivitet. Dette er også en styrke ved metoden, fordi dokumentene vil i seg selv ikke påvirkes av datainnsamlingen, og tekstene vil ikke endre seg som resultat av at de analyseres (Grønmo, 2016, s. 180). Samtidig er det viktig å være observant på at tekstutvalget kan være for smalt, og at det dermed ikke representerer Bergen kommune på en helhetlig måte. Dette vil potensielt kunne påvirke det endelige datagrunnlaget.

Intervjudataene kan i høyere grad bestrides om de er bekreftbare eller ikke, fordi de er hentet inn av forsker selv. Dette kan ha både fordeler og ulemper. Samtidig understreker Guba (1981) at det er ikke forskningsmetoden som bedømmer hvorvidt data er bekreftbare eller ikke, det er dataene selv. Som forsker og intervjuer er jeg derfor klar over rollen jeg har under intervjuet. Det må være en balanse mellom eget engasjement og betydningen av at dataen skal være i fokus.

3.6.2 Metodiske styrker og svakheter

Innenfor kvalitativ forskning vil det foreligge mangler og svakheter som kan påvirke forskningens kvalitet. Det er derfor nødvendig at den vurderes etter gjeldende kvalitetspremisser. En slik vurdering tas ved å drøfte samspillet mellom metodiske valg som er tatt, datamaterialet som utgjør oppgavens empiriske grunnlag og samspillet mellom de to.

Som nevnt ovenfor, gir både kvalitative intervjuer og den kvalitative innholdsanalysen fleksible forskningsopplegg. Dette betyr at jeg som forsker har større frihet til å justere på datainnsamlingen underveis, dersom nødvendig. Ved å anvende kvalitative intervjuer som metode vil jeg også ha en bedre forutsetning for ærlige og gjennomtenkte svar fra informantene, enn hvis metoden hadde vært kvantitativ. Samtidig er det, ifølge Grønmo, viktig å etablere et tillitsforhold mellom meg i forskerrollen og informantene, da dette vil kunne påvirke det endelige datagrunnlaget (Grønmo, 2016, s. 171). En semi-strukturert intervjuguide vil også kunne lede til informasjon som ellers kan være vanskelig å få tak i. Dette er en klar fordel med å ha et fleksibelt forskningsopplegg, da det gir rom for spontane spørsmål som i en fastsatt intervjuguide kunne blitt oversett.

Ved å kun bruke informanter som er ansatt i kommunen, gir dette meg et godt informasjonsgrunnlag. Det kan problematiseres hvorvidt utvalget av informanter er variert *nok*, men da oppgaven har som hensikt å gå i dybden på Bergen kommune, ville det vært lite formålstjenlig å bruke informanter fra eksempelvis andre kommuner. Oppgavens tidsbegrensning støtter også opp valget om å begrense utvalget av informanter til Bergen kommune. Dersom oppgaven av tidsmessige årsaker ikke måttet begrenses, kunne det vært interessant å intervjue informanter med liknende stillinger i andre kommuner. Med dette kunne jeg belyst likheter og forskjeller knyttet til hvordan kommunene forholder seg til-og jobber med sikkerhetskultur i lys av personvern. For denne oppgaven anser jeg det også som en styrke at

informantene er ansatt i ulike avdelinger i kommunen, da dette gir grunnlag for ulike tolkninger av arbeidet kommunen gjør.

Kvalitativ innholdsanalyse kan, ifølge Grønmo, brukes på de alle former for dokumenter (Grønmo, 2016, s. 175). Som forsker er det jeg som står for utvalget av hvilke dokumenter som skal inngå i analysen. Tidsbegrensning på oppgaveløpet gjør at enkelte dokumenter må utelukkes, samtidig som jeg står fritt til å inkludere de dokumentene som best belyser oppgavens tema og problemstilling. Valg av dokumenter kan i seg selv også begrense studien, da eldre dokumenter kan tegne et feilaktig bilde av hvordan dagens situasjon er. Det ble derfor viktig å kun inkludere nyere dokumenter.

En utfordring med kvalitativ data, er hvordan den tolkes. Grønmo påpeker at forskers eget perspektiv kan påvirke hvordan resultatet tolkes. Med dette menes at forsker kan tolke dataen med enten et for snevert eller et for bredt perspektiv. Dette kan lede til flere utfordringer, blant annet at tekster som ellers vil fremstå som relevant for oppgaven blir ignorert, tolkningsmuligheter blir oversett eller ikke tilstrekkelig drøftet fordi det samsvarer ikke med forskers perspektiv (Grønmo, 2016, s. 180).

Samtidig er jeg som forsker bevisst på egen kildekritisk- og kontekstuelle forståelse, og hvordan dette kan virke inn på forskningens resultater. For å unngå at dokumentene fremstår som lite representative, som ikke-autentiske eller lite troverdige, har jeg vurdert ulike dem opp mot forskjellige perspektiver og etter ulike kategorier. På denne måten blir dokumentenes relevans for oppgaven i høyere grad sikret (Grønmo, 2016, s. 180-181). Kategoriene brukt i den kvalitative innholdsanalysen samsvarer med den tematiske oversikten i intervjuguiden. Dette sikrer at jeg som forsker leter etter informasjon som enten bekrefter eller avkrefter data som fremkommer ved de kvalitative intervjuene.

Å gjennomføre kvalitative intervjuer krever en inngående kunnskap om temaene som skal gjennomgås, samtidig som det foreligger et behov for å vite *hvem* du intervjuer og *hvorfor* nettopp de utvalgte informantene vil utgjøre det beste datagrunnlaget for oppgaven. Informantene kan miste motivasjonen til å delta og/eller bli skremt eller stresset av tanken på at det blir gjort opptak av intervjuene (Grønmo, 2016, s. 170-171). For å unngå dette er det viktig at jeg evner å opplyse informantene tilstrekkelig i forkant av intervjuet, samt å stille meg tilgjengelig for spørsmål eller videre informasjon i etterkant dersom det er behov.

En annen utfordring med å bruke intervju som metode er det subjektive aspektet ved det ferdige datagrunnlaget. Da alle informantene er tilknyttet Bergen kommune, kan intervjudataen bære preg av dette. Jeg stiller spørsmål om arbeidshverdag, om arbeidsoppgaver og hvordan Bergen kommune som organisasjon har valgt å organisere sitt arbeid tilknyttet ulike tema. Det er likevel at datagrunnlaget blir tolket med «en klype salt», grunnet det subjektive aspektet ved intervjudataen. I tillegg vil data som hentes fra den kvalitative innholdsanalysen kunne bygge opp under intervjudataen dersom de samsvarer. Samsvarer de ikke, vil dette være interessante diskusjonspunkter i analyse og drøftingskapittelet (kapittel 5).

3.6.3 Etiske vurderinger

For å sikre at datagrunnlaget basert på de kvalitative intervjuene skulle være tilstrekkelig, var det foretrukket å ta opp intervjuene. Det ble derfor nødvendig å melde inn oppgaven til NSD, da en personopplysning kan defineres som «... enhver opplysning som kan knyttes til en person» (NSD, u.å.). Ved å benytte en båndopptaker, sikret jeg at rollen min som intervjuer ble brukt for å lytte etter respons og bruke denne for å stille andre relevante spørsmål. I tråd med gjeldende retningslinjer, ble intervjuene gjennomført først etter godkjenning fra NSD gitt.

Ved å bruke en båndopptaker under intervjuene, sikret jeg at lydopptaket og tilhørende personopplysninger ble lagret på et uavhengig sted, hvor sjansen for at uvedkomne fikk tilgang var liten. Transkriberingene ble lagret uten informantenes navn i passord-beskyttede dokumenter. Hver informant ble tildelt en bokstav, som de vil refereres til videre gjennom oppgaven. Oversikten over informantenes navn og stilling i Bergen kommune ble også holdt separat fra transkriberingene

I samtykkeskjemaet som ble sendt ut i forkant av intervjuene, ble det opplyst om relevante forhold knyttet til deres rolle som informant. Informantene ble underrettet om oppgavens formål og hvorfor nettopp de var kontaktet. Videre måtte hver informant godkjenne; *å delta i kvalitativt intervju, at det gjøres opptak av intervjuet, at opplysninger publiseres om meg slik at jeg kan gjenkjennes*. Dersom informanten(e) ønsket å være anonyme var dette også en alternativ. Informantene måtte da krysse av for: *Jeg ønsker at (enkelte) opplysninger om meg er anonyme i publikasjonen (vennligst kryss av nedenfor), stilling, arbeidssted, rolle og ansvarsområde*. I tillegg ble det opplyst om at de når som helst, frem til oppgavens innleveringsdato 15 juni,

kunne tilbaketrekke sitt samtykke. Dersom samtykket tilbaketrekkes, vil bidraget og opplysninger som kan knyttes til vedkommende enten anonymiseres eller slettes.

4. Empiri

I dette kapittelet vil oppgavens empiriske funn presenteres. Funnene fra de kvalitative intervjuene løfter frem informantenes holdninger og tilnærming til arbeidet kommunen gjør og setter det i kontekst. Funn fra den kvalitative innholdsanalysen tegner et bilde av hvordan kommunen forsøker å jobbe med sikkerhetskultur, personvern og andre relevante områder som digitalisering, risiko, sårbarheter og kompetanse.

De empiriske funnene presenteres tematisk, i tråd med oppgavens to forskningsspørsmål. Kapittel 4.1- 4.3 presenterer funn relevant for forskningsspørsmål 1, mens kapittel 4.4 formidler funn relevant for forskningsspørsmål 2. Forskningsspørsmål 3 har som hensikt å vurdere den helhetlige sikkerhetskulturen og dens arbeid med å sikre arbeidet med personvern, i lys av hva som fremkommer i analysen og drøftingen av forskningsspørsmål 1 og 2. Dens tilnærming til sikkerhet skal vurderes opp mot teori om safety og security, og forskningsspørsmålet har av den grunn ingen direkte funn tilknyttet seg.

Dette gir oversiktlig og systematisk presentasjon som sikrer en dyp og gjennomgående forståelse for oppgavens tema og problemstilling: «*Hvordan kan Bergen sitt arbeid med sikkerhetskultur sikre en god og forsvarlig håndtering av digitale personopplysninger?».* Den tematiske presentasjonen av funnene sørger for at relevant data blir presentert og skaper dernest et godt grunnlag for analyse og drøfting av funnene i neste kapittel.

4.1 Personvern

I «Digitalisering og innovasjon i Bergen kommune 2017-2020» formidles det at personvern og informasjonssikkerhet skal fungere som en integrert og sammenhengende del av utviklingen og bruk av nye digitale løsninger i kommunen (Bergen kommune, 2017, s. 2 og 26). Dette samsvarer med fokuset personvern og informasjonssikkerhet har i digitaliseringsstrategien for kommunen. Digitaliseringen forutsetter dermed et kontinuerlig fokus på arbeidet med informasjonssikkerhet og personvern, da endringer og forbedringer i digitale systemer og verktøy krever nye tilpasninger og behov (Bergen kommune, 2021a, s. 7). «Oversikt og god

forvaltning av informasjonssikkerhet er en forutsetning for forsvarlig håndtering av personopplysninger [...]» (Bergen kommune, 2017, s. 14).

«Ivaretakelse av personvernet innebærer blant annet at [...] brukeren vet hvor informasjonen er hentet fra» (Bergen kommune, 2021a, s. 7). Dette er i tråd med målsetningen Bergen kommune har om å være en åpen og transparent kommune når det kommer til arbeid med informasjonssikkerhet og personvern. Dette formidles også av informantene.

4.1.1 Hvordan jobber Bergen kommune med personopplysninger og personvern

«Digitalisering og innovasjon for Bergen kommune 2017-2020» tar opp den nye personvernsforordningen GDPR, og konstaterer videre at kommunens strategi og håndtering av personopplysninger må oppdateres i forhold til denne (Bergen kommune, 2017, s. 14).

I høringsutkastet til «Temaplan for informasjonssikkerhet og personvern 2021-2025» presenterer Bergen kommune fem hovedmål som skal legge føringer for hvordan kommunen fremover skal arbeide med informasjonssikkerhet og personvern, hvor to av dem utpeker seg som særlig relevant; «1) Bergen kommune skal gi helhetlige og samordnede føringer for arbeidet med informasjonssikkerhet og personvern, som etterleves i hele organisasjonen. 2A) Ansatte og innleide skal ha kompetanse til å håndtere personopplysninger, slik at hensynet til informasjonssikkerhet og personvern ivaretas i tråd med gjeldende regler. 2B) Høy grad av innebygget sikkerhet gjennom design og utvikling skal være et grunnprinsipp for alle digitale systemer i Bergen kommune. Dette betyr at kommunens systemer skal være tilpasset rimeligere forventninger til kompetansenivå hos ansatte og innleide» (Bergen kommune, 2021b, s. 6).

I tråd med økt oppmerksomhet rundt personvern som fagområde, øker således behovet for å skape en organisatorisk standard som tar sikte på å oppfylle de krav og plikter som stilles til virksomheter, ovenfor for eksempel innbyggerne (Bergen kommune, 2021b, s. 17). «Digitaliseringsstrategien 2021-2025» formidler at «... digitalisering i Bergen kommune skal skje på en sikker måte der personvernet til ansatte og innbyggerne blir ivaretatt» (Bergen kommune, 2021a, s. 2). Kommunens arbeid med informasjonssikkerhet og personvern skal i tillegg være risikobasert. Dette betyr at alt arbeid kommunen gjør med behandling av personopplysninger skal være i tråd med gjeldende lover og retningslinjer (Bergen kommune, 2020c, s. 10).

På spørsmål om hvilke tiltak som er iverksatt for å sikre godt personvern i kommunen fremover, refererer flere av informantene til Helhetlig Gjennomgang, og trekker særlig frem kompetanse, kultur og læring som viktige læringspunkt for kommunen. Fra informantene fremkommer det også en økt bevissthet rundt regler, rutiner og krav som stilles til ansatte i forbindelse med å ivareta eget ansvar knyttet til informasjonssikkerhet og personvern. Det formidles videre at API i stor grad opplever økt pågang, og skal i etterkant av Helhetlig Gjennomgang være en større del av prosjekter enn tidligere.

4.1.2 Problemstillinger og utfordringer knyttet til personvern

Undersøkelser gjort på vegne av Bergen kommune viser at ansatte « [...] i varierende grad har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet, og at de ansatte derfor i varierende grad etterlever disse rutinene og retningslinjene» (Bergen kommune, 2021b, s. 14). Undersøkelsene konkluderer derfor med at arbeidet som blir gjort av kommunen her bryter med flere grunnleggende informasjonssikkerhetsprinsipp (Bergen kommune, 2021b, s. 14).

Dette samsvarer med en spørreundersøkelse gjennomført av Deloitte i en forvaltningsrevisjon av Bergen kommune. Undersøkelsen viste at kun rundt halvparten av kommunens ansatte var innforstått med ansvaret tillagt deres rolle vedrørende informasjonssikkerhet og personvern. På spørsmål om ansatte vet hvor de kan finne informasjon om retningslinjer og rutiner for å håndtere problemstillinger som reiser seg rundt personvern og informasjonssikkerhet, svarte 30% av respondentene «nei» (Deloitte, 2019, s. 31). Oppsummert er det Deloitte sin vurdering at ansatte generelt sett er innforstått med sitt informasjonssikkerhetsansvar, men er i liten grad kjent med kommunes regler og retningslinjer for håndtering av personopplysninger ol. samt hvor ansatte kan finne relevant informasjon (Deloitte, 2019, s. 31).

I internkontrollrapporten som kom i etterkant av Vigilo-saken påpekes det at interne ressurser fra avdeling personvern og informasjonssikkerhet i liten grad benyttes (Seksjon for internkontroll, 2019, s. 7). I samtale med informanter særlig tilknyttet API, fremkommer det at avdelingen ikke prioritert til å delta i prosjekter. Dette knytter informantene til at avdelingen ofte kan oppleves som en flaskehals i prosjekter, som hindrer rask fremgang. Informant B sier at «Erfaringsmessig så er det vel heller slik at vi blir koblet på for sent».

Informantene fikk spørsmål om de opplever ansatte at i kommunen er observante på problemstillinger tilknyttet personvern og håndtering av personopplysninger. Informantene synes å være enig i at arbeidet er blitt bedre med tiden, men at manglende kompetanse, misnøye rundt kvalitetssystemet BkKvalitet og spørsmål knyttet til hva som er «godt nok» kan gjøre at ansatte opplever slike problemstillinger som vanskelig og utfordrende. Flere at informantene trekker frem et klart forbedringspotensial blant de ansatte. Informant D opplever at kommunen arbeider aktivt med å finne trygge og robuste løsninger som enkelt kan tas i bruk av de ansatte.

Videre fikk informantene spørsmål om arbeidsmetoden rundt informasjonssikkerhet og personvern har vært i endring de siste årene. Informantene er tilsynelatende enig i at det har vært en endring, noe som har ledet til både positive og negative erfaringer. Informant F peker på økt arbeidsmengde og ansvar som følge av den økte bevisstheten rundt personvern og informasjonssikkerhet. Flere av informantene uttrykker at det er lettere å få tak i informasjon enn før, og en oppfatning av at kommunen aktivt setter det mer på agendaen. En annen utfordring kommunen må belage seg på å håndtere er ulik forståelse for fagområdet. Det fremkommer en ulik forståelse for, interesse av og fokus på personvern og informasjonssikkerhet blant informantene som er tilknyttet API og informantene som jobber med ulike prosjekter i kommunen.

4.1.3 Hvordan skal kommunen arbeide med å sikre godt personvern?

I «Byrådssak /20» presenteres hovedfunn fra Helhetlig Gjennomgang. Byrådet understreker behovet for å tilrettelegge for en «[...] god overgang mellom arbeidet som har vært gjort i gjennomgangen og det mer langsiktige arbeidet for å sette kommuneorganisasjonen i stand til å ivareta oppgaver knyttet til personvern og informasjonssikkerhet på en god måte fremover» (Bergen kommune, 2020b, s. 1).

På spørsmål om hvilke utfordringer som ligger i å sikre godt personvern fremover er det ressurser, ressursknapphet og kompetanse som går igjen hos informantene. Informant A sier at «Jeg mener jo på ingen måte at vi har kommet til modenhetsnivået, altså vi har jo en veldig lang vei å gå», og begrunner dette med at fordi personvern er forholdsvis nytt, det er komplekst og det er relativ liten kompetanse på det. Derfor må kommunen jobbe systematisk og med fokus på å heve kompetanse og utvikle kompetanse. Informant A trekker også frem et ønske om mer universelle krav til personvern og informasjonssikkerhet hos leverandører. Dette kan lette noe

av arbeidsmengden til kommunen, dersom det ble stilt like krav i forhold til ivaretakelse og beskyttelse av personopplysninger til alle leverandører.

Innebygget sikkerhet, manglende infrastruktur og manglende arbeidsprosesser trekkes også frem som utfordringer, av informantene. Med manglende infrastruktur mener Informant D at det ikke er godt nok tilrettelagt for deling av informasjon mellom ulike etater i kommunen. «Alle jobber på hver sin plattform, men flyten mellom de plattformene tror jeg er en utfordring». Flere av informantene trekker også frem manglende ledelsesforankring og manglende engasjement fra ledelsen til å etterleve krav og retningslinjer utover i organisasjonen.

4.2 Sikkerhetskultur i Bergen kommune

4.2.1 Dagens sikkerhetskultur

Ifølge «Digitaliseringsstrategien 2021-2025» skal kommunen etterstrebe personvern og informasjonssikkerhet som en integrert del av arbeidsplassen, og at videreutviklingen av sikkerhetskulturen i kommunen leder til de to blir en naturlig del av arbeidet Bergen kommune gjør (Bergen kommune, 2021a, s. 24). Digitaliseringsstrategien skal tilrettelegge for arbeidet som gjøres de neste årene med å forme en sikkerhetskultur, i tillegg til å « [..] sikre strategisk sammenheng og koordinering mellom byrådsavdelingenes digitaliseringsarbeid [...]» (Bergen kommune, 2021a, s. 10). Strategien trekker blant annet frem kompetanse som et viktig verktøy som skal sikre riktig bruk av kommunens digitale systemer, og minske sannsynligheten for uhell eller ulykker (Bergen kommune, 2021a, s. 2).

På spørsmål knyttet til sikkerhetskulturen i kommunen i dag, fremkommer det varierte beskrivelser fra informantene. Flere av informantene peker på ulik eller manglende forståelse og holdninger til sikkerhetskultur blant ansatte, og trekker videre frem at det inntil nylig ikke egentlig har vært en form for sikkerhetskultur i kommunen. Informant B sa «Så kulturen har nok vært-det har nok ikke vært en sikkerhetskultur i kommunen, men den har blitt sterkt forbedret det siste året [...]». Ifølge informantene fra API vil sikkerhetskultur med et særlig fokus på personvern og informasjonssikkerhet være arbeid kommunen skal prioritere fremover. Samtidig opplever Informant D frem at «[...] Bergen kommune som en såpass stor arbeidsplass at det å drive frem en sikkerhetskultur er noe utfordrende og et noe fragmentert arbeid».

4.2.2 Utfordringer knyttet til dagens sikkerhetskultur

Behovet for å «[...] etablere en felles forståelse i virksomheten på tvers av enheter for begge fagområdene [...]» (Bergen kommune, 2021b, s. 4), trekkes som et viktig innsatsområde i «Temaplan for informasjonssikkerhet og personvern». Bergen kommune er en stor organisasjon med mange ansatte, og arbeidet med å skape en felles forståelse for ulike fagområder kan være utfordrende, som påpekt av Informant D ovenfor.

Kompetanse, ressursknapphet, ulik forståelse og manglende ledelsesforankring trekkes frem som utfordringer knyttet til sikkerhetskultur i kommunen. Tre av informantene trekker i tillegg frem en silo-orientert organisering som en klar utfordring knyttet til dagens sikkerhetskultur. Det er sterke fagmiljøer som jobber stykkevis med sikkerhetskultur. Da dette arbeidet ikke er samkjørt kan miljøene havne i konkurranse med hverandre, noe som leder til at de ansatte får en fragmentert og ulik forståelse av hva sikkerhetskultur er. Informant D sier videre at ansatte ikke er tjent med en slik tilnærming til sikkerhetsarbeidet, samtidig som det er vanskelig å utpeke hva som kunne vært gjort bedre.

På oppfølgingsspørsmål om hvorvidt kommunen bør fokusere på å implementere sikkerhetskultur blant ledelse eller ansatte, fremkommer det blant informantene at arbeidet må starte hos ledelsen. En engasjert og kunnskapsrik ledelse kan sette gode premisser for å innføre sikkerhetskulturen hos sine ansatte. Noen av informantene trekker videre frem at ledelsesforankring er viktigst, men poengterer at kommunen bør ta sikte på å nå ut til alle.

4.2.3 Hvordan skal sikkerhetskulturen i kommunen forbedres?

«Endring og omstilling krever at ledere på alle nivåer i kommunen må ha kunnskap og evne til å forstå det digitale landskapet» (Bergen kommune, 2021a, s. 2). Kompetanseheving og kompetansebygging beskrives i strategien som sentralt for at ansatte skal anvende digitale verktøy korrekt. Dette fremkommer også i «Temaplan for informasjonssikkerhet og personvern», som påpeker viktigheten av at både ansatte og ledere er innforstått med hvilke oppgaver som er tillagt deres rolle, samt hvordan oppgavene skal løses (Bergen kommune, 2021b, s. 22).

Byrådet påpeker videre at det er nødvendig at kommunen videreutvikler gode læringssituasjoner og læringsarenaer for ansatte, hvor kunnskap om informasjonssikkerhet og

personvern er i fokus. «Kun en organisasjon med ansatte som evner å avdekke brudd på informasjonssikkerhet og personvern kan utvikle den sikkerhetskulturen som kreves i den digitale transformasjonen» (Bergen kommune, 2021b, s. 22). Ifølge «Reglement for personvern og informasjonssikkerhet» skal alle kommunens ansatte ha «... kunnskap om og gode holdninger til informasjonssikkerhet og personvern for å underbygge en betryggende sikkerhetskultur» (Bergen kommune, 2020c, s. 7), altså kunnskap om det immaterielle med en kultur.

Blant flere av informantene oppleves ikke sikkerhetskultur som noe nytt, men har i etterkant av diverse mediesaker og et mer aktivt Datatilsyn fått et annet fokus enn tidligere. Det trekkes også linjer mellom mediesakene tilknyttet Vigilo og skoleeleven som fant sikkerhetshullet, og Helhetlig Gjennomgang. Flere av informantene trekker synergier på tvers av arbeidet som skal gjøres fremover knyttet til sikkerhetskultur og Helhetlig Gjennomgang, og opplever dette som et godt utgangspunkt. Kun Informant D som stiller spørsmål til selve gjennomgangen. Selv var ikke informanten en del av arbeidet, men stiller spørsmål til tempoet de ulike systemene har vært gjennomgått i. «Det er min refleksjon i ettertid [...] at ting må ha gått for fort, altså da har man ikke gått i dybden [...].

På spørsmål om hvorvidt sikkerhetskultur er noe Bergen kommune aktivt arbeidet med, deler informantene samme formening om at sikkerhetskultur er et fokusområde i kommunen. Det formidles videre at sikkerhetskultur er komplisert, og informantene trekker også her frem ledelsesforankring som essensielt for arbeidet kommunen gjør videre. Samtidig forventes det gjerne at ledere også skal gå foran som et godt eksempel. Dette vil sikre at arbeidet med personvern og informasjonssikkerhet gir reelle virkninger, ifølge Informant A og B.

Informantene fikk oppfølgingsspørsmål om de opplever at kommunen har en straffekultur, altså om handlinger kan få negative konsekvenser for den ansatte. Den generelle oppfatningen blant informantene er at kommunen ikke har en straffekultur. Samtidig trekker to av informantene frem at dersom en handling er et klart tjenestebrudd eller direkte mislighold av den ansattes arbeidsoppgaver, kan det vente konsekvenser. Informant B derimot opplever ikke at handlinger får noe negative konsekvenser for den ansatte. Dersom noe går galt er kommunens fokus å skjerme den ansatte, og heller fokusere på prosesser rundt-og derav finne ut hva som gikk gale, og hvorfor.

4.2.4 Avvik og avviksmeldinger

Flere av informantene formidler at kommunen arbeider mot å ha en åpenhetskultur rundt avvik og avviksmeldinger. Informant A sier at «[...] du skal melde, det skal håndteres, snakkes om og forbedres». I «Reglement for digitalisering og IKT» understreker Bergen kommune at avviksmeldinger skal alltid følge gjeldende retningslinjer og de riktige systemene (Bergen kommune, 2020d, s. 4). I «Reglement for personvern og informasjonssikkerhet» utdypes dette med «Avvik [...] skal rapporteres og håndteres etter nærmere fastsatte prosedyrer for å begrense skader, sikre gjenoppretting av normaltilstand og innarbeide læring for å hindre gjentakelse av avvik» (Bergen kommune, 2020c, s. 13).

Kommunen har en aktiv tilnærming til forebyggende arbeid med informasjonssikkerhet og personvern. Dette skal gjøre omfang og konsekvenser av avvik og uønskede hendelser så liten som mulig. Arbeidet innebærer at kommunen aktivt må lære av tidligere feil og herunder vurdere endringer eller nye tiltak i prosedyrer og risikovurderinger (Bergen kommune, 2020c, s. 13). «Temaplan for informasjonssikkerhet og personvern 2021-2025» understreker videre viktigheten av å melde avvik. Den vektlegger at både ansatte, men ledere spesielt, sammen har et ansvar for å danne en meldekultur i kommunen. En leder sitt arbeid blir herunder å sørge for å «[...] trygge de ansatte, slik at avvik meldes inn i tråd med retningslinjene og de fristene virksomheten har for å eventuelt melde videre i Datatilsynet» (Bergen kommune, 2021b, s. 29).

Deloitte undersøkte Bergen kommunes avviksstatistikk, og konkluderer med at avvikskulturen i kommunen «[...] ikke fullt ut samsvarer med relevante anbefalinger eller generelle prinsipper for god internkontroll» (Deloitte, 2019, s. 3). Da undersøkelsen ble gjennomført i tidsrommet februar til september 2019 opplyste 33% av respondentene at de ikke kjente til rutinene knyttet til avviksmelding ved informasjonssikkerhetsbrudd. Dette er en nedgang fra da samme undersøkelse ble gjennomført i 2014, hvor 62% ikke var kjent med rutinene (Deloitte, 2019, s. 18). Deloitte påpeker videre at et nytt kvalitetssystem for avviksmeldinger ble innført tidligere samme år, men konkluderer likevel med at avvik ikke blir tilstrekkelig meldt blant ansatte i kommunen (Deloitte, 2019, s. 26).

Videre formidler Deloitte at i intervju med ansatte som jobber tett opp mot informasjonssikkerhet og personvern, presiseres det at det (da) nye kvalitetssystemet, *BkKvalitet*, skulle gjøre det enklere for ansatte å finne frem til informasjon om hvordan avvik

skulle meldes. Samlet skulle dette lede til mindre feilrapportering enn tidligere erfart i kommunen (Deloitte, 2019, s. 18). Dette tydeliggjøres også av «forhenværende konstituert personvernombud opplever, basert på innmeldte avvik, at ansatte i kommunen har et bevisst forhold til informasjonssikkerhet, også utover det som knytter seg til personvern og personopplysninger» (Deloitte, 2019, s. 19). Likevel erkjenner vedkommende at det sannsynligvis er store mørketall på «[...] faktiske avvik knyttet til informasjonssikkerhet sett opp mot innmeldte avvik» (Deloitte, 2019, s. 19). Dette samsvarer også med informantenes oppfattelsr tilknyttet avviksmeldinger. På spørsmål om hvor mange avvik ansatte har opplevd og meldt fra om, svarte 18% at «de færreste» ble meldt, mens 21% svarte at ingen avvik ble meldt videre (Deloitte, 2019, s. 56).

Seksjon for internkontroll sin rapport om Vigilo-saken understrekte betydningen av å melde inn hendelser slik at det raskt kunne igangsettes tiltak, samt trekke lærdom ut av hendelsen (Seksjon for internkontroll, 2019, s. 13). I sin gjennomgang ble det avslørt at flere av avviksmeldingene knyttet til Vigilo-saken ikke ble meldt inn på tidspunktet de ble oppdaget, men ble registrert i ettertid. Rapporten peker videre på manglende kompetanse som en forklaring til hvorfor avvik ikke blir meldt (Seksjon for internkontroll, 2019, s. 13). «Det er derfor grunn til å anta at det kan være flere avvik på området, enn det som er registrert i kommunens system for avviksmeldinger» (Seksjon for internkontroll, 2019, s. 14).

På spørsmål om hvorvidt ansatte i kommunen er flinke til å melde avvik, sier Informant B «Nei, jeg tror ikke det. Jeg tror fortsatt det er underrapportering». Samtidig påpeker informanten at kommunen ser en stigende trend i antall avvik som meldes, og trekker linjer mellom dette og kvalitetssystemet til kommunen. Informanten tror dog at kommunen fortsatt har en vei å gå før det ikke lenger er underrapportering. Denne oppfatningen deles som nevnt blant flere av informantene.

På spørsmål knyttet til BkKvalitet, kommunens kvalitetssystem, har informantene delte meninger i forhold til brukervennlighet og hvor godt systemet egentlig fungerer. Flere av informantene ser fordelen med å ha et felles system hvor avvik meldes, og beskriver systemet som enkelt og effektivt å bruke, og opplever også selv en stigende trend på avviksmeldinger i kommunen. Informant E og F avviker fra den generelle enigheten, og beskriver systemet som «BkKvalitet er et drita dårlig system som har veldig dårlig bruketerskel», og opplever at dette kan føre til at ansatte ikke melder avvik.

Informantene fikk oppfølgingsspørsmål om hvorfor avvik ikke blir meldt i kommunen. Manglende forståelse, kompetanse og frykt (for å se dum ut og eksponere arbeidsplassen) og manglende synlige ettervirkninger av innmeldte avvik trekkes frem som eksempler. Samtidig opplever informantene som nevnt at kommunen stadig blir bedre i å melde avvik, men trekker videre frem at avvikskultur er en kontinuerlig prosess, som aldri blir god nok. Informantene er enig i at dersom avvik ikke meldes, er det følgelig vanskelig å si noe om tall kommunen ikke har. Av denne grunn er det også enighet om at det kan være store mørketall på avviksmeldinger, og at kommunen har klare forbedringspotensial tilknyttet det å bygge en god avvikskultur.

4.2.5 Tillit

«Befolkningens tillit til offentlig sektor er høy i Norge sammenliknet med mange andre land» sier «Digitaliseringsstrategien for Bergen kommune 2021-2025» (Bergen kommune, 2021a, s. 9). Hvordan kommunen velger å arbeide med å sikre innbyggernes informasjon og således ivaretar den enkeltes personvern, kan ha innvirkning på innbyggernes tillit til kommunen og informasjonen kommunen gir (Bergen kommune, 2021b, s. 3). Ifølge «Temaplan for informasjonssikkerhet og personvern» ønsker byrådet at kommunen «[...] skal jobbe systematisk for å [...] etablere en informasjonssikkerhetskultur i hele kommunens organisasjon. Det vil skape tillit til at kommunen ivaretar den enkeltes personvern på en trygg måte» (Bergen kommune, 2021b, s. 4).

På spørsmål om hvordan kommunen sikrer tillitsforholdet mellom seg selv og innbyggerne, peker Informant A på et tillitsbrudd, som kan være vanskelig å reparere. Samtidig understreker informanten at «[...] jeg tror også at forståelsen for personvern ikke nødvendigvis er så mye større hos innbyggerne heller». Det er en generell konsensus blant informantene at kommunen aktivt jobber med å styrke dette tillitsforholdet, men informantene fremhever ulike metoder for hvordan dette arbeidet gjøres.

På spørsmål knyttet til tillit trekker flere informanter igjen frem Helhetlig gjennomgang. En av informantene beskriver den som det største tiltaket knyttet til tillit, sammen med «Digitaliseringsstrategien 2021-2025» og «Temaplan for informasjonssikkerhet og personvern». På spørsmål om informantene opplever at kommunens tidligere svake håndtering av personopplysninger, har svekket dens tillit hos befolkningen, svarer Informant F at «Det som er med sånne hendelser er at det er aldri alt som kommer frem i media [...]». Et sterkt

mediefokus kan et sterkt mediefokus svekke arbeidet som gjøres av kommunen, samtidig som ikke alle sider av saken blir belyst, ifølge informanten.

I 2019 gjennomførte Deloitte et nettfiskeforsøk (phising) på ansatte i Bergen kommune. Rundt 13 000 ansatte fikk e-post med en undersøkelse om «etikk, holdninger og adferd». For å svare på undersøkelsen måtte ansatte oppgi brukernavn og passord (Deloitte, 2019, s. 5 (vedlegg)). Av ansatte som mottok e-posten valgte 3226 ansatte å trykke på lenken som var vedlagt i e-posten, og ga fra seg brukernavn og passord. Ifølge Deloitte var det dermed 24% (nesten en av fire) som valgte å trykke på lenken, mens 16% av denne andelen valgte å dele brukernavn og passord (Deloitte, 2019, s. 58).

4.2.6 Hvordan trekker Bergen kommune lærdom ut av hendelser?

Informantene fikk spørsmål om Bergen kommunes evne til å trekke lærdom ut av hendelser som ikke har ledet til ønsket resultat. Det foreligger en generell konsensus om at kommunen arbeider godt med å trekke lærdom ut av hendelser, men informantenes oppfatning av hva som er viktig i dette arbeidet er varierende.

Igjen blir Helhetlig Gjennomgang referert til blant flere av informantene, særlig blant informantene fra API. Gjennomgangen representerer et godt eksempel på hvordan kommunen trekker lærdom ut av hendelser, ifølge informantene. Andre informanter trekker også frem at kommunen burde arbeidet mot å ligge i forkant av hendelser som kan true personvern og informasjonssikkerheten. Dette krever at kommunen aktivt arbeidet med å implementere tiltak og rutiner, samt bevisstgjøre ansatte på hva som kan gå gale. På denne måten vil kommunen kunne forebygge for nye hendelser som kan komme fremover.

Noen av informantene fikk oppfølgingsspørsmål om lærdommen kommunen trekker ut aktivt brukes i arbeidet videre, og om informantene oppfatter dette arbeidet som bra eller dårlig. Flere av informantene fremsto som tilfreds med arbeidet kommunen gjør. Manglende risikostyring, mangelfull kultur og silo-tenking i kommunen trekkes dog frem som utfordringer kommunen har med å trekke lærdom ut av hendelser.

4.3 Digitalisering i Bergen kommune

For at Bergen kommune skal nå sine målsetninger og således løse samfunnsoppdraget sitt, har fokuset på digitalisering vært beskrevet som et innsatsområde kommunen *må* vektlegge i tiden fremover (Bergen kommune, 2017, s. 1-2). Dette fremkommer i blant annet «Digitalisering og innovasjon i Bergen kommune 2017-2020» og «Digitaliseringsstrategi Bergen kommune 2021-2025». Arbeidet har skapt en forventning blant innbyggerne i kommunen til mer brukervennlige og effektive tjenester parallelt som kommunen arbeider med implementeringen av nye digitale løsninger (Bergen kommune, 2021a, s. 2).

Kommunen har dermed som mål at ny teknologi skal gjøre at tjenestene oppleves som mer effektive og brukervennlige (Bergen kommune, 2021a, s. 2). «Bergen kommunes viktigste oppgave er å tilby gode tjenester av høy kvalitet til innbyggerne» (Bergen kommune, 2021b, s. 5). Det fremkommer i samtaler med informantene at anskaffelse av nye digitale verktøy og tjenester skjer på grunnlag av et behov, samtidig som det er en forutsetning for å holde følge med samfunnsutviklingen. En systematisk tilnærming til informasjonssikkerhet og personvern beskrives herunder som en forutsetning for å nå dette målet (Bergen kommune, 2021b, s. 5). Blant informantene utvises det også en enighet om betydningen av å vektlegge informasjonssikkerhet og personvern i arbeidet med anskaffelse av nye digitale systemer og verktøy til kommunen.

4.3.1 Målsetning med kommunens arbeid tilknyttet digitalisering

På spørsmål om hvordan tidligere hendelser har formet arbeidet som Bergen kommune gjør i dag, fremkommer det en generell enighet om dette blant de fleste informantene. Informantene opplever Bergen kommune som en lærende organisasjon og at tidligere hendelser har ledet til en viss grad av holdnings-og perspektivendring. Samtidig formidler flere av informantene at kommunen fortsatt har en vei å gå. Informant A sa at «Man blir jo aldri perfekt». Med utsagnet, «Jeg vet ikke om enkeltsaker gjør det», viker Informant C noe fra den generelle holdningen blant de øvrige informantene.

Målsetningen med arbeidet Bergen kommune gjør vedrørende digitalisering er å skape en langvarig og stødig digitaliseringskultur som forankres på alle nivå innad i kommunen (Bergen kommune, 2017, s. 15). Videre fremkommer det i digitaliseringsstrategien at «Gjennom digitalisering kan vi utforme sammenhengende tjenester på tvers av forvaltningsnivåer,

byrådsavdelinger og sektorer [...]» (Bergen kommune, 2021a, s. 2). Blant informantene er det en delt enighet om at Bergen kommunes aktive tilnærming til digitaliseringen de siste årene har skapt et godt grunnlag for arbeidet kommunen skal gjøre videre.

Kommunens digitaliseringsstrategi går videre inn på hvordan kommunen beveger seg bort fra digitalisering og arbeider mot en «digital transformasjon». Dette innebærer å bevege seg fra et fokus på utvikling og implementering av digitale tjenester, til et perspektiv som innebærer et sterkere fokus på ansatte, kompetanse og således hvordan kommunen fullt kan utnytte digitaliseringens innebygde potensiale (Bergen kommune, 2021a, s. 6). Kommunens fokus på digital transformasjon understøttes av «Én digital offentlig sektor» som er den nasjonale strategien for digitalisering i Norge.

Digital transformasjon fremstår som et viktig fokuspunkt i kommunens digitaliseringsstrategi. Arbeidet vil innebære endringer i hvordan kommunen arbeider i form av endring i regelverk, endringer innad i organisasjonen og designprosesser. Dette har som formål å skape mer brukervennlige og smidige tjenester for brukerne. «Digitaliseringsarbeidet handler ikke bare lenger om *hva* vi skal digitalisere, men *hvordan* digitalisering kan skape innovasjon og bidra til effektivisering» (Bergen kommune, 2021a, s. 7). Ifølge «Byrådssak /20» er Bergen kommune teknologisk klar for den digitale transformasjonen, men at dette arbeidet kan hindres av uendret organisatorisk struktur i kommunen. Det er derfor nødvendig med tilpasningsbehov slik at nye digitale verktøy og systemer best kan utnyttes (Bergen kommune, 2020b, s. 4). Omorganisering av avdelinger, oppbemanning, nye retningslinjer og rutiner for arbeid med personvern og informasjonssikkerhet trekkes frem som eksempler fra informantene om hva kommunen har gjort i arbeidet med digital transformasjon.

På spørsmål om hvordan digitaliseringen kommer til å påvirke kommunens arbeid fremover, er det flere aspekter som trekkes frem blant informantene. Et aspekt som nevnes av informantene er kompetanse, og viktigheten av å vedlikeholde denne både for ansatte og ledere. Informant A trekker frem at «[...] digitaliseringen løper fra menneskene» som en utfordring for kommunen. Manglende kommunikasjon mellom de ulike etatene i forhold til det å dele opplysninger, trekkes frem av Informant D. «Jeg tror det kan bli bedre, teknologien ligger jo til rette for at det skal kunne bli bedre [...]».

4.3.2 Avhengighet til digitale systemer og verktøy

I «Digitalisering og innovasjon i Bergen kommune» påpekes det at kommunen fortsatt har en vei å gå vedrørende områder som skal digitaliseres og effektiviseres. Arbeidet vil dog kreve nye og innovative løsninger (Bergen kommune, 2017, s. 5).

Økt avhengighet til digitale løsninger skal ikke gå på bekostning av befolkningen, og kommunen arbeider derfor med en tilnærming som setter mennesket i sentrum (Bergen kommune, 2017, s. 1). «Temaplan for informasjonssikkerhet og personvern 2021-2025» formidler hvordan den personvern og den teknologiske utviklingen genererer merverdi for Bergen kommune, men og hvordan økt avhengighet til systemer og verktøy som digitaliseres kan gjøre kommunen sårbar (Bergen kommune, 2021b, s. 3). Dette samsvarer med Informant D, som formidler at systemene i kommunen skaper gode muligheter når de fungerer, men skaper store problemer for kommunen dersom de faller ned. Informanten beskriver dette som et tveegget sverd. Kommunen peker videre på hvordan sårbarheter i systemer og bruk av teknologi kan utnyttes av eksterne aktører (Bergen kommune, 2021b, s. 3).

På spørsmål om hvor avhengig Bergen kommune er av digitale systemer og verktøy, er det en sterk konsensus blant informantene om at kommunen er særdeles avhengig. Informant E sier at «[...] jeg tenker at kommunen har ikke sjans i havet på å klare seg, uten digitaliseringen fremover». Informanten setter dette i sammenheng med utgiftene som tilfaller kommunen fordi den må ha ansatte på jobb til å gjennomføre lovpålagte tjenester, og hvordan digitalisering potensielt kan lette noe av dette arbeidet fordi kommunen digitaliserer.

4.3.3 Kommunens tilnærming til arbeid med digitalisering

Bergen kommune etterstreber det å være en transparent og åpen kommune hvor det skal være lett for innbyggere å ta kontakt. Kommunen ser derfor et behov for å videreutvikle en praksis for kommunikasjon mellom kommunen og innbyggere digitalt. Dette vil også være et viktig middel for å kunne nå ut til flere målgrupper i kommunen (Bergen kommune, 2017, s. 10).

I Digitaliseringsstrategien 2021-2025 legges det frem at kommunen bør gå vekk fra å utvikle tjenester selv, til å benytte løsninger som allerede eksisterer i markedet (Bergen kommune, 2021a, s. 17). Informant F påpeker dog, på spørsmål om hvordan Bergen kommune fremover skal møte utfordringene som følger av digitalisering og økt fokus på personvern, at kommunen kunne dratt fordel av å ansette egne utviklere og kompetanse, i stedet å leie inn konsulenter.

Dette vil skape mer stabilitet og ansatte vil ha «[...] mer eierskap til ting man skal forvalte videre, som man vet man skal arbeide med, i forhold til når man bare er inne for å gjøre noe også er man ute igjen».

«Kommunens ansatte skal være trygge på at systemene og de digitale hjelpemidlene de benytter i arbeidet er utformet på en måte som minimere risikoen for feil» (Bergen kommune, 2021a, s. 39). For å nå denne målsetningen trekker informantene frem betydningen av å involvere riktig kunnskap på riktig tidspunkt. I tråd med arbeidet mot en digital transformasjon, har kommunen omorganisert flere avdelinger. Dette har blant annet ført til at prosjektledere nå i stor grad er samlet på en avdeling. Informantene beskriver dette som positivt, da det er lettere for prosjektlederne å bruke hverandres kompetanse i arbeidshverdagen.

På spørsmål om hvorvidt API i tilstrekkelig grad blir involvert i prosjekter tilknyttet personvern og informasjonssikkerhet, er informantene enig i at frem til nå har ikke dette blitt gjort nok. Flere av informantene trekker igjen frem Helhetlig Gjennomgang og forventer en endring i APIs rolle tilknyttet prosjekter når implementeringen av nye tiltak og retningslinjer er fullført.

Informantene fikk oppfølgingsspørsmål om hvordan de selv synes kommunen har håndtert digitaliseringen som har pågått de siste årene. Informantene er enig i at kommunen har håndtert digitaliseringen på en svært god måte. Informant E trekker paralleller til da Gro Harlem Brundtland en gang sa «Look to Norway», mens ansatte i kommunen kan gjerne si «Look to Bergen» i forhold til digitalisering av kommunal sektor. Samtidig påpekes det blant flere av informantene at det alltid er rom for å bli bedre, og at Bergen kommune fortsatt har forbedringspotensial. Informant A formidler at det kan ha «gått fort i svingene mange ganger» fordi samfunnsutviklingen krever at kommunen digitaliserer så fort.

4.3.4 Problemstillinger og utfordringer knyttet til digitaliseringen

Økt avhengighet til digitale systemer og verktøy kan lede til en rekke nye utfordringer og problemstillinger for Bergen kommune. Ifølge «Digitalisering og innovasjon i Bergen kommune 2017-2020» medfører digitaliseringen utfordringer som ulike forvaltningsnivå ikke kan løse hver for seg (Bergen kommune, 2017, s. 2). «Digitaliseringen øker i offentlig sektor, men utviklingen av avanserte digitale tjenester til brukerne stagnerer» (Bergen kommune, 2021a, s. 14). Undersøkelser viser til resultater som gjør at kommunen må utvikle mer sammenhengende tjenester, og dette er et krevende arbeid. Mer sammenhengende tjenester

forutsetter et godt samarbeid mellom byrådsavdelingene, og dette har vist seg å være utfordrende, ifølge noen av informantene.

Digitaliseringsstrategien peker på et behov for å gjøre de digitale systemene mer robust og hardfør slik at møte med situasjoner som for eksempel pandemi, naturkatastrofer ol. ikke går utover kommunens brukeropplevelse og effektivitet (Bergen kommune, 2021a, s. 26). Kommunens arbeid med dette kommer frem i samtale med Informant E. Informanten peker på hvor raskt Bergen kommune, etter at pandemien brøt ut i 2020, klarte å tilby alle ansatte hjemmekontorløsninger. Videre sier informanten at «Der en ganske stor jobb egentlig, å få på plass så mye teknologi [...], på så kort tid».

På spørsmål om hvilke utfordringer kommunen kan forvente seg vedrørende økt bruk av digitale systemer og verktøy trekker informantene frem flere aspekter. Økt kompleksitet, evne til å se hele risikobildet, manglende oversikt og kontroll, samt evne til å holde følge med regelverk og retningslinjer knyttet til personvern og informasjonssikkerhet, trekkes frem som utfordringer for kommunen. Kommunens størrelse kan gjøre arbeidet med digitalisering vanskelig, og en av informantene formidler at organiseringen innad i kommunen kan vanskeliggjøre det å trekke synergier på tvers av de ulike byrådsavdelingene. Dette kan således utfordre arbeidet med å innføre en sikkerhetskultur som favner om hele kommunen, ifølge en informant.

4.4 Hvordan jobber Bergen kommune med risiko og sårbarheter?

4.4.1 Helhetlig risikoarbeid i kommunen

2014 og 2020 markerer årene Bergen kommune presenterte sine første helhetlige ROS-analyser. Analysene har som hensikt å danne et grunnlag for kommunens arbeid fremover tilknyttet samfunnssikkerhet og beredskap (Bergen kommune, 2014, s. 6). «Ved å skaffe oss bedre kunnskap om risikoen, blir vi som samfunn bedre i stand til å håndtere den på en forsvarlig måte» (Bergen kommune, 2020a, s. 4). I begge analysene er «svikt i informasjonssikkerhet» beskrevet som en potensiell hendelse, som med høy sannsynlighet kan forekomme.

ROS-2014 formidler at angrep rettet mot informasjonssikkerhet er økende, samtidig som økt kompleksitet og avhengighet til digitale systemer og verktøy gir en større sikkerhetsrisiko. En

god sikkerhetskultur blir således avgjørende for arbeidet kommunen gjør fremover (Bergen kommune, 2014, s. 6). 2020-analysen skisserer eksempler på hvilke trusler og sårbarheter som kan ramme kommunen, og hendelsene skiller henholdsvis likt mellom hendelser gjort med-og uten en (ondsinnet) hensikt (Bergen kommune, 2020a, s. 59). Hendelsene som ikke tar utgangspunkt i en ondsinnet hensikt er; «menneskelig svikt, manglende prosesser for å sikre kontinuerlig oppmerksomhet, ufullstendig oversikt over risikobildet og manglende sikkerhetskompetanse» (Bergen kommune, 2020a, s. 59), mens hendelsene med ondsinnet hensikts er henholdsvis; «virus- og malwareinfeksjon, phishing eller annen manipulering for å oppnå tilgang/informasjon/økonomiske utbetalinger og målrettede digitale angrep utført av fremmede stater» (Bergen kommune, 2020a, s. 59).

I forvaltningsrevisjonen gjennomført av Deloitte fremkommer det en manglende praksis i kommunen på å gjennomføre risikovurderinger og at ROS-analyser mangler på flere av kommunens systemer (Deloitte, 2019, s. 3). Få gjennomførte risikovurderinger gjør det således vanskelig for kommunen å ha en fullstendig oversikt over arbeidet som gjøres med personvern og personopplysninger, og gir således et fragmentert og uoversiktlig bilde over aktuelle risikoer knyttet til personvern og informasjonssikkerhet (Deloitte, 2019, s. 27).

På spørsmål om informantene opplever at fokuset på ROS-analyser har endret seg i kommunen de siste årene, er alle enig om at de opplever at det er mer fokus på det nå enn før. Flere av informantene peker på Helhetlig Gjennomgang, Vigilo-saken og GDPR-forordningen grunner til det økte fokuset. Informant B sier «En grov beregning fra min side er at det kanskje ikke har vært samsvar mellom oppmerksomhet og fokuset på sikkerhet og digitalisering». Hendelsene kommunen var involvert i fra 2018 og til høsten 2019 ledet til en politisk beslutning om å iverksette Helhetlig Gjennomgang. Gjennomgangen har således hatt mål om å tette det gapet som har oppstått mellom digitalisering og sikkerhet, og påse at informasjonssikkerhet og personvern alltid ligger i forkant av digitaliseringen. Dette sikrer at digitaliseringen i stor grad kan bevege seg fremover, uten å måtte stoppe opp ved uidentifiserte hindringer.

4.4.2 Risikoanalyser på prosjektnivå

«Ingen aktivitet kan foregå uten risiko, men risikoen kan som oftest styres» (Seksjon for internkontroll, 2019, s. 11). I internkontrollrapporten om Vigilo-saken gjør Seksjon for internkontroll rede for hva som menes med risikostyring i Bergen kommune. Arbeidet innebærer å identifisere hvilke hendelser som potensielt kan ramme virksomheten dersom de

inntreffer. I tillegg må sannsynligheten for-og konsekvenser av hendelser vurderes, samt eventuelle tiltak som kan påvirke risikoen til et nivå som er akseptabelt for kommunen (Seksjon for internkontroll, 2019, s. 12). «Kommunen skal benytte risikovurderinger aktivt for å sikre at informasjonen er tilstrekkelig beskyttet mot uautorisert innsyn, endringer og permanent eller midlertidig tap av tilgjengelighet-konfidensialitet, integritet og tilgjengelighet» (Bergen kommune, 2020c, s. 7).

Informantene er bevisst på at risikoanalyser skal gjennomføres jevnlig i prosjekter. Ifølge Informant A er dette et krav, og kommunen har prosedyrer som sier at det skal gjøres før et nytt system eller tjeneste tas i bruk. Dersom systemet blir vurdert til høy risiko, er dette meldepliktig i kvalitetssystemet til kommunen. Noen av informantene sier at risikovurderinger handler om å stille de rette spørsmålene, og videre at «Altså vi kan ikke risikovurdere alt» (Informant C).

Arbeidet med Helhetlig Gjennomgang viste at kommunen ikke har vært gode nok med ROS-analyser på prosjektnivå. Gjennomgangen viste også at på enkelte områder blir risikoanalyser gjennomført helt ukritisk, og Informant B beskriver dette som en bakside med økt fokus på personvern og informasjonssikkerhet. Ifølge informanten er det problematisk at ukritiske ROS-analyser gjennomføres på rent «måfå» uten at det er tatt vurderinger knyttet til hvorvidt tidspunktet er riktig eller om den er gjennomført på riktig nivå.

Av informantene som fikk oppfølgingsspørsmål om hvem som utfører ROS-analyser, fremkommer det at vurderingene rundt analysen gjøres i samarbeid med de som har faglig kunnskap om løsningen som skal vurderes, eller området hvor løsningen skal implementeres. På denne måten sikres det at både fagkompetanse og involverte i prosjektet får være en del av vurderingene tilknyttet risiko. Informant D trekker frem at modulen som brukes til ROS-analyser i kommunen oppleves som styrt. Dette gjør at den nødvendigvis ikke treffer alle nødvendige bruksområder, og snevrer dermed inn gruppen ansatte som evner å bruke den i praksis.

På spørsmål om hvorvidt usikkerhet er en faktor som vurderes i arbeidet med risikoanalyser er kontinuitet og kontinuerlig forbedring begreper som nevnes av flere av informantene. Informant A sier at «[...] man kan ikke påvirke all usikkerhet som finnes der ute, men kan jobbe systematisk med å minske risikoen for det, eller sannsynligheten for at noe skal skje». Flere av

informantene trekker frem at ansatte har mindre risikovilje nå enn før, som et resultat av tidligere erfaringer og historier.

4.4.3 Hva gjør kommunen sårbar?

«Nye sårbarheter som oppstår ved innføring og bruk av ny teknologi stiller nye krav til kommunen som arbeidsgiver, tjenesteleverandør, samfunnsutvikler og myndighetsutøver» (Bergen kommune, 2021b, s. 3). Det er derfor viktig å iverksette tiltak som gjør kommunen i stand til å identifisere, forhindre og gjøre rede for ulike sårbarheter og trusler, som kan true den enkelte innbyggers personvern eller informasjonssikkerhet (Bergen kommune, 2021b, s. 3).

Informantene fikk spørsmål om hva som gjorde Bergen kommune sårbar som organisasjon. Manglende kompetanse var den sårbarheten som ble nevnt av samtlige. Videre ble også manglende forståelse, se det store bildet, sikre riktig kompetanse på riktig sted, sikre etterlevelse i kommunen, samt manglende opplæring nevnt som sårbarheter. Informant B trekker frem manglende forankring i ledelsen som en sårbarhet og ringvirkningene dette kan ha. Ifølge Informant F er også kommunens størrelse og organisering å anse som en sårbarhet. Manglede evne til å samarbeide og se synergier på tvers av byrådsavdelingene gjør at «[...] man sitter på to tuer [...]» og arbeider.

På hvilke sårbarheter som kan sees i sammenheng med å ha mennesker som ansatte ble manglende kompetanse og kunnskap igjen fremhevet som eksempler. Informant A trekker frem manglende ressurser og hvordan dette kan stoppe opp prosjekter. Som respons på dette fremkommer det i «Temaplan for informasjonssikkerhet og personvern» at kommunen skal styrke fagmiljøet med nye ansettelser. Informant D formidler at vedrørende feil som gjøres i systemer, sier «All historie rundt tekniske systemer viser oss at 70-80% er brukerfeil». Informanten fikk oppfølgingsspørsmål om kommunen tar høyde for slike sårbarheter. Informant D trekker frem forskjeller mellom offentlig og privat sektor. Videre sier informanten at vedkommende opplever ikke Bergen som verken dårligere eller bedre enn andre organisasjoner, og at «[...] de utvikler seg hele tiden knyttet til personvern [...]». På spørsmål om kommunen krever mer av de ansatte nå enn før, fremkommer det en klar enighet blant informantene om at dette er faktum. Høyere krav i form av obligatoriske kurs, mer ansvar skrevet inn i arbeidsoppgavene og endring i regelverk er noen av faktorene som trekkes frem i svar fra informantene.

4.4.4 Kompetanse

Dagens kompetansenivå i kommunen

«Kompetansehevende tiltak for å utvikle de kommunale tjenestene er nødvendig for å møte nye utfordringer» (Bergen kommune, 2017, s. 1). Dette fremkommer også i «Byrådssak /20», hvor det fremheves at kompetanse i kommunen burde struktureres og organiseres på en sånn måte at hele kommunen og dens ansatte kan dra nytte av den (Bergen kommune, 2020b, s. 4). Ifølge «Forvaltningsrevisjon: Bergen kommune» har kommunen lagt opp til kurs og kompetanseheving for de ansatte, særlig tilknyttet informasjonssikkerhet og personvern. Fra spørreundersøkelsen gjennomført av Deloitte fremkommer det dog at en rekke ansatte (18%) ikke er klar over, eller ikke har blitt informert om hvilket ansvar de selv har for relevante IKT-systemer som brukes i jobbsammenheng (Deloitte, 2019, s. 59).

Undersøkelsen konkluderer med at kommunen ikke i tilstrekkelig grad sikrer gode rutiner og informasjon blant de ansatte, gjennom opplæringstiltak. Manglende kompetanse om informasjonssikkerhet kan således øke risikoen for brudd i regelverk og på denne måten svekke kommunens arbeid vedrørende behandling av personopplysninger og informasjonssikkerhet (Deloitte, 2019, s. 59).

Byrådet understreker hvor viktig nødvendig kompetanse er for kommunens ledere og ansatte. Det er nødvendig for å kunne fylle rollen og utøve det ansvaret hver enkelt ansatt og leder har, samtidig som kommunen systematisk skal arbeide med å sikre fremtidens kompetanse (Bergen kommune, 2021b, s. 29). Informantene fikk spørsmål om hvorvidt ansatte hadde god og riktig kompetanse om de ulike systemene som daglig brukes i deres arbeid i kommunen. Informantenes generelle oppfatning er at ansatte i kommunen har kompetanse, eller har tilgang til fagmiljøer som sitter med riktig kompetanse.

Informantene fikk deretter et oppfølgingsspørsmål om hvorvidt det er viktig for Bergen kommune at ansatte innehar god kunnskap. Her er det en felles enighet blant informantene, hvor det påpekes at kompetanse er helt avgjørende og nødvendig. Informant B trekker frem at dette med kompetanse er en pågående diskusjon i kommunen, som handler om ressursutnyttelse. «Hvis du bruker et system en gang i året, så er det kanskje ikke hensiktsmessig at du trenger å lære og bruke det systemet».

Kompetanseheving

I «Digitaliseringsstrategien for Bergen kommune 2021-2025» beskrives kompetanseheving og kompetansebygging som sentralt for at ansatte skal kunne bruke digitale verktøy korrekt (Bergen kommune, 2021a, s. 2). Det vil fremover være behov for ulike former av digital kompetanse for å få dekket alle ansvars-og arbeidsområdene kommunen har.

I «Temaplan for informasjonssikkerhet og personvern» har kompetanse, kunnskap og rutiner over tid vært et fokusområde i kommunens arbeid med informasjonssikkerhet og personvern. Videre peker kommunen på at «[...] det har vært, og fortsatt er, et stort forbedringspotensial i måten vi jobber med i disse to fagområdene» (Bergen kommune, 2021b, s. 4). Deloitte sine undersøkelser viser at store deler av ansatte i kommunen ikke har gjort seg innforstått med obligatorisk opplæringsmateriell tilknyttet informasjonssikkerhet og personvern. Det fremkommer også at rundt halvparten av respondentene i Deloitte sine undersøkelser mener at kommunen ikke har gitt tilfredsstillende opplæring rundt de to temaene (Deloitte, 2019, s. 4).

Blant informantene fremkommer det stort sett en generell enighet om at kommunen tilbyr ansatte ulike muligheter for å heve egen kompetanse. Informantene etterlyser dog tid til å få dette gjort, samt et sterkere engasjement fra kommunen som oppfordrer ansatte (i større grad) til å gjennomføre kurs og andre former for kompetanseheving.

5. Analyse og drøfting

I dette kapittelet vil oppgavens funn analyseres og drøftes opp mot det teoretiske rammeverket for oppgaven. Kapittelet er strukturert etter forskningsspørsmål, for å sikre en systematisk oversikt. I kapittelet skal Bergen kommunes arbeid med sikkerhetskultur drøftes opp mot James Reason sine premisser for hva som danner en god sikkerhetskultur. I tillegg skal det undersøkes hvordan kommunen kan tilrettelegge for sikker håndtering av digitale personopplysninger drøftes, herunder kommunens arbeid med å skape en bevissthet rundt digitale sårbarheter og risikoer i kommunen. Kommunens tilnærming til sikkerhet skal også vurderes. Samlet vil drøftingen lede opp mot å besvare oppgavens problemstilling, nemlig hvordan kan Bergen kommune jobbe med sikkerhetskultur for å tilrettelegge for forsvarlig håndtering av personopplysninger? Problemstillingen vil i sin helhet besvares i kapittel 6, konklusjon.

5.1 Hvordan jobber Bergen kommune med sikkerhetskultur i forhold til personvern?

For å undersøke hvordan kommunen jobber med sikkerhetskultur i forhold til personvern, er det flere aspekter som må belyses. Først må det avgjøres hvorvidt kommunens arbeid kan beskrives som det å utforme en kultur. Videre må det drøftes om kommunen arbeider mot en sikkerhetskultur som en subkultur, eller om sikkerhetskultur kan defineres som en egen kultur. Kommunens arbeid skal deretter analyseres og drøftes opp mot sikkerhetskultur presentert av James Reason, og det skal vurderes hvorvidt kommunens arbeid er i tråd med dette.

5.1.1 Hva kjennetegner en sikkerhetskultur?

Hva er en kultur?

Som vist til i oppgavens teorikapittel, skilles det i dag mellom en rekke definisjoner av, og forståelser for hva en kultur er. Felles for flere av dem er fellesskap, læring, delte verdier og holdninger gjeldende for en gruppe mennesker, ifølge (Bergsjø et al., 2020, s. 34). Begrepet kultur nevnes i ulike sammenhenger i empirien (digitaliseringskultur, sikkerhetskultur og avvikskultur), og viser med dette at Bergen kommune aktivt benytter begrepet i organisasjonens arbeid.

Nye retningslinjer, rutiner, strategier og gjennomganger viser en aktiv tilnærming til digitaliseringsarbeidet, hvor målet er å forankre en digitaliseringskultur på alle kommunens nivåer (Bergen kommune, 2017, s. 15). I tråd med Schein & Schein (2016) sin definisjon av kultur, samt Bergsjø et al. (2020) sin samlede forståelse av hva som tillegges begrepet kultur, kan arbeidet kommunen gjør forstås som det å forme en kultur i organisasjonen.

Organisasjonskultur eller sikkerhetskultur?

En av den mest kjente definisjonen av organisasjonskultur presenterte Schein i 1992, med utsagnet «The way we do things around here» (Schein, 1992, s. 8-9). Definisjonen er anvendelig, men vag. Dette betyr at den kan gjøres gjeldende for en rekke organisasjoners arbeid, også Bergen kommune sitt. I tråd med denne definisjonen, og den presentert av Trice & Beyer (1993) er det naturlig å trekke linjer til arbeidet Bergen kommune gjør med digitalisering. Som en forutsetning for å holde følge med samfunnsutviklingen må kommunen digitalisere. I tråd med digitaliseringen settes det også stadig høyere krav til forvaltning av personopplysninger. Endringer i arbeidsoppgaver og ansvarsområder kan således føre til at grupper i organisasjonen finner det utfordrende å følge utviklingen, og begrenser derfor

samhandling til hverandre. Dette samsvarer også med hva Reason formidler om organisasjonskultur (Reason, 1997, s. 192).

Definisjonene av organisasjonskultur sier likevel lite om hvordan organisasjoner skal tilnærme seg, og forholde seg til sikkerhet. Derfor blir definisjonen av Antonsen (2009b) viktig, da den inkluderer en klar referanse til sikkerhetsarbeid i organisasjonen, i motsetning til Reason sin definisjon. Av empirien fremkommer det også at Bergen kommune har en aktiv tilnærming til sikkerhetsaspektet ved kulturen. Dette samsvarer derfor i stor grad med hva Antonsen definerer som en sikkerhetskultur, og videre hva Reason presenterer som en informert kultur.

Definisjonene av sikkerhetskultur tilsier også at kulturen skal favne om alle ansatte i en organisasjon og ikke det Sander beskriver som en «[...] begrenset kulturell gruppe» (Sander, 2019). Empirien formidler at kommunen ønsker å implementere kulturen i hele kommunen, noe som videre argumenterer for at den må tolkes som en egen kultur. Samtidig er det viktig å være innforstått med at manglende forståelse for og kunnskap om sikkerhetskultur blant ansatte og ledere i kommunen kan lede til at den forstås mer som en subkultur, og blir av den grunn lite vektlagt og videreutviklet. Det blir dermed viktig for kommunen å jobbe mot en helhetlig forankring av kulturen, særlig for å tilrettelegge for god håndtering av personopplysninger.

Hva menes med sikkerhetskultur ifølge Bergen kommune?

Empirien viser til ulik forståelse blant informantene tilknyttet hva som menes med sikkerhetskultur kommunen. Ifølge Informant B «Så har nok kulturen vært- det har nok ikke vært en sikkerhetskultur i kommunen [...]», noe som understøttes de fleste informantene. I lys av økt oppmerksomhet og bevissthet rundt informasjonssikkerhet og personvern, har det ifølge informantene skjedd en merkbar endring i kommunens arbeid. Skjerpet fokus på informasjon, retningslinjer og rutiner knyttet til arbeid med personvern trekkes frem som eksempler av informantene.

Reason formidler at en sikkerhetskultur må sosialt utformes før den samles og implementeres i en fungerende enhet (Reason, 1997, s. 192). Sikkerhetskultur er derfor noe som aktivt må formes, og er sjeldent noe som oppstår av seg selv. På denne måten kan Jore (2016) sitt argument om at kun organisasjoner som har et overveiende fokus på sikkerhet, har grunnlag til å utvikle en sikkerhetskultur, forstås (Jore, 2016, s. 470). På en annen side kan mangelen på en

akseptert definisjon av kulturbegrepet forstås som at sikkerhetskultur ikke er noe som kan defineres eksplisitt og er av den grunn umålbar i en organisasjon, i tråd med hva Malcomson (2009) formidler.

Bergen kommune har som nevnt en aktiv tilnærming til arbeidet med sikkerhetskultur. Dette fremkommer i empirien ved at kommunen skal ha økt fokus på å utforme oppdaterte retningslinjer og rutiner, utforme kurs, fokusere på kompetanseheving og læring i kommunen. Dette viser til en metode for å heve det immaterielle ved en kultur, nemlig holdninger og verdier. Samtidig fremkommer det at kommunen arbeider for at systemene kommunen bruker, skal være sikre for ansatte og bruke, og på denne måten redusere konsekvenser av feil. Dette viser til en kulturutforming som også inkluderer de mer materielle aspektene i en organisasjon, som verktøy og systemer. Dette samsvarer med hva Engen et al. (2016) definerer som kultur.

Formålet er å oppnå en felles enighet og forståelse for hva som skal utgjøre en helhetlig sikkerhetskultur i kommunen. På denne måten sikres det at målsetningene kommunen har satt tilknyttet arbeid med personvern og informasjonssikkerhet når ut til ansatte, og at alle ansatte følgelig har et bevisst forhold til dette arbeidet. Som empirien formidler har ikke dette tidligere vært noe kommunen har hatt et overveiende fokus på, men flere av informantene opplever at kommunen nå har et større fokus på nettopp dette.

Reason problematiserer hvorvidt sikkerhetskultur er noe en organisasjon er, eller om det er noe en organisasjon har. Selv argumenterer han for sistnevnte, og begrunner dette med at endringer i regi av ledelsen som for eksempel introduksjon av nye målsetninger eller tiltak, kan således påvirke eller endre sikkerhetskulturen i en organisasjon (Reason, 1997, s. 192). Som det skal redegjøres videre, kan kommunens arbeid med omstrukturering, gjennomganger av digitale systemer og økt fokus på informasjonssikkerhet og personvern tolkes som et tiltak for å påvirke eller endre sikkerhetskulturen, i tråd med hva Reason beskriver.

I tråd Reason sine premisser for en informert kultur, skal kommunens arbeid nå analyseres og drøftes opp en rapporterende kultur, en rettferdig kultur, en fleksibel kultur og en lærende kultur.

5.1.2 En rapporterende kultur

Reason (1997) trekker frem at en rapporterende kultur forutsetter at ansatte jobber nær ulykker og at disse er villige til å rapportere inn egne feil og avvik (Reason, 1997, s. 195). Her viser Reason tidlig en tilnærming til safety, hvor systemer skal ta høyde for menneskelige feil. Dette vektlegges også av Weick & Sutcliffe (2007). Ifølge empirien skal ansatte i Bergen kommune til enhver tid etterleve gjeldende regler og retningslinjer for rapportering av hendelser. Målsetningen med dette er å begrense eventuelle skader, gjenopprette normaltilstand og avslutningsvis trekke lærdom ut hendelsen, for å kunne forebygge mot at lignende avvik skjer igjen (Bergen kommune, 2020c, s. 13). For å kunne bygge en sikkerhetskultur som ivaretar kommunens ansvar knyttet til personvern og informasjonssikkerhet, blir således arbeidet med å innarbeide en god avvikskultur avgjørende, ifølge empirien.

Informantene synes å være enig i at det er underrapportering og mørketall på avviksmeldinger i kommunen. Dette kan være fordi en avviksmelding vil innebære å innrømme feil, noe som kan være krevende for den ansatte. Empirien formidler videre at det således blir viktig å bygge en avvikskultur som oppfordrer til åpenhet rundt det å melde avvik. På denne måten kan vi forstå kommunens arbeid i tråd med hva Reason (1997) og Weick & Sutcliffe (2007) tillegger en rapporterende kultur, hvor ansatte oppmuntres til å melde inn avvik. I lys av hendelsene nevnt innledningsvis, fremkommer dette som et naturlig fokuspunkt i kommunen, for å sikre at noe lignende ikke skjer igjen. Dette formidles også av informantene.

Det fremkommer dog fra empirien at kommunen fortsatt har en jobb å gjøre for å nå målsetningen satt for avviksmeldinger. Flere av informantene trekker frem en misnøye rundt kvalitetssystemet som brukes for å melde avvik, og nevner dårlig implementering, dårlig utforming og manglende informasjon tilknyttet systemet som grunner til hvorfor ansatte velger å ikke melde avvik. Samtidig viser undersøkelser at flere ansatte ikke er klar over rutiner knyttet til avviksmeldinger. Reason (1997) trekker frem bekymring tilknyttet ledelsens reaksjon, kollegiale forhold, skepsis og ekstra arbeid som grunner til hvorfor ansatte ikke rapporterer, som samsvarer med hva empirien formidler.

I teorien presenterer Reason (1997) fem punkter som skal tilrettelegge for rapportering i en organisasjon. Ved å sammenligne empiri om kvalitetssystemet og de fem punktene presentert av Reason kan det trekkes frem likheter, som for eksempel at et avvik skal være enkelt å melde, tilbakemeldingene må være forståelig og ansatte skal beskyttes mot disiplinære handlinger.

En annen likhet er at avdelingen som mottar avviket er ikke den avdelingen som sanksjonerer og disiplinerer, i tråd med hva Reason beskriver. En forskjell er dog at ansatte ikke har anledning til å melde inn anonymt. Det kan derfor stilles spørsmål til hvorvidt et slik tiltak ville hatt en målbar effekt på antall avvik som meldes. Samtidig fremkommer det fra empirien at informantene oppfatter at ansatte blir flinkere til å melde avvik, og beskriver dette som en økende trend. Dette kan ha sammenheng med bevisstgjøring av ansatte knyttet til hvor sårbare personopplysninger er dersom de blir tilgjengelig for andre. Dette kan i så fall være et viktig læringspunkt i etterkant av Vigilo-saken. Samtidig kan opplysningenes sårbarhet også være en grunn til at avvik tilknyttet dette ikke meldes inn.

Tillit og en åpenhetskultur rundt det å melde avvik trekkes frem av Reason (1997) som en viktig faktor i det å skape en rapporterende kultur. Således blir ledelsens respons på avviksmeldinger vesentlig, da en utpreget straffekultur kan svekke tilliten ansatte har til systemet. Det samme kan sies om innbyggerne i kommunen. Oppleves det et tillitsbrudd som ikke håndteres på en god måte, kan dette svekke tilliten innbyggerne har til kommunen, noe som er naturlig å tenke er et resultat av Vigilo-saken. Det kan således problematiseres om graden av tillit befolkningen har til offentlig sektor er for høy, men som nevnt i litteraturgjennomgangen er digitaliseringen og ivaretakelse av personopplysninger avhengig av en høy grad av tillit fra befolkningen.

I empirien vektlegges også ledelsesforankring ved arbeidet med sikkerhetskultur og da særlig knyttet til informasjonssikkerhet og personvern. Forankring hos ledelsen er ikke noe som i stor grad vektlegges av Reason, noe som videre kan problematiseres. For å oppnå en informert kultur vil det være naturlig at kunnskap hos alle ledd i en organisasjon er en forutsetning. Manglende ledelsesforankring kan således tolkes som en svakhet i Reason sin teori.

5.1.3 En rettferdig kultur

Reason (1997) bygger videre på hvordan konsekvenser av handlinger må håndteres riktig for å kunne bygge en rettferdig kultur. Dette innebærer å finne en balanse mellom en ikke-skyld-kultur og en rent straffegivende kultur (Reason, 1997, s. 195). Det fremkommer ikke av empirien at kommunen har en straffekultur dersom ansatte gjør feil eller ikke handler etter gitte retningslinjer og rutiner. Dette er i tråd med hva Reason formidler om at organisasjoner ikke er tjent med å straffe ansatte for feil som gjøres. Igjen fremkommer safety-tilnærmingen Reason har til sikkerhet, og som hittil også kan identifiseres hos Bergen kommune.

For kommunen vil det følgelig være ideelt å tydeliggjøre grensen mellom akseptabel-og ikke akseptabel oppførsel og handlinger, noe empirien formilder at kommunen er godt på vei til å gjøre. Ifølge informantene oppfattes kommunen som rettferdig, og ingen av informantene trekker frem en ren straffekultur. Det blir dog påpekt at dersom ansatte begår tjenestebrudd eller direkte misligholder sine arbeidsoppgaver, kan dette medføre konsekvenser. Den generelle oppfatningen er dog at kommunen ikke utpreget vektlegger straff og informant B formidler at kommunen fokuserer heller på prosessene rundt handlingen for å finne ut hvorfor det gikk gale. Informant A trekker også frem at kommunen arbeider mot en åpenhetskultur rundt det å melde avvik, som kan ses i lys av hva Weick & Sutcliffe (2007) formidler om at ansatte bør belønnes for å innrømme feil, som et tiltak for å sikre en rapporterende kultur.

I både teori og empiri fremkommer det en tydelig sammenheng mellom en rapporterende og rettferdig kultur. Det vil derfor være nødvendig for kommunen å finne en gylden middelvei mellom å gjøre ansatte bevisst på at handlinger tilknyttet informasjonssikkerhet og personvern kan få alvorlige konsekvenser, uten at dette skremmer ansatte fra å melde inn avvik. En informant trekker frem at dersom det ikke meldes avvik, har kommunen heller ingen informasjon om hvilke reelle avvik som forekommer. Dette kan således skape en falsk trygghet i kommunen. Kompetanse om hva som definerer et avvik, tid og vilje til å melde, trekkes frem som eksempler på hvorfor avvik ikke meldes blant informantene. Manglende avviksmeldinger gir lite informasjon om hvorvidt konsekvenser-eller mangelen på konsekvenser som straff er akseptabelt blant de ansatte.

Reason (1997) trekker frem tre punkter som beskriver hvordan ansatte handler. De tre punktene vektlegger hvorvidt en handling er gjort med intensjon om å skade eller ikke. Med dette trekker Reason enda en linje til diskusjonen rundt safety og security, uten å problematisere konsekvenser som kan forekomme dersom handlingen er gjort med intensjon (ondsinnet hensikt). I tråd med de overnevnte premissene, bærer også denne preg av en safety-tilnærming. I et digitalt samfunn som i større grad er mer sårbar for angrep eller handlinger gjort med intensjon om å skade, kan det stilles spørsmål til hvorvidt det er nødvendig å i større grad inkludere security i sikkerhetskulturen Flere systemer er svært sårbare, ikke bare for tilsiktede angrep, men også for dårlig håndtering av ansatte. Går dette på bekostning av innbyggerne i kommunen, må det således vurderes om en security tilnærming som i større grad vektlegger barrierer, risiko og sårbarheter er nødvendig.

5.1.4 En fleksibel kultur

Fra empirien fremkommer fleksibilitet blant annet ved Bergen kommunes arbeid mot en digital transformasjon, som innebærer økt fokus på ansatte, deres kompetanse og hvordan denne kan brukes for å fullt utnytte digitaliseringens potensiale (Bergen kommune, 2021a, s. 6). Blant informantene trekkes nye metoder for kompetanseheving, rutiner og retningslinjer frem som eksempler på arbeidet som gjøres med digital transformasjon. På denne måten kan digital transformasjon forstås som kommunens evne til å tilpasse seg eller å være fleksibel i et skiftende samfunnsbilde, etter definisjon av Nilstun (2018) og Reason (1997).

Helhetlig Gjennomgang blir hyppig referert til i empirien. Identifiserte sårbarheter fra gjennomgangen vil således skape et endrings- og tilpasningsgrunnlag for kommunen. Gjennomgangen vektla å identifisere sårbarheter, risikoer og manglende risikoanalyser på systemer tilknyttet personvern og informasjonssikkerhet, hvor gjennomgangen kartla en rekke mangler. Derfor kan også arbeidet med Helhetlig Gjennomgang forstås i sammenheng med hva Reason tillegger en fleksibel kultur. Ifølge empirien har arbeidet med gjennomgangen klargjort kommunen for en digital transformasjon, men påpeker videre at det forutsetter strukturelle endringer i kommunens organisering. At kommunen evner å foreta strukturelle endringer i kommunen kan således bli viktig i arbeidet mot en fleksibel kultur, som Reason (1997) formidler. I praksis kan dette dog vise seg å være utfordrende, da kommunen er bygget på en parlamentarisk styringsmodell, som vanskelig lar seg omorganisere. Dette kan også vanskeliggjøre det Reason (1997) og Weick & Sutcliffe (2007) formidler om samarbeid i en organisasjon.

Ifølge Reason bør avgjørelser tas av den eller de ansatte som har best kompetanse på området (Reason, 1997, s. 216). I empirien knyttes kompetanse og manglende kompetanse til informasjonssikkerhet og personvern. Dette belyses blant annet av Informant B, som trekker frem at endringer gjort i veiledende materiell skal påse at kompetanse innenfor informasjonssikkerhet og personvern er på plass tidlig i prosjekter. På denne måten sikrer kommunen at avgjørelser rundt problemstillinger knyttet til informasjonssikkerhet og personvern tas av ansatte som har best forutsetning for å ta riktige og gode avgjørelser, i tråd med Reason sin tankegang. Det fremkommer ikke av empirien hvorvidt arbeidet med å etterleve krav som stilles til ansatte følges opp. Dette kan være problematisk for kommunen i arbeidet med å kontinuerlig sikre at kompetanse er tilgjengelig på riktig sted, og på riktig tidspunkt.

Kommunikasjon skaper en kultur som evner å tilpasse seg perioder preget av høyt tempo og stress, og på denne måten sikre påliteligheten i en organisasjon (Reason, 1997, s. 216). Fra empirien fremkommer det at manglende kommunikasjon og samarbeid mellom de ulike byrådsavdelingene kan vanskeliggjøre dette arbeidet. Flere av informantene formidler at samarbeidet oppleves som dårlig eller manglende, men påpeker at kommunen har gode forutsetninger for å forbedre dette arbeidet. Det kan likevel argumenteres for at ved å vektlegge bedre samarbeid på tvers av de ulike byrådsavdelingene, løftes organisasjonen frem som en helhet og vil derfor kunne takle perioder med stress og høyt tempo bedre. Informantene formidler en enighet om at for problemstillinger knyttet til informasjonssikkerhet og personvern, må ansatte med relevant fagkunnskap inkluderes som en naturlig del av beslutningsprosessen.

Det fremkommer ikke eksplisitt fra empirien hvorvidt kommunen aktivt leter etter feil og jobber med en «kronisk uro» som presentert av Reason (Reason, 1997, s. 213-214). Likevel formidles det at kommunen i dag er svært avhengig av digitale systemer og verktøy. Økt bruk og etterspørsel av digitale systemer fører således til økt avhengighet, og gjør dermed kommunen sårbar dersom systemene ikke fungerer som forventet. Blant informantene er det også en generell konsensus om at kommunens avhengighet øker, og at kommunen derfor «[...] ikke hadde hatt sjans i havet på å klare seg uten digitaliseringen fremover» (Informant E). Empirien formidler også en rekke utfordringer tilknyttet digitalisering, enkelte mer alvorlig enn andre. Dette betyr at kommunen aktivt må påse og tilrettelegge for at systemene fungerer som forventet, samt planlegge hvordan et eventuelt brudd og medfølgende konsekvenser skal håndteres, i tråd med hva Reason (1997) og Wick & Sutcliffe (2007) formidler.

Samtidig kan manglende fokus på kompetanseheving trekkes frem som en svakhet i teorien til forfatterne. Empirien formidler at kommunen har et stort fokus på kompetanseheving, hvor ansatte i dag har tilbud om en kurs, e-læring og lignende. Samtidig påpekes det av kommunen selv og blant informantene, at kommunen har forbedringspotensial rundt det å sikre kompetanseheving blant ansatte. Dette kommer dog ikke frem i hos Reason (1997) eller Weick & Sutcliffe (2007), noe som kan tolkes som en klar svakhet i teorien om sikkerhetskultur.

5.1.5 En lærende kultur

Ifølge Reason (1997) er en lærende kultur den enkleste å konstruere, men den vanskeligste å etterleve i praksis, fordi organisasjoner vanskelig kan måle læring. Informantene opplever Bergen kommune som en lærende organisasjon, likevel vektlegges det ulike aspekter for hva som er viktig i arbeidet med å trekke lærdom ut av hendelser. Reason (1997) trekker synergier mellom de ulike kulturene som danner en informert kultur, og formidler at en lærende kultur forutsetter et godt tillitsforhold mellom ledelsen og ansatte (rapporterende kultur) og at organisasjoner er kritiske til eget arbeid (fleksibel kultur).

Helhetlig Gjennomgang blir nevnt av informantene som et tiltak som viser kommunens evne til å trekke lærdom av hendelser. Informant B fremhever hvor viktig arbeidet med å implementere tiltakene utarbeidet i etterkant av gjennomgangen er. Lyktes ikke kommunen med dette, risikerer den å falle tilbake til gamle vaner og rutiner. Dette kan hindre eller skade arbeidet gjør for å skape en god sikkerhetskultur og lede til at arbeidet tilknyttet personvern ikke tilstrekkelig blir vektlagt, i tråd med hva Weick & Sutcliffe (2007) formidler om «mindfulness». Sett i lys av hendelsene nevnt innledningsvis kan dette være eksempler på hendelser kommunen ikke ønsker å oppleve igjen, men som kan være reelle dersom det videre arbeidet med Helhetlig Gjennomgang ikke tilstrekkelig vektlegges.

Reason (1997) formidler at organisasjoner må være kritiske til eget arbeid for å være i forkant av hendelser. Dette fremkommer også i empirien hvor det trekkes frem at kommunen må kunne være i forkant av hendelser, for å best kunne håndtere dem. Det er derfor viktig at kommunen får bygget en kultur rundt det å trekke lærdom av hendelser. Ifølge Informant B skal kommunen løse dette med å sørge for at personvern og informasjonssikkerhet alltid ligger i forkant av digitaliseringen. Dermed kan digitaliseringen foregå uten at kommunen møter på uforutsette hindringer eller problemer. Flertallet av informantene opplever dog at tidligere hendelser har ledet til en holdnings-og perspektivendring i kommunen, mens en informant er usikker på hvorvidt enkeltsaker kan lede til endringer.

Kommunens organisering blir også her problematisert. Ifølge Informant D «lider» kommunen av at de ulike byrådsavdelingene er organisert som siloer, og det vil derfor være vanskelig for kommunen å trekke lærdom på tvers av disse. Kommunen vil derfor ha stor nytte av å bryte opp denne tankegangen, slik at læring inngår som en naturlig del av de ansattes kunnskapsbase,

slik som Njå et al. formidler (Njå et al., 2020, s. 430). Engen et al. (2016) trekker også frem at forvaltningen må bli bedre til å trekke lærdom av hendelser, noe som samsvarer med hva empirien formidler om at Bergen kommune har forbedringspotensial.

5.1.6 Kan kommunens sikkerhetskultur beskrives som en informert kultur?

Det er tydelig at kommunen har en aktiv tilnærming til arbeidet med sikkerhetskultur, i forhold til å skape et godt grunnlag for å fremover håndtere og forvalte personopplysninger. Empirien har formidlet at det foreligger noen uenigheter om hvorvidt sikkerhetskultur er noe som har eksistert over tid i kommunen, eller om det er nylig etablert. I lys av digitaliseringen og økt sårbarhet rundt personvern og informasjonssikkerhet er ikke bare sikkerhetskultur ønsket, den er også nødvendig for at kommunen fremover skal kunne gjennomføre sine arbeidsoppgaver og således kunne løse sitt samfunnsoppdrag.

I tråd med de fire premissene som utgjør en informert kultur, formidler empirien at kommunens arbeid i stor grad er i tråd med hva Reason presenterer. Hvor Reason sin teori tidvis oppleves som mangelfull, fremtrer kommunens tilnærming til digitalisering, kompetanse, kompetanseheving og et generelt arbeid for å bedre sikkerhetskulturen som godt utarbeidet, og skaper dernest et godt grunnlag for videre arbeid. Samtidig fremstår kommunen som innforstått med de områdende som krever forbedring, og evner selv ser svakheter i eget arbeid.

Det kan derfor konkluderes med at kommunen dynamisk jobber med en sikkerhetskultur ved å tilrettelegge for de fire premissene presentert av Reason (1997) i oppgavens teorikapittel. Som vist danner denne sikkerhetskulturen et grunnlag for det videre arbeidet med personopplysninger og personvern. I tråd med hva Engen et al. (2016) definerer som kultur, viser også kommunen at den (tidvis) inkluderer de mer materielle aspektene ved en organisasjon, og ikke bare de immaterielle. Likevel er det viktig å trekke frem at arbeidet kan vanskeliggjøres på grunnlag av utfordringer kommunen står ovenfor. Blant disse er silo-tenking i kommunen (særlig i byrådsavdelingene), manglende ledelsesforankring, underrapportering på avvik og manglende kompetanse. Det fremkommer dog at foruten disse utfordringene, har kommunen utarbeidet et godt grunnlag for å videreutvikle en gjennomført og helhetlig sikkerhetskultur i kommunen. Kulturen skal sørge for at ansatte er forberedt på utfordringer og problemstillinger tilknyttet personopplysninger og personvern, ved å enten inne ha riktig kunnskap selv, eller være klar over hvor fagkunnskap befinner seg.

5.2 Hva kjennetegner en sikker og forsvarlig håndtering av digitale personopplysninger, ifølge Bergen kommune?

Reason (1997) sin teori om sikkerhetskultur gir en god forståelse for hva som er viktig for å utvikle en sikkerhetskultur. For kommunens arbeid med å sikre forsvarlig håndtering og forvaltning av personopplysninger, er det enkelte områder som Reason sin teori oppleves som manglende. Likevel fremkommer de som en naturlig del av arbeidet kommunen gjør, og gjør dem således viktig for hva kommunen selv anser som forsvarlig håndtering av digitale personopplysninger. Blant disse utpeker særlig kompetanse, tillit og risiko seg fra empirien. En sikker og forsvarlig håndtering av digitale personopplysninger forutsetter at kommunen er bevisst på hvilke sårbarheter og risikoer som kan påvirke arbeidet med personopplysninger, og aktivt arbeider med å skape bevissthet rundt dette blant de ansatte i kommunen. I det følgende skal det derfor analyseres og drøftes hva kommunen tillegger i en sikker og forsvarlig håndtering av personopplysninger.

5.2.1 Hvordan jobber kommunen med risiko?

Ifølge Njå et al. (2020) kan risiko handle om konsekvenser og utfall av usikkerhet og uønskede hendelser, det kan handle om vurderinger knyttet til verdier, menneskeliv, omdømme og klima. (Njå, 2020, s. 46) Risiko kan også handle om usikkerhet og konsekvensvurderinger. Ifølge Engen et al. (2016) kan risiko handle om sannsynlighet og konsekvens, Aven og Renn (2010) beskriver risiko som en kombinasjon av hendelser og konsekvenser, samt usikkerheten tilknyttet disse. I kommunens arbeid vil dermed risiko forstås som en naturlig del av arbeidet kommunen gjør for å bygge en sikkerhetskultur som tilrettelegger for forsvarlig håndtering av personopplysninger og som herunder sikrer opplysningenes tilgjengelighet, integritet og konfidensialitet (Digdir, u.å.-a).

Fra empirien fremkommer det at kommunen i det daglige arbeider med risiko og ROS-analyser, for å påse at nye digitale systemer som innføres er sikre, men også for å sørge for at rutiner og retningslinjer knyttet til informasjonssikkerhet og personvern er ivaretatt. I tråd hva Weick & Sutcliffe (2007) formidler om en «mindful» organisasjon, innebærer dette hva en organisasjon gjør for å forhindre uønskede hendelser. Arbeidet med personvern og informasjonssikkerhet er komplekst. Regler og rutiner er kontinuerlig i endring, og ansatte må forholde seg til stadig ny informasjon om hva som er lov, og hva som ikke er lov. På denne måten blir arbeidet med risiko og risikoanalyser viktig for kommunen. Empirien formidler at ved hjelp av analysene kan

risikoer metodisk identifiseres og det kan utarbeides risikoreduserende tiltak dersom nødvendig. Dette arbeidet blir således viktig i å sikre opplysningenes tilgjengelighet, integritet og konfidensialitet.

Blant informantene er det delte meninger tilknyttet hvor godt kvalitetssystemet hvor risikovurderingen gjennomføres er, og videre hvor gode resultater det gir. I tråd med kommunens arbeid med å identifisere risikoer, er det nødvendig med et system som enkelt tilrettelegger for rapportering og bruk i form av å gjennomføre ROS-analyser. Kvalitetssystemet er det samme som brukes for å melde inn avvik. Som vist til i forskningsspørsmål 1, har informantene svært delte meninger tilknyttet dette systemet. For å ivareta hva kommunen mener med sikker og forsvarlig håndtering av personopplysninger, er det således viktig og også tilrettelegge for en rapporterende kultur, som presentert av Reason (1997).

Det kan videre argumenteres for at Reason sin teori i lys av arbeid med risiko er mangelfull. For å oppnå en informert kultur er det viktig å ha kunnskap om hvilke risikoer som potensielt kan true organisasjonen og det arbeidet den gjør. For å kunne identifisere risikoer må Bergen kommune ha en aktiv tilnærming til arbeidet med risikoanalyser, både på et overordnet nivå, men særlig i prosjekter som arbeider med å anskaffe nye systemer. Dette vil gi ansatte kunnskap om potensielle risikoer, usikkerhet knytte til risikoene og samtidig vil muligheten for å sette inn reduserende tiltak gi kommunen anledning til å bedre takle konsekvensene. Dette arbeidet sammenfaller i stor grad med hvordan Aven og Renn (2010) definerer risiko, og viser dermed hvordan kommunens tilnærming til og arbeid med risiko inngår som en naturlig del av å skape en god sikkerhetskultur, som presentert av Antonsen (2009b).

5.2.2 Hva gjør kommunen sårbar?

Som redegjort for i teorikapittelet, kan det i praksis være vanskelig å måle sårbarhet i en organisasjon. Ifølge Njå et al. (2020) kan sårbarhet handle om manglende evne til å motstå konsekvensene av en uønsket hendelse, sårbarhet kan handle om usikkerhet knytte til fremtiden og det kan handle om manglende evne til å gjenoppta sin funksjon (Njå et al., 2020, s. 52). Engen et al. (2016) formidler at en teknologisk sårbarhet kan handle om et systems utfordring med å gjenopprette sin normale funksjon dersom systemet belastes utover normalen, i likhet med Njå et al. (2020).

Fra empirien fremkommer det at kommunens arbeid med å identifisere og forhindre sårbarheter og trusler er viktig for å sikre den enkelte innbyggers personvern og informasjonssikkerhet. Informantene trekker også frem manglende kompetanse, manglende etterlevelse i kommunen og manglende forståelse som eksempler på sårbarheter kommunen står ovenfor. Samtidig fremkommer det et overordnet fokus fra kommunens side mot å aktivt arbeide for å identifisere sårbarhetene, og tilrettelegge for at konsekvenser av en hendelse ikke har særlig stor innvirkning på de systemene som belastes. Kommunens tilnærming til å identifisere sårbarheter, både menneskelige og teknologiske, viser at arbeidet kan tolkes i lys av kommunens arbeid med å skape en sikkerhetskultur. Dersom kommunen har kunnskap om hvilke hendelser som kan true kommunens håndtering av personopplysninger, og simultant bevisstgjør ansatte på hva handlinger kan føre til, gjør dette kommunen således i stand til å tilrettelegge for forsvarlig håndtering.

Det fremkommer også av empirien at kommunen skal tilrettelegge for at systemene som ansatte bruker er så trygge som mulig. Informantene opplever også et økt fokus på kompetanse rundt systemene som brukes, og har en generell oppfatning om at ansatte er i stand til å håndtere de systemene som inngår i arbeidshverdagen. Samtidig påpekes det av Informant D at «All historie rundt tekniske systemer viser oss at 70-80% er brukerfeil», viser til at kommunen fortsatt må belage seg på feil og ulykker knyttet til systemene fremover. Likevel er det viktig for kommunen å fortsette arbeidet med å trygge systemene, og gjøre ansatte kompetent nok til å takle utfordringer og problemstillinger som reiser seg tilknyttet personvern og informasjonssikkerhet.

Således blir arbeidet kommunen gjør med å identifisere hendelser og redusere risikoer en naturlig del av arbeidet kommunen gjør for å skape en sikkerhetskultur. Å gjøre ansatte bevisst på sårbarheter og konsekvenser har en innvirkning på deres holdninger og verdier knyttet til sårbarheter knyttet til personvern og informasjonssikkerhet, men også til de teknologiske systemene kommunen bruker. Dette gjør at det kan trekkes linjer mellom kommunens arbeid med å skape kultur og det å være bevisst på sårbarheter som kan true organisasjonen. Dermed blir kommunens tilnærming til og arbeid med sårbarheter en naturlig del av hva kommunen selv tillegger en forsvarlig håndtering av personopplysninger, ved å presentere en overordnet tilnærming til det, og en aktiv innsats for å bevisstgjøre ansatte på hva sårbarhetene kan være, og videre om konsekvensene. Her kan det også trekkes linjer til hva Reason (1997) presenterer om en rettferdig kultur. Videre kan arbeidet således beskrives som en del av kommunens

videreføring av sikkerhetskulturen i kommunen, som presentert av Antonsen (2009b) og Reason (1997).

5.2.3 Betydningen av kompetanse i kommunen

En god sikkerhetskultur forutsetter at ansatte med riktige kompetanse får ta avgjørelser i de situasjonene som krever det, ifølge Weick & Sutcliffe (2007) og Reason (1997. Det fremkommer altså et behov for kompetanse, men forfatterne går i liten grad inn på viktigheten av *kompetanseheving* i en organisasjon. Dette fremkommer dog i arbeidet Bergen kommune gjør. Empirien formidler at det er et stort fokus på kompetanseheving, og flertallet av informantene opplever at kommunen tilbyr gode muligheter for at ansatte kan heve egen kompetanse. I tråd med hva Reason presenterer om kompetanse hos ansatte, vil det derfor være naturlig å argumentere for at kompetanseheving bør inngå som et naturlig element blant det som presenteres i en fleksibel kultur.

Alle informantene er dog ikke enig i at kommunen tilrettelegger for kompetanseheving. Manglende tid, dårlig utformet kurs og lite tilrettelegging fra ledere trekkes frem av informantene som utfordringer rundt å heve egen kompetanse. Samtidig er flertallet av informantene enig i at det er viktig for kommunen at ansatte har god kompetanse om de digitale systemene og verktøyene som inngår i det daglige arbeidet, men at dette kan være begrenset av tekniske ferdigheter og ansattes egen vilje til å ta til seg kompetanse knyttet til de digitale systemene. For at kommunens arbeid med informasjonssikkerhet og personvern fremover skal følge gjeldende lovverk og retningslinjer, blir det således viktig at ansatte er villig til å tilegne seg kunnskap om dette fagfeltet. Personvern og informasjonssikkerhet er et fagfelt som kontinuerlig er i endring, og fokus på kompetanse-og særlig kompetanseheving blir en viktig forutsetning for at kommunen skal klare å holde følge.

Som det fremkommer av delkapitlene ovenfor, trekkes kompetanse også frem som viktig i forhold til kommunens arbeid med risiko og sårbarheter. Samlet gjør dette at kompetanse også inngår som en naturlig forlengelse av kommunens sikkerhetskultur, og blir dermed en viktig faktor i hva kommunen tillegg en forsvarlig håndtering av personopplysninger.

5.2.4 Hva kjennetegner forsvarlig håndtering av personopplysninger?

Med dette kan det konkluderes med at i kommunen forstås forsvarlig håndtering av personopplysninger som et nøye fokus på blant annet risiko og arbeid med risikoanalyser. Dette

arbeidet er således avgjørende for å hindre fremtidige glipp i personvern og informasjonssikkerhet. Flere av informantene gjorde det klart at lignende hendelser som skjedde i 2018 og 2019 vil neppe kommunen oppleve igjen. Videre fremkommer det at kommunens arbeid med å identifisere sårbarheter som potensielt kan true arbeidet med å sikre personvern og informasjonssikkerhet i kommunen fremstår som vesentlig. Kommunen vektlegger også betydningen av kompetanse og kompetanseheving for å sikre arbeidet med å sikre forsvarlig personvern og håndtering av personopplysninger. Dette, sammen med arbeidet som gjøres med å utforme en sikkerhetskultur, utgjør dermed viktige premisser for å tilrettelegge for sikker forsvarlig håndtering av personopplysninger i Bergen kommune.

5.3. Hvilken tilnærming til sikkerhet danner det beste utgangspunktet for håndtering av personopplysninger?

Det fremkommer av forskningsspørsmål 1 at arbeidet kommunen gjør samsvarer med hva Reason (1997) tillegger en god sikkerhetskultur, samtidig som det tydeliggjøres i forskningsspørsmål 2 at kommunen også aktivt arbeider med sårbarheter, risiko og kompetanse. Det er videre konkludert med at dette inngår som viktige deler av arbeidet kommunen gjør med å skape en kultur, og forstås således som en naturlig forlengelse av hva Reason presenterer som en sikkerhetskultur. Dette viser at Reason (1997) sin teori om sikkerhetskultur ikke kan fremstilles som en oppskrift på hvordan sikkerhetskultur skal etableres.

I lys av arbeidsoppgavene kommunen har tilknyttet personvern og informasjonssikkerhet, kan det dermed stilles spørsmål til hvorvidt kultur er riktig tilnærming å følge. Kultur er noe som implementeres i en organisasjon med et langtidsperspektiv. Som tidligere nevnt henviser definisjoner av kultur til de immaterielle aspektene ved en organisasjon, og tar i mindre grad høyde for det materielle som inngår som en naturlig del av ansattes arbeidshverdag. Samtidig er det ovenfor vist til at personvern og informasjonssikkerhet er fagområder som stadig tar nye vendinger, og som stadig blir mer komplekst å håndtere. Å innføre en kultur rundt noe som kontinuerlig er i endring, kan dermed være problematisk. Det må likevel trekkes frem at mangel på andre metoder og tilnærminger er det vanskelig å si noe om hvilken alternativ metode som kunne vært hensiktsmessig å benytte.

Det fremkommer fra teorien om kultur i safety og security at tradisjonell sikkerhetskultur i stor grad bærer preg av safety. Tradisjonell sikkerhetskultur vektlegger felles verdier, holdninger

og forståelser i en organisasjon. Fra empirien fremkommer det at kommunens tilnærming til sikkerhetskultur også kan forstås på denne måten, nemlig som en kultur med hensikt om å forberede, ta høyde for og håndtere uhell, feil og ulykker som er gjort uten en ondsinnet hensikt (Jore, 2016: Jore, 2020).

Det er likevel viktig å trekke frem at empirien formidler videre at kommunen dels jobber mot en kultur som også inkluderer de materielle aspektene ved organisasjonen, som digitale systemer og verktøy. En slik definisjon av kultur presenteres av Engen et al. (2016) og Antonsen (2009a). Forfatterne formidler at kultur også må handle om det materielle ved en organisasjon, og ikke bare fokusere på det immaterielle. I lys av hva forfatterne formidler, kan det være hensiktsmessig for kommunen og i større grad arbeide mot en kultur som inkluderer det materielle med en kultur, som for eksempel digitale systemer og verktøy, og som dermed verdsetter arbeidet med barrierer, konsekvensredusering og tilsiktede feil. Dette fremkommer noe i drøftingen av forskningsspørsmål 2, hvor det formidles at kommunen har en aktiv tilnærming til arbeid tilknyttet risiko, ROS-analyser og sårbarheter i kommunen. Dette viser starten på skifte i kommunens tilnærming til sikkerhet, hvor arbeidet tilknyttet personvern og informasjonssikkerhet krever et økt fokus på risiko, sårbarheter og kunnskap, og en kultur som i større grad retter seg mot security.

På denne måten kan kommunens arbeid forstås i tråd med Kongsvik et al. (2018) sin argumentasjon om at de to tilnærmingene (safety og security) er i ferd med å vokse sammen. Forfatterne argumenterer for at dette er et resultat av den teknologiske utviklingen, noe som også kan sies å gjelde for Bergen kommune. I tråd med kommunens avhengighet til digitale systemer og verktøy, kan sårbarheten dette representerer, samt konsekvensene som følger av feilt bruk, gjøre at det også kan ses tendenser til en sammensmelting av de to tilnærmingene, som Kongsvik et al. (2018) formidler. Systemene kommunen bruker og kompleksiteten knyttet til personopplysninger, gjør følgelig at hverken safety eller security alene kan takle dette alene. I tråd med dette forstås drøftingen i forskningsspørsmål 2 som et steg i denne retningen. Ifølge forfatterne kan ikke dagens risikobilde fjernes, og fokuset må dermed være på å «[...] bygge konsekvensreduserende barrierer og motstandskraft blir de viktigste virkemidlene» (Kongsvik et al., 2018, s. 280), slik tendensene hos Bergen kommune viser.

Slik kan kommunens arbeid også forstås i samsvar med hva Kriaa et al. (2015) formidler, om at safety og security fungerer som to forskjellige tilnærminger til sikkerhet, men som gir hverandre gjensidig støtte. Det er vel etablert at sikkerhetskultur tradisjonelt sett har en safety-tilnærming til sikkerhet. Likevel gjør arbeidet knyttet til personvern og informasjonssikkerhet det nødvendig å i større grad kunne ta høyde for utenfor det safety dekker. Ved å utvide kulturens definisjon til en som også tar høyde for de materielle aspektene ved kultur, som digitale systemer og verktøy viser Bergen kommune at det er ikke bare de immaterielle aspektene som verdier, holdninger og forståelse som utgjør en kultur.

Tilnærming til risiko, sårbarheter og å være innforstått med viktigheten av kompetanse-og kompetanseheving, at kommunens arbeid med personvern og informasjonssikkerhet beveger seg utenfor hva safety definerer. Kommunen viser at en sikker forsvarlig håndtering av personopplysninger krever mer «bare» de immaterielle aspektene ved kultur, noe som tydeliggjør behovet for en kulturdefinisjon som også griper om det materielle.

Kongsvik et al (2018) formidler at de to tilnærmingene begynner å vokse sammen grunnet digitaliseringen, også her kan det trekkes synergier til Bergen kommune. Videre vektlegges det virkemidler som tradisjonelt sett knyttes til security (barrierer, konsekvensreduserende tiltak og motstandskraft) som er viktige for å sikre kommunens arbeid med personvern og informasjonssikkerhet. I lys av hva forfatterne formidler, kan det således være hensiktsmessig å vektlegge noen av disse fremover.

Med dette kan det følgelig konkluderes med at den tradisjonelle sikkerhetskulturen i stor grad preges av safety, men at det i lys av nye teknologiske systemer er behov for et skifte som i større grad tar for seg security. Dette er et resultat av digitalisering av samfunnet, og personopplysningenes økte sårbarhet i en digital kontekst. Fremover vil det derfor være behov for å tilrettelegge for enten en tilnærming til sikkerhet som samlet kan skape et godt grunnlag for å bygge en sikkerhetskultur, eller så må kommunen i større grad følge Kongsvik et al. (2018) sin tankegang om at de to tilnærmingene er i ferd med å vokse sammen, og videre bygge en kultur rundt dette.

6. Konklusjon

Med utgangspunkt i oppgavens empiriske datagrunnlag, analyse og drøfting, vil dette kapittelet presentere et svar på oppgavens problemstilling. Kapittelets første del vil fremheve sentrale funn, særlig knyttet til forskningsspørsmålene. Disse vil samlet brukes for å besvare oppgavens problemstilling. Kapittel 6.2 vil ta for seg «veien videre» tilknyttet en eventuell forlengelse av studien eller videre forskning relatert til oppgaven.

6.1 Hvordan kan kommunens arbeid med sikkerhetskultur tilrettelegge for forsvarlig håndtering av digitale personopplysninger?

Denne oppgaven har hatt som formål å undersøke hvordan kommunen sitt arbeid med sikkerhetskultur kan tilrettelegge for en forsvarlig håndtering av digitale personopplysninger. For å gi forskningen ytterlig dybde, har det i tillegg vært presentert tre forskningsspørsmål, som i og for seg har hatt som hensikt å belyse deler av oppgavens problemstilling. Problemstillingen har vært som følger:

«Hvordan kan kommunens arbeid med sikkerhetskultur tilrettelegge for forsvarlig håndtering av digitale personopplysninger?»

Arbeidet Bergen kommune gjør med å sikre personopplysningene som forvaltes av kommunen, kan tydelig beskrives som en kulturbygging med et sikkerhetsperspektiv, i tråd med hva Reason (1997) og Antonsen (2009) beskriver. Kulturen står frem som en egen kultur (i motsetning til en subkultur), som også samsvarer med hva relevant litteratur sier om sikkerhetskultur. Empirien formidler at sikkerhetskultur er noe kommunen arbeider med, men informantenes inntrykk av hva som menes med en sikkerhetskultur er noe varierende. Fra empirien fremkommer det dog tydelig at personvern og informasjonssikkerhet er viktige innsatsområder i kommunen, og en god og helhetlig sikkerhetskultur er vesentlig for at kommunen skal kunne håndtere dette stadig mer avanserte arbeidsområdet fremover.

Videre samsvarer kommunens arbeid i stor grad overens med hva Reason formidler om sikkerhetskultur, samtidig som det kan trekkes frem svakheter ved det teoretiske grunnlaget, og områder hvor kommunens arbeid er tilsynelatende mer enn hva Reason formidler som nødvendig. Kommunens arbeid med å skape en sikkerhetskultur fremstår dermed som en god tilnærming til hvordan utfordringer og problemstillinger som reiser seg tilknyttet personvern,

kan håndteres. Samtidig er det viktig å påpeke at kommunen fortsatt har en del gjenstår før sikkerhetskulturen er på et nivå som bør-og kan forventes av en aktør av Bergen kommunes størrelse og betydning. Dette er særlig arbeid tilknyttet avvik-og avviksrapportering med personvernbrudd, ledelsesforankring og kompetanse-og kompetanseheving.

For å illustrere hva kommunen selv forstår som en sikker og forsvarlig håndtering av personopplysninger, trekker kommunen frem arbeid med risiko og risikoanalyser helt ned på prosjektnivå, aktivt arbeide med å identifisere sårbarheter som kan true innbyggernes personvern samt være innforstått med betydningen kompetanse-og kompetanseheving har for de ansatte i kommunen.

Betydningen av å se sammenhengen mellom sårbarheter, risiko og kompetanse blir således også viktig, for å kunne se «hele bildet», og ikke bare fragmenterte deler. Som det trekkes frem har kommunen fortsatt forbedringspotensial tilknyttet dette arbeidet, men slik det fremkommer av empirien har kommunen opparbeidet seg et godt grunnlag for veien videre. Arbeidet tilknyttet risiko, sårbarheter og kompetanse forstås dermed som en naturlig forlengelse av arbeidet kommunen gjør med å skape en sikkerhetskultur, som skal sikre kommunens arbeid videre med personvern og informasjonssikkerhet.

Med en slik safety-tilnærming til sikkerhet skal kommunen kunne være i stand til å håndtere feil, uhell og ulykker som ikke er gjort med en ondsinnet hensikt. Likevel gjør digitaliseringen og faktumet om at personvern i stor grad omtales i en digital kontekst i dag det nødvendig å stille spørsmål til hvorvidt dette tilnærmingen til sikkerhet er tilstrekkelig for kommunen fremover. Komplekse systemer kan vise seg å være sårbar dersom de brukes feil, samtidig som de kan være attraktive mål for personer som ønsker å gjøre skade. Det blir derfor naturlig å trekke slutninger til at det fremover bør etterstrebes en tilnærming til sikkerhet som evner å gripe om feil, ulykker og uhell, men også tilsiktede handlinger som kan ha store konsekvenser for kommunen, men særlig for innbyggerne.

Med dette til grunn konkluderes det med at Bergen kommune sitt arbeid med å sikre innbyggernes personopplysninger er forankret i sikkerhetskulturen som kommunen nå skaper. Kommunen har skapet et godt utgangspunkt for arbeidet som skal gjøres fremover, og viser at de også evner å tenke «utenfor boksen». Ved å tilrettelegge for arbeid tilknyttet risiko og risikoanalyser, identifisere sårbarheter samt se betydningen av kompetanse blant ansatte, viser

kommunen at dette inngår som en naturlig del av sikkerhetskulturen som videre skal tilrettelegge for sikker og forsvarlig håndtering av digitale personopplysninger. For å håndtere et fagområde som kontinuerlig er i endring og som stadig blir mer komplekst, identifiseres det likevel et behov for en bredere tilnærming til sikkerhet. For Bergen kommune blir det dermed viktig å i større grad kunne inkludere security som en naturlig del av sikkerhetskulturen i kommunen. På denne måten kan digitale personopplysninger i tiden fremover sikkert og forsvarlig håndteres.

6.2 Veien videre

Det fremkommer av oppgaven at sikkerhetskultur er noe som defineres, forstås og brukes ulikt på tvers av antatte i en og samme organisasjon. Som teorien og kommunens egne målsetninger formidler, er sikkerhetskultur noe som skal være felles for alle ansatte. En videre studie som tar for seg sikkerhetskultur som fenomen i hele Bergen kommune kan derfor være hensiktsmessig. Ved å undersøke dette med en kvantitativ tilnærming, vil ansattes egen tilnærming til sikkerhetskultur komme bedre frem, i tillegg til at den vil operasjonalisere sikkerhetskultur i praksis i større grad enn hva det er gjort her.

Videre er dette få studier som tar for seg sikkerhetskulturen sin rolle i lys av håndtering av personopplysninger og personvern. I tråd med raske utviklingen av teknologiske systemer og verktøy som vi i dag opplever, kan det således være hensiktsmessig å gjennomføre flere kvalitative studier som kan utdype feltet enda mer. Videre kan det være interessant å gjennomføre en lignende studie av kommunen noen år frem i tid, for å se hvorvidt målsetninger tilknyttet implementering av sikkerhetskultur og håndtering av personopplysninger er nådd, og gå i dybden på eventuelle grunner til hvorfor det ikke er det.

Referanseliste

Ale, B. (2009). *Risk: An Introduction- The Concepts of Risk* Routledge

Antonsen, S. (2009a). The relationship between culture and safety on offshore supply vessels. *Safety Science*, *47*(8), 1118-1128. https://doi.org/https://doi.org/10.1016/j.ssci.2008.12.006

Antonsen, S. (2009b). *Safety culture : theory, method and improvement*. Ashgate.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H. & Sandve, K. (2004). *Samfunnssikkerhet*. Universitetsforlaget.

Aven, T. & Renn, O. (2010). *Risk management and governance* (Bd. 16). Springer.

Bergen kommune. (2014). *Bergen, en trygg by- Bergen ROS 2014: Overordnet risiko-og sårbarhetsanalyse for Bergen* Bergen kommune https://www.bergen.kommune.no/omkommunen/planer-i-kommunen/informasjon-om-enkeltplaner/byradsleders-avdeling/risikoog-sarbarhetsanalyse-for-bergen

Bergen kommune. (2017). *Digitalisering og innovasjon i Bergen kommune 2017-2020*. Bergen kommune https://docplayer.me/47133345-Byradssak-1124-17-digitalisering-og-innovasjon-i-bergen-kommune-stca-inkv-esark.html

Bergen kommune. (2020a). *Bergen ROS 2020- «En trygg by for fremtiden»* Bergen kommune https://www.bergen.kommune.no/omkommunen/planer-i-kommunen/informasjon-om-enkeltplaner/byradsleders-avdeling/risikoog-sarbarhetsanalyse-for-bergen

Bergen kommune. (2020b). *Byrådssak /20: Avslutning av helhetlig gjennomgang personvern og informasjonssikkerhet og overføring av ansvar for videre oppfølging til ordinær virksomhet* (2020/107491-1). Bergen kommune https://www.bergen.kommune.no/politikere-utvalg/api/fil/3896985/Framstilling-Avslutning-av-helhetlig-gjennomgang-personvern-og-informasjonssikkerhet-og-overforing-av-ansvar-for-videre-oppfolging-til-ordinaer-virksomhet-

Bergen kommune. (2020c). *Reglement for personvern og informasjonssikkerhet* Bergen kommune https://www.bergen.kommune.no/politikere-utvalg/api/fil/3901088/Reglement-for-personvern-og-informasjonssikkerhet

Bergen kommune. (2020d). *Reglementet for digitalisering og IKT*. Bergen kommune https://www.bergen.kommune.no/politikere-utvalg/api/fil/3903572/Reglement-for-Digitalisering-og-IKT-i-Bergen-kommune

Bergen kommune. (2021a). *Digitaliseringsstrategi Bergen kommune 2021-2025*. Bergen kommnune. https://www.bergen.kommune.no/politikere-utvalg/api/fil/3837015/Digitaliseringsstrategi-Bergen-kommune-2021-25

Bergen kommune. (2021b). *Temaplan for informasjonssikkerhet og personvern: 2021-2025*. Bergen kommune. https://www.bergen.kommune.no/politikere-utvalg/api/fil/3579734/Horingsutkast-Temaplan-for-informasjonssikkerhet-og-personvern

Bergen kommune. (u.å.). *Hvorfor kommunen?* Bergen kommune Hentet 05.05.2021 fra https://www.bergen.kommune.no/jobb/hvorfor-kommunen

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

Blaikie, N. & Priest, J. (2019). *Designing social research : the logic of anticipation* (3rd edition. utg.). Polity Press.

Danermark, B. (2002). *Explaining society : critical realism in the social sciences*. Routledge.

Datatilsynet. (2019a, 19 mars.). *Endelig vedtak om gebyr til Bergen kommune.* Datatilsynet https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2019/endelig-vedtak-om-gebyr-til-bergen-kommune/

Datatilsynet. (2019b, 17 juli). *Hva er en personopplysning?* . Datatilsynet https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/
Datatilsynet. (2019c, 17 juli). *Hva er personvern?* . Datatilsynet https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/
Datatilsynet. (2020, 20 mai). *Varsel om overtredelsesgebyr til Bergen kommune.* Datatilsynet https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-overtredelsesgebyr-til-bergen-kommune/
Deloitte. (2019). *Forvaltningsrevisjon- Bergen kommune* https://www.bergen.kommune.no/politikere-utvalg/api/fil/2200932/Bergen-kommune-forvaltningsrevisjon-av-informasjonssikkerhet
Dey, I. (2004). Grounded theory IC. Seale, Gobo, G., Gubrium, J. F. & Silverman, D. (Red.), *Qualitative research practice* (1. utgave. utg., s. 80-93). Publications Ltd.
Digdir. (u.å.-a). *Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål*. Digitaliseringsdirektoratet Hentet 28.05.2021 fra https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123
Digdir. (u.å.-b). *Informasjonssikkerhet for personopplysninger* Digitaliseringsdirektoratet https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-personopplysninger/2282
Dvergsdal, H. (2019, 28 oktober). *Digitalisering.* Store norske leksikon https://snl.no/digitalisering
Engen, O. A., Kruke, B. I., Lindøe, P., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm akademisk.
Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Fagbokforl.
Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (2. utg. utg.). Fagbokforl.
Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *ECTJ*, *29*(2), 75. https://doi.org/10.1007/BF02766777
Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (2. utg. utg.). Høyskoleforl.
Jansen, K. (2019, 14 februar). *– Vi kan ikke ha det sånn at barns personvern har så liten verdi som det vi opplever nå*. Bergen Tidende.
Jansen, K., Tjeldflåt, G. & Lambrechts, L. (2020, 20 januar). *Dette er feilene som førte til Vigilo-skandalen.* Bergens Tidende https://www.bt.no/nyheter/lokalt/i/naJQmL/her-er-feilene-som-foerte-til-vigilo-skandalen
JBD & FD. (2019). *Nasjonal strategi for digital sikkerhet.* . Justis-og beredskapsdepartementet & Forsvarsdepartementet. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf
JBD & KD. (2019). *Nasjonal strategi for digital sikkerhetskompetanse* Justis-og beredskapsdepartementet & Kunnskapsdepartementet. https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf
Jore, S. (2016). Security culture—a sufficient explanation for a terrorist attack? I (s. 467-474). https://doi.org/10.1201/9781315374987-72
Jore, S. H. (2020). Security and Safety Culture—Dual or Distinct Phenomena? I C. Bieder & K. Pettersen Gould (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 43-51). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_5
KMD. (2019a). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*. Kommunal- og moderniseringsdepartementet.

https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?ch=1
KMD. (2019b, 30 oktober). *Hva er personvern?* . Regjeringen https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/
Kongsvik, T. Ø., Albrechtsen, E., Antonsen, S., Herrera, I., Hovden, J. & Schiefloe, P. M. (2018). *Sikkerhet i arbeidslivet*. Fagbokforl.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156-178. https://doi.org/https://doi.org/10.1016/j.ress.2015.02.008
Kvale, S. (2015). *Det kvalitative forskningsintervju* (3. utg. utg.). Gyldendal akademisk.
Mark, M. S., Tømte, C., Næss, T. & Røsdal, T. (2017). *IKT-sikkerhetskompetanse i arbeidslivet- behov og tilbud* (Rapport 2017:32). f. o. u. N. Nordisk institutt for studier av innovasjon.
Martin, J. (1992). *Cultures in Organizations : Three Perspectives*. Oxford University Press USA - OSO. http://ebookcentral.proquest.com/lib/uisbib/detail.action?docID=716689
Meld. St. 38 (2016-2017). *IKT-sikkerhet: Et felles ansvar* J.-o. beredskapsdepartementet. https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf
Meld.St. 27 (2015-2016). *Digital agenda for Norge: IKT for en enklere hverdag og økt produktivitet.* Kommunal og moderniseringsdepartementet. https://www.regjeringen.no/contentassets/fe3e34b866034b82b9c623c5cec39823/no/pdfs/stm201520160027000dddpdfs.pdf
[Record #68 is using a reference type undefined in this output style.]
Nilstun, C. (2018, 14. mai). *Fleksibilitet.* Store Norske Leksikon. https://snl.no/fleksibel
Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet: analyse, styring og evaluering*. Universitetsforlaget.
NSD. (u.å.). *Fylle ut meldeskjema for personopplysninger* Norsk senter for forskningsdata Hentet 31.03.2021. fra https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/
NSM. (2017). *Helhetlig IKT-risikobilde 2017* Nasjonal sikkerhetsmyndighet https://nsm.no/getfile.php/133675-1592831718/Demo/Dokumenter/Rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf
NSM. (u.å,). *Grunnprinsipper for personellsikkerhet* Nasjonal Sikkerhetsmyndighet Hentet 20.05.2021 fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/
NTB & Nilsen, L. (2018). *Skoleelev varslet om datahull.* Bergens Avisen https://www.ba.no/bergen/datakriminalitet/bergen-kommune/skoleelev-varslet-om-datahull/s/5-8-860854
Opheim, T. (2018, 17 august). *Barneskoleelev varslet om sikkerhetshull for seks måneder sieen* Bergen Tidende https://www.bt.no/nyheter/lokalt/i/yvjMAe/barneskoleelev-varslet-om-sikkerhetshull-for-seks-maaneder-siden
Reason, J. (1997). *Managing the Risks of Organizational Accidents* (1. utg.). Aldershot: Taylor & Francis. https://doi.org/10.4324/9781315543543
Reniers, G. L. L., Cremer, K. & Buytaert, J. (2011). Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL

S&S) model. *Journal of Cleaner Production*, *19*(11), 1239-1249. https://doi.org/https://doi.org/10.1016/j.jclepro.2011.03.002
Rosa, E. A. (1998). Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, *1*(1), 15-44. https://doi.org/10.1080/136698798377303
Sagberg, I. (2020, 05 november). *Organisasjonskultur* https://snl.no/organisasjonskultur
Sander, K. (2019, 30 august). *Subkultur* https://estudie.no/sub-kultur/
Schein, E. H. (1992). *Organizational culture and leadership* (Second Edition. utg., Bd. 26). Elsevier Ltd. https://doi.org/10.1016/0024-6301(93)90120-5
Schein, E. H. & Schein, P. A. (2017). *Organizational Culture and Leadership*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/uisbib/detail.action?docID=4766585
Seksjon for internkontroll. (2019). *Gjennomgang av avvik i kommunikasjonsløsning.* (Saksdokument: 2019/102953-1). Bergen kommune, . https://www.bergen.kommune.no/hvaskjer/barnehage-og-skole/har-mottatt-rapport-etter-intern-gjennomgang-av-avviket-i-vigilo
Smith, C. & Brooks, D. J. (2013). *Security Science: The Theory and Practice of Security*. Oxford: Elsevier Science & Technology.
Sommerfelt, A. (2015, 24 februar). *Etnografi*. Store norske leksikon. https://snl.no/etnografi
Trice, H. M. & Beyer, J. M. (1993). *The cultures of work organizations*. Prentice-Hall.
Weick, K. & Sutcliffe, K. (2007). Managing the Unexpected Resilient Performance in an Age of Uncertainty. *8*.
Wessel-Aas, J. & Ødegaard, M. (2018). *Personvern : publisering og behandling av personopplysninger*. Gyldendal.

Vedlegg

Vedlegg A: Informasjonsskriv

Vil du delta i forskningsprosjektet «Digital sikkerhet i kommunal sektor»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan Bergen kommune arbeider med digitalisering og personopplysninger, risikoer knyttet til dette og om sikkerhetskulturen i kommunen. I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Studien har foreløpig følgende problemstilling: *«Hvordan kan Bergen kommune tilrettelegge for sikker og forsvarlig håndtering av digitale personopplysninger?»*. Prosjektet er begrenset til Bergen kommune, men dens formål er å være overførbar slik at andre kommuner i Norge også kan nyttiggjøre seg av prosjektets funn. Med utgangspunkt i valgt problemstilling vil jeg undersøke hvordan kommunen arbeider med digitalisering og hvordan den takler den økende graden av digitalisering i offentlig sektor. Videre vil jeg undersøke kommunens arbeid for å sikre tilstrekkelig vern om personopplysninger, samt risikoer knyttet til dette.

Formålet med prosjektet er å få et innblikk i kommunens sikkerhetskultur, samt belyse hvordan kommunale retningslinjer blir anvendt i det praktiske arbeidet. Jeg skal undersøke hvorvidt kommunen er kjent med risikoene som foreligger ved å håndtere mengden personopplysninger den i det daglige gjør, samt hvordan kommunen kan tilrettelegge for tilstrekkelig sikring og håndtering av særlige kategorier av personopplysninger.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Jeg kontakter deg fordi du er ansatt i Bergen kommune, og arbeider daglig med enten digitalisering, personvern, prosjektarbeid innenfor de to førstnevnte områdene eller samfunnssikkerhet i kommunen.

Hva innebærer det for deg å delta?

- Dersom du ønsker å delta vil dette innebære å bli intervjuet av meg.
- Intervjuet vil foregå over Microsoft Teams eller ansikt-til-ansikt, dette avtales nærmere.
- Intervjuet vil sannsynligvis ha en varighet på ca. 60 minutter.
- Intervjuene vil bli tatt opp ved hjelp av en båndopptaker, og vil deretter transkriberes i sin helhet.
- Spørsmålene vil omhandle kommunens arbeid med digitalisering, personvern, IKT-kompetanse og kultur, sårbarheter (menneskelige, teknologiske og organisatoriske) og spørsmål om kommunens planer fremover vedrørende de overnevnte temaene.

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 dine opplysninger blir oppbevart og brukt.

- Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket.
- Det er kun jeg, Camilla Smedhaug, om min veileder Sissel Haugdal Jore, ved Universitetet i Stavanger, som vil ha tilgang til opplysningene om deg.
- Intervjuene vil tas opp ved hjelp av en båndopptaker. Dette for å sikre meg mot hacking ol. som kan lede til at informasjon om deg tilfaller uvedkomne.
- Ditt navn og kontaktopplysninger vil ikke lagres på samme enhet som opptaket av intervjuet eller transkriberingen. Navn og andre kontaktopplysninger vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data.

Intervjuobjektene for dette prosjektet kan gjenkjennes i publikasjonen. Opplysningene jeg ønsker å publisere i forbindelse med prosjektet er stilling, arbeidssted og ansvarsområde/rolle i Bergen kommune.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, som etter planen er 15. juni. Personopplysninger, opptak av intervju og transkripsjon vil da slettes.

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?

Jeg behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger 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:

- Meg, Camilla Smedhaug, på e-post: csmedhaug@gmail.com, eller per telefon: 991 05 662
- Min veileder, Sissel Haugdal Jore, på e-post: sissel.h.jore@uis.no, eller per telefon 518 31 830

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

Camilla Smedhaug

Student, Universitetet i Stavanger

Vedlegg B: Samtykkeerklæring

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Digital Sikkerhet i Kommunal Sektor»*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i kvalitativt intervju
- ☐ at det gjøres opptak av intervjuet
- ☐ at opplysninger om meg publiseres slik at jeg kan gjenkjennes

- ☐ Jeg ønsker at (enkelte) opplysninger om meg er anonyme i publikasjonen (vennligst kryss av nedenfor)
- ☐ *Stilling*
- ☐ *Arbeidssted*
- ☐ *Rolle og ansvarsområde*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 15.06.2021.

(Signert av prosjektdeltaker, dato)

Vedlegg C: Intervjuguide

Intervjuguide masteroppgave vår-2021

Tema 1: Bakgrunn

1. Hva er din rolle og ditt ansvar i din stilling?

Tema 2: Digitalisering

2. Hvordan arbeider dere med digitalisering i Bergen kommune?
3. Hvor avhengig er Bergen kommune av sine digitale systemer og verktøy?
4. Hva vil du beskrive som den største utfordringen for Bergen kommune når det kommer til økt bruk av digitale verktøy, og hvordan løser dere disse utfordringene?
5. Hvilke tiltak er iverksatt i og av kommunen i etterkant av den offentlige satsingen på økt digitalisering av og i samfunnet?

Tema 3: Kompetanse og kultur

6. Hvordan vil du beskrive ansattes IKT-kompetanse vedrørende systemene som brukes i det daglige arbeidet?
7. Hvor viktig er det for kommunen at ansatte sitter med god og korrekt kompetanse vedrørende bruk av digitale systemer?
8. Hvordan vil du beskrive sikkerhetskulturen i Bergen kommune?
9. Hvilke utfordringer er knyttet til sikkerhetskulturen i kommunen?
10. Hvordan trekker Bergen kommune som organisasjon lærdom ut av hendelser som har avviket fra ønsket resultat?

Tema 4: Personvern

11. Hvilke tiltak er iverksatt for å sikre tilstrekkelig personvern i kommunen?
12. Til hvilken grad er ansatte observant på problemstillinger som reiser seg vedrørende personvern?
13. Hvordan sikres det at arbeidet med informasjonssikkerhet og personvern er tilfredsstillende?
14. Har det skjedd en endring i rutinene deres de siste fem årene, med tanke på den økte offentlige satsingen på digitalisering og vernet om personsensitive opplysninger?

15. Hvilke utfordringer knyttet til å sikre godt personvern tror du kan være aktuell fremover?
16. Vil kommunens rolle som aktør og forvalter av personopplysninger endre seg fremover?

Tema 5: Sårbarheter: menneskelige, teknologiske og organisatoriske

17. Hvor ofte foretar dere risikovurderinger?
18. Hva er de største sårbarhetene knyttet til kommunen som organisasjon?
19. Hva er de største sårbarhetene knyttet til mennesker som ansatte?
20. Hvordan sikrer kommunen digitale systemer og verktøy mot tilgang fra uvedkomne?
21. Hvordan vil du beskrive kommunens evne til å respondere på hendelser som avviker fra normalen?
22. I hvilken grad evner Bergen kommune å identifisere hendelser som kan være truende for arbeidet kommunen gjør og innbyggerne i kommunen?

Tema 6: Fremtiden

23. Hvordan har tidligere hendelser formet Bergen kommune og det arbeidet kommunen gjør i dag?
24. Hvordan bruker kommunen informasjon fra for eksempel risikoanalyser til å planlegge for fremtiden?
25. Hvilke utfordringer er det forventet at digitaliseringen bringer med seg fremover, og hvordan planlegger kommunen å møte utfordringene?