Hvordan har bedrifter forholdt seg til GDPR etter bevisstgjøring av sin nåværende situasjon: En casestudie i samarbeid med Sticos AS.

Thobias Bjørseth, bachelor i Digital forretningsutvikling.

Forord

Denne bacheloroppgaven utgjør den avsluttende delen av bachelorstudiet i Digital forretningsutvikling ved NTNU.

Takk til Sticos AS for all hjelp og tilrettelegging. Spesiell takk til Christian Langvatn, Ranveig Fjellheim Tunaal og Fredrik Aakvik.

Jeg vil også takke alle informantene som var med på å gjøre denne studien mulig.

En stor takk til veileder Gunhild Marie Lundberg for god hjelp og støtte underveis.

Takk også til Lise Galaasen.

Sammendrag

Bakgrunnen for valg av emne til studien var en interesse for sikkerhet og personvern. I dagens digitaliserte hverdag og hurtige teknologiske utvikling står personvern i sentrum. Sticos la til rette for undersøkelse på bakgrunn av GDPR-kurset kalt Serious Game, et spill hvor bedrifters nåsituasjon angående GDPR, blir kartlagt.

Problemstillingen ble utformet på bakgrunn av GDPRs effekt på bedriftslandskapet, og hvordan bedriftene forholder seg til GDPR etter å ha blitt gjort bevisst på sin nåsituasjon. Følgende problemstilling ble utarbeidet: «Hvordan har bedrifter forholdt seg til GDPR etter bevisstgjøring av sin nåværende situasjon.» Målet med studien er å belyse aspektene rundt arbeidet med GDPR, samt oppmuntre til videre forskning.

Metoden brukt i denne studien var en kvalitativ undersøkelse av syv bedrifter som hadde tatt Sticos' GDPR-kurs, Serious Game. Kursene ble holdt i 2017 og 2018. Det ble undersøkt hvorvidt bedriftene hadde jobbet med GDPR slik det ble foreslått på kurset. Også intervjuobjektenes tanker om, og holdninger til innføringen og viktigheten av GDPR ble undersøkt. Datamaterialet ble innhentet ved hjelp av et utdypende spørreskjema via e-post. Dataene ble analysert ved bruk av koding. Funnene drøftes i sammenheng med teori.

Resultatene i studien viser at bedriftene jobbet godt med GDPR i tiden rett etter kurset. Et fåtall av bedriftene (2) kan sies å ha god kontroll på GDPR. Resultatene avdekker generelt at arbeidet med GDPR faller litt av etter hvert, og at kategoriene *databehandleravtaler* og *roller* fra Serious Game blir høyere prioritert enn de andre kategoriene i spillet. Resultatene forteller videre om noe forvirring rundt GDPR-reglene i gitte situasjoner. Det kommer også frem at intervjuobjektene synes GDPR er et stort tema å sette seg inn i, og det oppleves som et styr. Det blir nevnt at når GDPR er innarbeidet i rutiner og man har fått utarbeidet nødvendige dokumenter, er ikke GDPR så «slitsomt» som i initieringsfasen. Studien viser at GDPR-arbeidet likevel stagnerer, på tross av dette.

Innhold

Figurliste

1.0 Innledning

Denne studien tar for seg Personvernforordningen (engelsk: General Data Protection Regulation, forkortet GDPR) og ordningens effekt på bedrifter. GDPR er en forordning som *«regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU»* (European Comission, 2019). GDPR gjelder som felles standard i EU og er en lov (*regulation*), ikke et direktiv. Det vil si at den er rettskraftig i alle EUs medlemsland, samt for alle bedrifter som prosesserer data fra EU, uansett i hvilket land i verden de befinner seg. Disse virksomhetene er derfor nødt til å følge GDPR, i motsetning til tidligere, da man hadde retningslinjer (direktiv) som ga rom for egne tolkninger (Politou, Alepis og Patsakis, 2017).

En viktig del av forordningen fungerer slik at lagring og prosessering av persondata ikke kan foregå uten samtykke. Individet har også rett til å trekke et samtykke når som helst (Intersoft Consulting, Artikkel 7, 2019). Prosessering av sensitive persondata som sier noe om rase, etnisitet, genetiske data, biometriske data, samliv, helse, seksuell orientering, politiske synspunkter, religion eller fagforening er forbudt. Det finnes imidlertid ti unntak fra denne regelen, der eksplisitt samtykke fra prosesseringssubjektet er et av de viktigste unntakene (Intersoft Consulting, Artikkel 9, 2019). Unnlater man å følge lovene, resulterer det i bøter på opptil 20 millioner euro, eller 4 % av totale årlige inntekter (GDPR EU.ORG, 2019). Forordningen erstatter det tidligere direktivet kalt Data Protection Directive (DPD), som ble introdusert i 1995 (Politou, Alepis og Patsakis, 2017).

Studien ser på hvordan bedrifter forholder seg til den nye forordningen og prosessene rundt det å innføre den. Studien fokuserer på norske bedrifter som har tatt Sticos' GDPR-kurs, og i hvilken grad bedriften har etterlevd det som er lært/foreslått på kurset. Hvordan følger bedriftene opp GDPR-innføringen etter endt kurs?

1.1 Valg av emne

Ettersom GDPR er essensielt for europeiske og internasjonale bedrifter samtidig som den teknologiske utviklingen er i hurtig vekst - vil det være hendig for bedriftene å ha en bevissthet rundt hvordan de skal implementere GDPR. Det er videre interessant å se på hvilke virksomheter som ligger foran skjema, og hvilke som sliter eller henger etter når det gjelder GDPR, og hvorfor. Det vil samtidig være betydningsfullt å se på hvordan innføringen av GDPR påvirker sikkerhetsfokuset i bedriften. Flere selskaper som utvikler applikasjoner, lar utviklere bygge inn en sesjons-gjenspilling i appen sin, noe som vil si at datainnsamling baserer seg på sveip, knappetrykk og skjerminnhold (Smedsrud, 2019 for Tek.no). Dette eksempelet reiser nye spørsmål, for eksempel om hvordan opplysningene som innhentes på denne måten, skal håndteres i bedriftene, og hvilken rolle GDPR vil spille her – og ikke minst hva opplysningene skal klassifiseres som. Slik anvendes altså ny teknologi for å samle inn brukeropplysninger, og det er sannsynlig at det vil oppstå ytterlige utfordringer i fremtiden, forårsaket av teknologi som ennå ikke er funnet opp.

GDPR er noe helt nytt, og effektene av ordningen er derfor ikke undersøkt eller studert i stor grad. Personvern er imidlertid et høyaktuelt tema i dagens digitale samfunn, og forordninger som beskytter personinformasjon, vil i større grad enn tidligere debatteres og utforskes. Målet med studien er å bidra til dette, slik at fremtidige ledere og bedrifter vil stå bedre rustet i møtet med personvern.

1.2 Problemstilling og forskningsspørsmål

Ettersom GDPR har gjort sitt inntog i bedrifter rundt om i EU, har følgende problemstilling tatt form: *«Hvordan har bedrifter forholdt seg til GDPR etter bevisstgjøring av sin nåværende situasjon?»* Det er viktig å vite for samfunnet og næringsbransjen hvordan bedrifter jobber - eller ikke jobber - med GDPR. Hvordan skal bedriftene få innført GDPR? Hva er det som hindrer dem i å begynne eller gjennomføre? Viktigheten av forordningen gjenspeiles i talløse persondatalekkasjer fra store selskaper og organisasjoner, der individet ikke er klar over, eller har noen påvirkning på hvordan ens persondata blir behandlet. Denne studien vil være aktuell for alle bedrifter i Europa, spesielt norske. Den vil samtidig være nyttig for myndighetene i alle europeiske land, samt i land utenfor Europa som behandler europeiske persondata, i tillegg globale bedrifter og myndigheter som blir påvirket av GDPR.

2.0 Casebeskrivelse

Sticos AS er en IT-bedrift som holder norske virksomheter oppdatert på lover og regelverk gjennom praktiske verktøy, kurs og rådgivning. Bedriften ble grunnlagt i 1983 og holder til på Lade i Trondheim. Sticos har 120 ansatte og over 10 000 kunder, noe som tilsvarer rundt 60 000 brukere. Sticos' mål er å tilby trygghet og smarte løsninger i arbeidshverdagen – enten man er regnskapsfører, revisor, økonomisk rådgiver, HR-sjef, lønnsmedarbeider eller daglig leder (Sticos, 2019).

Bedriften har utviklet et kurs kalt Serious Game, som er et brettspill (og under utvikling til å bli et digitalt spill) for å kartlegge norske bedrifters kompetanse og nåværende situasjon når det kommer til GDPR. Spilleren (kunden) går igjennom forskjellige nivåer og kartlegger nåsituasjonen i bedriften for GDPR. De forskjellige nivåene er:

- **Behandlingsgrunnlag**. Hvilke vilkår og krav som må oppfylles for å få lov til å behandle personopplysninger.
- **Databehandling**. GDPR pålegger både databehandlere og de som bruker databehandlere en rekke nye plikter og dokumentasjonskrav. Inngå databehandleravtaler.
- **Roller**. Beskrivelse av ansvar og roller for innføring av GDPR i bedrift.
- **Informasjonssikkerhet**. Identifisere risikofaktorer. Bedre sikkerhet og rutiner med tanke på integritet, konfidensialitet og tilgjengelighet.
- **Brudd på reglene**. Konsekvenser ved brudd på GDPR-reglene.
- **Handlingsplan**. Prosedyrer for gjennomgang og etterlevelse av rutinene. Opprette handlingsplan, slik at man sørger for at bedriften til enhver tid overholder regelverket.

Spilleren finner ut av hvilke «hull» som må tettes for at bedriften skal være kompatibel med GDPR. Når man har fullført et emne, kan man gå til neste nivå, og slik fortsetter man helt til man er ferdig med (har vunnet) spillet. Spilleren må også gjennom stresstester: Vedkommende må løse problemer knyttet til fiktive scenarier i bedriften. Dette for å teste hvordan kunden vil håndtere en vanskelig situasjon, samtidig som man kartlegger kunnskapen og ser på hvor kunden trenger å forbedre seg. Etter fullført kurs sitter kunden igjen med en handlingsplan og tiltak hvor alle områder bedriften trenger å jobbe med for å komme «over vann» og sikre et godt GDPR-arbeid i fremtiden, er listet opp.

3.0 Teori

Teoridelen vil se på litteratur fra forskjellige forfattere for å få et innblikk i GDPR og hvilken betydning den har for hvordan virksomheter behandler personopplysninger. Det vil i tillegg undersøkes hvordan endringer påvirker menneskene i en bedrift. Det vil bli sett på forskjellige casestudier og utsagn, samt hva tidligere studier og forskere har funnet ut.

3.1 Innrulling av GDPR i Europa

Etter avtalen mellom Europaparlamentet og Det europeiske råd i 2015, vedtatt i 2016, har GDPR kommet for fullt hos virksomheter i Europa (Albrecht, 2016). Mange virksomheter har hatt GDPR som hovedfokus på ledelsesnivå, og noen har også endret sin strategi for å bli ledende innen datasikkerhetsvennlige produkter og tjenester, som følge av GDPR (Albrecht, 2016). Ifølge Jan Philipp Albrecht (2016) ville virksomheter som hadde forberedt seg tidlig, ha store fordeler da Personvernforordningen trådte i kraft 24. mai 2018. Videre påpeker han at virksomheter som ikke var på forskudd, ville stille svakere konkurransemessig, da GDPR vil fungere som «gullstandarden» for forbrukertillit og ny innovasjon og forbrukertillit i digital teknologi. Det gjennomføres sanksjoner for virksomheter som ikke har innført GDPR på tilstrekkelig måte, noe som igjen vil føre til økonomisk tap for de som er på etterskudd (GDPR EU.ORG, 2019).

Politou, Alepis og Patsakis (2017) mener i tillegg at innrulleringen av GDPR vil føre til harmonisering av nåværende databeskyttelseslover på tvers av EU - samtidig som det forsterker databeskyttelsesrettigheter og businessmuligheter i Det indre marked, det vil si avtalen mellom EU og EØS-landene om fri flyt av varer, tjenester, personer og kapital (Utenriksdepartementet, 2016). De forklarer videre at GDPR eksplisitt i artikkel 25 pålegger organisasjoner å overholde *«data protection by design and by default»* (Intersoft Consulting, Artikkel 25, 2019), det vil si dataminimalisering som en standardisert tilnærming til datainnsamling og bruk (Politou, Alepis og Patsakis, 2017). Dataminimalisering vil si å bare bruke den dataen som er nødvendig for å fullføre en oppgave/handling. Data brukt til en ting kan ikke brukes til noe annet uten videre samtykke (Privazyplan, 2018).

Dette har videre sammenheng med artikkel 17, som omhandler retten til å bli glemt, noe som innebærer at dataansvarlig sletter persondata, stopper videre formidling og sørger for at tredjeparter avslutter prosessering av dataene (EU GDPR.ORG, 2019). For store bedrifter og

organisasjoner betyr dette omstrukturering i flere ledd, samt at de må inngå nye databehandleravtaler med leverandører. Alle som behandler persondata er databehandlere, og kan beskrives som *«en person eller virksomhet som behandler personopplysninger på vegne av den behandlingsansvarlige bedriften. GDPR krever at det foreligger en avtale mellom partene, kalt databehandleravtaler»* (NHO, 2019). En databehandleravtale skal sikre at personopplysninger blir behandlet i tråd med GPDR-regelverket og setter en tydelig ramme for hvordan en databehandler skal opptre (Datatilsynet, 2019).

Store bedrifter, det vil si bedrifter med flere enn 250 ansatte, vil ha større behov for grundig gjennomføring av GDPR-innføringsprosessen. Det vil kreves store endringer i bedriften med hensyn til rutiner, programmering, digitalisering og lagring. I en storbedrift må alle avdelinger opp på samme standardiserte plan slik at man er kompatibel i hele organisasjonen. Ifølge European Commission (2019), er 1 % av alle bedrifter i EU storbedrifter. De resterende er små og mellomstore bedrifter (SMB). Det vil si at de har mellom 1 og 250 ansatte og omsetter for fra 2 millioner og 50 millioner euro (European Commission, 2019). Disse virksomhetene har ofte færre ledd og avdelinger, og det kan være at det ses på som gunstig at de gjør en del av GDPR-arbeidet selv. Det kan også tenkes at det er en vanskeligere jobb, da mindre bedrifter har færre ressurser.

Når en bedrift skal innføre GDPR burde ledelsen fordele roller. Finne ut av hvem som skal ha ansvar for hva, slik at ansatte i bedriften har god kontroll over hvilken rolle man har i GDPR-innføringen. Prendergast (1995) fant i sin studie ut at ledere ofte tar på seg for mye ansvar, gir rutineoppgaver til ansatte, samtidig som de bruker for mye energi og krefter på egne oppgaver. Av den grunn burde bedriftsledere fordele ansvar og roller til andre, helst opprette et personvernombud, i innføringsprosessen av GDPR. Personvernombud i bedrifter skal *«samarbeide med Datatilsynet og fungere som et kontaktpunkt for tilsynet ved eventuelle spørsmål. Ombudet skal også ved behov kunne rådføre seg med tilsynet, slik at det sikres god kommunikasjon»* (Datatilsynet, 2019). Ikke alle bedrifter er pålagt å ha personvernombud, men Datatilsynet oppfordrer alle virksomheter til å opprette dette og never at *«erfaringsmessig har Datatilsynet sett at det å ha en person med kunnskap om og fokus på personvern i en virksomhet kan gjøre en stor forskjell»* (Datatilsynet, 2019). Bedrifter som er pålagt å ha personvernombud er bedrifter der databehandlingen utføres av en offentlig myndighet eller et offentlig organ (foruten domstoler), eller der databehandlerens

hovedvirksomhet består av behandling av sensitive personopplysninger (se 1.0) i stor skala, eller der databehandlerens hovedvirksomhet består av behandlingsaktiviteter som krever regelmessig og systematisk overvåking i stor skala (Datatilsynet, 2019).

Videre forbyr GDPR virksomheter i å overføre personlig informasjon (data) ut av EU og det Europeiske Økonomiske Samarbeidsområde (EØS) (andre regler gjelder for Sveits som har sin egen avtale), med unntak av lagring i skyen fra USA-baserte selskaper (Google, Dropbox, Amazon). Denne ordningen er kalt EU-US Privacy Shield agreement (International Trade Administration, 2019). Avtalen er designet av U.S. Department of Commerce og European Commission for å tilby bedrifter på begge sider av Atlanterhavet en måte å innrette seg etter datasikkerhetskrav på ved overføring av personlig informasjon (International Trade Administration, 2019). Hyland (2017) mener Privacy Shield kan by på problemer i personvernsaker som kommer til retten i henhold til GDPR, og peker derfor på at virksomheter burde ha en plan B som sikrer at data i skyen forblir i EØS. Dette betyr at virksomheter som bruker slike skyløsninger i dag (Google, Dropbox, Amazon), også burde vurdere andre langsiktige løsninger.

3.2 Tilgang på informasjon

Det at GDPR er en lov (Politou, Alepis og Patsakis, 2017), pålegger bedrifter i EU å følge den. Dette resulterer i millioner av bedrifter som i løpet av kort tid må endre produktene og tjenestene sine. Det må også gjøres organisatoriske endringer, slik at man er kompatibel med GDPR. Spørsmålet blir da: Hvor skal bedriften starte? Er det opp til hver enkelt bedrift å sette seg inn i og innføre GDPR? Det kan være vanskelig for ledelsen å vite hvor man skal begynne, derfor er det flere bedrifter (som Sticos) som tilbyr hjelp. Man kan også kjøpe implementerings og kompatibilitetsguider til GDPR på nett (IT Governance Privacy Team, 2017). Det kreves et solid informasjonsgrunnlag før man kan gå i gang med innføringen av GDPR, og tilgangen på viktig og riktig informasjon er derfor essensielt for å lykkes. Det er også viktig å merke seg at guidene man får kjøpt ikke passer alle bedrifter. Organisasjoner opererer på forskjellige måter og med ulike leverandører og samarbeidspartnere, det er ikke slik at ett felles rammeverk passer alle – og burde heller ikke være normen for tilnærming på kompatibilitet for GDPR, men heller som et sted å begynne (IT Governance Privacy Team, 2017).

Ved å vedta GDPR skapte EU et behov om å skaffe informasjon for bedrifter som behandler persondata. Bedriftene trengte nå informasjon om lover, regelverk og hjelp til innføring av

GDPR. IT-bedrifter som jobber med lover og regelverk, begynte å tilby tjenester i form av kurs og rådgiving. Det finnes også mye gratis informasjon på nettet, og enkelte bedrifter vurderer at de kan innføre GPDR selv, slik at de på denne måten kutte ned på kostandene. Som nevnt tidligere i kapittelet finnes det ikke et klart rammeverk som passer til alle bedrifter, ettersom guidene ikke dekker enhver bedriftssituasjon. Guidene foreslår for eksempel å få rådgiving fra advokatbyråer når det gjelder kontrakter og juridiske uttalelser, og at GDPR må bli en del av «grunnmuren» i organisasjonen, slik helse og sikkerhet er (IT Governance Privacy Team, 2017). Det kan altså virke som om man må betale for informasjon, som igjen forteller at man må skaffe seg mer informasjon et annet sted, noe som forsterker inntrykket av at GDPR er svært komplekst. Bedrifter må belage seg på å bruke ressurser for å skaffe nødvendig informasjon om GDPR. Man må dessuten være trygg på at informasjonen kommer fra kredible kilder for å sikre at bedriften etterlever GDPRs regelverk i alle ledd.

3.3 Psykologisk aspekt ved endring i en bedrift

Endringer i en bedrift påvirker flere ledd og avdelinger, og medfører en rekke konsekvenser for de ansatte. Scott og Jaffe (1988) mener at de ansatte gjennomgår en reaksjonsprosess i fire faser: fornektelse, motstand, gradvis utforskning og til slutt forpliktelse. Til sammenligning undersøkte Bovey og Hede (2001) i sin studie «Resistance to organisational change» ni virksomheter som var i en endringsprosess. De fant ut at de ansatte ubevisst bruker velutviklede og innebygde forsvarsmekanismer for å motvirke den angsten forandring forårsaker. Disse forsvarsmekanismene hindrer ofte en person i å tilpasse seg endringer. Motstand mot endring dukker opp fordi man går fra det kjente til det ukjente (forandring), noen er imidlertid mer tilbøyelige til å godta og tilpasse seg endringer enn andre (Coghlan, 1993).

Bovey og Hede (2001) beskriver videre at folk som brukte humor for å håndtere angstfølelsene som gjerne kommer i forbindelse med endring, hadde mindre sannsynlighet for å motarbeide endringsprosessen. Ifølge Bond (1995) er humor sterkt knyttet til positiv håndtering av stressende situasjoner, og hjelper individer med å akseptere splid på en forstandig måte. Når man kan le av et problem, blir problemet ufarliggjort, samtidig som det gir en følelse av kontroll (Wade og Tavris, 1996). På den andre siden har man det Bovey og Hede (2001) mener er den mest skadelige forsvarsmekanismen ovenfor endring, nemlig projeksjon. Projeksjon kan beskrives som at man ubevisst og feilaktig tillegger en annen person sine egne negative

følelser, impulser og tanker (Wade og Tavris, 1996). De personene som rapporterte over medianen i kategorien projeksjon, var de som oftest motsatte seg endringer i en virksomhet. En projiserende person har en tendens til å legge skyld og ansvar over på andre istedenfor å akseptere sine egne mangler og impulser (Bond, 1995). Det vil si at hjernen på en måte lurer seg selv til å tro at årsaken til angsten ligger hos noen andre enn en selv (de Board, 1983).

Det er naturlig å trekke den konklusjon at ansatte i virksomheter som innrullerer GDPR, vil gå igjennom disse fasene og følelsene. Det vil derfor være fordelaktig for ledelsen i bedrifter som skal implementere GDPR, å gjøre overgangene og endringene så sømløse som mulig og vise forståelse for hvordan de påvirker arbeidstakerne. Bovey og Hede (2001) identifiserer to strategier ledelsen kan bruke for å motvirke forsvarsmekanismene mot endring i virksomheten, nemlig rådgivning og -informasjonsbasert intervensjon. Informasjonsbasert intervensjon gjør den ansatte oppmerksom på ubevisste tankeprosesser og på hvordan de påvirker motivasjon og atferd i en organisatorisk endringsprosess. Rådgivning fokuserer på aktiviteter som hjelper den ansatte med å forstå hvordan indre forsvarsmekanismer påvirker valg og oppfatninger i forbindelse med endring (Bovey og Hede, 2001). Det er med andre ord viktig å ikke bare konsentrere seg om det tekniske virksomheten gjennomfører i en endringsprosess, men også legge vekt på de menneskelige faktorene. Ledelsen må sørge for at endringene forankres blant de ansatte, slik at man sikrer kontinuerlig oppfølging av arbeidet. En slik forankring vil føre til at flere i bedriften forstår endringen, og at de tidligere går over til utforskning- og forpliktelsesfasen.

3.4 Personvern og ny teknologi

Datalagring har blitt markant effektivisert med tiden (Rajakumari og Nalini, 2014), samtidig som nyutviklinger preger teknologilandskapet. Såkalte «wearables» som smartklokker, smartbriller og smartsko, måler livsaktiviteter – også kalt «lifelogging» - i håp om at man bedre vil forstå menneskelig oppførsel (Gurrin, Smeaton og Doherty, 2014). Lifelogging er 'et fenomen der man digitalt tar opp/sporer livet sitt i varierende detalj. I en forstand en «svart boks» (ferdskriver på fly), som gir et unikt innblikk i hvordan man lever livet sitt (for eksempel hvor lenge man sover om natten eller hvor mange skritt man går per dag)' (Gurrin, Smeaton og Doherty, 2014). Fremgangen i ny teknologi resulterer i avanserte sensorer som sporer selve personen, i tillegg til å registrere miljøet rundt. Sensorene lages billig og er robuste og diskré. Også biler, veier, gater, fly og tog blir digitalisert. Det finnes «smartgater» og «smarthus», teknologi som har blitt inkorporert i allerede eksisterende infrastruktur (Moore, 2018).

Bilde 1 (Interactive tiles, 2017). Interaktivt fotgjengerfelt som konverterer steg/gåing til energi, i London.

Digitaliseringsrevolusjonen i dagens samfunn åpner for en rekke muligheter for bedrifter til å samle brukerinformasjon, som de igjen kan anvende videre. Lifelogging foregår ofte passivt, uten at personen trenger å initiere den eller trykke på noe. Ofte starter også lifeloggingen automatisk uten at man i noen tilfeller er klar over det (Gurrin, Smeaton og Doherty, 2014). I andre tilfeller er loggføringen bevisst, for eksempel når man tar bilder i en sosial situasjon.

Mye av den nye teknologien vil kunne samle personlig informasjon om enkeltmennesker, informasjon som kan brukes til å lage markedsstrategier eller selges videre, og derfor er hyperaktuell for markedsførings- og dataminingsbedrifter. I den forbindelse er det viktig å

tenke på hvem som eier dataene. Er det personen selv eller er det selskapet som leverer produktet eller tjenesten? Hvem skal ha autorisasjon til å slette, redigere og legge til informasjon? GDPRs inntog gjør forhåpentligvis bildet klarere for mange bedrifter og forbrukere i EU. Med en standardisert tilnærming til personvern vil det bli tydeligere hvem som eier dataen, og hva de blir brukt til, og hvert individ avgjør forhåpentligvis hvem som skal ha tilgang. Som nevnt i 3.1 mener noen at det fortsatt vil finnes gråsoner og uklare regler for forskjellige scenarier knytte til personvern (spesielt persondata som krysser grenser), og at det ikke vil finnes noen opplagt dom om slike saker kommer opp i retten. Man har i tillegg tilfeller der bedrifter lekker/selger informasjon uten forbrukerens samtykke, slik som Facebook i Cambridge Analytica-skandalen. Her samlet en quizapp på Facebook informasjon fra mer enn 85 millioner mennesker (305 000 lastet ned appen, men appen samlet også informasjon om vennene av de som installerte appen), der noen av dataene ble solgt til Cambridge Analytica (CA), som brukte informasjonen til å påvirke amerikansk politikk. CA hevder på sin side at de ikke brøt noen lover. Facebook har siden bedt sine brukere om unnskyldning, og medga at hendelsen førte til et tillitsbrudd mellom selskapet og brukerne (BBC NEWS, 2019).

3.5 Big data og digital sikkerhet

Behandling av *big data* og ivaretakelse av digital sikkerhet er omdiskuterte temaer i dagens forskningsmiljøer. Big data kan beskrives som *«maximizing computation power and algorithmic accuracy to gather, analyze, link and compare large data sets, and to draw on these sets to identify patterns in order to make economic, social, technical, and legal claims»* (Boyd og Crawford, 2012). Analyser av *big data* muliggjør funn av mønstre og trender som kan bli brukt til alt fra forskning til markedsføring (McAfee og Brynjolfsson, 2012). Den hurtige utviklingen og utbredte bruken av internett gjør at enorme mengder med spor legges igjen der hver dag. Dette åpner for at personer med uærlige hensikter kan samle inn informasjonen til ondsinnet bruk. Hvis *big data* ikke er godt nok sikret for brukerdata i bruksprosessen, vil personvernet og datasikkerheten trues (Zhang, 2018). Den infame Cambridge Analytica-skandalen er et godt eksempel på *big data* og hva de kan bli brukt til, samt på hvor enkelt personlig informasjon kan komme på avveie.

Ettersom informasjon er «den nye valutaen» (Shan, 2017) og mye av informasjonen lagres digitalt, er det enormt fokus på digital sikkerhet. Ny teknologi utvikles hyppig, og det skaper kontinuerlig nye trusler. Når hus, klær, biler og infrastruktur i større grad digitaliseres, vil det

lagres informasjon om individer overalt. I teknologisk skiftende samfunn kreves det derfor at bedrifter og enkeltmennesker hele tiden er skjerpet og oppdatert på digital sikkerhet og personvern. Ifølge Nasjonal sikkerhetsmyndighets årlige sikkerhetsrapport (2018) står Norge overfor økende risiko når det kommer til digital sikkerhet. Rapporten sier at dette skyldes *«vedvarende, nye og raskt økende antall sårbarheter»* (NSM, 2018). Rapporten forklarer at fremmede stater retter nettverksoperasjoner mot norske virksomheter som ikke forvalter skjermingsverdig informasjon, og som tidligere har vært mindre aktuelle mål. Dette krever at norske myndigheter og virksomheter fostrer et godt sikkerhetsarbeid, og viser samtidig at skillet mellom stats- og samfunnssikkerhet viskes ut (NSM, 2018).

Trusselbildet mot digital sikkerhet består av forskjellige typer trusler, for eksempel informasjonstyveri, vanvare, løsepengevirus, direktørsvindel, industrispionasje, sabotasje, identitetstyveri, datingsvindel, personutpressing og krenkelser. Den mest utbredte trusselen er vanvare, som betyr at man utsetter seg selv eller bedriften for risiko, ofte ved uaktsomhet som følge av for lav bevissthet eller manglende kunnskap (NorSIS, 2017). Det kan for eksempel være lett å forsnakke seg når man snakker om jobbrelaterte temaer med personer utenfor bedriften. Videre er løsepengevirus en økende trend. Det vil ofte si at filer krypteres og det kreves penger for å låse dem opp igjen. Metoden som brukes er spredning av skadevare, ofte via falske e-poster eller pop-ups på nettsider. Det blir også utnyttet sikkerhetshull i programvare til å spre viruset (NorSIS, 2017). Nasjonal sikkerhetsmyndighet forklarer at den *«totale digitale angrepsflaten øker. Elementer som i utgangspunktet er godt sikret, eksponeres av sårbarheter hos svakt sikrede elementer i den samme verdikjeden»* (NSM, 2018). Det er altså et større digitalt spekter som kan angripes, og det skapes hele tiden mer komplekse digitale verdikjeder, noe som gjør det utfordrende å sikre seg hundre prosent i alle ledd. For at personlige data ikke skal komme på avveie, vil det være essensielt at bedrifter følger med på utviklingen, og at det skapes gode rutiner for digital sikkerhet i bedriften.

4.0 Metode

I denne studien ble det brukt en kvalitativ tilnærming. Bryman og Bell (2011) beskriver kvalitativ metode som en *«research strategy that usually emphasizes words rather than quantification in the collection and analysis of data and that: predominantly emphasizes an inductive approach to the relationship between theory and research, in which the emphasis is placed on the generation of theories; has rejected the practices and norms of the natural scientific model and of positivism in particular in preference for an emphasis on the ways in which individuals interpret their social world; and embodies a view of social reality as a constantly shifting emergent property of individuals' creation.»* Kvalitativ metode fokuserer altså mer på ord enn på tall (som er kvantifiserbare), og ser på hvordan mennesket oppfatter den sosiale verdenen rundt seg.

Metoden ble valgt grunnet et ønske om å bedre forstå bedrifters holdning og handlinger i møte med GDPR. Kvalitativ metode gjør det mulig for bedriften å fortelle hvordan den oppfatter prosessen med innføring og etterlevelse av GDPR, og gir en bredere forståelse enn kvantitativ metode av hvorfor og hvordan, noe som ipso facto gir svar på problemstilling og forskningsspørsmål. Metoden er utmerket for å finne sammenhengen mellom teori og forskning. Det ble også vurdert å bruke kvantitativ metode, men det ble konkludert med at antall respondenter ikke ville samsvare med kravene som stilles for å trekke riktige generelle konklusjoner, og at kvantitativ metode dessuten var mindre egnet til å finne ut av problemstilling og forskningsspørsmål.

Informanter ble valgt på grunnlag av kundelisten til Sticos, det vil si de som deltok på GDPR-kursene. Det ble ikke valgt ut en spesiell bransje, da GDPR er aktuell for alle bransjer, selv om det kunne vært interessant å se på om svarene fra studien peker på trender i bestemte bransjer. I denne studien var det mulig å undersøke hvordan GDPR håndteres på tvers av ulike bransjer. Videre forskning kan avdekke trender innad i samme bransje. Alle bedriftene som deltok i undersøkelsen, er SMB-bedrifter (små og mellomstore bedrifter, se 3.1 for fullstendig definisjon). Dette er bedriftene:

Bedrift	Kjerneområde
Bedrift 1	Energiselskap
Bedrift 2	Regnskapsbyrå
Bedrift 3	Olje og energiselskap
Bedrift 4	Vann og avløp
Bedrift 5	Utdanningsinstitusjon
Bedrift 6	Inkassobyrå
Bedrift 7	Endringsbyrå

Figur 2: Bedriftstabell.

4.1 Innsamlingsmetode

Et spørreskjema ble grundig utarbeidet for å styre samtalene dit de var ønsket (se Vedlegg 1). Spørreskjemaet var et Word-dokument som respondentene fylte ut. De kvalitative dataene ble samlet inn ved hjelp av intervju på e-post og telefon (telefon brukt for å komme i kontakt med intervjuobjekter, ikke til selve intervjuene), da dette ble foretrukket som den beste metoden av respondentene. Fordelene med en slik innsamlingsmetode (e-post) er at respondentene får tid til å reflektere rundt spørsmålene og ikke må svare med én gang. Undersøkelsen inneholdt også noen tekniske kvaliteter, og respondenten måtte ha forkunnskaper om emnet for å kunne svare. Bruk av e-post ga respondentene tid til å innhente nødvendige kunnskaper, samt friske opp hukommelsen, ettersom alle kursene (Serious Game) ble gjennomført i 2017 og 2018. Ulempene med innsamlingsmetoden er at den gir respondentene tid til å «bare» finne positive svar. Det kunne tenkes at respondenter som hadde jobbet godt med GDPR, var de eneste som ville svare, eller at de som ikke hadde jobbet så godt, fikk tid til å pynte på sannheten. Metoden gir heller ikke mulighet til å lese kroppsspråk. Det var derfor viktig at tilnærmingen til innsamlingen, og utformingen av spørsmålene, var av en slik karakter at bedrifter som ikke hadde jobbet godt med GDPR, likevel ville delta i undersøkelsen.

Til å analysere svarene fra undersøkelsen ble det brukt koding. Koding i kvalitativ metode er å *«finne ord eller korte fraser som symbolsk tildeler en summativ, fremtredende eller stemningsfull egenskap til en del av språkbaserte- eller visuelle data»* (Saldana, 2009). Det ble

brukt tre typer koding for analyse av intervjuene: Åpen koding – å lete etter og sette navn på foreløpige kategorier; aksial koding – å analysere og modifisere disse kategoriene; selektiv koding – å identifisere noen kjernekategorier eller begreper (Bryman og Bell, 2011). Koding brukes i kvalitativ analyse også som en metode for å organisere transkribert tekst, samt oppdage mønstre (Auerbach og Silverstein, 2003).

5.0 Resultat

Resultatene fra de kvalitative undersøkelsene peker mot interessante funn. GDPR-arbeidet for bedrifter vil prege industrien i årene som kommer, og det er medrivende å se på hvilke virkninger personvernsforordning har. Et av nøkkelfunnen er et bedrifter prioriterer noen kategorier fremfor andre. Resultatene viser også at GDPR er oppfattet som omfattende.

5.1 Prioriteringer

Resultatene fra spørreundersøkelsen viser en tendens til at bedrifter velger å prioritere bare enkelte av kategoriene de gjennomgikk på kurset. Noen av bedriftene beskriver nettopp dette: at spesifikke kategorier blir sett på som viktigere enn andre, og at det er disse som ble fokusert på etter endt kurs. En av kategoriene som ofte ble prioritert, var kategori 2, *databehandleravtaler*. Bedrift 1 svarer for eksempel dette på spørsmål om hvordan de ligger an med databehandleravtaler: *«Dette er nok det som har vært prioritert mest i etterkant av gjennomgangen».* Det kommer også fram av studien at dette er en av kategoriene flest bedrifter har fått på plass etter gjennomført kurs, og det nevnes at *«det ble overraskende mange (databehandleravtaler)*» (Bedrift 4). Denne kommentaren illustrerer at bedriftene ofte ikke er klar over hvor mange andre bedrifter/personer som behandler deres data. Som nevnt i 3.5 er bekymringen for datalekkasje større enn tidligere på grunn av at den digitale angrepsflaten er større og verdikjedene stadig blir mer komplekse. Databehandleravtalene er med på å gjøre disse verdikjedene sikrere, noe som kan være en av årsakene til at avtalene står høyt på prioriteringslisten.

I tillegg viser studien at bedriftene ikke har helt kontroll på behandlingsgrunnlaget (se 2.0 for definisjon). Bare to av bedriftene svarte at de hadde alt på plass. De resterende fem mangler fortsatt en del for å få alt under kontroll (oppdatert på vilkår og krav). Alle bedrifter utenom én sier de har nok ting på plass til å kunne behandle personopplysninger, men at de mangler en del etterarbeid. Resultatene viser at bedriftene ikke alltid er klar over hvilke vilkår og krav som ligger til grunn for å kunne behandle personopplysninger, og at videre arbeid med dette ikke er prioritert. Resultatene kan tolkes i den retning at bedriftene har planlagt å få alt på plass, men ikke har tid/ressurser/lyst til å gjøre noe med det. Bedrift 7 sier blant annet: *«Vi har jobbet målrettet til å begynne med, men etter å ha fått på plass det mest kritiske, så har vi dabbet av litt.»* De to bedriftene som har alt på plass (for behandlingsgrunnlag), gir en mer detaljert beskrivelse på hva de har på plass, og hvordan de jobber med oppfølging. Som for

eksempel Bedrift 5: «*Det er i tillegg laget rutiner for oppbevaring av personopplysninger, samt rutiner for gjennomgang av kartleggingsskjema jevnlig. Vi er ferdig med vår gjennomgang av virksomhetens oppbevaring av personopplysninger.»*

Ettersom arbeidet med GDPR er dynamisk, vil bedriftene til enhver tid måtte holde seg oppdatert på lover og regelverk, og det vil derfor være fordelaktig å ha gode rutiner for behandlingsgrunnlag. Resultatene viser at setningen *«etter å ha fått på plass det mest kritiske, så har vi dabbet av litt»*, er beskrivende for de fem bedriftene som ikke har kommet i mål med databehandlingsgrunnlaget.

Videre fremkommer det at *roller* er høyt prioritert blant bedriftene. Seks av sju har tildelt roller og ansvar i etterkant av kurset. Bare én bedrift har ikke gjennomført dette i særlig stor grad. Det er viktig for bedriftene at ansvaret blir fordelt slik at GDPR-arbeidet blir kontrollert og gjennomført. Det er dog forskjell på hvordan og hvor ansvaret blir tildelt. To av bedriftene har opprettet team som jobber med GDPR, mens to andre bare har én eller to personer som har ansvar for dette området. Størrelsen på bedriften kan ha innvirkning på antall personer som jobber med GDPR. I tillegg sier bare én av bedriftene at personvernombud er på plass, og at dette er meldt inn til Datatilsynet.

Når det gjelder kategorien *informasjonssikkerhet* svarer Bedrift 1 at «*enkelte områder er gått igjennom»,* og at de valgte å bare prioriterte to områder: adgangskontroll og sletterutiner. I tillegg viste studien at seks av bedriftene fant røde flagg, hvor fire av bedriftene har tettet disse hullene (røde flaggene). Det vil si at to av bedriftene som oppdaget røde flagg ved hjelp av Serious Game, ikke har gjort nok for å tette dem i ettertid. Dette er en indikasjon på at bedriftene som nevnt ser på enkelte kategorier som viktigere enn andre, og at de to aktuelle bedriftene ikke så på de røde flaggene som så viktige å ta hensyn til. To av bedriftene svarte at de har skjerpet rutinene etter at de ble bevisstgjort på GDPR-situasjonen når det gjaldt informasjonssikkerhet. Det har altså vært fokus på sikkerhetsrutiner og viktigheten av at disse er gode. Seks av sju bedrifter er klar over konsekvensene av ikke å følge opp GDPRs regelverk. Det fremkommer av studien at hver enkelt bedrift prioriterer ulikt, selv om noen prioriteringstrender kom til syne (prioritering av databehandleravtaler og å tildele roller). Det virker imidlertid som om prioriteringene skjer i henhold til hva som passer den enkelte bedrift best, og etter hva bedriften legger vekt på.

Studien viser at fullføring av en handlingsplan og jobbing med denne er en av de kategoriene som er lavest prioritert blant bedriftene. Over halvparten av bedriftene (fire av sju) sier de ikke er ferdig med handlingsplanen, og to av de som er ferdige med den, mangler rutiner på oppfølging av GDPR-arbeidet. Dette viser at nedskrevne dokumenter og rutiner har blitt nedprioritert til fordel for databehandleravtaler og tildeling av roller. Handlingsplanen beskriver tiltak, internkontroll, rutiner og hvordan oppfølgingen av dette skal foregå. Det kan virke som om roller har blitt tildelt og rutiner er laget, men så har det har stoppet opp. Bare to av bedriftene svarer at de har god kontroll på handlingsplan og oppfølging. Det mangler på oppfølging og kontroll av rutinene blant de resterende bedriftene. Bedrift 7 sier blant annet at «*vi har ikke laget prosedyre for gjennomgang og etterlevelse av rutiner. Vi har de fleste rutinene på plass, og alt er ført på i en handlingsplan».* Noe som bekrefter at rutinene er laget, men at oppfølging og gjennomgang mangler. Igjen ser man at det mest kritiske er på plass, men at det har «dabbet av» etter dette. Studien viser at bedriftene ikke ser på oppfølging og internkontroll som noe det er et poeng å allokere ressurser til. Det kan ha sammenheng med at bedriftene ikke ser konsekvensene av mangelfull oppfølging av rutiner, så lenge rutinene faktisk er laget.

5.2 Mye å sette seg inn i

Konsensus for bedriftene er at det er mye å sette seg inn i, og det oppleves som et styr å begynne på GDPR-arbeidet. Seks av syv erkjente at det var strevsomt med GDPR. Bedrift 2 forteller at *«det er mye styr og veldig mye å sette seg inn i. Jobber i en relativ stor bedrift hvor vi har satt av masse ressurser for å få dette på plass».* Andre skildringer beskriver *«klart at man tenker om dette skulle kunne gjøres enklere»* (Bedrift 3), og *«I vårt GDPR-prosjekt ble det brukt mange arbeidstimer. Så ja, det var mye styr»* (Bedrift 4). Videre fremkommer det at bedriftene synes det var mye arbeid i starten, men etter at arbeidet var i gang, så hvor viktig det var med arbeidet. Bedrift 7 sier at *«etter hvert så ser man jo hvor viktig dette er, og jobben (med GDPR) er blitt en naturlig del av vår hverdag.»* Når GDPR ble inkorporert i bedriften ble arbeidet sett på som lettere, og det ble ikke betegnet som «et styr» lenger. Bedrift 5 støtter oppom dette: *«Det var svært stort arbeid i starten, men når vi fikk utarbeidet alle dokumentene er det en grei jobb å følge opp og etterleve disse.*»

Videre forklarte noen av bedriftene at de syntes mye av reglementet for GDPR var uklart, og at det var vanskelig å vite hva man skulle gjøre i gitte situasjoner. Bedrift 5 sier *«noen*

momenter har vært svært krevende å forstå, da det er noen dilemmaer som har vist seg å være uklare i hvordan man skal håndtere.» Denne problematikken trekkes også frem i 3.1, der Hyland (2017) snakker om hvordan reglene for GDPR ikke er helt svart hvitt med persondata som forlater EU. Bedrift 4 never også forvirring angående GDPR-reglene: *«Det som gjenstår hos oss er noe sletting av personopplysninger. Rutinen er laget, men det gjenstår noe arbeid knyttet til dette. Årsaken er usikkerheten rundt konsekvensen av å slette opplysninger om f.eks. tidligere ansatte.»* Dette tyder på at GDPR kan tolkes på ulike måter, og at forskjellige tolkninger skaper dilemmaer som bedrifter har vansker med å håndtere, selv etter endt kurs.

I tillegg tilsier resultatene at bedriftene var fornøyde med kurset til Sticos, og at de så på det som nødvendig for å vite hvor man skal begynne. De beskriver at prosessen var lærerik og at det ga bedre bevissthet på hvordan man behandler personopplysninger. Bedrift 6 forteller for eksempel at *«innledningsvis fikk vi god drahjelp med gjennomføringen av Serious Game. Her ble mye avdekt og avklart. Hva gjelder og hva gjelder ikke for vår virksomhet.»* Her kan det trekkes paralleller til 3.2 som sier at det ikke finnes et felles rammeverk for GDPR som passer til alle bedrifter. Derfor er det greit å vite hva som gjelder for ens bedrift. Bedrift 4 snakker også om at *«arbeidet (med personvern) har vært nødvendig og ikke minst lærerikt for oss»* og bedrift 7 sier *«man blir jo mer og mer opptatt av eget personvern, og dermed også hvordan man behandler opplysninger i forhold til kunder, kollegaer og samarbeidspartnere.»* Kurset til Sticos har ifølge empiriske funn i denne studien, skapt en økt bevissthet rundt behandlingen av personopplysninger og hvilken rolle GDPR spiller her. Dog virker det som den økte bevisstheten bare varer i en kort periode etter endt kurs for de fleste bedriftene.

Seks av syv bedrifter hevder at de synes personvern er viktig. Bedriftene har vist dette i praksis ved å ta initiativ til å få hjelp av Sticos. Bedrift 2 skriver blant annet at *«personvern er meget viktig i den verden vi lever i, i dag. Personlig applauderer jeg derfor denne loven».* Ettersom bedriftene virker enige om at personvern er viktig, kan det settes spørsmålstegn ved hvorfor innføringen av GDPR ikke er – som det kommer frem i studien – like viktig. De fleste av bedriftene har flere mangler i mange av kategoriene som ble gjennomgått på kurset, og det kommer ikke frem at alle bedriftene har konkrete planer om oppfølging for å fullføre implementeringen av GDPR. Resultatene viser at bare to av bedriftene har det meste på stell. Det er derfor rimelig å konkludere med at bedriftene snakker om hvor viktig GDPR er, men

ikke evner å gjennomføre arbeidet som skal til for å få alle deler av personvernforordningen på plass. Neste kapittel vil ta for seg mulige årsaker til dette.

6.0 Diskusjon

Denne diskusjonsdelen tar for seg hvilke årsaker som kan ligge til grunn for hvorfor bedriftene prioriterer som de gjør. Videre spekuleres det i om motstand mot endring har en betydning på hvorfor GDPR-arbeidet stagnerer. Det blir også undersøkt muligheter for satsing på oppfølgings- og GDPR-kurs for bedrifter.

6.1 Prioriteringer og stagnasjon

I 5.1 ble det presentert funn som tilsa at bedriftene prioriterer etter hva de mener er viktigst. Databehandleravtaler viste seg å være høyt oppe på prioriteringslisten. Det kan komme av at en slik avtale er et håndfast dokument som bedriften har kjennskap til fra før. Bedriftene forstår også hvorfor man trenger databehandleravtaler. De påvirker dessuten eksterne samarbeidspartnere direkte, og er enkle for kontrollorganer å «ta» bedrifter på. Dette kan være grunnen til at det blir prioritert over andre områder (som handlingsplan). Det ses på som kritisk å ikke ha disse avtalene på plass.

Roller er også noe bedriftene har lagt vekt på å delegere. Å gi ansvar til team eller enkeltpersoner betyr at noen alltid jobber eller har ansvar for GDPR, og som nevnt i 3.1 vil det være lurt for bedriftene å opprette personvernombud. Imidlertid viser studien at tildeling av roller ikke er en garanti for at for eksempel rutiner følges opp. Som nevnt i 5.1 har det hos noen «dabbet av litt» med arbeidet etter startfasen. Det kan virke som at bedriftene nedprioriterer GDPR så lenge de har delegert ansvaret og tatt hånd om det de ser på som kritisk - og kanskje også så lenge de har lagt ned det de anser som minimal innsats for ikke å få bøter. Så lenge rutinen er laget, har de noe å vise til hvis de blir kontrollert. Dette kommer også frem i studien, da to bedrifter ikke håndterte røde flagg som ble funnet. Varslene ble ikke ansett som alvorlige nok til at bedriftene satte av ressurser til å ta hånd om flaggene. Det er vanskeligere for en bedriftsledelse eller et kontrollorgan å kontrollere oppfølging av GDPR-rutiner, så lenge det kan vises til dokumenter for rutinene. Det er også en mulighet for at bøtene er lavere enn det ressursene som kreves for å komme i mål med GDPR, koster. Dermed blir bare det mest kritiske prioritert. Et annet funn i studien at kunnskap om konsekvens ikke

nødvendigvis fører til handling. Seks av syv bedrifter sier at de er klar over konsekvensene av brudd på GDPR-reglene, likevel ligger noen av bedriftene etter med GDPR-arbeidet.

På den andre siden er GDPR veldig omfattende, slik at bedrifter kan tro de er kompatible, eller de har slått seg til ro med at de aldri kommer til å bli det. Bedrift 6 sier for eksempel: *«GDPR er nå en integrert del av vår produksjon og vi har fokus på dette i alle ledd. Vi greier nok ikke tette alle skott, men vi føler at vi har kommet langt på vei.»* Det er vanskelig for bedriftene å være 100 % kompatible i alle ledd, og det kan derfor være greit å slå seg til ro med dette, så lenge man innlemmer GDPR i sin produksjonsprosess. Fokus på GDPR i alle ledd er også en kritisk suksessfaktor for kompatibilitet. Har man GDPR som grunnstein i bedriften, blir arbeidet med forordningen mye lettere. Hvis man har fokus på å få GDPR inn i grunnmuren til bedriftsoperasjoner og -kultur, i stedet for bare på enkeltområder, vil arbeidet med GDPR kanskje virke mindre som «styr» og mer som en integrert del av arbeidshverdagen.

Som nevnt i 3.5 blir det stadig flere digitale ledd som må sikres i en bedrift. Dette krever kontinuerlig arbeid i bedriften, slik at man er oppdatert og klar for eventuelle sikkerhetsbrudd. Samme kapittel nevner videre hvordan stadig flere bedrifter som ble sett på som «uviktige», blir angrepet, og digital sikkerhet burde stå høyt på agendaen slik at personvernet blir ivaretatt. Denne studien peker mot funn som tilsier at dette ikke er virkeligheten, ettersom seks av syv bedrifter fant røde flagg, hvor bare fire av dem tok hånd om disse. Det ble videre beskrevet at det ikke ble jobbet tilstrekkelig med rutiner og interkontroll, og at det på mange andre områder «dabbet av» etter endt kurs. Mangelen på oppfølging kan by på problemer i fremtiden, enten i form av bøter eller datalekkasjer. Spesielt i dagens hurtig voksende digitalsamfunn vil det være essensielt å være føre var. Det er naturlig å trekke den konklusjonen at bedriftene vil skjerpe seg først når de blir utsatt for et angrep, eller det skjer en datalekkasje. Brent barn skyr jo ilden.

6.2 Endring i bedriften – ledelsens ansvar

Endring i bedrifter skjer stadig vekk. GDPR er intet unntak. Når slike endringer skjer, er det viktig at ledelsen tar ansvar og sørger for at alle parter er involvert og forstår hvorfor endringen gjøres. I kapittel 3.3 beskriver Scott og Jaffe (1988) hvordan personer går igjennom en reaksjonsprosess når de står overfor en endring. I etterkant av Sticos' GDPR-kurs gikk antakelig mange av de ansatte i bedriftene som skulle innføre GDPR, gjennom denne prosessen. Resultatene fra 5.0 kan peke svakt mot at det kan ha oppstått motstand mot endring i noen av bedriftene, noe som også kan være en forklaring på at de ikke har kommet lenger enn de har gjort med innføringen av GDPR. Kanskje er mange fortsatt i fornektelses- eller motstandsfasen, og derfor skjer endringene sakte. I kapittel 3.3 beskriver Bovey og Hede (2001) at humor er et godt redskap for å få alle med på endringen. Sticos' Serious Game kan være et steg i riktig retning for å avvæpne motstand mot endringsprosessen, både med tanke på at det er et brettspill, og at det heter Serious Game (spiller på humor).

I 3.3 blir det foreslått virkemidler ledelsen kan bruke for at endringen skal gå så glatt som mulig. Det viktigste er at ledelsen involverer seg i og følger opp prosessen. Som nevnt tidligere vil GDPR-fokus i grunnmuren til en bedrift føre til en enklere prosess for alle ansatte. Som bedrift 4 beskriver: *«Prosjektets arbeid, personvernerklæringen og de tilhørende rutiner er gjennomgått i et allmøte, samt i avdelingsmøter.»* Dette er et godt eksempel på hvordan GDPR har blitt satt på agendaen og hele bedriften involvert. Oppfølging fra ledelsen må kunne sies å være essensielt for innføringen av GDPR. Humor kan være et godt virkemiddel, ettersom det er sterkt knyttet til positiv håndtering av stressende situasjoner (Bovey og Hede, 2001). Ledelsen har også andre verktøy den kan bruke (som intervensjon og rådgiving, 3.3), men det viktigste er at den er involvert og står frem som eksempel på hvordan endringen vil påvirke bedriften positivt. Det kan lønne seg for bedrifter som tar Serious Game, at personer fra forskjellige avdelinger i bedriften deltar på kurset slik at alle er med i den samme prosessen og befinner seg på samme plan når endringen skal gjennomføres.

6.3 Markedsmuligheter

Ettersom GDPR er noe bedrifter er pålagt å innføre og etterleve, samtidig som det er så stort og komplisert, er det skapt et marked for salg av tjenester for å bistå bedriftene. Som denne studien viser, sliter mange bedrifter med å forstå hvor de skal starte, og de synes det er vanskelig å gjennomføre implementeringen. Dette åpner muligheter for bedrifter som Sticos til å selge kurs og rådgivning og skape en sikrere digitalhverdag for bedriftene de bistår (samt bedriftene disse er i kontakt med). Mange startet med innføringen av forordningen etter at bestemmelsen trådte i kraft i 2018. På nyåret i 2019 begynte bøtene for brudd på GDPR-reglene for alvor å komme. 21. januar 2019, fikk Google LLC en bot på 50 millioner euro av National Commission on Informatics and Liberty (CNIL, Commission Nationale de l'informatique et des Libertés) for brudd på GDPR (CNIL, 2019). Hill (2019) skriver i sin at bedrifter er bøtelagt for 56 millioner euro i Europa etter brudd på GDPR-reglene. Dette betyr at Google hittil står for 89 % av utbetalingene. Hill (2019) skriver videre at det ble rapportert inn litt over 200 000 GDPR-saker de første ni månedene etter innføringen av forordningen. Det betyr at det var mange småsaker utenom Googles brudd på reglene, og at mange bedrifter betalte mindre summer i bøter.

Nå som konsekvensene av GDPR begynner å bli synlige, er det en mulighet for at markedet for GDPR-kurs vil eksplodere. Bedrifter som har sett denne ekspansjonen komme (bedrifter som selger GDPR-rådgivning), vil ha gode forretningsmuligheter. Før GDPR trådte i kraft, var det vanskelig for bedrifter som Sticos å selge inn GDPR-kurs, ettersom GDPR ikke er noe man «tjener penger på». Nå som bøtene begynner å komme, er GDPR fortsatt noe man ikke tjener penger på, men man ønsker ikke å *tape* penger på det. Slik situasjonen ifølge studien ser ut nå, bryr ikke bedriftene seg så mye om konsekvensene av å bryte GDPR-regelverket (se 5.1). Men det kan snu den dagen de kanskje selv blir bøtelagt. Da kan motivasjonen til å jobbe godt med GDPR ligge i å slippe å betale bøter.

En mulig salgsvinkling for bedrifter som Sticos kan være at bedrifter som er kompatible med GDPR, blir GDPR-sertifisert. GDPR-sertifiseringen burde oppdateres hvert år, ettersom det digitale landskapet endrer seg stadig. Dette gjør at en bedrift virker troverdig og sikker, noe som vil appellere til kundene. Studien viser at det ligger salgsmuligheter i oppfølgingen av GDPR, ettersom mange av bedriftene snakker om å gjøre mye, men gjennomføringen ikke stemmer helt overens med hva de sier. Det «dabbet av litt» med jobbingen etter kurset,

samtidig som de ser på personvern som viktig. Ut fra denne studien vil salg av oppfølgingspakker som inneholder kurs og møter kunne være et område å satse på for bedrifter som tilbyr tjenester knyttet til innføringen av GDPR. Dette kan utføres ved å tilby en type abonnementstjeneste (man betaler en månedlig sum for at Sticos skal stå til disposisjon med oppfølging og veiledning), eller man betaler en gitt sum for hver gang man bruker Sticos, for eksempel én sum for introduksjonskurs og én sum for oppfølgingskurs.

6.4 Videre forskning

GDPRs effekt på bedrifter, og arbeidet med dette, trengs å utforskes mer. Tett oppfølging av utviklingen til GDPR ses på som fordelaktig for bedrifter. Det vil uten tvil åpenbare seg trender og nye problemstillinger etter hvert som GDPR har vært i bruk og blitt håndhevet noen år. Det kreves derfor mer forskning på et større utvalg virksomheter. Det vil også være en fordel med forskning innad i ulike bransjer, for at man skal få en bredere forståelse av hvordan personvernarbeid påvirker bedrifter, individer og organisasjoner. Ny teknologi vil som nevnt tidligere (3.4), påvirke hvordan ansatte og bedrifter jobber med personvern. GDPR som grunnstein i implementering og ibruktakelse av dette, ses på som essensielt for en god og sikker personvernfremtid.

7.0 Konklusjon

Det viktigste funnet i denne studien er at bedrifter jobber godt med GDPR i en kort periode etter bevisstgjøring av sin nåsituasjon. Etter denne perioden, dabber det litt av. Det kan skje av flere årsaker, både mangel på oppfølging og motstand mot endring hos ansatte og ledelse. Fokus på noen utvalgte kategorier innenfor GDPR ses ikke på som fordelaktig. Det anbefales å inkorporere GDPR som grunnpilar i alle bedriftens ledd, slik at personvernet er sikret. Videre avdekker studien at bedriftene i hovedsak prioriterer å gjennomføre databehandleravtaler og tildeling av roller etter endt kurs. Opprettelse av personvernombud blir ikke prioritert.

Studien viser at det hersker forvirring i bedriftene over deler av GDPR-reglene i gitte situasjoner. Selv etter gjennomført kurs. Dette tyder på at oppfølging fra kursholdere burde være et satsningsområde. Bedriftsledere burde samtidig sørge for at de implementerer GDPR som en grunnpilar i bedriften, og ikke venter til de har fått en bot før de handler.

Denne studien konkluderer med at bedrifter har forholdt seg til GDPR i så måte at de skjerpet GDPR-arbeidet i tiden etter bevisstgjøring av nåsituasjon. GDPR-arbeidet dabber av etter en periode, og det er lite fokus på oppfølging. Studien forteller også at etter bevisstgjøring av nåsituasjon fokuseres det på enkeltområder innfor GDPR, som resulterer i at andre områder bortprioriteres. Det forklares videre i studien at personvern er sett på som viktig, men at rutiner og internkontroll burde skjerpes ytterligere. Utviklingen til *big data* og den hyppige digitaliseringen av organisasjoner, bedrifter, infrastruktur og produkter, kreves det at bedrifter holder tungen rett i munnen.

Studiens resultater vil være nyttig å kjenne til for alle ledere og ansatte i bedrifter innenfor EU, og alle bedrifter som behandler data fra EU. I tillegg kan resultatene være av interesse for både regjeringer og myndigheter i EU, på den måten at internasjonale og innenlands avtaler kan inngås med et bredere kunnskapsgrunnlag når det gjelder hvordan bedrifter jobber med GDPR, og hva som kan kreves av oppfølging fra bedriftene. Personer som vurderer å starte egen bedrift, vil også dra nytte av studien ettersom studien gir et godt innblikk i hva man bør gjøre for å sikre en god implementeringsprosess, og hvilke fallgruver man bør unngå.

8.0 Litteraturliste

Albrecht, J.P. (2016). How the GDPR Will Change the World. *European data protection law review*. https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf

Auerbach, C., og Silverstein, B. (2003). *Qualitative Data: An Introduction to Coding and Analysis.* New York, United States of America: New York University press., New York.

BBC NEWS (2019). Facebook security app used to 'spy' on competitors. *BBC NEWS Technology*. https://www.bbc.com/news/technology-47281906?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-scandal&link_location=live-reporting-story

Bond, M. P. (1995). The development and properties of the defense style questionnaire, i Conte, H.R. og Plutchik, R. (Eds). *Ego Defenses: Theory and Measurement*. John Wiley & Sons, New York, NY.

Bovey, W., og Hede, A. (2001). Resistance to organisational change: The role of defence mechanisms. *Journal of Managerial Psychology*. 16(7):534-548. DOI: 10.1108/EUM0000000006166

Boyd, D. og Crawford, K. (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication, & Society.* 15:5, s. 662-679. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.441.9822&rep=rep1&type=pdf

Bryman, A., og Bell, E. (2011). *Business Research Methods.* (3. utg.). New York, United States of America: Oxford University Press Inc., New York.

CNIL (2019). The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. *CNIL.fr.* https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Coghlan, D. (1993). A Person-centered Approach to Dealing with Resistance to Change. *Leadership & Organization Development Journal*, Vol 14., utgave 4, s.10-14. https://doi.org/10.1108/01437739310039433

Datatilsynet (2019). Databehandleravtale. *Datatilsynet.no.* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/

Datatilsynet (2019). Samarbeid med Datatilsynet og funksjon som kontaktpunkt. *Datatilsynet.no*. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/personvernombudets-oppgaver/

de Board, R. (1983). Counselling Skills. Gower Publishing, Aldershot.

EU GDPR.ORG (2019). Right to be forgotten. *EU GDPR.ORG. https://eugdpr.org/the-regulation/*

European Commission (2019). What does the General Data Protection Regulation (GDPR) govern? *European Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

European Commission (2019). What is an SME? *Internal Market, Industry, Entrepreneurship and SMEs*, *European Commission*. https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

GDPR EU.ORG (2019). Fines and penalties. *GDPR EU.ORG, Web learning resources for the EU General Data Protection Regulation*. https://www.gdpreu.org/compliance/fines-and-penalties/

Gurrin, C., Smeation, A., og Doherty, A. (2014). LifeLogging: Personal Big Data. *Foundations and Trends in Information Retrieval*, Vol. 8, utgave 1. http://dx.doi.org/10.1561/1500000033

Hill, R. (2019). Year 1 of GDPR: Over 200,000 cases reported, firms fined 56 meeelli… Oh, that's mostly Google. *The Register: Business*. https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/

Hyland, J. (2017). Data Protection in EU businesses: an introduction to GDPR. *DBS Business Review.*

https://esource.dbs.ie/bitstream/handle/10788/3390/update_hyland_j_2017.pdf?sequence=1

International Trade Administration (2019). Welcome to the privacy shield. *Privacy Shield Framework*. https://www.privacyshield.gov/welcome

Intersoft Consulting. (2019). Art. 7 GDPR Conditions for consent. *Intersoft Consulting*. https://gdpr-info.eu/art-7-gdpr/

Intersoft Consulting. (2019). Art. 9. Processing of special categories of personal data. *Intersoft Consulting*. https://gdpr-info.eu/art-9-gdpr/

Intersoft Consulting. (2019). Art. 25 GDPR Data protection by design and by default. *Intersoft Consulting*. https://gdpr-info.eu/art-25-gdpr/

IT Governance Privacy Team (2017). EU General data Protection regulation (GDPR) An Implementation and Compliance Guide. *IT Governance Publishing*. Cambridgeshire Business Park, Ely Cambridgeshire, United Kingdom.

Joiner, B.L. (1985). The key role of statisticians in the transformation of North American industry. *American Statistician*. 39(3), 233-234.

McAfee, A., og Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Business Review*. http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf

Moore, D. (2018). The smart streets coming soon to Dallas. *SmartCitiesWorld*. https://www.smartcitiesworld.net/special-reports/special-reports/the-smart-streets-coming-soon-to-dallas

NSM (2018). RISIKO 2018. *Nasjonal sikkerhetsmyndighet*. https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

NHO (2019). Databehandleravtale. *NHO.no*. https://arbinn.nho.no/forretningsdrift/personvern/artikler/databehandleravtale/

NorSIS (2017). Trusler og trender 2017-2018. *Norsk senter for informasjonssikring.* https://norsis.no/wp-content/uploads/2017/12/tt17-18_web_endelig_v2.pdf

Prendergast, J., C. (1995). A Theory of Responsibility in Organizations. *Journal of Labor Economics*, Vol. 13, Utgave 3. S. 387-400. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.496.7904&rep=rep1&type=pdf

Politou, E., Alepis, E., og Patsakis, C. (2017). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyy001

Privazyplan. (2018). Data protection by design and by default. *Article 25 EU GDPR*. http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

Rajakumari, B., S. og Nalini C. (2014). An Efficient Cost Model for Data Storage with Horizontal Layout in the Cloud. *Indian Journal of Science and Technology*. Vol 7(3S), 45-46. https://s3.amazonaws.com/academia.edu.documents/35905785/5.An_Efficient_cost_model_for_data_storage.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1557535025&Signature=CVIgwn8ML5w%2BnchwQ7k1doZfcvo%3D&response-content-disposition=inline%3B%20filename%3DAn_Efficient_Cost_Model_for_Data_Storage.pdf

Saldana, J. (2009). The Coding Manual For Qualitative Researchers. *SAGE Publications Inc.* Teller Road, Thousand Oaks, California, CA.

Scott, C., og Jaffe, D. (1988). Survive and Thrive in Times of Change. *Training and Development Journal*. https://www.questia.com/magazine/1G1-6682063/survive-and-thrive-in-times-of-change

Shan, P. (2017). Data: The New Currency. *D!gitalist Magazine*. https://www.digitalistmag.com/cio-knowledge/2017/12/11/data-new-currency-05592449

Smedsrud, A. (2019). Nettsted: Disse appene spionerer på deg. *TEK.NO.* https://www.tek.no/artikler/populaere-apper-spionerer-pa-iphone-skjermen-din/457428

Sticos (2019). To streker under svaret. *Sticos*. https://www.sticos.no/

Utenriksdepartementet (2016). Ny utgave av EU/EØS-håndboken. *Regjeringen.no.*

Wade, C. og Tavris, C. (1996). Psychology, 4th ed., HarperCollins, New York, NY.

Zhang, D. (2018). Big data Security and Privacy Protection. *ATLANTIS PRESS*, College of Computer and Information Engineering, Zhengzhou University of Industrial Technology. https://doi.org/10.2991/icmcs-18.2018.56

Vedlegg

Vedlegg 1: Koding av kvalitative intervju

Spørsmål til kunder av Sticos som har gjennomført Serious Game

Ja, ja – GDPR ja. Det kan være noen vriene greier å sette seg inn i. Denne undersøkelsens mål er å finne ut av hvordan det står til med GDPR-arbeidet til bedrifter som har gjennomført Serious game i regi av Sticos. Den skal ikke brukes til noe annet enn bacheloroppgaven, og er ikke ment som noe fælt eller vondt. Den skal bare undersøke interessante spørsmål om hvor landet ligger i jobbingen med GDPR og hvor komplisert dette arbeidet er. Det vil ikke bli brukt navn på bedriften i oppgaven (bedrift 1, bedrift 2 osv), hvis ikke dette er ønskelig. Undersøkelsen er kvalitativ og det ses på som positivt om dere deler tanker og følelser som dere måtte ha på spørsmålene. Tusen takk og lykke til!

1. **Behandlingsgrunnlag**

Etter å ha gjennomført Serious Game, er bedriften oppdatert og klar over hvilke vilkår og krav som må oppfylles for å få lov til å behandle personopplysninger? Hvor langt har dere kommet nå? Er dere ferdige?

SVAR

Energiselskap (Bedrift 1): Vi har systematisert det som kom fram i gjennomgangen, og vi har hatt oppfølgingsmøter i et av selskapene høsten 2018. Etter den tid har det ikke vært noen systematisk gjennomgang.

Systematisert etter endt kurs. Ikke jobbet videre med dette. Kan behandle personopplysninger.

Regnskapsbyrå (Bedrift 2): Ja, i land for å kunne behandle personopplysninger. Man blir aldri ferdig med denne jobben, GDPR er en kontinuerlig jobb i et firma.

Kan behandle personopplysninger. Ikke alt på plass.

Olje og energiselskap (Bedrift 3): Ja, vi har fått et godt innblikk. Vi har begynt å opprette en handlingsplan og fått noen aksjoner på plass. Vi er ikke ferdige.

Startet arbeid. Ikke fått alt på plass.

Hias (Bedrift 4): Vi er ferdige med vårt prosjekt angående ivaretakelse av den nye personvernlovgivningen (som startet med Serious Game fra Sticos). Prosjektgruppen besto utelukkende av egne ansatte. I prosjektet ble det kartlagt omfanget av

Kan behandle personopplysninger. Er kommet i mål med alt, og er veldig kompatible med GDPR.

personopplysninger som behandles i selskapet og hvilke formål de har. Retningslinjer og vilkår er beskrevet i personvernserklæring som ble utarbeidet i prosjektet. Denne er godkjent og signert av ledelsen.

Utdanningsinstitusjon (Bedrift 5): Ja, vi er informert om hvilke krav som må oppfylles og det er lagd oversikter over alle opplysningsgruppene tilegnet virksomheten og hvordan disse skal behandles. Det er i tillegg lagd rutiner for oppbevaring av personopplysninger, samt rutiner for gjennomgang av kartleggingsskjema jevnlig. Vi er ferdig med vår gjennomgang av virksomhetens oppbevaring av personopplysninger.

Kan behandle personopplysninger. Er kommet i mål med alt, og er veldig kompatible med GDPR.

Orkla Credit (Bedrift 6): Vilkår og krav kom lettere(?) frem i vår virksomhet etter gjennomført Serious Game. Vi fikk gått gjennom alle våre virksomhetsområder og listet opp hovedpunktene. Disse har vi nå fått brutt ned til enkeltområder og tatt en gjennomgang. Dette er og blir en løpende prosess for oss, og vi kan vel derfor ikke si oss ferdige. Imidlertid har vi i vårt daglige virke kontinuerlig fokus på GDPR. I tillegg drøfter vi i dette våre ukentlige faste møter og i våre produksjonsmøter gjennom året.

Kan behandle personopplysninger. Fikk bedre innsyn etter Serious Game. Ukentlige møter.

Engasjert Byrå (Bedrift 7): Vi er nok ikke helt i mål ifht GDPR. Det å gjennomføre Serious Game hjalp oss veldig ifht det å forstå hvilke vilkår og krav som må oppfylles, og hjalp oss til å komme i gang med jobben. Vi jobbet målrettet til å begynne med, men etter å ha fått på plass det mest kritiske, så har vi dabbet av litt. Men, dette er jo en jobb man aldri blir ferdig med, så vi holder koken.

Ikke helt i mål med alt. Kan behandle personopplysninger. Fikk god hjelp etter Serious Game. Dabbet litt av etter det mest kritiske var i orden.

2. Databehandling

GDPR (Personvernsforordningen) pålegger både databehandlere og de som bruker databehandlere (behandlingsansvarlig) en rekke nye plikter og dokumentasjonskrav (eksempel på databehandlere kan være e-postleverandør, søsterselskap, lønnskjøring, evt. om dere utvikler datasystem for andre). Etter å ha gjennomført Serious Game med Sticos, hvordan ligger dere an med databehandleravtaler. Mangler dere databehandleravtaler med samarbeidspartnere, evt. hvorfor?

SVAR

Energiselskap (Bedrift 1): Dette er nok det som har vært prioritert mest i etterkant av gjennomgangen, så her har enkelte selskap i konsernet kommet langt.	**Kommet langt. Databehandleravtaler ble prioritert mest.**
Regnskapsbyrå (Bedrift 2): Databehandleravtaler er på plass.	**Databehandleravtaler på plass.**
Olje og energiselskap (Bedrift 3): Vi mangler noen.	**Mangler noen avtaler.**
Hias (Bedrift 4): I prosjektet ble det laget en oversikt som viste hvilke databehandlere selskapet har. Det er i etterkant utarbeidet avtaler med alle disse. Det ble overraskende mange.	**Databehandleravtaler på plass. Overrasket over hvor mange.**
Utdanningsinstitusjon (Bedrift 5): Vi har opprettet databehandleravtaler med alle være samarbeidspartnere.	**Databehandleravtaler på plass.**
Orkla Credit (Bedrift 6): Vi har sørget for å hente inn de databehandleravtaler som er nødvendig for oss, så dette skal være på plass.	**Databehandleravtaler på plass.**
Engasjert Byrå (Bedrift 7): Her tror jeg faktisk vi er i mål.	**Databehandleravtaler på plass.**

3. Roller

GDPR-ansvaret kan sjelden plasseres hos én enkelt person. Det er likevel noen som vil ha større ansvarsområde enn andre. Etter å ha gjennomført Serious Game med Sticos, er det satt opp ansvarlige (beskrivelse av ansvar og roller) for innføringen av GDPR i din bedrift (F.eks. behandlingsansvarlig og personvernombud)? Eventuelt om dere har planer om det?

SVAR

Energiselskap (Bedrift 1): Dette er det selvsagt planer om, men jeg kjenner ikke til at dette er gjennomført i særlig grad.	**Ikke gjennomført i særlig stor grad.**
Regnskapsbyrå (Bedrift 2): Vi har et team som jobber med GDPR ved siden av våre vanlige arbeidsoppgaver. En person er ansvarlig for å følge opp dette teamet. Teamet møtes minst en gang pr måned nå, oftere ved behov.	**Satt opp et team. En person er ansvarlig for oppfølging av teamet. Teamet møtes 1 gang i mnd.**
Olje og energiselskap (Bedrift 3): Foreløpig er det kvalitetsansvarlig som arbeider med GDPR. Vi har ikke noen planer på personvernombud.	**Satt opp 1 ansvarlig. Ingen planer om personvernombud.**
Hias (Bedrift 4): Rollen som behandlingsansvarlig og personvernombud er definert. Ansvaret er beskrevet i vår personvernerklæring. Personvernombudet er meldt inn til Datatilsynet sin oversikt.	**Roller er definert. Personvernombud meldt inn til datatilsynet.**
Utdanningsinstitusjon (Bedrift 5): Ja, vi har laget en oversikt over roller og hvem som har ansvar for hva. I tillegg til at hver enkelt ansatt har ansvar for å følge rutiner.	**Roller er definert.**
Orkla Credit (Bedrift 6): Nestleder/produksjonsleder er den som har hovedansvaret hos oss. I tillegg har vi definert en personvernrådgiver i virksomheten. Hadde nylig møte med Sticos om dette, og vi har landet på at vi benevner vedkommende som «rådgiver».	**Roller er definert. Produksjonsleder har hovedansvar. 1 person har person har i tillegg også ansvar.**
Engasjert Byrå (Bedrift 7): Ja, vi har satt opp ansvarlige hos oss.	**Ansvarlige er satt opp.**

4. Informasjonssikkerhet

Uønskede hendelser kan skje med tanke på integritet, konfidensialitet og tilgjengelighet. Dere har sikkert informasjon på deres servere som kan være interessant for utenforstående å få tak i. Etter å ha gjennomført Serious Game med Sticos, fant dere noen røde flagg? Er alle riskfaktorer identifisert? Er det tatt steg for bedre sikkerhet og rutiner, evt. hvorfor ikke?

SVAR

Energiselskap (Bedrift 1): Ja, på enkelte områder er det gått igjennom rutiner og dokumentasjon for å avgrense tilgangen til informasjon for uvedkommende. Dette gjelder spesielt for kundeinformasjonssystemet til kraftselskapet og nettselskapet. Dette systemet er spesielt oppgradert på adgangskontroll og sletterutiner.

Enkelte områder er gått igjennom. Spesielt kundesystemet er oppdatert på adgangskontroll og sletterutiner.

Regnskapsbyrå (Bedrift 2): Egen risikovurdering har blitt gjort, røde flagg er tettet. Vi har et eget sikkerhetsteam som har ansvar her. Sikkerhetsteamet og GDPR-teamet samarbeider der det er hensiktsmessig.

Røde flagg ble funnet og tettet. Samarbeid mellom sikkerhetsteam og GDPR-team.

Olje og energiselskap (Bedrift 3): Noen barrierer har vi fra tidligere. Men vi har en pågående aksjon på å gjøre en mer helhetlig vurdering og om det er noe vi bør forandre/utbedre.

Risikofaktorer er identifisert. Ikke tettet alle enda.

Hias (Bedrift 4): Prosjektet utarbeidet en ROS-analyse. Aktuelle uønskede hendelser ble identifisert med hjelp fra de ansatte. ROS-analyse inneholder også en handlingsplan og prioritering av tiltak.

Gjennomført risiko- og sårbarhetsanalyse. Risikofaktorer ble identifisert og tiltak iverksatt.

Utdanningsinstitusjon (Bedrift 5): Det oppstod ingen røde flagg hos oss. Vi har forsøkt å identifisere alle risikofaktorer og hatt gjennomgang av sikkerhet og rutiner. Ja, vi har tatt noen steg for sikkerhet. Mye er forbedret etter strengere og mer detaljerte rutiner.

Fant ingen røde flagg, men har skjerpet sikkerheten etter gjennomgang av rutiner.

Orkla Credit (Bedrift 6): Vi kjører asp (Application Service Provider) hos ekstern leverandør. Dette er en god samarbeidspartner som vi har benyttet de siste 15 år. Gjennom året har vi minst 2 driftsmøter med disse. Har ellers innhentet det som kreves for å dekke opp mot mulige inntrengere og vi har avdekt de nødvendige risikofaktorer for vår virksomhet.

Ekstern leverandør av sikkerhet. Identifisert risikoer og gjennomført tiltak.

Engasjert Byrå (Bedrift 7): Ja, her fant vi noen røde flagg. Disse er tatt hånd om. Vi har laget et sett med rutiner for noe, men her har vi fremdeles en jobb å gjøre.

Fant røde flagg. Tatt hånd om. Mangler fortsatt en del jobb på rutiner.

5. Brudd på reglene

Er virksomheten klar over hvilke konsekvenser som foreligger hvis det forekommer brudd på GDPR-reglene? (ja/nei)

SVAR

Energiselskap (Bedrift 1): Nei, vi er nok ikke det.

Regnskapsbyrå (Bedrift 2): Ja.

Olje og energiselskap (Bedrift 3): Ja.

Hias (Bedrift 4): Ja, konsekvensene ved brudd på personvernlovgivningen fremgår i rapporten som prosjektet utarbeidet. Dette er formidlet i ledermøte og allmøte blant annet.

Utdanningsinstitusjon (Bedrift 5): Ja.

Orkla Credit (Bedrift 6): Ja, vi er nok det.

Engasjert Byrå (Bedrift 7): Ja.

6. Handlingsplan

Arbeid med personvern er et dynamisk arbeid. Det er viktig å sørge for at virksomheten til enhver tid overholder regelverket. Etter å ha gjennomført kurset med Sticos, er det laget prosedyrer for gjennomgang og etterlevelse av rutinene? Hvor langt har dere kommet nå (er for eksempel rutinene som manglet ført opp på en handlingsplan?), eventuelt om dere er ferdige?

SVAR

Energiselskap (Bedrift 1): På det litt overordnende plan gjenstår det mye. Så langt har vi vært mest mulig fokusert på enkeltområder innen GDPR.

Mangler mye. Fokusert på enkeltområder.

Regnskapsbyrå (Bedrift 2): Rutiner er på plass, og internkontroll skjer i noen grad men her burde vi ha vært bedre.

Rutiner på plass. Burde vært flinkere på internkontroll.

Olje og energiselskap (Bedrift 3): Vi har begynt å opprette en handlingsplan og fått noen rutiner på plass.

Jobber med handlingsplan. Ikke ferdig.

Hias (Bedrift 4): Prosjektet har utarbeidet en personvernerklæring, GDPR ROS-analyse og en systemoversikt som viser alle selskapets systemer og hvilke personopplysninger vi har lagret, samt formål. I tillegg ble det utarbeidet følgende dokumenter og rutiner:

Handlingsplan er utarbeidet. Alle ledd i bedriften ble gått igjennom. Nødvendige dokumenter er produsert.

- Personvernombud – rolle og oppgaver
- Rutiner for håndtering av personopplysninger. Denne rutinen inneholder beskrivelse av hvordan selskapet håndterer:
    1. Iverksettelse eller opphør av behandling
    2. Sletting av personopplysninger
    3. Forespørsel om innsyn
    4. Innhenting av samtykke
    5. Ivaretakelse av reservasjonsrett
    6. Innsyn i personlig e-post eller fil-område
    7. Deling av bilder (internett og intranett)
    8. Kameraovervåking
    9. Databehandleravtaler

- Rutine for avvikshåndtering – personvern. Rutinen beskriver både intern avvikshåndtering og avvik som skal meldes Datatilsynet.
- Rutine for internkontroll. Rutinen beskriver en årlig dokumentkontroll (personalhåndbok, personvernerklæring, rutiner og databehandleravtaler osv.). Kontroll og oppdatering av systemoversikten og kontroll av formål. Oppdatering ROS-analyse og tiltak i handlingsplanen. Utførelse av ledelsens gjennomgåelse.

Utdanningsinstitusjon (Bedrift 5): Vi har satt opp jevnlige møter for gjennomgang av GDPR. Disse er også lagt inn i egen handlingsplan vi har for virksomheten.

Laget handlingsplan. Jevnlige møter.

Orkla Credit (Bedrift 6): Her har vi nok noe som enda ikke er helt på plass. Handlingsplanen er nesten komplett, men noen detaljer står igjen.

Mangler noen områder. Handlingsplan nesten komplett.

Engasjert Byrå (Bedrift 7): Nei, vi har ikke laget prosedyre for gjennomgang og etterlevelse av rutiner. Vi har de fleste rutinene på plass, og alt er ført på i en handlingsplan.

Ikke laget prosedyrer for gjennomgang av rutiner. Mangler noen rutiner. Har laget handlingsplan.

7. Tanker og erfaringer

Hvilke tanker sitter du igjen med om innføringen av GPDR. Er det et styr? Synes du det er viktig med tanke på personvern? Del gjerne erfaringer og inntrykk du sitter igjen med.

SVAR

Energiselskap (Bedrift 1): GDPR er bra i forhold til personvernet, men pga. omfanget er det nok riktig å ta det som selskapet/konsernet oppfatter som viktigst først.

Synes omfanget er stort. Synes GDPR er en bra ting. Prioriteringer.

Regnskapsbyrå (Bedrift 2): Ja, det er mye styr og veldig mye å sette seg inn i. Jobber i en relativt stor bedrift hvor vi har satt av masse ressurser for å få dette på plass. Har full forståelse for at mindre bedrifter sliter med dette. Jeg har en mistanke om at det er stor forskjell på gjennomføring av GDPR i en bedrift som har tatt Serious Game, kontra en liten bedrift som ikke har tatt seg råd til dette. Personvern er meget viktig i den verden vi lever i i dag. Personlig applauderer jeg derfor denne loven, men ser at den kan gi små bedrifter mye jobb og derfor vanskelig å etterleve.

Synes det er mye styr. Mener mindre bedrifter vil slite. Mener man burde ta seg råd til hjelp. Synes GDPR er en bra ting.

Olje og energiselskap (Bedrift 3): Personvernet er viktig, men klart at man tenker om dette skulle kunne gjøres enklere. Viktig for oss er blitt at vi inkluderer det i vårt kvalitetsstyringssystem – og ha et system i tillegg blir ikke holdbart for oss.

Synes det er styr. Viktig at det blir inkludert i eksisterende kvalitetsstyringssystem. Synes personvern er viktig.

Hias (Bedrift 4): I vårt GDPR-prosjekt ble det brukt mange arbeidstimer. Så ja, det var mye styr. Men vi synes selv at resultatet vi har kommet frem til er bra og riktig for de ansatte, samt tilstrekkelig for å dekke lovkrav. Personvern er viktig så arbeidet har vært nødvendig og ikke minst lærerikt for oss. Det som gjenstår hos oss er noe sletting av personopplysninger. Rutinen er laget, men det gjenstår noe arbeid knyttet til dette. Årsaken er usikkerheten rundt konsekvensen av å slette opplysninger om f.eks. tidligere ansatte. Men tiltak er iverksatt i henhold til handlingsplan. Prosjektets arbeid, personvernerklæringen og de tilhørende rutiner er gjennomgått i et allmøte, samt i avdelingsmøter.

Mye styr. Synes GDPR er viktig. Arbeidet har vært lærerikt. Gjenstår arbeid (GDPR kontinuerlig arbeid?). Usikkerhet ang sletting.

Utdanningsinstitusjon (Bedrift 5): Det var svært stort arbeid i starten, men når vi fikk utarbeidet alle dokumentene er det en grei jobb å følge opp og etterleve disse. Noen momenter har vært svært krevende å forstå, da det er noen dilemmaer som har vist seg å være litt uklare i hvordan man skal håndtere. Dette på grunn av at det ikke er så detaljerte eksempler i GDPR og alle virksomheter er forskjellige. Jeg finner det svært viktig med tanke på personvern, selv om enkelte deler virker unødvendig og tungvinne.

Mye arbeid/styr. Når ting var på plass ble det lettere. Usikkerhet ang noen momenter og dilemmaer. Synes GDPR er viktig.

Orkla Credit (Bedrift 6): Innledningsvis fikk vi god drahjelp med gjennomføringen av Serious Game. Her ble mye avdekt og avklart. Hva gjelder og hva gjelder ikke for vår virksomhet. Som inkassobyrå jobber vi tett opp mot både skyldnere og fordringshavere og mange personopplysninger tilflyter oss. GDPR er nå en integrert del av vår

Fikk god hjelp (fra Sticos). GDPR er integrert i produksjon. Fokus på GDPR i alle ledd. Regner med at de aldri vil bli 100% kompatible.

produksjon og vi har fokus på dette i alle ledd. Vi greier nok ikke tette alle skott, men vi føler at vi har kommet langt på vei.

Engasjert Byrå (Bedrift 7): Det kjentes ut som et styr da vi startet arbeidet, men etter hvert så ser man jo hvor viktig dette er, og jobben er blitt en naturlig del av vår hverdag. Man blir jo mer og mer opptatt av eget personvern, og dermed også hvordan man behandler opplysninger ifht kunder, kollegaer og samarbeidspartnere.

Synes det var styr i starten. Synes GDPR er viktig. Lærerik prosess.

1. **Behandlingsgrunnlag**

Ikke alt på plass: 5
Alt på plass: 2
Kommentarer: 2 dabbet av etter det mest kritiske var på plass. 2 sier kurset var til stor hjelp.

2. **Databehandling**

Databehandleravtaler på plass: 6
Ikke på plass: 1
Kommentarer: 1 mener dette var prioritert mest. 1 ble overrasket over hvor mange avtaler som trengtes.

3. **Roller**

Tildelt roller: 6
Ikke gjennomført i stor grad: 1
Kommentarer: Personvernombud ikke satt opp hos alle bedrifter. Bare 1 sier de har registrert personvernombud til datatilsynet. 2 bedrifter har bare en eller to personer som ansvarlige. 2 har satt opp team.

4. **Informasjonssikkerhet**

Fant røde flagg: 6
Fant ingen røde flagg: 1
Tatt hånd om røde flagg: 4

Ikke ferdige enda: 2
Kommentarer: Noen mangler en del jobb på rutiner (selv om røde flagg har blitt tettet), samt at rutiner også har blitt skjerpet for andre. Det ble utført risiko og sårbarhetsanalyser. 1 bedrift prioriterte to områder (adgangskontroll og sletterutiner) innenfor informasjonssikkerhet.

5. Brudd på reglene

Klar over konsekvenser: 6
Ikke klar over: 1

6. Handlingsplan

Ikke ferdig: 4
Ferdig: 3
Kommentarer: En del mangler prosedyrer for gjennomgang av rutiner. Burde vært flinkere på internkontroll. Selv om handlingsplan er laget, mangler det rutiner og internkontroll på mange (oppfølging). Bare 2 har god kontroll.

7. Tanker og erfaringer

Synes det var mye styr: 6
Ukjent: 1
Synes det var helt greit: 0

Synes GDPR/personvern er viktig: 6
Ukjent: 1

Kommentarer: Synes det er et stort omfang, mye å sette seg inn i (i hvert fall i begynnelsen av prosessen). Fortsatt forvirring ang. noen områder innenfor GDPR, de er fortsatt ikke helt sikre på hva man skal gjøre i alle situasjoner/litt forvirring. 4 synes prosessen var lærerikt, og synes Sticos ga god hjelp. 3 ukjent.