Handelshøyskolen BI - campus Oslo

BTH 36201

Bacheloroppgave - Økonomi og administrasjon

Bacheloroppgave

Hvordan påvirker GDPR norske netthandelsaktører - risiko og muligheter

Navn:	Fredrik Bjanger Gundersen, Martin Georg Bie Andreassen

Utlevering:	07.01.2019 09.00
Innlevering:	03.06.2019 12.00

Bacheloroppgave

ved Handelshøyskolen BI

Hvordan påvirker GDPR norske netthandelsaktører - risiko og muligheter

BTH36201

Bacheloroppgave, Økonomi og administrasjon

Utleveringsdato:
08.01.2019

Innleveringsdato:
03.06.2019

Studiested:
BI, Campus Oslo

"GDPR skulle vært innført for ti år siden"

- Intervjuobjekt D

I. Forord

Dette er vår avsluttende bacheloroppgave etter tre år på Økonomi og Administrasjon ved Handelshøyskolen BI, Oslo.

Felles interesse for personvern og netthandel har utformet oppgavens tema og problemstilling. Det har vært en krevende og lærerik prosess hvor vi har møtt på flere utfordringer underveis. Vi startet arbeidet med bacheloroppgaven tidlig i semesteret og vinkling på oppgaven har endret seg flere ganger. Det er lite etablert forskning om vårt tema, noe som har vanskeliggjort prosessen. Vi er likevel svært fornøyde med å presentere resultatet av mange måneders hardt arbeid. Vi ønsker å benytte anledningen til å takke vår veileder, Tor Olav Nordtømme, for gode innspill og god hjelp underveis i prosessen.

Denne oppgaven ville ikke vært mulig uten hjelp og innspill fra våre intervjuobjekter. Vi ønsker å takke Virke E-handel, Cookie Information AS, Komplett Group AS, Elkjøp Nordic AS, Ræder Advokatfirma AS, Forbrukertilsynet og StayClassy AS. En ekstra takk rettes til Virke E-handel for å ha gitt oss muligheten til å delta på deres vårsamling på Soria Moria, og Cookie Information AS for å ha gitt oss tilgang til deres analyseverktøy. En takk rettes også til respondentene i spørreundersøkelsen.

Oslo, mai 2019.

II. Personvern i oppgaven

Norsk Senter for Forskningsdata (NSD) stiller krav til meldeplikt dersom man behandler personopplysninger i oppgaven. Ingen personer skal kunne identifiseres, hverken direkte eller indirekte. Vi mener at vi har anonymisert alle intervjuobjektene og respondentene i spørreundersøkelsen ved å hverken nevne navn eller stilling. Siden den kvantitative spørreundersøkelsen fant sted på Soria Moria i Oslo, er også organisasjon anonymisert. Vi har valgt å ta med organisasjon for intervjuobjektene fra de kvalitative intervjuene da vi ser oss nødt til det for å besvare oppgavens problemstilling. Vi mener selv at vi oppfyller kravene som stilles til personvern.

III. Sammendrag

Den norske netthandelsbransjen har opplevd en enorm vekst de siste 20 årene og er fortsatt bare i startfasen. Norske netthandelsaktører behandler stadig større mengder med persondata. EUs nye personvernforordning - GDPR - trådte i kraft i alle EU- og EØS-land den 25. mai 2018. For norske virksomheter som behandler store mengder data har dette ført til store omstillinger og risikoene kan være mange dersom de ikke etterlever GDPR-regelverket.

Problemstillingen som drøftes i denne oppgaven er:

Hvordan har norske netthandelsaktører blitt påvirket av GDPR og hvilke risikoer står de ovenfor ved å ikke etterleve GDPR-regelverket?

GDPR-regelverket stiller en rekke krav til alle norske virksomheter som behandler persondata og har som hensikt å gi enkeltindividet større kontroll over egne personopplysninger. Oppgaven fokuserer på norske netthandelsaktører og hvordan de har blitt påvirket av GDPR-regelverket. En annen sentral faktor i oppgaven er å vurdere risikofaktorer som norske netthandelsaktører står ovenfor ved å ikke etterleve GDPR-regelverket.

Datagrunnlaget baserer seg på både primær- og sekundærdata. Primærdata er hentet inn fra kvalitative intervjuer og en kvantitativ spørreundersøkelse. Oppgaven er utforskende og eksperimenterende med et kausalt forskningsdesign.

I siste del av oppgaven knyttetes teori og dataanalyse sammen, før vi i konklusjonen oppsummerer våre funn i lys av problemstillingen. Problemstillingen er todelt, og forskningsspørsmålene kan enten ses individuelt eller i sammenheng.. Helt avslutningsvis lanserer vi noen generelle anbefalinger til tiltak som kan iverksettes av norske netthandelsaktører/myndigheter.

IV. Innholdsfortegnelse

V. Begrepsforklaring

Behandlingsansvarlig

Fysisk eller juridisk person, offentlig myndighet, institusjon eller annet organ som *bestemmer formålet med behandlingen av personopplysninger*. Den ansvarlige part.

COSO

Forkortelse for «The Committee of Sponsoring Organizations of the Treadway Commission».

Databehandler

Fysisk eller juridisk person, offentlig myndighet, institusjon eller annet organ som behandler personopplysninger på vegne av andre.

Den registrerte

Den registrerte er personen som er registrert i virksomhetens databaser. Personen som virksomheten behandler personopplysningene til, er den registrerte.

Direktiv

Rammevedtak som setter opp mål og betingelser som medlemslandene selv må utforme en lovtekst til for innen en viss tidsfrist.

DPIA

Data Protection Impact Assessement

Vurdering av personvernkonsekvenser.

EDPB

European Data Protection Board

Bidrar til opprettholdelse av databeskyttelsesreglene i EU.

EU

Den europeiske union

Består av 28 medlemsland.

EØS

Det europeiske økonomiske samarbeidsområdet

Avtale mellom EU-land, EUs medlemsstater og EFTA-landene. Norge er et av EFTA-landene.

Forordning

Identisk for alle EU/EØS-land. Gir mindre nasjonalt handlingsrom enn et direktiv.

GDPR

General Data Protection Regulation

EUs nye personvernforordning som gjelder for alle land innenfor EU/EØS og alle land som handler med land innenfor EU/EØS.

GDPR-compliant

En virksomhet blir GDPR-compliant når den etterlever regelverket.

Informant nr. 1

Er en tidligere leder i en stor norsk netthandelsbedrift. Forfatterne har benyttet Informant nr. 1 som kilde til inspirasjon og ressursperson i arbeidet med denne oppgaven. Vedkommende er ikke en del av den kvalitative undersøkelsen fordi vedkommende ikke lenger jobber med B2C-rettet netthandel.

Leads

Person som har vist mer interesse enn vanlige abonnenter for dine produkter eller tjenester.

Personopplysning

Alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson. Eksempler på personopplysninger er navn, adresse, telefonnummer, e-post, fødselsnummer, IP-adresser og opplysninger om atferdsmønstre.

Session

Tiden fra du åpner en nettside til du lukker den kan betegnes som en «session».

1. Innledning

GDPR er forkortelsen for General Data Protection Regulation som er EUs personvernforordning. Den trådte i kraft i alle land innenfor EU og EØS den 25. mai 2018. Forordningen har til hensikt å beskytte og styrke personvernet til alle EU-borgere, og standardisere personvernlovgivningen i medlemslandene. Forordningen stiller høyere krav til enkelhet, åpenhet og gir at forbrukeren rett til innsyn og sletting av egne personopplysningen (Datatilsynet, 2018). Det tidligere regelverket var ikke like detaljert m.h.t forbrukerens rettigheter. EUs personverndirektiv fra 1995 resulterte i at flere EU-land hadde ulike personvernlover, der noe som var lov i et land ikke var lov i et annet. Innføringen av forordningen er den viktigste endringen i reguleringen av personvernet de 20 siste årene. (Voigt & Bussche, 2017).

I 2018 var innføringen av GDPR – «General Data Protection Regulation» høyt på dagsorden til mange norske bedrifter. Netthandelsbransjen, som generelt behandler store mengder persondata, måtte virkelig gjøre et løft for å tilpasse seg det nye regelverket, og det har vært ressurskrevende for mange å bli GDPR-compliant.

Det er flere aktører som hevder at GDPR er kommet for sent, og at den tidligere personopplysningsloven for lengst var utdatert. Påstanden er at Facebook og Google i en årrekke nesten uforstyrret har fått forme måten vi bruker internett på, delvis grunnet manglende lovverk som regulerer bruken av persondata (Intervjuobjekt D).

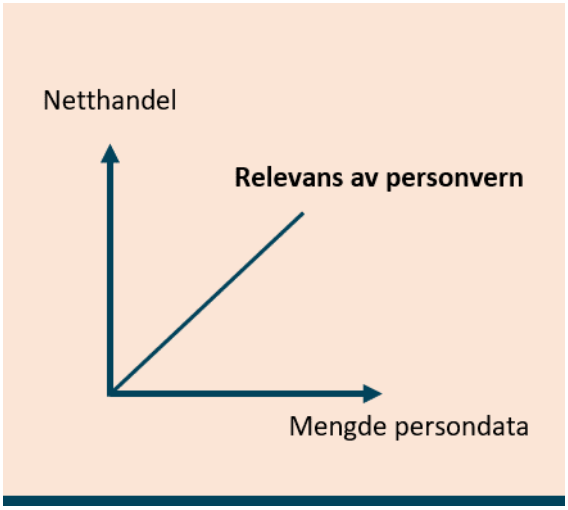
Det er liten tvil om at innføringen av GDPR har satt søkelyset på personvern og forbrukerens rettigheter. Høsten 2018 måtte eksempelvis Telenor stanse deler av den digital overvåkningen av 400 ansattes datamaskiner etter en uttalelse fra datatilsynet, ettersom det strider imot reglene for personvern (Grimstad, 2018). Telenor fikk ingen bot som følge av uttalelse fra datatilsynet, men det er all grunn til å anta at fokuset på personvern vil være viktig i tiden fremover, etterhvert som GDPR regelverket får gått seg til og myndighetene iverksetter sanksjoner mot de som ikke følger regelverket.

1.1. Bakgrunn for problemstillingen

Forfatterne av oppgaven er begge fra Sandefjord, ofte omtalt som "netthandelens by" i Norge. Vi besluttet tidlig i prosessen med Bacheloroppgaven at vi ønsket å skrive om et dagsaktuelt tema innen netthandelsbransjen, og fant det interessant å analysere hvordan norske netthandelsaktører er blitt påvirket av innføringen av den nye GDPR-regelverket, og hvordan netthandelsaktørene har tilpasset seg, samt i hvilken grad de håndterer den betydelige forretningsmessige risikoen som følger av GDPR-regelverket.

Netthandelen har de siste 19 årene vokst med 475%, og aldri før har så mange personer hatt tilgang til internett. Konsekvensen er at hver og en av oss legger igjen flere digitale spor enn noen gang tidligere.

Det er lite etablert teori og forskning som belyser problemstillingen vi har valgt, ei heller etterlevelseproblematikken. Det er tilsvarende like lite fokus på mulighetene som følger av de nye personvernreglene.



Figur 1 – Relevans av personvern

1.2. Problemstilling

Oppgavens tema har fått langt mer oppmerksomhet fra relevante aktører enn vi hadde regnet med. Flere har sagt det er behov for mer diskusjon rundt personvern, og at enkelte behandlingsansvarlige ikke er klar over hvem de deler data med selv om de er GDPR-compliant. De understreker også kompleksiteten i GDPR-regelverket, som kan være overveldende. Etter avgrensninger kom vi frem til følgende problemstilling:

«Hvordan har GDPR-regelverket påvirket norske netthandelsaktører og hvilke risikoer står de ovenfor ved å ikke etterleve GDPR-regelverket?»

Problemstillingen er todelt og fokuserer på to forskningsspørsmål som enten kan sees individuelt, eller i sammenheng:

1. Hvordan har GDPR påvirket norske netthandelsaktører?
2. Hvilke risikoer står netthandelsaktørene ovenfor ved å ikke etterleve GDPR regelverket?

Problemstillingen er tilsynelatende bred og omfattende, men vi har valgt avgrensninger som behandles i kapittel 1.3 Vi har videre valgt å besvare forskningsspørsmålene sammensatt, for dermed å kunne redegjøre for utfordringene med GDPR og etterlevelsesproblematikken hver for seg. Nøkkelordene i problemstillingen er «påvirkning» og «risiko». Vi belyser både positive og negative konsekvenser som følge av GDPR, og vi ser også på hvilke muligheter innføringen har medført. Med risiko menes hvilke konsekvenser norske netthandelsaktører kan stå overfor dersom de ikke etterlever GDPR regelverket. Etter vår oppfatning er problemstillingen både relevant og dagsaktuell, og setter fokus på viktigheten på personvern.

Et viktig element i diskusjonen om personvern er bruken av informasjonskapsler på internett. Dette er ikke direkte regulert i GDPR, men reguleres av Ekomloven §2-7b. Vi trekker inn bruken av informasjonskapsler i oppgaven der det er relevant i lys av GDPR.

1.3. Avgrensninger

GDPR er et nytt og svært omfattende regelverk. Det lar seg således ikke gjøre å dekke alle aspektene omkring hvilke påvirkninger regelverket har for alle bedrifter i alle bransjer. Vi har derfor valgt å avgrense oppgaven til å drøfte konsekvenser og risikofaktorer for norske netthandelsaktører.

Oppgaven avgrenses til norske netthandelsaktører som tilbyr varer til forbrukere, såkalt B2C. Oppgaven setter søkelys på økonomiske konsekvenser for norske netthandelsaktører, men unnlater å tolke det juridiske aspektet rundt GDPR regelverket. Den samme avgrensningen gjelder Ekomloven §2-7b.

Oppgaven fokuserer ikke på utenlandske netthandelsaktører som retter sin virksomhet mot norske forbrukere, da dette ville blitt for omfattende, men det er vi trekker inn nordmenns forbruk i utlandet for å belyse viktigheten av enhetlige regler for personvern.

Selv om fokuset i oppgaven er norske netthandelsaktører, er våre funn og konklusjoner relevante for andre bransjer, da GDPR er et generelt regelverk for behandling av persondata.

1.4. Valg av metode

Vårt datagrunnlag er hentet fra kvalitative intervjuer med relevante fagpersoner, og vi har gjennomført en kvantitativ spørreundersøkelse blant 25 bedrifter, som supplerer og underbygger fagpersonenes vurderinger. Oppgaven har en induktiv tilnærming da oppgaven i hovedsak benytter kvalitativ metode. Forskningsdesignet er undersøkende, og oppgaven er eksperimenterende.

I metodekapittelet har vi redegjort for oppgavens tilnærming og metodisk fremgangsmåte.

1.5. Redegjørelse for teorifundament

Vi har anvendt relevant teori om GDPR, informasjonskapsler, samfunnsansvar, etikk og internkontroll (risk management). Vi drøfter hvordan GDPR har påvirket de norske netthandelsaktørene, og etterlevelseproblematikk knyttet til GDPR. Samfunnsansvar, etikk og internkontroll henger tett sammen og det er derfor relevant å anvende teori innenfor disse fagområdene.

I tillegg til teorien har vi benyttet relevante artikler, nettsider og rapporter som sekundærdata. Dette er nødvendig for å underbygge funn og argumentasjon. For å begrunne og argumentere fremgangsmåten i oppgaven har vi benyttet teoretisk rammeverk innenfor økonomisk-administrativ forskning.

2. Bakgrunn

Med en stadig økende andel av den norske befolkningen som handler på nett, øker også behovet for regulering av digital persondata, omtalt som e-Privacy. Dette kapittelet har til hensikt å kontekstualisere problemstillingen ved å se på nåværende situasjon, utviklingen i norsk netthandel, tidligere personvernlovgivning og bakgrunnen for GDPR.

2.1. Netthandelens utvikling

I løpet av de siste 20 årene har norsk netthandel opplevd en enorm vekst og stadig flere forbrukere benytter digitale kanaler for å handle varer og tjenester (DIBS, 2018). For å belyse utviklingen i norsk netthandel har vi tatt utgangspunkt i DIBS' rapport om norsk e-handel i 2018. DIBS er et datterselskap av Nets og er en ledende aktør innen betalingsformidling på internett. De har 15.000 nettbutikker som kunder, og har over 2 milliarder gjennomførte transaksjoner (DIBS, 2018). Informant nr. 1 mener DIBS' målinger er de mest troverdige, og hevder dette er en generell bransjeoppfatning. I rapporten fremkom det bl.a. at 2018 ville bli et rekordår for norsk netthandel og veksten er stadig økende.

Fra 2017 til 2018 økte norsk netthandel med 17 % og på de siste fem årene har norsk netthandel nesten doblet seg. I 2018 handlet norske forbrukere for 144,8 milliarder kroner på internett mot 124,2 milliarder året før (DIBS, 2018). Tallene inkluderer reiser og tjenester og inkluderer netthandel hos utenlandske aktører. Det følger implisitt av nordmenns økende appetitt for netthandel at vi legger igjen stadig flere digitale spor. Ifølge Anthun (2018) referert i Taylor (2018) er norsk netthandel bare i startfasen, og den vokser tre ganger raskere enn fysiske butikker.

I år 2000 var netthandel et fenomen de færreste hadde et forhold til. Omsetningen i norske nettbutikker var på ca. 82 millioner kroner i år 2000 (Kaur, 2005). Kaur (2005) viser ikke til hvorvidt omsetningen i år 2000 tar høyde for utenlandske aktører, men det gir likevel en sterk indikasjon på hvordan norsk netthandel har vokst de siste 20 årene. I 2000 ble det innført en ny personopplysningslov som innarbeidet EUs personverndirektiv fra 1995 (Wessel-Aas & Ødegaard, 2018).

Statistikken over norsk netthandel er generelt sprikende og viser i stor grad ulike tall (Informant nr. 1). Dette skyldes at ulike aktører tar ulike forutsetninger når de beregner hvor mye nordmenn handler på internett.

Til tross for sprikende tall gir undersøkelsene likevel under en god indikasjon på veksten og utviklingen i norsk netthandel.

2.2. Nordmenn og utenlandsk netthandel

I 2017 hadde 75 % av alle nordmenn mellom 16 og 79 år handlet på internett i løpet av de 12 siste månedene (SSB, 2017), og norske forbrukere handler mye fra utenlandske aktører, spesielt fra Kina, Storbritannia og USA (Nordstrøm, 2017). Ifølge NTB (2018) er det Amazon, eBay og Zalando som er de mest populære utenlandske aktørene hos norske forbrukere. Ved at norske forbrukere handler hyppig hos utenlandske netthandelsaktører legger de igjen digitale spor i utlandet, som understreker viktigheten av et standardisert regelverk for personvern.

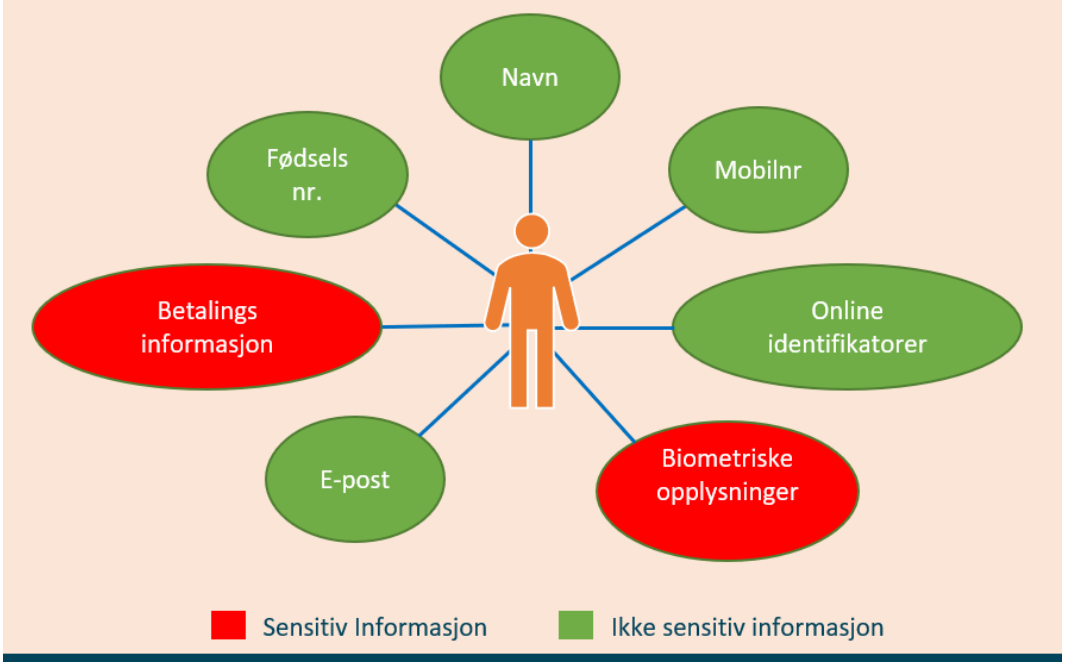
Tidligere har det vært ulike regelverk for norske- og utenlandske netthandelsaktører, som har resultert i en ulik konkurransesituasjon. Netthandelsaktører i for eksempel Asia har hatt et annet forhold til personvern og databehandling, som har ført til et konkurransefortrinn i forhold til norske netthandelsaktører (Informant nr.1). Det er heller ikke usannsynlig at 350-kronersgrensen for avgiftsfri privatimport fra utlandet har bidratt til å øke nordmenns netthandel hos utenlandske aktører, og således medført at store mengder personopplysninger om norske forbrukere blir tilgjengelig for utenlandske aktører.

Figur 2 – Fakta om 350-kronersgrensen

2.3. Personvern

Datatilsynet (2018) definerer personvern på følgende måte: «Personvern handler om retten til privatliv og retten til å bestemme over egne personopplysninger». Retten til privatliv er forankret både i Den europeiske menneskerettighetskonvensjonen og i den norske grunnloven (Datatilsynet,

2018b). Alle opplysninger som direkte eller indirekte kan knyttes til en fysisk person går under betegnelsen personopplysninger (Wessel-Aas & Ødegaard, 2018).



Figur 3 – Personopplysning

Figuren illustrerer hva som kan defineres som personopplysninger. Ifølge intervjuobjekt F kan man se på en personopplysning som et puslespill. Dersom en eller flere av disse opplysningene kan knyttes sammen og danne et bilde om deg som person, så er det definert som personopplysning.

2.4. Verdien av persondata

Selskaper betaler store summer for å få tilgang til relevante persondata som kan brukes til rettet markedsføring (Kaldestad, 2018), og ifølge Nyvold (2018) har EU beregnet at verdien av EU-borgernes persondata ligger på 950 milliarder kroner. Verdien av personopplysninger gir et insentiv til å samle inn mest mulig informasjon og bruke dem til flest mulig formål (Kaldestad, 2018).

En av de viktigste grunnene til at mange applikasjoner og tjenester er gratis på internett er for å samle inn kundedata som igjen selges videre til

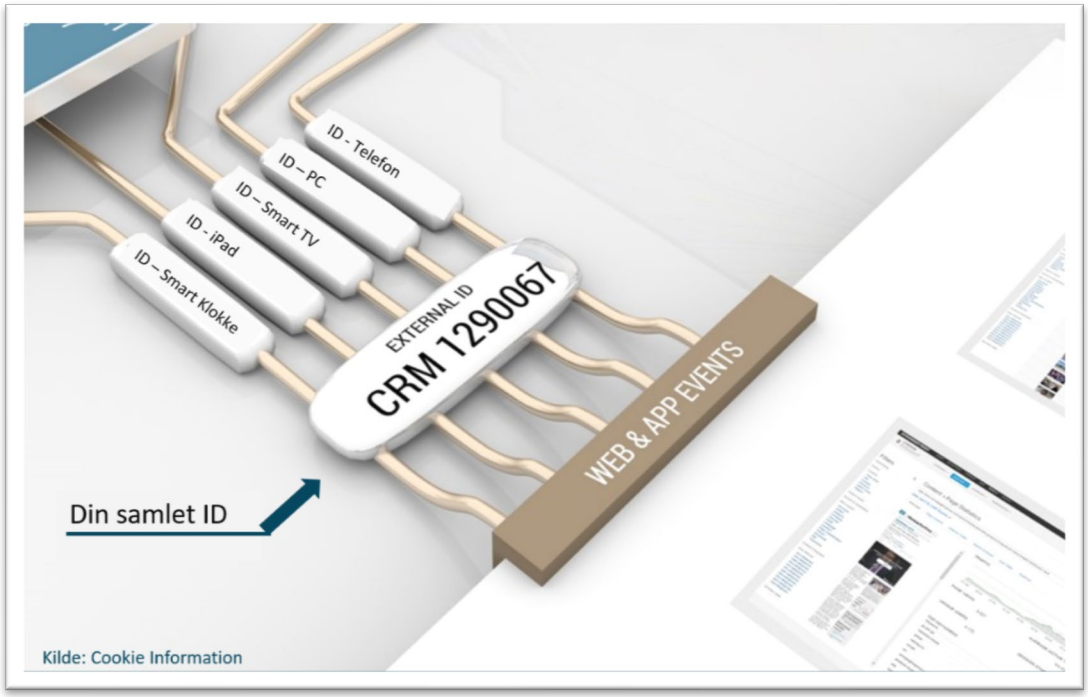
Informasjonskapsler i mobil applikasjoner

- 82% Leser device – ID
- 80% Tracker lokasjon
- 57% Tracker når man ringer
- 26% Leser hvilke app'er man bruker
- 26% Lagrer brukerens SIM-kortnr.

Figur 4 – Informasjonskapsler i apper

andre virksomheter (Cookie Information, 2019). Mobiltelefoner er blant verstingene, og samler inn mengder av persondata som vises i en undersøkelse IBM gjorde for noen år siden (Cookie Information, 2019).

De fleste personer i Norge har telefon, pc, Smart-Tv og iPad eller Smartklokke. Alle disse enhetene har sin egen informasjonskapsel-ID, og ulike plattformer som eksempelvis Xcense kobler sammen disse forskjellige ID-ene på tvers av enhetene, som knyttes opp til en person (Intervjuobjekt F).



Figur 5 – ID-nummer

Figur 5 er en grafisk fremstilling av hvordan alle enhetene (PC, mobil, etc.) har en egen ID, som på grunn av teknologi blir samlet til én felles ID på tvers av enhetene som identifiserer brukeren.

Innsamling av persondata kan være nyttig, men også virke mot sitt formål. Ved å samle inn og analysere persondata kan selskapene kartlegge enkeltindivider på en slik måte at opplysningene kan misbrukes (Kaldestad, 2018).

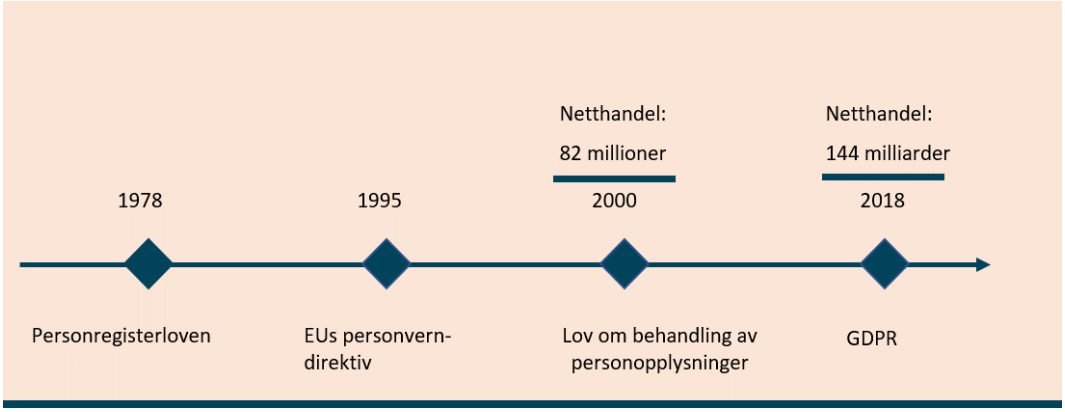
Manipulasjon og misbruk av personopplysninger kan føre til at forbrukeren eksempelvis betaler mer for en vare eller tjeneste basert på interesse og kjøpekraft (Virke vårsamling, 2018). Fra forbrukerperspektiv illustrerer dette viktigheten av å ivareta personvernet for å unngå misbrukt av personopplysninger.

2.5. Personvern i Norge

Personvernlovgivning i Norge strekker seg tilbake til 1978. Personregisterloven fra 1978 trådte i kraft i Norge den 1. januar 1980. Den ble innført som følge av økende bruk av elektronisk databehandling (Wessel-Aas & Ødegaard, 2018).

EUs personverndirektiv ble vedtatt 24. oktober 1995 og skulle sikre standarder for databeskyttelse innenfor EU. Direktivet ble implementert som nasjonal lovtekst i medlemslandene. Det var derfor noen forskjeller i regelverket i de ulike landene innenfor EU og EØS (Wessel-Aas & Ødegaard, 2018).

I år 2000 ble det innført en ny personopplysningslov i Norge. Personregisterloven fra 1978 ble erstattet av den nye personopplysningsloven med virkning fra 1. januar 2001. Loven av år 2000 inkluderte EUs personverndirektiv og ga klarere regler om hvordan personopplysninger skulle behandles i Norge (Wessel-Aas & Ødegaard, 2018). Direktivet levde ikke opp til sine forventninger og medførte at noen databehandlinger var lov i et land, men ikke et annet (Voigt & Bussche, 2017). Dette ble bakgrunnen for EUs nye personvernforordning – GDPR.



Figur 6 – Tidslinje

2.6. GDPR i Norge

Personopplysningsloven fra år 2000 ble i 2018 erstattet med GDPR - EUs nye personvernforordning. GDPR ble vedtatt i EU i 2016 etter å ha blitt utarbeidet siden 2012 (Voigt & Bussche, 2017). GDPR trådte i kraft i Norge 25. mai 2018, men ble ikke gjeldende før 20. juli samme år (Wessel-Aas & Ødegaard, 2018).

I Norge har man også noen nasjonale lovbestemmelser som utfyller forordningen slik at personvernet til norske borgere står sterkere enn det GDPR-regelverket legger opp til (Wessel-Aas & Ødegaard, 2018). Som følge av den nye forordningen vil det norske regelverket være litt mindre detaljert på noen områder, og strengere på andre områder (Wessel-Aas & Ødegaard, 2018).

I denne oppgaven vil vi ha det norske lovverket som utgangspunkt. Flere av bestemmelsene i det nye lovverket har allerede vært gjeldende i Norge siden år 2000. Innføringen av GDPR-regelverket setter strengere krav til virksomheter for å regulere flyten av personopplysninger og tilrettelegger for at den registrerte skal ha større kontroll over egne personopplysninger (Datatilsynet, 2018b). De viktigste endringene i norsk personvernlovgivning som følge av GDPR er illustrert i tabellen nedenfor.

Dette er nytt med GDPR
• Større geografisk område • Opplysninger brukes kun til forhåndsdefinerte formål • Nye rettigheter for borgere • Krav til klarhet og åpenhet i språket • Større ansvar for virksomhetene • Internasjonal samarbeidsplikt • Større sanksjoner
Kilde: Datatilsynet (2018f).

Figur 7 – Dette er nytt med GDPR

3. Teoretisk rammeverk

Kapittelet presenterer og gjennomgår det teoretiske rammeverket som er anvendt i oppgaven. Formålet med oppgaven er å undersøke hvordan GDPR-regelverket har påvirket norske netthandelsaktører og anvender pensum om GDPR, informasjonskapsler (cookies), etikk og samfunnsansvar. Etterlevelsesproblematikk er også et tema knyttet til problemstillingen og vi ser derfor på pensum om risk management. Teorifundamentet er hentet inn gjennom relevant litteratur, artikler og andre relevante kilder.

3.1. General Data Protection Regulation (GDPR)

I forrige kapittel redegjorde vi for tidligere personvernlovgivning og gjennomgikk bakgrunnen for GDPR. I dette delkapittelet ser vi på virksomheters plikter etter innføringen av GDPR-regelverket, som kan oppsummeres i 14 punkter. GDPR-regelverket gjelder for et mye større geografisk område. Virksomheter som ikke er en del av EU/EØS, men som tilbyr varer og tjenester til EU-borgere, vil også omfattes av det nye regelverket (Voigt & Bussche, 2017).

1. Fastsette formål

Det må foreligge et eller flere formål for at en virksomhet skal kunne behandle personopplysninger. Personopplysninger kan kun brukes til spesifikke og lovlige formål. Formålet må være formulert konkret og åpent.

2. Legge til rette for brukerens rettigheter

Den registrerte skal kunne bruke sine rettigheter på en enkel måte. Vurdering, behandling og svar på forespørsel må forekomme senest innen én måned og det skal være gratis å bruke sine rettigheter. Virksomheten har også ansvar for at personopplysninger ikke gis ut til uvedkommende eller kommer på avveie.

3. Vurdering av personvernkonsekvenser og forhåndsdrøftelse

Personvernet til den registrerte skal ivaretas gjennom en vurdering av personvernkonsekvenser (Data Protection Impact Assessment).

4. Informasjonssikkerhet

Opplysningene skal være tilgjengelige for den registrerte når de har behov for dem, og skal beskyttes på en god måte mot uberettiget innsyn og endringer.

5. Håndtere avvik

Den behandlingsansvarlige virksomheten må melde avvik til Datatilsynet så fort som mulig og senest innen 72 timer etter at avviket er oppdaget.

6. Ha behandlingsgrunnlag

Det må foreligge et behandlingsgrunnlag for å kunne samle inn og behandle personopplysninger.

Eksempler på behandlingsgrunnlag kan være:

- Samtykke
- Oppfylle en avtale
- Oppfylle en rettslig plikt
- Beskytte vitale interesser
- Utføre en oppgave i offentlig interesse eller utøve offentlig myndighet.
- Ivareta legitime interesser

7. Retting og sletting

Det er virksomhetens plikt å sørge for at personopplysningene er korrekte og av god kvalitet. Ved feil opplysninger må virksomheten rette disse. Personopplysninger kan ikke beholdes lenger enn nødvendig. Ved behandlingsgrunnlag som følge av samtykke, må virksomheten slette personopplysningene om samtykke trekkes tilbake, med mindre noe annet fremkommer av lov.

8. Innebygd personvern

Personvern må tas hensyn til i alle faser ved utvikling av et nytt system eller en løsning.

9. Protokoll over behandlingsaktiviteter

Det skal føres en protokoll over alle behandlingsaktiviteter som utføres under virksomhetens ansvar.

10. Spesielt om overføring av personopplysninger til utlandet

Dersom en virksomhet overfører personopplysninger til et land som ikke omfattes av GDPR, må de likevel forholde seg til personvernregelverket.

11. Informasjon og åpenhet

Personopplysninger skal behandles på en åpen måte. Det skal gis kort og forståelig informasjon om hvordan en virksomhet behandler personopplysninger.

12. Personvernombud

Ikke alle virksomheter er pliktet til å ha et personvernombud. Offentlige myndigheter og virksomheter som har som hovedvirksomhet å behandle data i stor grad, må ha et personvernombud. Datatilsynet oppfordrer alle virksomheter til å ha et personvernombud.

13. Etablere internkontroll

Alle virksomheter skal behandle personopplysninger lovlig, sikkert og forsvarlig. Ved å etablere og vedlikeholde tiltak gjennom god internkontroll skal virksomheten sikre at personopplysninger behandles i samsvar med regelverket. Det skal kunne fremvises dokumentasjon på at personopplysninger behandles i tråd med regelverkets personvernprinsipper.

14. Databehandleravtale

Dersom den behandlingsansvarlige benytter underleverandører er man pliktig til å ha en databehandleravtale med hver av dem. Databehandleravtalen må sikre at underleverandører behandler personopplysninger i samsvar med regelverket. Databehandleravtalen setter en klar ramme for behandling av personopplysninger på vegne av den behandlingsansvarlige. (Datatilsynet, 2018c).

3.2. Informasjonskapsler (Cookies)

En informasjonskapsel (også kalt "cookie") er en liten tekstfil som lastes ned og lagres på brukers datamaskin når brukeren åpner en nettside. En informasjonskapsel brukes til å lagre informasjon om nettbesøket, som for eksempel innstillinger/preferanser, innloggingsdetaljer, eller handlekurv (Cookie Information, 2019).

Vi skiller mellom flere ulike typer informasjonskapsler:

- **Sesjonsavhengig informasjonskapsel**
  Informasjonskapsler som slettes når brukeren lukker nettstedet. Brukes til å registrere aktivitet på nettsiden.
- **Fast informasjonskapsel**
  Informasjonskapsler som brukes til å tilpasse brukerens opplevelse av nettsiden, og beholde informasjonen til fremtidige besøk. Faste informasjonskapsler lagrer blant annet brukerens innstillinger og preferanser.
- **Førsteparts informasjonskapsel**
  Informasjonskapsler som er nødvendige for at en nettside skal fungere. Denne typen informasjonskapsler kan ikke fjernes.
- **Tredjeparts informasjonskapsel**
  Informasjonskapsler som brukes til analyser, markedsføring og personalisering av brukeropplevelsen, f.eks. visning av annonser. Informasjonskapslene kan som oftest velges bort, men det kan føre til at enkelte funksjoner på nettsiden ikke lenger fungerer. Kan være enten sesjonsavhengig eller fast.

(Nasjonal kommunikasjonsmyndighet, 2019).

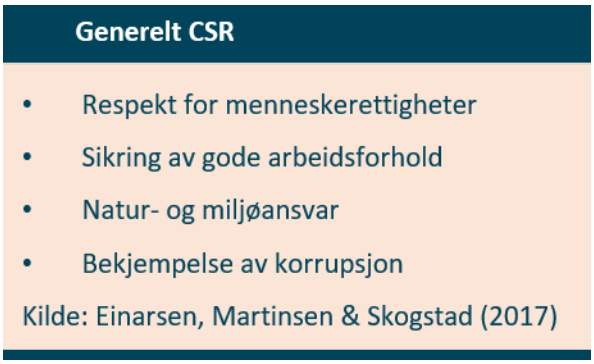
Bruken av informasjonskapsler reguleres i Ekomloven §2-7b. Denne lovbestemmelsen er relevant i lys av GDPR-regelverkets påvirkning på norske netthandelsaktører. Ifølge lovbestemmelsen er det ikke lov å bruke informasjonskapsler uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til bruk av informasjonskapsler (Nasjonal kommunikasjonsmyndighet, 2019). Unntaket er nødvendige informasjonskapsler som ikke samler inn persondata (Cookie Information, 2019).

Samtykke anses som avgitt ved en forhåndsinnstilling i nettleser på at man aksepterer bruk av informasjonskapsler (Nasjonal kommunikasjonsmyndighet, 2019). Informasjonen skal være lett synlig og det skal tydelig fremkomme at nettstedet informerer om bruken av informasjonskapsler (Nasjonal kommunikasjonsmyndighet, 2019).

3.3. Samfunnsansvar (Corporate Social Responsibilty - CSR)

Med samfunnsansvar mener vi bedriftenes ivaretakelse av sitt samfunnsansvar og hvordan de opptrer overfor samfunnet. Samfunnsansvar handler bl.a. om hvilke standarder bedrifter har når det gjelder helse, miljø og sikkerhet (Christensen & Sogner, 2013).

Regjeringen (2017) definerer samfunnsansvar slik: *«Med samfunnsansvar menes hvilket ansvar selskaper forventes å påta seg overfor mennesker, samfunn og miljø som påvirkes av virksomheten, dvs. hensyn utover det som er pålagt ved lov»*.



Figur 8 – Generelt CSR

Carroll (1991) referert i Christensen & Sogner (2013, s. 85) har utarbeidet en modell som beskriver bedriftens samfunnsansvar. Denne består av fire komponenter: ansvarlighet, lovlydighet, etisk opptreden og ansvaret for å delta og bidra i samfunnet på en god måte.

Gjennom å ta samfunnsansvar kan bedriftene oppnå økonomiske gevinster. For eksempel kan det å ta samfunnsansvar føre til bedre omdømme, redusert risiko,

økt attraktivitet for ansatte, samt at bedriften kan bli oppfattet mer positivt av myndighetene og og andre (Einarsen et al., 2017).

3.4. Etikk

Kvalnes (2012) referert i Christensen & Sogner (2013, s. 152) definerer etikk slik: «Systematisk refleksjon over hva som er rett og galt i omgang med mennesker». To sentrale faktorer i etikken er at det knytter seg opp mot handlinger og tankemessige prinsipper (Brønn & Arnulf, 2019).

For å forklare etikk kommer vi ikke utenom begrepet moral. Ifølge Kvalnes (2012) referert i Christen & Sogner (2013, s. 152) er moral er et annet ord for holdning, mens etikk er å begrunne moralen. Forretningsetikk handler om hvordan enkeltpersoner eller hele organisasjoner reflekterer over sine moralske utfordringer (Kvalnes, 2012, referert i Christensen & Sogner, 2013, s. 165). Navigasjonshjulet er et verktøy for å analysere hvorvidt de handlingsalternativene man står ovenfor er etiske eller ikke. Navigasjonshjulet deles inn i jus, identitet, moral, omdømme, økonomi og etikk (Kvalnes, 2012, referert i Christensen & Sogner, 2013, s. 165).

Kilde: (Kvalnes, 2012, referert i Christensen & Sogner, 2013, s. 165)

Figur 9 – Navigasjonshjulet

3.5. Risk Management

Det er ikke alle områder innenfor risk management som er relevant for oppgaven. Vårt fokus vil være på internkontroll knytte opp mot personvern. Ved god internkontroll med hensyn til personvern skal virksomheten sikre at personopplysninger behandles i samsvar med regelverket (Datatilsynet, 2018c).

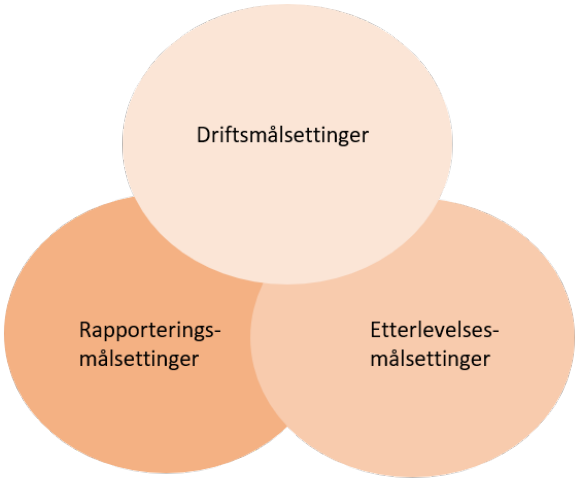
Ifølge Moen & Havstein (2017) er internkontroll et begrep som benyttes i forbindelse med styring og kontroll av organisasjoner. Internkontroll kan ses på som et verktøy som skal sikre at virksomheten når fastsatte mål, at ressurser blir tilfredsstillende forvaltet, at rapportering er pålitelig og at lover og regler overholdes (Moen & Havstein, 2017). Videre definerer Moen & Havstein (2017) begrepet internkontroll slik: "De strukturene og prosessene som er etablert for å styre og kontrollere en virksomhet – herunder også identifikasjon og styring av risiko".

Hensikten med internkontroll er å etablere kontrollsystemer som fjerner eller reduserer risikoen for at det oppstår uønskede hendelser (Moen & Havstein, 2017). COSO-rapporten er et rammeverk for internkontroll og har vært det viktigste bidraget for internkontroll hittil (Moen & Havstein, 2017).

3.5.1. COSO-rapporten

Akronymet COSO står for «The Committee of Sponsoring Organizations of the Treadway Commission» og er en amerikansk stiftelse med bakgrunn i regnskaps-, revisjons- og ledelsesmiljøer (Moen & Havstein, 2017). COSO ble opprettet i 1985 etter en rekke økonomiske skandaler som høy inflasjon, høye rentesatser og og aggressive fremgangsmåter for finansiell rapportering (Moeller, 2007). Hensikten til COSO var å sikre effektiv forretningsdrift og forbedre den finansielle rapporteringen (Moen & Havstein, 2017). I 1992 publiserte COSO sin rapport om internkontroll som et rammeverk for å forbedre/utvikle styrings- og kontrollrutiner (Moen & Havstein, 2017). COSO-rapporten om internkontroll vektla virksomhetsledelse, styrearbeid, etikk og internkontroll. I 2013 kom en oppdatert versjon som var bedre tilpasset endringene i næringslivet siden 1992 (Moen & Havstein, 2017).

COSO-rapporten for internkontroll er sammensatt av tre overordnede målsettinger som er vist i figur 10.



Kilde: Moen & Havstein (2017)

Figur 10 – Målsettinger i internkontroll

Målsettingene må ses i sammenheng, og illustrerer hvordan kvaliteten i internkontrollen avhenger av sammenhengen mellom målsettingene. Internkontrollen består av fire komponenter:

- **Internt kontrollmiljø:**
  Integritet og etiske verdier, holdninger til kontroll og styring i en organisasjon og fordeling av ansvar.
- **Risikovurdering:**
  Identifisering og vurdering av risikofaktorer som kan påvirke måloppnåelsen.
- **Informasjon og kommunikasjon:**
  Identifisering, registrering, bearbeiding og kommunikasjon av informasjon, slik at ledelsen og ansatte har nødvendig informasjon for å kunne utføre sine oppgaver.
- **Oppfølging:**
  Vurdering og oppfølging av internkontrollen og hvorvidt den fungerer som planlagt.

(Moen & Havstein, 2017).

COSO-rapporten er et rammeverk og kan brukes til å forstå hvilke elementer som påvirker internkontrollen i en organisasjon. Rammeverket brukes til å utforme og vurdere hva som er hensiktsmessig og effektiv internkontroll, men gir ikke noe oppskrift på hvordan internkontroll skal utformes eller iverksettes (Moen & Havstein, 2017).

3.5.2. ISO 27000-serien

ISO er den internasjonale standardiseringsorganisasjonen og er et verdensomspennende forbund av nasjonale standardiseringsorganisasjoner (Moen & Havstein, 2017). ISO-seriene inneholder prinsipper og generelle retningslinjer for risikostyring. Den er ikke utarbeidet for noen spesielle bransjer eller virksomhetsområder og kan benyttes av alle virksomheter (Moen & Havstein, 2017).

Moen & Havstein (2017) definerer helhetlig risikostyring som «en prosess gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og for å håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetens måloppnåelse».

For vårt formål er ISO 27000-serien den mest relevante. Denne standarden tar for seg informasjonssikkerhet og er det mest utbredte og omfattende rammeverket for styring, planlegging og implementering av informasjonssikkerhet (Moen & Havstein, 2017). ISO 27000-serien tar for seg prosesser, roller, ansvar og krav som bør inngå i alle nivåer av informasjonssikkerhet. Den inneholder flere mål og skal gjennom involvering av interessenter og sikring av gode risikostyringsprosesser støtte under virksomhetens måloppnåelse og etterlevelse av krav som stilles til virksomheten (Moen & Havstein, 2017). ISO 27005 er en av de mest sentrale standardene under ISO 27000-serien. ISO 27005 er et rammeverk for identifisering og håndtering av risiko knyttet til informasjonssikkerhet (Moen & Havstein, 2017).

3.6. Sammenheng mellom teori og problemstilling

Figur 11 – Sammenheng mellom teori og problemstilling

For å vurdere hvordan GDPR-regelverket har påvirket norske netthandelsaktører har vi anvendt pensum om GDPR som tar for seg de viktigste endringene sett fra et bedriftsperspektiv. Vi kan dermed vurdere endringene i lys av de omstillinger dette har ført til, og hvordan GDPR-regelverket har påvirket norske netthandelsaktører.

Informasjonskapsler omhandler digitale fotspor og vil derfor være relevant for å se på sammenhengen mellom GDPR-regelverket og regler for bruk av informasjonskapsler.

Vi undersøker også hvilke risikofaktorer virksomheten står ovenfor ved å ikke være GDPR-compliant. Risk management tar for seg internkontroll og rutiner for etterlevelsesproblematikk. COSO-rammeverket og ISO 27000-serien (herunder ISO 27005) er anvendt som et rammeverk som kan benyttes ved utarbeidelse av internkontroll.

Retten til privatliv er en menneskerettighet, og dette gjelder også digitalt. Teoretisk rammeverk innen samfunnsansvar og etikk er derfor relevant for å se på det etiske perspektivet rundt personvern.

4. Metode

I forskningsprosjekter skiller vi mellom kvalitativ og kvantitativ metode. Ifølge Sigmund Grønmo (1996) refererer begrepene kvalitativ og kvantitativ til egenskaper ved data. Kvalitative data viser til egenskaper ved et fenomen, og innsamlet data foreligger ofte i en form der de ikke uten videre kan telles opp i ulike kategorier (Johannessen, Christoffersen & Tufte, 2011). Kvantitative data derimot, er tilrettelagt på en slik måte at kjennetegnene ved et fenomen kan telles opp, og innsamlet data kan i stor grad struktureres (Johannessen et al, 2011). Den kvalitative metoden har en induktiv tilnærming, som vil si at man innhenter data for deretter å utvikle en teori basert på resultatet av analysen (Bryman & Bell, 2011).

Vi skiller mellom tre forskjellige forskningsdesign:

- Undersøkende: Formålet er å finne nye perspektiver og gi innsikt og forståelse.
- Beskrivende: Formålet er å kartlegge variabler og gi en beskrivelse av situasjonen eller fenomenet.
- Kausalt: Formålet er å undersøke sammenhengen mellom variabler.

(Saunders, Lewis & Thornhill, 2016), (Sander, 2017)

Målet med vår oppgave er å undersøke hvordan GDPR-regelverket har påvirket norske netthandelsaktører og hvilke risikoer de står ovenfor ved å ikke etterleve regelverket. Det er således mest hensiktsmessig med *kvalitativ* metode med en *induktiv* tilnærming. GDPR er et nytt regelverk og det finnes derfor lite etablert teori om regelverket vi undersøker. Data er innhentet i hovedsak gjennom kvalitative intervjuer, i tillegg til relevant litteratur og sekundærdata. Dette er derfor en *undersøkende* og *eksperimenterende* oppgave med et *kausalt* forskningsdesign. Videre i metodekapittelet går vi gjennom forberedelser til oppgaven, datainnsamling, intervjuguider, analyse av data og evalueringskriterier.

4.1. Forberedelser til oppgaven

Forskningsprosessen går som regel over fire faser:

1. Forberedelse
2. Datainnsamling
3. Dataanalyse
4. Rapportering

(Johannessen et al., 2011).

Ifølge Johannessen et al. (2011) er bakgrunnen for all forskning en eller annen virkelighet man ønsker å vite mer om. Vi besluttet at vi ønsket å skrive om EUs nye personvernforordning (GDPR) og knytte denne opp mot norske netthandelsaktører. Vi ønsket å undersøke hvordan GDPR har påvirket netthandelsaktører i Norge.
Etterhvert hadde vi tema, problemstilling og vinkling klart. Vi begynte å lese enda mer relevant teori og begynte med datainnhenting gjennom kvalitative intervjuer og en kvantitativ spørreundersøkelse.

4.2. Datainnsamling

Datainnsamling er foretatt primært gjennom kvalitative intervjuer. Vi har gjennomført en rekke intervjuer med relevante aktører, både fagpersoner og norske netthandelsaktører. Intervjuobjektene har delt sine syn på muligheter og utfordringer som følge av GDPR, hvordan det har påvirket dem og hva de gjør for å sørge for etterlevelse av lovverket. Vi har intervjuet kvalifiserte personer hos relevante aktører. Alle intervjuobjektene fikk oversendt en tilpasset intervjuguide i forkant av intervjuet. Alle intervjuer ble transkribert i etterkant og ligger som vedlegg til oppgaven.

Vi har også gjennomført en kvantitativ spørreundersøkelse for medlemsbedrifter i Virke E-handel. Totalt fikk vi 25 respondenter på undersøkelsen, og innsamlede data brukes aktivt i oppgaven for å underbygge argumentasjon og refleksjoner. Vi har også innhentet relevant sekundærdata i hovedsak fra teoretiske rammeverk, artikler på internett og materiell vi har fått fra intervjuobjektene.

4.2.1. Kvalitative intervjuer

Qu & Dumay (2011) skiller mellom tre ulike typer av det kvalitative forskningsintervjuet:

- **Ustrukturert:** Uformelt med åpne spørsmål. Tema er gitt på forhånd, men spørsmålene tilpasses underveis.
- **Semi-strukturert:** Overordnet intervjuguide som en mal for intervjuet. Spørsmål, tema og rekkefølge kan variere.
- **Strukturert:** På forhånd fastlagte spørsmål og temaer med faste svaralternativer.

(Johannessen et al., 2011).

Ifølge Kvale & Brinkmann (2009) er det kvalitative forskningsintervjuet som en samtale med en struktur og et formål. Kvalitative intervjuer egner seg godt dersom man har behov for at intervjuobjektene er mer frittalende rundt et tema og kommer med egne refleksjoner (Johannessen et al., 2011). Kvale & Brinkmann (2009) hevder også at den mest effektive måten å samle informasjon er gjennom det kvalitative forskningsintervjuet (Johannessen et al., 2011). Vi ønsket med våre intervjuer at intervjuobjektene skulle få rom til å svare fritt på spørsmålene og reflektere rundt svarene som ble gitt. Alle våre kvalitative intervjuer hadde derfor en semi-strukturert utforming for å gi intervjuobjektet mer frihet. Vi mener også at dette gir de kvalitative dataene en stor grad av pålitelighet og validitet.

4.2.1.1. Utvalg av intervjuobjekter

Nøyaktig hvor mange intervjuobjekter som er hensiktsmessig for formålet er vanskelig å avgjøre, men det det bør gjennomføres intervjuer helt til intervjuerne ikke får noe vesentlig ny informasjon (Seidmann 1998; Kvale & Brinkmann, 2009). Siden vi skriver om et tema det er svært lite forskning på, har vi vært helt avhengige av å intervjue relevante fagpersoner som kan mye om temaet vi skriver om. Ettersom vi har vinklet oppgaven inn mot norske netthandelsaktører og GDPR, var vi også avhengige av å snakke med både store og små netthandelsaktører i Norge. Vi har gjennomført dybdeintervjuer med fagpersoner i Komplett Group, Elkjøp Nordic, Stayclassy, Cookie Information, Ræder Advokatfirma og Forbrukertilsynet. Alle intervjuobjektene har høy kompetanse om GDPR-regelverket og hvordan dette har påvirket virksomheter som håndterer store mengder persondata.

Dette utvalget representerer bred og ulik kompetanse der vi får et godt innblikk i hvordan problemstillingen kan besvares. Vi har vært i dialog med Datatilsynet, men vi fikk vite at det var lite de kunne tilføre oppgaven foruten informasjonen på deres nettside. Informasjonen på Datatilsynets nettside har derfor blitt brukt aktivt i analysen. Vi har også valgt å intervjue Cookie Information AS. De leverer løsninger for bruk av informasjonskapsler på nettsider. Cookie Information sitter på mye kunnskap om problematikken rundt GDPR og informasjonskapsler og er derfor tatt med som et intervjuobjekt.

Vi har hatt jevnlig dialog over telefon og e-post med en tidligere netthandels-topp i Norge. Vedkommende jobber ikke lenger med netthandel, men er likevel brukt som en sparringspartner i prosessen og har kommet med mange gode innspill. Ved henvisninger til vedkommende refererer vi til informant nr. 1.

Alle intervjuene som vi har gjennomført tar utgangspunkt i problemstillingen, og baserer seg på det teoretiske rammeverket som er benyttet i oppgaven.. I forkant av utarbeidelsen av intervjuguider leste vi oss opp på relevant teori. Dette gjorde vi for å kunne reflektere rundt spørsmålene sammen med de respektive intervjuobjektene.

Alle intervjuene ble innledet med at vi presentere problemstillingen for intervjuobjektene. Vi utarbeidet to sett med individuelt tilpasset intervjuguider hvor spørsmålene var tilpasset hvert enkelt intervjuobjekt, men hadde de samme overordnede temaene: GDPR, Risk management, og andre spørsmål. Det ene settet ble tildelt norske netthandelsaktører som vi kalte *praktiserende,* mens det andre settet ble tildelt *fagpersoner*.

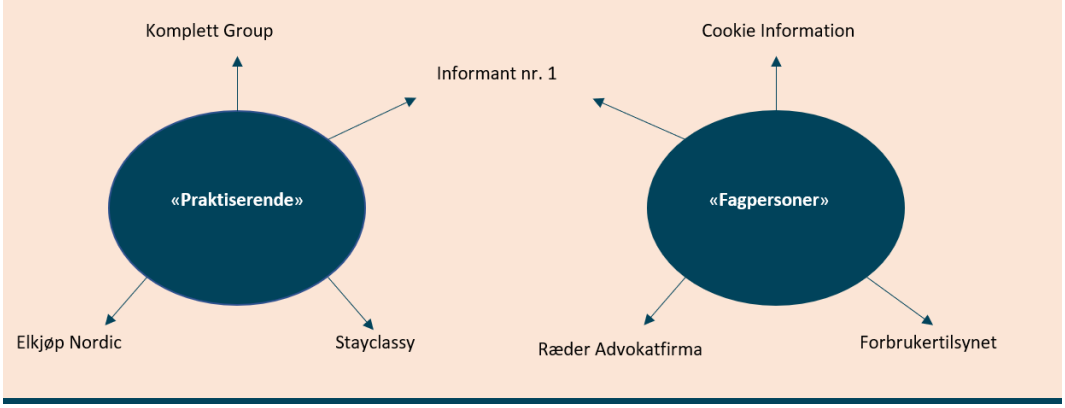
Intervjuene som ble gjort med de *praktiserende* var fokuset i stor grad rettet mot hvordan de hadde innrettet seg etter GDPR, muligheter og konsekvenser de har identifisert og hvordan de behandler og samler inn data. Intervjuene i den andre gruppen, *fagpersoner*, la større vekt på generelle utfordringer ved GDPR, hvordan dette har påvirket samfunnet og kompleksiteten av lovverket. I de fleste tilfellene var flere av spørsmålene relativt åpne slik at intervjuobjektene kunne reflektere rundt svarene. Dette gjorde det enklere for oss å stille oppfølgingsspørsmål ved behov.

Intervjuguider og informasjon om oppgaven ble oversendt til intervjuobjektene i god tid før intervjuet. Dette gjorde vi fordi det ga intervjuobjektene mulighet til å

se over og reflektere rundt spørsmålene før intervjuet. Selve gjennomføringen av intervjuene foregikk stort sett i lokalene til intervjuobjektet. Vi var to personer som foretok intervjuene, og vi byttet på å notere og stille spørsmål. Det ble gjort lydopptak av intervjuene med godkjennelse fra intervjuobjektene. I etterkant av gjennomføringen ble lydopptakene og intervjuene transkribert. Vi opplevde at de respektive intervjuene i gjennomsnitt tok i underkant av en time å gjennomføre. Som vedlegg ligger transkribering av alle kvalitative intervjuer som vi har gjennomført.

For å enklere kunne referere til intervjuobjektene har vi delt dem inn på følgende måte i analysen:

- Informant nr. 1: Tidligere direktør hos en netthandelsaktør
- Intervjuobjekt A: Komplett Group AS
- Intervjuobjekt B: Elkjøp Nordic AS
- Intervjuobjekt C: Stayclassy AS
- Intervjuobjekt D: Ræder Advokatfirma AS
- Intervjuobjekt E: Forbrukertilsynet
- Intervjuobjekt F: Cookie Information AS



Figur 12 – Inndeling av intervjuobjekter

4.2.2. Kvantitativ spørreundersøkelse

I hovedsak har vi benyttet kvalitativ metode for datainnhenting i oppgaven fordi vi mener det er mest hensiktsmessig med tanke på problemstillingen og tema. Som et supplement til de kvalitative dataene fikk vi anledning til å gjennomføre en spørreundersøkelse blant medlemsbedrifter i organisasjonen Virke E-handel. Spørreundersøkelsen ble sendt ut i nyhetsbrevet til Virke E-handel. Undersøkelsen er utelukkende besvart av norske netthandelsaktører og vi ser den derfor som

relevant for vår oppgave. For å øke antall respondenter ble vi invitert på vårsamlingen til Virke E-handel torsdag 28. mars på Soria Moria i Oslo. Spørreundersøkelsen er besvart av 22 respondenter.

Formålet med spørreundersøkelsen var å kartlegge hvorvidt det bl.a. var forskjellige oppfatninger blant store og små aktører. Undersøkelsen var relativt overordnet og gikk ikke i dybden slik som de kvalitative intervjuene. Dette gjorde vi fordi den skulle være kvantifiserbar og enkel å besvare. Vi utformet spørreundersøkelsen slik at den kunne være med på å underbygge våre funn. Spørreskjemaet baserer seg på det teoretiske rammeverket og problemstillingen.

Spørreskjemaer deles inn i tre ulike grader av strukturering:

- Prekodet: forhåndsoppgitte svaralternativer
- Åpne spørsmål: respondentene fyller selv inn svar
- Semistrukturert: kombinasjon av åpne og prekodede svar.

(Johannessen et al., 2011).

Vi har valgt å prekode spørreundersøkelsen, som vil si at den består av spørsmål med forhåndsoppgitte svar (Johannessen et al., 2011). Fordelen med prekodede spørreundersøkelser er at det gjør det lettere for respondentene å besvare undersøkelsen (Johannessen et al., 2011). Det var et kriterie for oss at det ikke skulle ta lenger enn fem minutter å gjennomføre undersøkelsen. Undersøkelsen er anonymisert for å øke påliteligheten.

For å trekke linjer og kartlegge forskjeller blant svarene valgte vi å dele inn respondentene etter omsetning i 2018. Det første spørsmålet kartla derfor omsetningen og blir benyttet til å trekke paralleller til svarene. Alle spørsmålene med unntak av det første (omsetning) ble formulert som påstander som rangeres mellom 1 (helt uenig) til 5 (helt enig). På denne måten kunne vi enklere analysere innsamlet data. Undersøkelsen bestod av syv spørsmål knyttet til GDPR og risk management.

4.3. Analyse av innsamlet data

Kvalitative og kvantitative data analyseres på forskjellige måter.

4.3.1. Analyse av kvalitative data

Kvalitative data kan analyseres på flere måter. Datainnsamling, dataanalyse og utvikling er i stor grad sammenhengende i kvalitativ forskning (Saunders et al., 2016). En måte å analysere kvalitative data er å lese nøye gjennom transkripter av intervjuer flere ganger. Vi kan ikke uten videre standardisere, organisere og kategorisere kvalitative data (Saunders et al., 2016). Innhold og struktur kan variere, men vi ønsker å se sammenhenger og forhold (Johannessen et al., 2011).

I analysen av de kvalitative dataene har vi skilt mellom to grupper: *praktiserende* og *fagpersoner*. I etterkant av alle intervjuene transkriberte vi og lagde et sammendrag som viser den viktigste informasjon fra hvert intervju. Flere av spørsmålene var tilpasset de ulike intervjuobjektene, men etter å ha gått nøye gjennom hvert intervju kunne vi likevel trekke linjer og gjøre oss opp konklusjoner. Det teoretiske rammeverket og sekundærdata er koblet inn i analysene for å bygge opp under argumentasjon og drøfting.

4.3.2. Analyse av kvantitativ spørreundersøkelse

For å analysere spørreundersøkelsen har vi gått gjennom alle svarene og forsøkt å trekke paralleller basert på omsetning i 2018. Vi har forsøkt å se sammenhenger mellom oppfatning av GDPR basert på ulik omsetning, og undersøkt hvorvidt det er forskjellig oppfatning.

4.4. Kvalitetskriterier

Vi har først tatt for oss kvalitetskriterier for kvalitative data og deretter for kvantitative data. Guba og Lincoln (1989) mener kvantitative og kvalitative undersøkelser må vurderes på ulike måter.

For kvantitative data brukes reliabilitet og ulike validitetsformer for vurdering av kvalitet. Guba og Lincoln (1989) opererer med fire mål på kvalitet for kvalitative data:

- Pålitelighet (Reliabilitet)
- Troverdighet (Begrepsvaliditet)

- Overførbarhet (Ekstern validitet)
- Bekreftbarhet (Objektivitet)

(Johannessen et al., 2011).

4.4.1. Pålitelighet (Reliabilitet)

Reliabilitet handler om hvilke data som brukes, hvordan de samles inn og hvordan de bearbeides (Johannessen et al., 2011). Kravet om reliabilitet står ikke like sterkt i kvalitativ forskning fordi det er ikke like hensiktsmessig å benytte. Dette er fordi det ofte ikke brukes strukturerte datainnsamlingsmetoder og ofte er det samtalen som er datainnsamlingen (Johannessen et al., 2011). Hvordan svarene tolkes og hvilke konklusjoner som trekkes kommer an på forskerne. I forkant av intervjuene ga vi en inngående beskrivelse av formål og oppgave. Vi forsikret oss under intervjuene at vi hadde forstått svarene riktig. Dette vil være med på å styrke reliabiliteten av innhentet data (Johannessen et al., 2011).

4.4.2. Troverdighet (Begrepsvaliditet)

Begrepsvaliditet handler om om hvorvidt forskeren måler det han eller hun har til hensikt å undersøke. Det handler om i hvilken grad fremgangsmåter og funn reflekterer formålet med studien og gir et bilde av virkeligheten (Johannessen et al., 2011). Vi ser på metoder som er brukt i datainnsamling, intervju-metode og analyse av transkripter. Alle våre intervjuer er dokumenterte gjennom sammendrag av transkripter der vi har trukket ut det viktigste fra hvert intervju. Videre har vi styrket validiteten ved å kategorisere intervjuobjektene. Videre mener vi oppgaven har en stor grad av validitet fordi vi har snakket med relevante fagpersoner med høy kompetanse om temaet.

4.4.3. Overførbarhet (Ekstern validitet)

Overførbarhet handler om hvorvidt resultater fra et forskningsprosjekt kan overføres til andre sammenlignbare områder(Johannessen et al., 2011). GDPR er et regelverk som omfatter alle virksomheter og bransjer som behandler persondata. Resultatene kan i stor grad overføres til andre bransjer og liknende formål.

4.4.4. Bekreftbarhet (Objektivitet)

Det som menes med objektivitet er at det er viktig at funnene ikke er et resultat av forskernes subjektive holdninger, men er et resultat av forskningen (Johannessen et al., 2011). Våre påstander og konklusjoner som fremkommer i oppgaven er hele tiden argumentert for og vi bruker relevante data for å underbygge påstander og konklusjoner. Vi mener derfor at dette gir oppgaven en stor grad av objektivitet.

4.4.5. Evaluering av kvantitativ spørreundersøkelse

Som nevnt har vi også gjennomført en kvantitativ spørreundersøkelse for datainnsamling vil det være relevant å evaluere denne. Vi vil kort diskutere reliabiliteten og validiteten i undersøkelsen fordi dette er kritisk i kvantitative undersøkelser (Johannessen et al., 2011).

Ettersom spørreundersøkelsen utelukkende er besvart av medlemsbedrifter i Virke E-handel, mener vi undersøkelsen har en høy grad av pålitelighet. Utvalget var direkte relevant for vår problemstilling siden den er besvart av norske netthandelsaktører. For å påliteligheten ytterligere hadde vi anonymisert undersøkelsen.

Spørsmålene er formulert slik at de konkrete og lette å forstå. Mange av svarene innhentet vi da vi besøkte vårsamlingen til Virke E-handel og vi var til stede dersom respondentene ønsket at vi skulle utdype noen av spørsmålene. Spørsmålene er utarbeidet på bakgrunn av problemstillingen for å forsikre oss om at vi undersøker det vi skal.

5. Analyse og drøfting

Funnene i undersøkelsen bygger på vår analyse av de kvalitative intervjuene og den kvantitative spørreundersøkelsen. Med utgangspunkt i det teoretiske rammeverket og sekundærdata, analyserer vi innsamlede data i lys av problemstillingen, samt i hvilken grad GDPR har påvirket norske netthandelsaktører, hvorfor regelverket tolkes ulikt og problematikken rundt GDPR og informasjonskapsler. Vi drøfter risikoene som følger av å ikke innrette seg etter regelverket.

5.1. GDPR og påvirkning på norske netthandelsaktører

Basert på de kvalitative intervjuene og sekundærdata er det vår vurdering at GDPR-regelverket har påvirket norske netthandelsaktører på flere måter. Selv om vi har hatt personvernregler i Norge siden 2000, har innføring av GDPR likevel ført til en omstilling hos norske bedrifter, og satt personvern langt opp på dagsorden igjen.

5.1.1. Administrative kostnader- og ressursbruk

Innføringen av GDPR har vært krevende for alle netthandelsaktørene (Intervjuobjekt A; B; C). Et av kravene som stilles til behandlingsansvarlig er at den registrerte skal kunne få innsyn i egne personopplysninger som er lagret hos den behandlingsansvarlige, samt retten til å få egne persondata slettet, om ikke annet følger av lov (Datatilsynet, 2018c). I den kvantitative spørreundersøkelsen og fra våre intervjuobjekter kom det frem at innføringen av GDPR-regelverket har resultert i stor ressursbruk, både i form av arbeidskraft og penger (Intervjuobjekt A; B; C; D, Vedlegg 9.8, spørsmål 6). For de små aktørene har det vært en tidkrevende prosess og krevd ressurser som ikke nødvendigvis er tilgjengelige, for å bli GDPR – compliant (Intervjuobjekt C). Videre sier intervjuobjekt C at flere små netthandelsaktører ikke har samme rutiner på håndtering og behandling av persondata som større aktører, og nøkkelpersoner har brukt all sin tid på å gjøre bedriften GDPR-compliant istedenfor for å bruke tiden på aktiviteter som er direkte verdiskapende.

En fellesnevner for de største aktørene er ressursbruken på å få kontroll og oversikt over systemene der persondata lagres, samt å forbedre og automatisere rutiner for utlevering- og sletting av persondata (Intervjuobjekt A; B). GDPR-

regelverket stiller krav til at den behandlingsansvarlige må inngå en databehandleravtaler med alle sine underleverandører (Datatilsynet, 2018d). Det har blant annet medført mye arbeid opp mot underleverandører, noe som har vært krevende ettersom store mengder persondata ofte håndteres av underleverandører. GDPR har påført næringslivet til dels store administrative kostnader og det brukes kontinuerlig ressurser på etterlevelse, blant annet gjennom investeringer i nye interne systemer (Intervjuobjekt B; D). I oppkjøringen til innføring av regelverket i 2018 var det stor etterspørsel etter ekspertkompetanse fra advokater og konsulenter, for å bistå virksomheter med råd og kompetanse på personvern og GDPR (Intervjuobjekt D). Vi har ikke fått tilgang til nøyaktige tall på hvilke kostnader GDPR. Dette skyldes at GDPR er integrert i alle prosesser og avdelinger, noe som gjør det vanskelig å estimere nøyaktig hvor mye som er brukt og hvor mye som brukes løpende (Intervjuobjekt A; B). Aktørene er likevel enige at det har kostet mye både i penger og ressurser (Intervjuobjekt A; B; C). At GDPR har krevd mye ressurser kommer frem i den kvantitative undersøkelsen, der 82% svarer bekreftende på at de har brukt mye ressurser på GDPR-regelverket (Vedlegg 9.8, spørsmål 6)

5.1.2. Fordelen av enhetlig regelverk

En av konsekvensene for GDPR sammenlignet med tidligere lovgiving, er at regelverket omfatter ikke bare land innenfor EU/EØS, men også land utenfor EU som tilbyr varer og tjenester til borgere i EU- og EØS (Datatilsynet, 2018d). Regelverket gjør ingen unntak på hvilket land den behandlingsansvarlige virksomheten kommer fra, eller størrelse på virksomheten. Med andre ord gir dette like konkurranseregler for alle netthandelsaktører, uavhengig om virksomheten er lokalisert i Norge, USA eller Kina. Dette vil utelukkende være positivt for norske netthandelsaktører, som tidligere har opplevd ulike regler avhengig av hvor virksomheten er lokalisert. En felles oppfatning blant våre intervjuobjekter er at GDPR burde vært innført for ti år siden og regelverket kommer som et etterslep i utviklingen i teknologi, bruken av informasjonskapsler og digital markedsføring.

5.1.3. Konkurransesituasjonen

Gjennom kvalitative intervju og sekundærkilder har vi sett at det å være GDPR-compliant kan medføre konkurransefortrinn, selv om det kanskje ikke er noe som forbindes med GDPR.

Tillit kan ifølge Hennyng (2019) være et konkurransefortrinn som følger av å være GDPR-compliant. Dette kommer ved å vise at man tar personvern på alvor, som medfører tillit hos ansatte, kunder, leverandører og samarbeidspartnere. Man viser også at man etterlever regelverket, som er utelukkende positivt (Intervjuobjekt E). I den kvantitative undersøkelsen trekker 27,3 % av respondentene frem økt tillit hos kunden som en viktig konsekvens av GDPR (Vedlegg 9.8, spørsmål 2). Ved å vise at virksomheten tar personvern på alvor er det trolig enklere å få samtykke til elektronisk kommunikasjon og markedsføring fra brukerne, og det kan være et konkurransefortrinn. Det er positivt for forbrukeren å motta relevant informasjon etter eget ønske (Intervjuobjekt B).

5.1.4. Kompetanse

I 2017 gjennomførte teknologiselskapet Atea en undersøkelse blant 611 norske bedriftsledere, hvor formålet var å avdekke kompetanse knyttet til personvern. Fra undersøkelsen fremkom det at 4 av 5 norske bedriftsledere ikke hadde satt seg inn i den nye personvernforordningen og 60% var usikre på om de kunne legge frem dokumentasjon på hvordan deres bedrift håndterte personopplysninger (Eidem, 2017). I en undersøkelse gjennomført av NTT Security i 2017 ble holdninger til risiko og informasjonssikkerhet hos virksomhetsledere i 11 land undersøkt. Resultatet viste at 53 % av de norske bedriftslederne som var med i undersøkelsen mente at GDPR ikke angikk deres virksomhet (Brombach, 2017).

Med dagens fokus på teknologi og digitalisering antar vi at omtrent alle norske virksomheter blir påvirket av GDPR på en eller annen måte. Tidligere var personlovgiving noe de færreste hadde tilstrekkelig kompetanse om, men våre intervjuobjekter i gruppen *«fagpersoner»* har forklart at gjennom det siste året har kompetansen om personvern og GDPR økt relativt mye, og at virksomhetslederne har vært tvunget til å gjøre seg kjent med rutinene for håndtering av persondata (Intervjuobjekt D; E). Kompetansen rundt personvern har økt betraktelig i tiden fra undersøkelsen ble gjennomført og til innføringen av GDPR.

5.1.5. Økonomiske gevinster

Vi ser fra intervjuene at den gjennomgående innstillingen til GDPR er at innføringen har vært tidkrevende og komplisert, men også nødvendig. Ingen av netthandelsaktørene vi intervjuet belyste hvilke økonomiske gevinster en kan oppnå ved å være GDPR-compliant og ved ha kontroll på dataene. Dette forteller oss at de negative sidene har vært vektet, og mange har ennå til gode å se de konkrete positive sidene ved loven utover kun nødvendigheten.

I dag er det enkelt og rimelig å samle inn- og lagre data, og følgelig enklere å miste oversikten over hvilke data som er samlet inn og hva de brukes til (Rustad, 2017). I tråd med veksten i netthandelen antar vi at mengden persondata også vil øke. Rustand (2017) erfarer at en kan oppnå økonomiske gevinster ved å være GDPR-compliant og ha kontroll på innsamlet data. Ettersom netthandelsaktører samler inn mye persondata, er det flere fordeler ved å ha kontroll på data, eksempelvis trenger man kun å lagre dataen som er relevant og slipper å lagre mengder med usortert data. Dette vil være kostnadsbesparende i lengden. Videre kan gode lagringsrutiner begrense og/eller forhindre uønskede hendelser, som potensielt kan føre til sanksjoner og en slipper å bruke ressurser på å følge opp feil (Rustand, 2017).

Intervjuobjekt E sier at ved å implementere gode rutiner for håndtering av data ved innføringen av GDPR, vil man i stor grad kunne ha trygghet dersom det er gjort en ordentlig og grunnleggende jobb. Økonomisk sett kan man være sikker på at personopplysningen blir håndtert i samsvar med loven, og ressurser kan brukes på andre områder i virksomheten (Intervjuobjekt E). Intervjuobjekt B sier blant annet at de har et eget system hvor samtykker og persondata bli systematisk lagret. På den måten har de full kontroll over hvilke data de har, og hva den brukes til.

Ifølge Tøndel (2017) er GDPR kun en begynnelse på innskjerpingen av personvern og GDPR legger opp til etterkontroll hvor det kan komme mer detaljerte regler (Wessel-Aas & Ødegaard, 2018). Dette tilsier at det vil lønne seg å være GDPR-compliant for å møte fremtidens reguleringer på best mulig måte.

5.2. Ulike tolkninger

Et felles syn hos våre informanter er at GDPR-lovverket er komplekst og gir i stor grad rom for egen tolkning (Intervjuobjekt A; B; D; E). Flere har benyttet seg av ekstern juridisk hjelp, og har opplevd at selv jurister svarer vagt på enkelte spørsmål rundt GDPR (Intervjuobjekt A). Det kan også se ut som loven tolkes ulikt basert på hvilken jurist som har vært involvert (Intervjuobjekt B). Dette tilsier at heller ikke «ekspertene» på området er helt klar over hvordan loven skal tolkes, og hva som er lov og ikke. Regelverket er på noen områder mindre detaljert enn tidligere, som også gjør at flere av bestemmelsene er opp til tolkning (Wessel-Aas & Ødegaard, 2018).

Et gjentagende spørsmål flere aktører har stått ovenfor er hvem som er databehandler og hvem som er behandlingsansvarlig. Forskjellen illustreres i tabellen nedenfor.

Behandlingsansvarlig	Databehandler
• Bestemmer formål med behandlingen av personopplysningene. • Ansvarlig for behandlingen. • Ansvarlig for å behandle personopplysninger etter lov.	• Håndterer og behandler personopplysninger på vegne av behandlingsansvarlig • Ofte en underleverandør eller samarbeidspartner • Kan ikke bestemme formål

Figur 13 – Behandlingsansvarlig og databehandler, (Datatilsynet, 2018a).

Grunnen til at flere aktører er usikre på dette spørsmålet er fordi praksisen er varierende (Intervjuobjekt A). Google er i så måte et godt eksempel, og det kan spekuleres i hvorvidt de gjør det med vilje eller ikke. Google kan ofte opptre både som databehandler og behandlingsansvarlig (Intervjuobjekt D), og man skal kjenne godt til personvernserklæringen til Google for å skjønne hvordan de behandler data. Etter å ha lest personvernserklæringen kan det også stilles spørsmålstegn ved om de bruker persondata til andre formål enn det de også har oppgitt (Intervjuobjekt D).

Dette strider i så fall mot GDPR-regelverkets krav til enkelhet og åpenhet.

Punktet i loven som tar for seg databehandler og behandlingsansvarlig er likevel nokså klar. Vi mistenker at den ulike tolkningen på dette punktet kommer av ulike insentiver fra bedriftene til å gjøre det mer komplisert enn det er, fordi det direkte

svekker mulighetene til bruk av informasjon. Dette kommer også frem i intervju med intervjuobjekt D.

Intervjuobjekt E sier at EU-regelverk har en tendens til å være mer kompliserte enn nødvendig. For å illustrere dette er det foretatt en tekst-analyse av GDPR som viser hvor lang tid en gjennomsnittlig person trenger for å tolke og forstå lovteksten i sin helhet. Konklusjonen på denne analysen viste at en gjennomsnittlig person trenger 40 år med utdanning fra universitet- eller høyskolenivå for å forstå lovverket fullt ut (Intervjuobjekt E). Det er altså helt klart et komplisert lovverk, og dette gir rom for mange fortolkninger.

5.3. GDPR-regelverket og Ekom-loven - en gråsone

Det er enighet blant våre intervjuobjekter at innføringen av GDPR-regelverket har vært nødvendig, men at regelverket er vanskelig å tolke. Parallelt med GDPR reguleres bruken av informasjonskapsler i Ekomloven §2-7b. Som redegjort for i kapittel 3.2, er det ikke krav til aktivt samtykke ved bruk av informasjonskapsler. Det er tilstrekkelig for virksomheten å opplyse om bruken, og at brukeren har godtatt forhåndsinnstilling som er gjort i nettleseren (Nasjonal kommunikasjonsmyndighet, 2019). GDPR-regelverket krever derimot at brukeren aktivt må samtykke til bruk og formidling av persondata.

Det er hovedsakelig tredjeparts informasjonskapsler som deler persondata (Intervjuobjekt F), og siden ekomloven §2-7b ikke stiller krav til aktivt samtykke, oppstår det gråsoner. Uklarheten om krav til samtykke gjør det også vanskeligere å tolke hva som er lov, og to av *fagpersonene (Intervjuobjekt D; F)* på området har ulik oppfatning på hva som er lov. Det er en kjent sak at EU for tiden jobber med en ny e-privacyforordning som vil stramme inn reglene for bruk av informasjonskapsler og stille strengerer krav til samtykke (Wessel-Aas & Ødegaard, 2018). Forordningen vil også være i tråd med GDPR-regelverket slik at man unngår gråsoner og feiltolkning (Intervjuobjekt D). Våre intervjuobjekter mener at dette er nødvendig, og at regelverket vil bli enklere å tolke.

5.3.1. Analyse av informasjonskapsler hos norske nettbutikker

I samarbeid med Cookie Information AS har vi analysert et utvalg norske netthandelsaktører og hvordan de bruker og opplyser om bruken av informasjonskapsler. Analysen består av 48 tilfeldig valgte norske

netthandelsaktører, og vi går nærmere inn på fem av dem. Ifølge GDPR-regelverket skal virksomheten vite hvem de deler persondata med, informere om hvem man deler dataen med og innhente samtykke (Datatilsynet, 2018d). Et problem med deling av persondata med tredjeparter er at persondata kan bli solgt til andre aktører. Kjøper kan i ytterste konsekvens være en konkurrerende virksomhet som igjen kan bruke persondata til målrettet markedsføring (Vedlegg 9.9). Analysen ligger som vedlegg til denne oppgaven (Vedlegg 9.9).

Mange av de undersøkte nettshandelsaktørene har løsninger der de ikke opplyser om hvilke informasjonskapsler de benytter, og hvem de deler data med. Mest sannsynlig er de heller ikke klar over det (Cookie Information, 2019). Flere av nettstedene deler også data med land som f.eks Russland, Kina og Jomfruøyene, som er usikre tredjeland som ikke oppfyller kravene til tilfredsstillende personvernlovgivning (European Commission, u.å). De 48 norske nettbutikkene i utvalget hadde totalt utplassert 914 informasjonskapsler og 214 av disse informasjonskapslene var relatert til markedsføring (Vedlegg 9.9).

Vi har gått nærmere inn på fem av netthandelsaktørene og analysert deres bruk av informasjonskapsler. I analysen ser vi kun på markedsførings-informasjonskapsler, ettersom det er disse som deler persondata. Fullstendig tabell i vedlegg.

Kategorier av informasjonskapsler				
Netthandels-aktør		**Markedsføring**	**Antall over 12. måneder**	**Maks år registrert**
Komplett.no	Opplyst (nett)	9	1	3 år
	Faktiske (CI)	5	2	2 år
	Avvik	**-4**	**1**	
Fjellsport.no	Opplyst (nett)	10	3	2 år
	Faktiske (CI)	89	7	4 år
	Avvik	**79**	**4**	
Dressmykid.no	Opplyst (nett)	0	0	
	Faktiske (CI)	7	1	2 år
	Avvik	**7**	**1**	
SunKost.no	Opplyst (nett)	19	2	4 år
	Faktiske (CI)	28	2	4 år
	Avvik	**9**	**0**	
Zalando.no	Opplyst (nett)	56	0	
	Faktiske (CI)	15	3	10 år
	Avvik	**-41**	**3**	

Figur 14 – Analyse av informasjonskapsler (Tallene i tabellen på forrige side er hentet 21.05.2019) – Faktisk (CI) = informasjon fra Cookie Information.

Tar vi eksempelvis for oss informasjonskapsler relatert til markedsføring, ser vi av figuren at tre av de fem utvalgte netthandelsaktørene har flere informasjonskapsler

for markedsføring enn de opplyser om. Dette kan tyde på at alle de fem aktørene deler persondata med tredjeparter som de ikke er klar over. Det største avviket finner vi hos Fjellsport.no, med et avvik på 79 informasjonskapsler.

Det er bekymringsverdig hvis det er slik at de fleste norske netthandelsaktører deler persondata med tredjeparter uten å ha informert brukerne og innhentet samtykke til dette. Avvikene kan skyldes at det ligger gamle informasjonskapsler plassert på nettsiden som sender data videre til andre aktører, uten at eierne av nettsiden er klar over det. Dette er likevel virksomhetens ansvar, og det strider med GDPR-regelverket fordi den behandlingsansvarlige deler persondata med tredjeparter uten å opplyse om det. Det er heller ikke utenkelig at avvik mellom faktiske og opplyste informasjonskapsler også betyr at virksomheten ikke har avtale med den/de som etter loven defineres som databehandlere.

5.3.2. Cookie Information AS – Analyse av norske offentlige nettsteder

Cookie Information AS gjennomførte i 2019 en undersøkelse om informasjonskapsler på offentlige myndigheters nettsider (Cookie Information, 2019). Undersøkelsen, som inntil nylig var konfidensiell, tok for seg 113 tilfeldig utvalgte norske offentlige myndigheters nettsteder (Cookie Information, 2019). Undersøkelsen viser at 97% av nettstedene utgir informasjon til tredjeparter som brukes til markedsføringsformål uten å ha innhentet aktivt samtykke. Videre kommer det frem i rapporten at 97% av nettstedene tillater tredjeparter å spore innbyggerne i mer enn 12 måneder. Det siste oppsiktsvekkende funnet er at 35% av innsamlet informasjon overføres til USA.

Funnene som er gjort i analysen til Cookie Information kan derfor tyde på at 97% av alle norske offentlige myndigheters nettsteder deler informasjon med tredjeparter. Flere av disse brukes til markedsføring og det opplyses ikke om på nettsidene at informasjonen deles. Intervjuobjekt F sier at de har grunn til å tro at mange av de utvalget i undersøkelsen ikke er klar over dette og ikke gjør det bevisst. Dette betyr at flere offentlige nettsteder ikke oppfyller kravene til gyldig samtykke, og således er i brudd med GDPR. Dette at vi fortsatt har en lang vei å gå i Norge med hensyn til personvernsregulering når til og med myndighetene deler persondata med tredjeparter i strid med regelverket, antagelig uten å være klar over det (Cookie Information. 2019).

5.4. Risk Management – Internkontroll og etterlevelsesproblematikk

Det er flere risikoer ved å ikke være GDPR-compliant og det kan ha store konsekvenser for lønnsomhet, drift og omdømme. Gjennom innhenting av primær- og sekundærdata har vi kommet frem til flere risikoer som norske netthandelsaktører bør merke seg.

En av de største økonomiske konsekvensene ved å ikke være GDPR-compliant er at man kan bli ilagt sanksjoner/bøter opptil 4 % av årlig omsetning eller 20 millioner euro (Datatilsynet, 2018d). Andre risikoer som ikke nødvendigvis sier seg selv er tap av omdømme, tillit og selskapsverdi. Foss (2017) deler inn risiko som følge av sikkerhetsmangler i følgende tre grupper:

1. **Driftstap**

   Varslingskostnader: GDPR-regelverket stiller krav til å varsle berørte personer dersom persondata kommer på avveie. For de større aktørene kan det føre til høye kostnader i form av oppfølging og varsling til berørte parter. Undersøkelser viser at kostnader for databrudd er gjennomsnittlig 150-200 dollar per datasubjekt (Foss, 2017).

   Tap av rennomme: Ved alvorlige databrudd kan det føre til tap av renomme og kundeflukt, ved at kundene velge andre aktører der man føler større trygghet. For norske netthandelsaktører som behandler store mengder data, kan tap av renomme påvirke omsetningen betraktelig. Facebook/Cambridge Analytica- skandalen illustrerer betydningen omdømmetap for virksomheten. Analyseselskapet Cambridge Analytica hentet ulovlig ut informasjon om 87 millioner Facebook-brukere som ble brukt til å påvirke det amerikanske presidentvalget i 2016 (Bach & Høgseth, 2018). Ifølge Brekke (2018) ble det senere kjent at Cambridge Analytica skal ha påvirket 200 valg verden over. Skandalen førte til at Cambridge Analytica måtte legge ned. Det ble foreslått fra det britiske datatilsynet å ilegge Facebook en bot på fem millioner kroner. Hadde skandalen funnet sted etter innføringen av GDPR kunne boten vært i milliardklassen (Andersen, 2018).

   Skade på driftsmiljø: Netthandelen i Norge er i stor grad avhengig av informasjonsteknologi for å kunne levere varer og tjenester (Informant nr.

1). Det kan få alvorlige konsekvenser for driften om data kommer på avveie eller skades.

2. **Bøter**

   Etter innføringen av GDPR-regelverket kan virksomheter bli ilagt en bot på inntil 4 % av årlig omsetning eller 20 millioner euro for alvorlige brudd, og 2% eller minimum 10 millioner Euro for mindre alvorlige brudd . Det skal riktignok alvorlige brudd til for å bli ilagt de strengeste sanksjonene, men mange norske netthandelsaktører, som behandler store mengder data, mye vurdere mulighetene for økonomiske sanksjoner som en risikofaktor (Datatilsynet, 2018d).

3. **Erstatningskrav**

   Datatap som rammer mange forbrukere, f.eks. ved større datainnbrudd, , kan føre til store erstatningskrav mot den behandlingsansvarlige. GDPR-regelverket fastslår at tap som er påført personer på grunn av datatap, kan utløse erstatningsplikt. (Foss, 2017). For å slippe å ansvar må den behandlingsansvarlige kunne bevise uskyld. Grunnen til at virksomheten må kunne bevise uskyld er fordi det er vanskelig for et enkeltindivid å bevise at virksomheten er skyldig (Foss, 2017).

I forbindelse med håndhevelse av lover og regler er det relevant å nevne at vi hittil har sett få bøter i Norge. Om dette er fordi Norge generelt er gode på personvern eller om det skyldes at ikke datatilsynet har nok kapasitet til å følge opp alle henvendelser vil tiden vise. Datatilsynet har i underkant av 60 ansatte som skal følge opp, håndheve og rådføre om GDPR for både privat- og offentlig sektor. Intervjuobjekt E mener at datatilsynets manglende kapasitet er årsaken til at vi foreløpig ikke har sett mange brudd på GDPR-regelverket i Norge.

Frem til nå har Datatilsynet fokusert på å rådføre, skrive veiledninger og kurse om GDPR-regelverket, slik at alle virksomheter etterlever de nye kravene (Intervjuobjekt E). Det er stor grunn til å tro at vil se flere bøter fremover, men det mangler fortsatt en viktig del med E-privacy forordningen (Intervjuobjekt E).

Påvirkning på norske netthandelsaktører	Risikoer ved å ikke etterleve GDPR-regelverket
POSITIVT: • Like konkurransevilkår • Konkurransefortrinn • Økonomiske gevinster • Økt kompetanse NEGATIVT: • Kostnader og ressursbruk • Gråsoner	• Sanksjoner • Tap av tillit og omdømme • Erstatningsansvar

Figur 15 – Oppsummering av påvirkning og risiko

5.4.1. COSO-rammeverket for internkontroll og ISO 27005

Vi mener at norske netthandelsaktører kan ha fordeler av en god internkontroll for behandling av personopplysninger. Ved å ha gode rutiner for internkontroll kan norske netthandelsaktører redusere risikoene som følger av å ikke være GDPR-compliant.

Eksempelvis varslet Datatilsynet en bot til Bergen kommune på 1,6 millioner kroner som følge av mangelfull sikkerhet i datasystemene (Datatilsynet, 2018f). Dette er hittil den eneste sanksjoner vi har sett i Norge. Filer med passord og brukernavn til 35 000 brukere var tilgjengelig for elever og ansatte i skolen etter at en elev logget seg inn i skolens systemer (E24, 2018).

GDPR-regelverket stiller mindre detaljerte krav til rutiner for internkontroll og skyver hele ansvaret over på virksomheten (Wessel-Aas & Ødegaard, 2018). Alle norske virksomheter skal likevel kunne dokumentere hvordan de sikrer internkontroll i organisasjonen. Alle våre intervjuobjekter i gruppen *praktiserende* mener at de har gode rutiner for innsamling og behandling av data (Intervjuobjekt A; B; C). Samtlige respondenter i den kvantitative undersøkelsen har svart at de selv mener de har gode rutiner for innsamling og behandling av data (Vedlegg, 9.8, spørsmål 5). Det ser likevel ut som at deres rutiner for internkontroll ikke har blitt utarbeidet etter COSO-rammeverket for internkontroll, selv om dette er et av de viktigste bidragene til internkontroll (Moen & Havstein, 2017). GDPR-regelverket stiller krav til innebygd personvern, som vil si at man må dokumentere internkontroll og sørge for at personvern er en del av alle nye løsninger eller systemer (Datatilsynet, 2018c). Kravene kan være problematiske og vanskeliggjøre etterlevelse på grunn av mangel på ressurser, særlig for de

minste netthandelsaktørene. De store aktørene har ofte kapital og kompetanse til å gjøre relevante investeringer, som kan gjøre det enklere for dem å være GDPR-compliant.

Vi mener at norske netthandelsaktører bør sikre seg gode rutiner for internkontroll og iverksette tiltak for å være GDPR-compliant til enhver tid. Ved å ha gode rutiner for internkontroll kan de redusere risikoene som følger ved brudd på GDPR-regelverket. COSO-rapporten er et rammeverk for internkontroll og et verktøy for å utforme effektiv internkontroll (Moen & Havstein, 2017). For å lykkes med internkontroll må komponentene internt kontrollmiljø, risikovurdering, informasjon og kommunikasjon og oppfølging fungere i en helhetlig sammenheng (Moen & Havstein, 2017).

COSO-rapporten gir ikke noe fasitsvar på hvordan internkontroll skal utformes eller implementeres, men kan brukes til å forstå hvilke elementer som må på plass for gode rutiner for internkontroll (Moen & Havstein, 2017). På denne måten kan COSO-rapporten tas i bruk for å utarbeide gode rutiner for internkontroll innad i virksomheten.

En sertifisering i ISO 27005 kan også være hensiktsmessig for å sikre gode risikostyringsprosesser (Moen & Havstein, 2017). Ved å ha en ISO 27005-sertifisering er det ikke dermed gitt at man etterlever GDPR, men det kan gi en god indikasjon på at virksomheten håndterer informasjonssikkerhet på en god måte.

5.5. Samfunnsansvar, etikk og personvern

Etikk, samfunnsansvar og personvern henger tett sammen. Retten til privatliv og personvern er nedfelt i FNs menneskerettigheter.

Å ta samfunnsansvar handler om å påta seg det ansvaret det forventes at virksomheter påtar seg utover det som er pålagt av lov (Christensen & Sogner, 2013). I Norge er retten til personvern regulert i grunnloven og noe alle norske virksomheter må overholde. Personvern gjelder like mye på internett som overalt ellers. I analysen av norske netthandelsaktørers bruk av informasjonskapsler ble det fastslått at alle de tilfeldig utvalgte virksomhetene benyttet flere informasjonskapsler enn de opplyser om, og samler inn persondata som ikke er redegjort for, eller gitt samtykke til. Dette er ikke i tråd med GDPR-regelverket

som sier at det på forhånd skal fastsettes formål for, og tillatelse til, behandling av persondata (Datatilsynet, 2018c).

Dette illustrerer at netthandelsaktørene overser retten til privatliv, og det strider imot etiske retningslinjer og utøvelse av samfunnsansvar ved ikke å respektere menneskerettighetene (Einarsen et al., 2017).

Et annet eksempel på misbruk av personopplysninger er dersom et selskap sporer brukersesjoner på internett og kobler dette opp mot f.eks. helsetilstanden til en person, for deretter bruke informasjonen til å prise eksempelvis helseforsikringer. Dette vil i aller høyeste grad være uetisk og et misbruk av personlige data. Selv om ingen selskaper vil innrømme dette, så er det iflg. Intervjuobjekt F, ingen tvil om at det skjer. Etter vår mening vil en slik praksis på flere måter stride imot etiske verdier og utøvelsen av samfunnsansvar.

Selv om GDPR-regelverket stiller strengere krav til samtykke, har norske netthandelsaktører fortsatt en lang vei å gå. Ved f.eks. ikke å være klar over hvilke informasjonskapsler de bruker, har de ikke kontroll over hvem de deler persondata med.

På en annen side kan norske netthandelsaktører dra fordeler av å vise samfunnsansvar. Å vise samfunnsansvar kan ifølge Einarsen et al (2017) føre til økonomiske gevinster gjennom bedret omdømme og risikoreduksjon. Norske netthandelsaktører kan bli bedre oppfattet av myndigheter og lettere få finansiering (Einarsen et al., 2017). Vår mening er at å vise samfunnsansvar og utøve etiske handlinger ved å verne om retten til privatliv, vil gi norske netthandelsaktører positive bivirkninger slik det er beskrevet i Einarsen et al (2017).

Ved å anvende navigasjonshjulet kan man se hvorvidt deling av persondata til uvedkommende er en etisk riktig handling. Navigasjonshjulet deles inn i jus, identitet, moral, omdømme, økonomi og etikk (Kvalnes, 2012, referert i Christensen & Sogner, 2013, s. 165).

- **Jus:** Deling av persondata med tredjeparter er ulovlig når dette ikke er opplyst om eller man aktivt har samtykket til det.
- **Identitet:** Det skal vanskelig la seg tro at det står i tråd med verdiene til norske netthandelsaktører å misbruke deres kunders persondata.

- **Moral:** For de aller fleste vil det være moralsk feil å misbruke persondata.
- **Omdømme:** I kapittel 5.4 var vi inne på hvilke risikoer man står ovenfor dersom man ikke etterlever GDPR-regelverket.
- **Økonomi:** I kapittel 2.4 har vi redegjort for verdien av persondata. Det er ingen tvil om at det vil være lønnsomt å dele persondata.
- **Etikk:** Det skal vanskelig la seg begrunne til sine kunder hvorfor man misbruker deres persondata.

Vi ser at det eneste insentivet for å dele persondata med tredjeparter er at det økonomisk lønnsomt. Det er hverken i tråd med moral og verdi, eller positivt for omdømme. Vurdering av personvernkonsekvenser (DPIA) skal sikre at personopplysninger ivaretas (Datatilsynet, 2018c). Denne vurderingen er virksomheten selv pliktig til å gjøre. Vi kan vanskelig tenke oss at det gjort en DPIA når samtlige netthandelsaktørene fra analysen i 5.3.1 deler persondata med tredjeparter uten å være klar over det. Deling av persondata med tredjeparter uten samtykke strider imot GDPR-regelverket og er en uetisk handling.

6. Konklusjon

GDPR har påvirket norske netthandelsaktører på flere måter, men det er fortsatt et stykke igjen før regelverket er helt tilpasset dagens bruk av digitale tjenester.

Innledningsvis definerte vi følgende problemstilling:

Hvordan har GDPR påvirket norske netthandelsaktører og hvilke risikoer står de ovenfor ved å ikke etterleve GDPR-regelverket?

Problemstillingen er todelt og fokuserer på hvordan GDPR har påvirket norske netthandelsaktører, og risikoen man løper ved ikke å etterleve regelverket.

Vår analyse har avdekket at de selskapene, hvis ledere har deltatt på intervju med oss eller besvart vår undersøkelse, har brukt mye ressurser på å tilpasse seg og innføre GDPR-regelverket i virksomheten. Det har vært vanskelig å få ut konkrete tall, men oppfatningen er at innsatsen har vært betydelig. Vi har også avdekket at aktørene generelt er positive til at GDPR-regelverket har jevnet ut konkurransevilkårene på tvers av landegrensene, gjennom at GDPR-regelverket også gjelder for utenlandske aktører som selger til EU/EØS. De fleste opplever at det er et konkurransefortrinn og ta personvern på alvor og således innrette seg etter regelverket, men det har ikke vært mulig å kvantifisere de økonomiske gevinstene. De fleste mener GDPR regelverket kom 10 år for sent, og at enkelte store aktører på sett og vis har fått sette praksis og dagsorden for lenge.

Vår konklusjon er også at så lenge lovverket knyttet til f.eks. informasjonskapsler ikke moderniseres og knyttet opp til GDPR-regelverket i en eller annen form, vil det alltid være smutthull og muligheter for innhenting og bruk (og misbruk) av personopplysninger, utover det som faller inn under GDPR-regelverket.

Når det gjelder risikoer ved å ikke etterleve GDPR-regelverket, kan vi konkludere at det potensielt er stor risiko, økonomisk og omdømmemessig, og ikke innrette virksomheten etter GDPR-regelverket eller unnlate å hensynta GDPR-regelverket i internkontroll i fremtiden. Myndighetene har selvsagt betydelig økonomisk sanksjonsmulighet, men like utfordrende kan det være for bedriftens omdømme å ikke ta GDPR-regelverket og personvern på alvor.

Avslutningsvis vil vi foreslå noen konkrete tiltak, basert på våre analyser: - Etter vår oppfatning er det behov for en bransjestandard som kan gjøre det enklere for norske netthandelsaktører å vite hva som en innenfor loven. Dette gjelder både for

å vite hvordan man skal stille seg til gråsoner og hvordan man bør behandle informasjonskapsler. Behovet for en slik standard er påfallende stort så lenge e-Privacyforordningen er under revisjon.

Videre har vi identifisert et behov for å oppfordre flere virksomheter til å ha et personvernombud, selv om virksomheten ikke er pålagt dette. Norske netthandelsaktører faller utenfor pålegget personvernombud, men vi vil likevel anbefale å opprette dette. Personvernombudet vil sørge for at GDPR-regelverket overholdes og således redusere risikoen for brudd på regelverket (og potensielle sanksjoner), og kan fungere som kontaktpunkt for behandling av personopplysninger.

7. Kritikk til oppgaven

Vi har i denne oppgaven forsøkt å belyse hvordan GDPR-regelverket har påvirket norske netthandelsaktører. Våre intervjuobjekter består av både små og store aktører. En svakhet ved datagrunnlaget er skjevhet i utvalget av netthandelsaktører, der de mindre aktørene er i mindretall. Intervjuobjekt C og en del av respondentene i spørreundersøkelsen veier opp noe for skjevheten. Det ville vært mange flere potensielle intervjuobjekter som kunne bidratt til våre undersøkelser, men på grunn av manglende tid hos de ulike aktørene og usikkerhet omkring omfanget av våre undersøkelser, har vi ikke fått tilgang til flere intervjuobjekter. Vi mener dog at våre intervjuobjekter er et tilstrekkelig representativt utvalg til at vi kan trekke våre konklusjoner og besvare forskningsspørsmålene.

Det er svært lite etablert forskning å støtte seg på, da det konkrete fagfeltet GDPR er forholdsvis nytt. Vi har forsøkt å konkretisere og belyse påvirkningen på norske netthandelsaktører på en forståelig og enkel måte, og vi har forsøkt å eksemplifisere ved å vise til konkrete selskaper eller hendelser. For å få enda flere synspunkter skulle vi gjerne vært i kontakt med enda flere aktører, men vi mener at våre intervjuobjekter har kommet med mange relevante innspill og synspunkter.

8. Referanseliste

Andersen, F. (2018, 11. juli). Storbritannia foreslår Facebook-bot. *Dagbladet*. Hentet fra: https://www.dagbladet.no/nyheter/storbritannia-foreslar-facebook-bot/70006462

Bach, D. & Høgseth, M. H. (2018, 02. mai). Cambridge Analytica legger ned etter Facebook-skandalen. *E24*. Hentet fra: https://e24.no/naeringsliv/cambridge-analytica-legger-ned-etter-facebook-skandalen/24324533

Blaker, M. (2018, 27. april). Eksplosiv vekst for bruker av netthandel i Norge. *Nettavisen.* Hentet fra: https://www.nettavisen.no/na24/eksplosiv-vekst-for-bruken-av-netthandel-i-norge/3423475295.html

Brekke, A. (2018, 22. mars). Dette er Cambridge Analytica. *Urix*. Hentet fra: https://www.nrk.no/urix/dette-er-cambridge-analytica-1.13974183

Brombach, H. (2017, 24. august). Over halvparten av norske bedriftsledere tror at GDPR ikke angår deres virksomhet. *Digi.* Hentet fra: https://www.digi.no/artikler/over-halvparten-av-norske-bedriftsledere-tror-at-gdpr-ikke-angar-deres-virksomhet/404103

Brønn, P. & Arnulf, J.K. (2019). *Kommunikasjon for ledere og organisasjoner* (2. utgave). Bergen: Fagbokforlaget.

Bryman, A. & Bell, E. (2015). *Business Research Methods* (4th ed.). Oxford: Oxford Univeristy Press.

Christensen, S. (2013). CSR – Bedriftenes samfunnsansvar. I S. A. Christensen & K. Sogner, *Bedriften: kompendium HIS 3410* (s. 83-132).

Cookie Information. (2019). *Mottar tredjeparter informasjon om norske innbyggeres besøk på offentlige nettsteder?*

Datatilsynet. (2018a). Behandlingsansvarlig og databehandler. Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/behandlingsansvarlig-og-databehandler/?id=11275

Datatilsynet. (2018b). Hva er en personopplysning? Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Datatilsynet. (2018c). Virksomhetens plikter. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Datatilsynet. (2018d). Hva er nytt med personvernforordningen? Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/hva-er-nytt/

Datatilsynet. (2018e). Personvernombudets oppgaver. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/personvernombudets-oppgaver/

Datatilsynet. (2018f). Endelig vedtak om gebyr til Bergen kommune. Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2019/endelig-vedtak-om-gebyr-til-bergen-kommune/

Datatilsynet. (2015). Personprofilering på det digitale annonsemarkedet. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/rapporter-og-utredninger/personopplysninger-og-det-digitale-annonsemarkedet/

DIBS. (2018). Norsk e-handel – alt du trenger å vite e-handel i Norge 2018. Hentet fra: https://info.dibs.no/hubfs/Norsk%20e-handel%202018/Final%20report/Norsk%20e-handel%202018.pdf?hsCtaTracking=d85599d8-68fa-4209-9d16-7956f84da9cd%7C79853611-1e6b-404e-9f6d-b85fd25a0028

E24. (2018, 18. desember). Bergen kommune får straffegebyr på 1,6 millioner etter sikkerhetsbrist. *E24.* Hentet fra: https://e24.no/digital/datatilsynet/bergen-kommune-faar-straffegebyr-paa-1-6-millioner-kroner-etter-sikkerhetsbrist/24521435

Eidem, M. (2018, 18. desember). Datatilsynet varsler millionbot til Bergen kommune. *Dagens Næringsliv.* Hentet fra: https://www.dn.no/teknologi/personvern/gdpr/bergen-kommune/datatilsynet-varsler-millionbot-til-bergen-kommune/2-1-503797

Eidem, M. (2017, 18. februar). Norske ledere uvitende om ny personvernlov. *Dagens Næringsliv.* Hentet fra: https://www.dn.no/teknologi/personvern/gdpr/datatilsynet/norske-ledere-uvitende-om-ny-personvernlov/2-1-43010

Einarsen, S., Martinsen, Ø.L. & Skogstad, A. (2017). *Organisasjon og ledelse* (1. utgave). Oslo: Gyldendal Akademisk.

EU GDPR. (u.å). Information Portal. Hentet fra: https://eugdpr.org/

FN. (2018). FNs verdenserklæring om menneskerettigheter. Hentet fra: https://www.fn.no/Om-FN/Avtaler/Menneskerettigheter/FNs-verdenserklaering-om-menneskerettigheter

Forsland, V. (2018, 20. november). 350-kronersgrensen fjernes fra 2020. *E24.* Hentet fra: https://e24.no/naeringsliv/netthandel/350-kronersgrensen-fjernes-fra-2020/24498408

Foss, K. (2017, 28. mars). EUs nye personvernregler: Dette er konsekvensene av å sove i timen. *Digi.* Hentet fra: https://www.digi.no/artikler/kommentar-eus-nye-personvernregler-dette-er-konsekvensene-av-a-sove-i-timen/378590

Førsund, E. (2018, 19. april). Hva er en lead, og hva er et prospect? *Markedspartner.* Hentet fra: https://blogg.markedspartner.no/hva-er-et-lead-og-hva-er-et-prospect

Grimstad, T. H. (2018, 15. november). GDPR – uttalelse fra Datatilsynet om bruk av lyd- og skjermopptak av ansatte. *Finans Norge*. Hentet fra: https://www.finansnorge.no/arbeidsgiver/tema/arbeidslivssporsmal/malinger-og-kontrolltiltak/gdpr---viktig-uttalelse-fra-datatilsynet-om-bruk-av-lyd--og-skjermopptak-av-ansatte/

Hennyng, A. W. (2019, 15. februar). GDPR som et konkurransefortrinn – ikke bare et «nødvendig onde». *Magnus Legal*. Hentet fra: https://blogg.magnuslegal.no/gdpr-som-konkurransefortrinn-ikke-bare-et-noedvendig-onde

Hopland, S. (2019, 12. april). Opposisjonen vil avvikle 350-kronersgrensen for netthandel i sommer. *E24.* Hentet fra: https://e24.no/naeringsliv/virke/opposisjonen-vil-avvikle-350-kroners-grensen-for-netthandel-i-sommer/24601223

Høgseth, M. H. (2018, 27. september). Vekst på 17 % fra fjoråret. *E24.* Hentet fra: https://e24.no/naeringsliv/netthandel/fersk-undersoekelse-nordmenn-bruker-144-milliarder-paa-netthandel/24450737

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag* (3. utgave). Oslo: Abstrakt forlag.

Kaldestad, Ø. H. (2018, 25. mai). Dette betyr de nye personvernreglene for deg. *Forbrukerrådet.* Hentet fra: https://www.forbrukerradet.no/siste-nytt/dette-betyr-de-nye-personvernreglene-for-deg/

Kaur, S. (2005, 17. juli). Netthandel til værs. *Aftenposten.* Hentet fra: https://www.aftenposten.no/norge/i/rl8e8/Netthandel-til-vars

Kvalnes, Ø. (2013). Etikk og samfunnsansvar. I S. A. Christensen & K. Sogner, *Bedriften kompendium HIS 3410* (s. 151-208).

Moeller, R. R. (2017). *COSO Enterprise Risk Management.* New Jersey: John Wiley & Sons Inc.

Moen, T. G. & Havstein, B. (2017). *Regnskapsorganisering: Virksomhetsstyring og intern kontroll* (7. utgave). Oslo: Cappelen Damm Akademisk.

Nasjonal kommunikasjonsmyndighet. (2019). Informasjonskapsler/cookies. Hentet fra: https://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies

Nordstrøm, J. (2017, 13. september). Voldsom vekst for norsk netthandel. *E24.* Hentet fra: https://e24.no/naeringsliv/netthandel/norsk-netthandel-omsetter-for-105-milliarder-i-aar/24139840

NTB. (2017). Nordmenn handler rekordmye på nett. *Din side.* Hentet fra: https://www.dinside.no/okonomi/nordmenn-handler-rekordmye-pa-nett/70257337

Nyvold, M. (2018, 9. juni). Snart kan du selge eller donere bort de personlige dataene dine. *Teknisk ukeblad.* Hentet fra: https://www.tu.no/artikler/snart-kan-du-selge-eller-donere-de-personlige-dataene-dine/439467

Qu, S. & Dumay, J. (2011). The qualitative research interview. *Qualitative research in Accounting & Management, 8* (3), pp. 238-264. Hentet fra: https://www-emeraldinsight-com.ezproxy.library.bi.no/doi/full/10.1108/11766091111162070

Regjeringen (2017, 18. mai). Næringslivets samfunnsansvar. *Regjeringen.* Hentet fra: https://www.regjeringen.no/no/tema/naringsliv/internasjonalt-naringssamarbeid-og-eksport/samfunnsansvar/id603511/

Regjeringen (2014, 5. desember). Hva er personvern? *Regjeringen.* Hentet fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/

Rustand, E. (2017, 11. desember). Kontroll på data gir gevinst – også for GDPR-arbeidet. *Teknograd.* Hentet fra: https://blogg.teknograd.no/kontroll-p%C3%A5-data-gir-gevinst-ogs%C3%A5-for-gdpr

Sander, K. (2018, 31. mai). GDPR («General Data Protection Regulation»). *Estudie.no.* Hentet fra: https://estudie.no/gdpr/

Sander, K. (2017, 28. juli). Hva er forskningsdesign? *Estudie.no.* Hentet fra: https://estudie.no/hva-er-forskningsdesign/

Saunders, M., Lewis, P. & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Essex: Pearson Education

SSB. (2018). Fire av fem nordmenn bruker sosiale medier. *Statistisk sentralbyrå.* Hentet fra: https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/fire-av-fem-nordmenn-bruker-sosiale-medier

SSB. (2017). Tre av fire nordmenn har handlet på nett det siste året. *Statistisk sentralbyrå.* Hentet fra: https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/tre-av-fire-har-handlet-pa-nett-det-siste-aret

Taylor, H. G. (2018, 18. oktober). Vi har bare sett begynnelsen på norsk netthandel. *DNB*. Hentet fra: https://www.dnbnyheter.no/bedrift/netthandel-i-norge/

Tøndel, Espen (2017, 24. november). GDPR er bare begynnelsen. *SVW.* Hentet fra: https://svw.no/aktuelt/aktuelt/2017/november/gdpr-er-bare-begynnelsen/

Voigt, P. & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) – A Practical Guide*. Cham: Springer.

Wessel-Aas, J. & Ødegaard, M. (2018). *Personvern – publisering og behandling av personopplysninger* (1. utgave). Oslo: Gyldendal.

9. Vedlegg

9.1. Figuroversikt

9.2. Komplett Group – Intervjuobjekt A

1. **Hvordan har GDPR påvirket dere i Komplett generelt sett?**
   For oss begynte GDPR med et stort innledende prosjekt hvor vi kartla all dataen vi har samlet inn tidligere. Komplett har hatt flere ulike butikker og operert i flere ulike land, så det har derfor vært mye data. Vi begynte med å få kontroll på dette og finne ut hvor vi har data og hvilke data vi har. Ettersom GDPR går mye mer i dybden på absolutt all data, var dette en nødvendig prosess. Vi gikk over alt fra IP-adresser og eposter til søkerhistorikk. Deretter prøvde vi å bli kloke på dataen og hva vi skulle gjøre med den. GDPR har en god del klare regler, men det er også mye av det som er vage tolkninger. Vi har brukt mye tid og ressurser på å få på plass det tekniske systemet. Slette og flytte data, systemendringer og utvikling. Som følge av GDPR har alle kunder krav på at vi skal slette deres data, dette kan bety mye jobb for kundeservice ettersom mye data også kan være lagres hos våre leverandører. Om vi tar inn en pc til reparasjon blir denne sendt videre og noen andre sitter plutselig på kundens data. Kundeservice må derfor kontakte disse og be om å få dataen slettet. Vi bruker derfor kun leverandører vi vet man kan stole på, slik at vi ikke får problemer på grunn av våre leverandører.
2. **Hvilke positive og negative sider har GDPR medført for dere som netthandelsaktør?**
   GDPR har ført til et bevisst forhold til mange av detaljene. Vi har alltid hatt gode systemer for lagring av kundens data, og sikkerhet i våre nettbutikker – men dette tvang oss til å gå grundig igjennom alt som er blitt lagret. Vi har rett og slett blitt tvunget til å rydde opp i systemene.
3. **Har dere oppfattet GDPR som uklart og vanskelig å forholde seg til?**
   GDPR er vagt på en god del områder. Det kommer ikke helt klart frem hva som er riktig eller galt, og derfor mange gråsoner. Det finnes heller ingen presedens, og vi vet ikke hvordan datatilsynet eller EU vil håndheve dette. Problemet er at når vi ikke vet, kan vi heller ikke ta noen sjanser. Det er ikke sikkert at vår tolkning av loven er korrekt, og vi kan ende opp med store bøter.
4. **Oppfatter dere GDPR som nødvendig?**

Ja, det er bra at det blir mer kontroll med personlig informasjon på nett, særlig i forhold til de store aktørene som Google, Facebook og liknende. Europa har historisk sett hatt et strengere forhold til personvern enn USA, så det er bra at EU stiller internasjonale krav som er mer i tråd med vår tradisjon.

5. **Oppfatter dere GDPR som lett å sette seg inn i?**
   Nei, det er veldig mye som har vært åpent for tolkning, med mange «gråsoner» og ingen etablert bransjestandard. Men vi forventer at dette vil bedre seg i løpet av 2-3 år. Da ser vi forhåpentligvis bedre hvordan datatilsynet følger opp de forskjellige områdene, og det vil bli etablert klarere bransjestandard for hva som er godtatt/ikke godtatt.
6. **Har dere noe estimat på hvor mye GDPR har kostet dere og koster dere per i dag?**
   Det er ikke gjort noen nøyaktig regnskap for hva GDPR har kostet hos oss. I forkant har vi totalt sett brukt flere tusen timer på alt fra møter, til utvikling og research for å sikre at vi er compliant. Nå i normal drift går det fremdeles med mye tid for å etterleve GDPR, særlig i forbindelse med rutineendringer, implementasjon av nye verktøy/systemer og kundeforespørsler om sletting/flytting av data og liknende. Det er ikke feil å si at vi har brukt veldig mange timer og flere millioner. Arbeidet fortsetter kontinuerlig og trekker både tid og penger i daglig drift.
7. **Hvordan er deres rutiner for innsamling, lagring og behandling av personlig data?**
   Her følger vi lovverket etter punkt og prikket. Alt blir gått igjennom fra bunn av, alt må være dokumentert og vi må dokumentere formålet. Vi må også definere behandlingsgrunnlaget for dataen.
8. **I hvilken grad er dere innforstått med regler og retningslinjer som må etterleves?**
   Vi er meget godt informert. Det er veldig viktig at tolkningen er korrekt. Vi har også benyttet juridisk hjelp til å se på våre tolkninger av loven. Ulempen her er at vi får mer generelle svar, noe som skyldes at juristene ikke er helt sikre de heller.
9. **Hva bruker dere personlig data til i Komplett?**
   Vi har tre behandlingsgrunnlag.

- Etter avtale: Rett og slett det som skal til for at kunden skal kunne ha et kundeforhold. Mange legger inn kun det nødvendige.
- Automatiserte tjenester: Mail som kan sendes ut. Det skal skape en felles nytte.
- Resten er samtykkebasert: Mail, SMS, og alt av cookies, pixel.
  Hele systemet vårt er egen utviklet.

10. **Hvordan har deres måte å benytte digital markedsføring endret seg som følge av GDPR?**
    Gjennomsiktighet for kunden. Med dette menes at personvernerklæringen på våre nettsider er oppdatert med veldig mye informasjon. Den skal dekke alt av det GDPR krever. Denne er også automatisk knyttet opp mot «pop-up». Vi har også som nevnt hatt mye kundedata som har vært samlet inn tidligere. Alt dette har vi gått igjennom og mye er slettet. Vi har begynt fra bunnen. Vi har også endret automatiske meldingsutsendelser. Endret mailmaler og sluttet å bruke funksjoner i Google.
11. **Er dere kjent med COSO-rammeverket om internkontroll og har dere tatt dette i bruk?**
    Jeg er ikke kjent med COSO-rammeverket for internkontroll, og tror ikke vi har benyttet dette i utarbeidelsen av rutiner for internkontroll.
12. **Andre kommentarer eller områder dere ønsker å belyse?**
    GDPR burde vært innført for 10 år siden. Regelverket er kommet for å slukke en brann som begynte for mange år siden. I dag dominerer Facebook og Google internett, og GDPR-regelverket hadde vært enklere og lettere å forholde seg til dersom det kom tidligere. Komplett generelt ønsker å forholde seg til personvern og etterleve kravene, men det er vanskelig når det er så vagt. Det er på den andre siden bra at det i det hele tatt kom et slikt lovverk. Det setter personvern på dagsordenen. Man blir tvunget til å rydde opp i filer. Et av de store problemene er at regelverket er tilpasset de store aktørene. Det er ekstremt mye man skal tilpasse seg og for små og mellomstore bedrifter som ikke har ressurser kan dette bety kroken på døren.

9.3. Elkjøp Nordic – Intervjuobjekt B

1. **Hvordan har GDPR påvirket dere?**

   Det har kommet tydeligere regler på hvordan man må forholde seg til personvern og samtykke, og vi må jobbe deretter. Sanksjonene gjør at man får et bedre rotfeste for problematikken i alle ledd i bedriften. Det tas på mange måter mer på alvor når trusler om sanksjoner hele tiden henger over oss. For vår del kan jo dette også bli veldig store sanksjoner. I 2018 ble persondata førsteprioritet for oss og det var en periode det var helt kaos og det ble brukt veldig mye penger på det. Alle systemer skal begynne å snakke sammen og det skal flyte på tvers av alle avdelinger. Innføringen av GDPR har påvirket i stor grad, men det har vært greit å få en nordisk policy på det. I Elkjøp Nordic nå har vi en klar regel på tvers av alle landegrensene.

2. **Har GDPR medført at dere gjør ting annerledes nå enn før? Eventuelt hva?**

   Ja, hvertfall fra CRM-perspektivet, som vi jobber mye med. Før kunne vi sende e-poster til alle som lå i våre databaser og nå må det innhentes samtykke. Vi jobber aktivt med å innhente samtykke og var nok litt slepphendte på dette tidligere. Vi har blitt mye tydeligere på dette med samtykke og informasjon ut mot kunden. Kunden skal hele tiden vite hva vi bruker data til og det skal også være lett å melde seg ut. I tillegg til dette har det vært mye internt i forhold til interne dokumenter, rapporteringer, systemer og integrasjoner. Det har vært en stor omveltning systemteknisk. Vi har ca. 10 000 ansatte i butikk, så den største utfordringen har vært å få de ansatte i butikk til å formidle til kunden på riktig måte. Signerer man seg opp nå får man både e-post og tekstmelding om at man har samtykket, slik at det er tydelig fra første stund. Dette ble ikke gjort tidligere. Man skal vite nøyaktig hva man melder seg opp til, hva vi bruker dataene til og hvordan man melder seg av. Om man har gitt samtykke skal informasjon flyte automatisk og om man trekker samtykket skal informasjonen slettes automatisk. Så vi skal slippe å sitte for mange millioner kunder å gjøre ting manuelt. Vi har vært heldig med mange av våre underleverandører siden vi eier mange av dem selv. Vi har gjort hele GDPR-runden med de

også. Laget behandleravtaler og liknende. Vi oppfordrer kundene våre til å ta kontakt med tredjeparter selv.

3. **Hvilke positive sider har dere identifisert som følge av GDPR?**
   Det har vi absolutt. De av kundene vi kommuniserer med nå vil jo ha informasjon ettersom de har samtykket. Vi kommer derfor med relevant informasjon og det er mer seriøst nå på grunn av konkurransen. Vi har også renset hele databasen og fått vekk det irritasjonsmomentet. Det trengtes en opprydning der.
4. **Mener dere innføringen av GDPR var nødvendig? Hvorfor/hvorfor ikke?**
   Isolert sett så er det ikke så mange av reglene som er nye i Norge. På grunn av de gamle reglene og at det ikke er så mye nytt, gjør at GDPR følges bedre. Sanksjonene er jo kanskje hovedgrunnen til at GDPR følges bedre, men vi er av den oppfatning av at vi tror mange var gode på personvern også før innføringen av GDPR. Boten ligger alltid som en fungerende trussel, og var nok nødvendig for å få bedriftene til å følge lovgivningen.
5. **Hvilke utfordringer har dere støtt på med GDPR? Er noen av disse bransjespesifikke?**
   For eksempel er det jo slik at har behandlingsgrunnlag på alle kvitteringer opp til fem år på grunn av garanti. Vi trenger denne informasjonen, men må også være compliant. Klesbutikker vil for eksempel ikke være i denne situasjonen. En annen utfordring er jo å få klarhet fra jurister og klarhet mellom landene. I Danmark er det for eksempel ikke lov å innhente samtykke i butikk, man må ha en digital signatur. Dette kommer utelukkende av hvordan loven er tolket, så det er et stort rom for tolkning av loven. Det har vært utfordrende å få sletting og utdeling av informasjon til å flyte automatisk. Vi må slette og anonymisere data i et enormt maskinverk. Det har vært veldig viktig å sikre at dette skal kunne gå automatisk, men krevende å få til. Loven tolkes ulikt blant forskjellige bransjer. Min oppfatning er at det kommer an på advokaten som har tolket loven for dem, heller en bransje og virksomhet. I tillegg har det vært en stor økonomisk belastning oppe i det hele. Elkjøp som en av gigantene må bane vei for andre mindre aktører, slik at de har noe å rette seg etter. Små bedrifter har ikke mulighet til å automatisere i samme grad, men vil jo

også motta færre henvendelser. Gigantene må nok investere og bruke en del penger, så kan de små bedriftene følge etter de som har banet vei. Forhåpentligvis kommer det en bransjestandard etterhvert. Det er viktig med seminarer og workshops som det nå, det må fortsette. Sist vi var på seminar satt det tre advokater og diskuterte lovverket fordi de var uenige om tolkningen. Noe kan oppfattes som gråsoner av noen, men ikke av andre. «Ratings» og «reviews» av produkter man har kjøpt er kanskje den største gråsonen. Det trengs en bransjestandard.

6. **Hvordan sørger dere for etterlevelse av lover og regler for GDPR?**
   Vi har fått veldig tydelige rutiner, men ulike deler for ulike avdelinger. Jurister er også med på å godkjenne beslutninger for å forsikre oss om at det er innenfor GDPR, for eksempel kommunikasjonsbeslutninger. Vi har også vektlagt systemautomatikk for å få bort en del av det manuelle arbeidet der det kan være risiko. Hvis man ikke har samtykket hos oss, så finnes man ikke i systemene våre. Fra CRM-perspektivet har vi en ressurs per land som sender ut nyhetsbrev. Vi tenker mye på etterlevelse ved nye prosesser. Vi har kuttet ut muligheten til å sende ut nyhetsbrev til de som ikke har samtykket. Et sikkerhetsnett som gjør det vanskeligst å bryte reglene er viktig. Det er også veldig viktig å kunne «backtracke» hvor feiler ligger, og det gjør at vi tester mange forskjellige scenarioer.
7. **Hvordan er deres rutiner for innsamling, lagring og behandling av persondata?**
   Når det kommer til behandlingsgrunnlag, så må vi lagre kvitteringer på grunn av garanti. Det er ingen som har tilgang til disse kvitteringene. Kun noen ytterst få høyt oppe i selskapet, i juridisk avdeling. I butikken opplyses det om i kassen og man spør om kunden aktivt ønsker å samtykke til elektronisk kommunikasjon. Dersom man samtykker vil man i ettertid motta nyhetsbrev og markedsføring. Online går brukeren inn og godkjenner, så det er en veldig ryddig prosess. Det er viktig å ha det ryddig og sørge for at man sletter og har oppdatert samtykke på lengre sikt. Bedrifter kan styre selv hvor dataene lagres, hos har vi vår egne interne løsning som vi bruker. Alle samtykker og data lagres i et system hos oss som heter «Promission Master» som andre systemer kobler seg opp mot. Om man trekker samtykke slettes man automatisk fra «Promission Master» og alle andre systemer.

8. **Hva bruker dere personlige data til?**

   Først og fremst benytter vi det til garanti (kvittering) og markedsføring. I personvernerklæringer vår ramses det også opp andre forhold vi bruker personlige data til. Vi skal kunne følge opp om du har gjort et kjøp og håper å sende så mye relevant informasjon til kunden som mulig. Det tilpasses også etter massekommunikasjon og personlig kommunikasjon. Før innføringen av GDPR hadde vi en høyere kundebase vi sendte nyhetsbrev til. Vi startet litt på nytt etter GDPR og kundebasen vi kan sende til har derfor gått litt ned. Basert på click-rate, open-rate og interaksjoner vet vi at det ikke er mindre aktive brukere. «Open-rate» har gått betraktelig opp. Det kan tyde på at kundene oppfatter det som mer seriøst og at de vil ha informasjonen siden de aktivt samtykker. Jo mer data vi har, jo mer kan vi tilpasse kommunikasjonen. Dette fører til at kunden opplever informasjonen som nyttig, og dermed blir det en positiv sirkel.

9. **Hvor mye har GDPR kostet dere så langt og hvor mye koster det dere i dag?**

   Vi sitter dessverre ikke med noen konkrete tall på hvor mye det har kostet oss. Vi er midt i et systembytte og det er snakk om vesentlige investeringer på grunn av dette. Dette systembytte kom ikke nødvendigvis på grunn av GDPR, men GDPR har nok ført til litt ekstra kostnader her også. Mange IT-ressurser har utelukkende sittet og arbeidet med GDPR. Nye løsninger for hvordan gi samtykke på nett har også kostet mye penger. Vi vet at pengesummen er høy og det brukes fortsatt mye ressurser på GDPR, men vi vet ikke et helt nøyaktig tall.

10. **Er dere kjent med COSO-rammeverket og har dere benyttet dette i utarbeidelsen av rutiner for internkontroll?**

    Vi er godt kjent med rammeverket ja, men vi har ikke brukt dette ved internkontroll. Det er i stor grad våre eiere som legger føringen for internkontroll i gruppen.

9.4. Stayclassy – Intervjuobjekt C

1. **Hvordan har GDPR påvirket dere og hvilke konsekvenser har det medført for dere?**
   Etter innførselen av GDPR har vi sett noen få direkte endringer, sammenlignet med hvordan det var før. Blant annet ser vi at antall personer som melder seg på nyhetsbrev har minsket betraktelig, noe som også indirekte reduserer salgstallene. Dette er et resultat av at vi ikke lenger kan forhåndsavkrysse «motta nyhetsbrev» for å være GDPR-compliant. Vi ser også at vi må tilpasse oss mye mer når det kommer til behandling av personvern, og at det har vært nødvendig å ha mer strukturerte rutiner rundt på dette området. Dette har også påført oss kostnader og tid siden vi har benyttet egendefinerte løsninger. Vi bruker opprinnelig noen amerikanske systemer som ikke har tilpasset seg GDPR 100%.
2. **Har dere identifisert noen sider ved GDPR som kan gi dere konkurransefortrinn?**
   Vi ser ingen direkte konkurransefortrinn ved innførselen av GDPR. De større konkurrentene våre er mye bedre på personvern fra før av (Elkjøp, Power, Komplett) på grunn av større tilgang til ressurser. Vi har brukt mye tid, ressurser og penger på GDPR og kan ikke per nå se noen direkte konkurransefortrinn. Vi ser likevel at det å være GDPR-compliant kan gi konkurransefortrinn på sikt. Ved å være GDPR-compliant kan vi sende et signal til våre kunder om at vi tar deres personvern på alvor og på den måten øke tilliten til våre kunder. Jeg tror også det kan gjøre det enklere for oss å møte eventuelle fremtidige reguleringer på en bedre måte. Grunnen til at vi ikke ser det enda er fordi jeg har brukt mesteparten av min tid over en god periode på implementering av GDPR, noe som har vært krevende. Jeg har ikke fått gjort mine vanlige oppgaver som er mer verdiskapende og derfor har vi hittil ikke identifisert noen konkurransefortrinn.
3. **Har dere brukt og bruker dere mye ressurser på å bli GDPR-compliant? (Tid, penger, ressurser).**
   Det er jeg som har vært ansvarlig for implementeringen. Det vil si at jeg har måttet bruke tiden min på å få oss compliant, kontra å gjøre andre

verdiskapende aktiviteter. Dette har kostet i ressurser og kroner indirekte fordi jeg har fokusert på GDPR.

4. **Oppfatter dere det nye regelverket som uklart og vanskelig å forholde seg til?**

   Det finnes veldig mange artikler og lesestoff man kan henvise seg til, men vi skulle ønske det var en offentlig oversikt som ga et bedre bilde på hva som kreves og ikke, på lik linje med hvordan f.eks. forbrukerrådet og forbrukertilsynet formidler informasjon om blant annet forbrukerrettigheter og lignende. For mindre bedrifter som ikke har så mye penger å bruke på riktig kompetanse ser jeg at dette kan være et større problem.

5. **Har dere noen mening om hvorvidt det behøves en bransjestandard for å enklere vite hvordan man skal etterleve GDPR?**

   Ja, vi mener det er nødvendig at enten myndigheter eller fagforeninger tar ansvar. Det må bli lettere for små aktører som ikke har de største ressursene å bli compliant uten å bruke all sin tid på det.

6. **Er dere kjent med COSO-rammeverket og har dere benyttet dette i utarbeidelsen av rutiner for internkontroll?**

   COSO-rammeverket er ukjent for oss, og dette er ikke noe vi har benyttet oss av i utarbeidelsen av rutiner for internkontroll.

7. **Hvordan er deres rutiner for innsamling, lagring og behandling av data?**

   Alle kunder som registrerer seg på nettsiden vår, enten ved brukerregistrering eller handel, vil få informasjonen lagret i vår database. Det er kun noen få ansatte som har tilgang til denne brukerinformasjonen, sammen med godkjente tredjepartsprogrammer og tjenester som vi benytter oss av i eksempelvis markedsføring og lignende. Betalingsinformasjon blir lagret gjennom Shopify sin egen 256-bits kryptering som er bransjestandard for beskyttelse av betalingsinformasjon. Vi bruker tracking-tjenester som blant annet Facebook, Google og Snapchat som analyserer hvordan brukerne våre handler på siden vår, hvilke sider de besøker og lignende. Vi opplyser kunden om dette ved hjelp av en popup som de må samtykke. For meg så kan det virke som at store og små netthandelsaktører har ganske forskjellige rutiner for behandling av persondata.

8. **Mener du det er rettferdig at lovverket og eventuelle sanksjoner skal være like uavhengig av størrelse på virksomheten? Hvorfor/ hvorfor ikke?**
   Vi mener ikke at det er rettferdig at de skal være like på tvers av størrelsen på bedriften. Nå er vi ikke 100% sikre på hvilke eventuelle bøter eller straffer som foreligger ved brudd, men en «bot» i forhold til prosentvis av inntekten ser vi på som en rettferdig løsning. Å bøtelegge et nyoppstartet firma med like store sanksjoner som de hadde gjort med en markedsledende aktør er urimelig på de fleste punkter.
9. **Har dere oversikt over hvilke tredjeparter som mottar informasjon om kunden gjennom informasjonskapsler på nettsiden deres?**
   Facebook, Google og Snapchat er de aktørene som har tilgang til informasjon om kundene våre. Vi bruker også noen mindre tredjepartsapplikasjoner som har tilgang til andre typer informasjon, som blant annet Omnisend (som forøvrig er eposttjeneren vår som vi benytter oss av for å sende eposter), men som bare innhenter informasjon som vi allerede har lagret og fått samtykke av. Istedenfor å sende eposter direkte fra Shopify, så sender vi fra Omnisend.

9.5. Ræder Advokatfirma – Intervjuobjekt D

1. **Hvilke konsekvenser ser dere GDPR har hatt for bedrifter?**
   Det vi ser er at veldig mange bedrifter har brukt mye ressurser på å kartlegge sin egen bruk av personopplysninger. GDPR stiller krav til dokumentering av behandling av data, og dette gjør at bedrifter må ha et internkontrollsystem. De har måttet gå igjennom hvilke data de behandler, hvorfor de gjør det, om sikkerheten er god nok og om de har informert menneskene det gjelder godt nok. Reelt sett er bevisstheten mye større og det er brukt mye ressurser for å implementere dette.

   Rent juridisk og konsekvensene for næringslivet er at risikoen øker betraktelig. Da er det snakk om risiko for behandling av persondata og man kan få veldig høye bøter. Dette er jo nytt med innføringen av GDPR. GDPR medfører også store administrative byrder for næringslivet. Kravene til internkontroll, risikovurderinger, rutiner og dokumentasjon er omfattende. Dette betyr at for små- og mellomstorebedrifter er de

administrative kostandene veldig høye. Det er for dyrt og komplisert for de små bedriftene å etterleve GDPR. For en stor virksomhet er dette greit og slik det bør være. Det er fortsatt uavklart om reglene forstås slik at det stilles lavere krav til små bedrifter kontra store. Reglene er nye og det eksisterer ikke så mye praksis enda. Virke tok opp dette spørsmålet med Datatilsynet og mente at det må stilles lavere krav til mindre bedrifter fordi det for dyrt å etterleve det i så stor grad som de store aktørene må. Datatilsynet svarte at dette ville de ikke være med på. Kravene er for store for små bedrifter, men for de store bedriftene så er dette veldig bra. Likevel i en virkelig situasjon dersom Datatilsynet foretar et tilsyn hos en mindre bedrift, og de tilfredsstiller minimumskravene, så tviler jeg på at de vil bli bøtelagt. De vil nok kunne få litt kjeft, men ikke bøter. Datatilsynet er ikke ute etter å bøtelegge bedrifter og vil ikke gjøre dette med mindre de må, tror jeg. Mange mennesker som kunder øker risikoen for personopplysninger på avveie og kravene bør naturligvis settes høyere for bedriftene dette gjelder.

2. **Forstår deres klienter omfanget av regelverket?**
   Det er et veldig godt spørsmål. Jobben min er jo å fortelle dem hva som gjelder, men svaret på dette er både ja og nei. Det er stor forskjell på bedriftene. GDPR er stort og består av over 90 bestemmelser, og de bruker ofte advokater til å ha kontroll på alle bestemmelsene for dem. De aller største bedriftene har jo ofte personvernombud som har mye kursing i dette og sitter på mye kunnskap. Min oppfatning er at bedrifter har blitt flinke til å få kontroll over de viktigste bestemmelsene. Dette gjelder da informasjonsplikt, personvernserklæringer, behandlingsgrunnlag og meldeplikt på 72 timer ved avvik.
3. **Benytter bedrifter seg av juridisk hjelp gjennom hele GDPR prosessen eller kun som konsultasjon?**
   Varierer litt, men jeg er av den oppfatning av at de aller fleste bedrifter benytter seg av juridisk rådgivning. Ofte er det slik at mindre aktører som ofte har spørsmål får oversendt maler fra oss og blir oppfordret til å gjøre det meste selv og heller ta en sjekk med oss etterpå. GDPR er et regelverk om at bedriftene selv som skal gjøre vurderingene også får man ikke svar på testen før Datatilsynet kommer på inspeksjon eller det oppstår et avvik.

4. **Hvilke utfordringer har dere identifisert knyttet til etterlevelse av lover og regler?**

   Det er veldig mange utfordringer, men vi kan ta topp tre. I starten var det veldig sånn at bedriftene ikke hadde oversikt i det hele tatt. Det å få en oversikt over hvilke personopplysninger bedriften sitter på og hva dette brukes til. Dette er absolutt en topp en utfordring. Likevel føler jeg at dette er noe de fleste bedrifter har kontroll på nå. Dokumentasjon av behandlingssystemene og risikovurderinger på informasjonssikkerhetssiden er helt klart noe som fortjener å være på topp tre. Det at man kan dokumentere at man vet hvilke systemer man bruker, hvor persondataene våre er og at sikkerheten er vurdert. Den behandlingen og vurderingen som omfattes av dette er også en topp tre. Når det gjelder informasjonen til de berørte, altså menneskene, så synes jeg dette har vært veldig bra. Personvernerklæringer har jo bedrifter hatt lenge og har blitt jobbet mye med det siste året, så dette mener jeg har blitt mye bedre. For større aktører har det også vært jobbet mye med rutiner for innsynsbegjæringer, og mitt inntrykk er at dette er ganske godt og lever opp til standardene. Et annet punkt bedriftene også er veldig klar over er hvilke rettigheter forbrukeren har. Veldig mange bedrifter har laget rutiner for dette og hvis man kontakter de, så leverer de ut det de skal. Jeg tror også bedriftene er gode på avviksrutiner. Det er meldeplikt innen 72 timer ved avvik, og jeg mener at bedriftene bør ha systemer på dette for å fange opp disse avvikene og melde inn til Datatilsynet. Den siste topp-tre utfordringen er hvorvidt bedriftene har god nok kontroll på sikkerheten hos sine databehandlere og samarbeidspartnere. Vi ser ofte nå, og stadig økende, i saker der personopplysninger kommer på avveie at dette skyldes en systemfeil hos underleverandør. Ansvaret ligger hos den behandlingsansvarlige som er bedriften, men feilen vil ofte ligge hos underleverandørene, tror jeg. Så bedrifter bør jo på grunn av dette bli flinkere til å kontrollere sine underleverandører slik at de kan avverge disse feilene. Dette er fordi bedriften er ansvarlig for feil hos underleverandørene sine.

5. **Hvis en bedrift blir hacket og persondata kommer på avveie. Hvilke konsekvenser kan dette ha for bedriten og hvordan håndhever man det?**

Det er to typer her. Den første er i forhold til datatilsynsmyndighetene hvis du blir hacket. Jeg kan for øvrig skyte inn at det vil du bli, spørsmålet er bare når det skjer. Derfor må man ha rutiner for å håndtere det når det skjer. Spørsmålet er om man hadde for dårlig sikkerhet, eller om man har latt være å gjøre grep man burde gjort. Det må raskt vurderes om personopplysninger har kommet på avveie og om dette er et avvik som må meldes til Datatilsynet. Må også vurdere om man har en plikt til å varsle de registrerte, dette må varsles om risikoen er høy. Høy risiko foreligger som oftest når uvedkommende har fått tak i finansiell informasjon eller personnummer. Du har også den sivilrettslige siden av dette. Innføringen av GDPR har gjort det enklere for mennesker å kreve erstatning for personopplysninger på avveie. I USA har det vært et par situasjoner med for eksempel passnumre på avveie hvor et par hundre tusen ble rammet. Det er klart at dersom disse går til et gruppesøksmål og krever 100 dollar hver av deg, så kan det ha ganske store konsekvenser. Ved for eksempel hacking skal du i første omgang melde ifra til Datatilsynet om hva som har skjedd og hvilke opplysninger som er på avveie, hvilken risiko foreligger og hva som er gjort for å lukke avviket. Videre skal du melde ifra når du vet mer og om avviket er lukket.

6. **GDPR er et omfattende regelverk. Hvor sikre kan vi være på at de som bryter loven blir oppdaget?**

   Det kan vi ikke være sikre på i det hele tatt. Datatilsynet i Norge er vel rundt 60 ansatte og disse må jo prioritere hvilke bransjer og sektorer de undersøker og hvilke saker de har kapasitet til å behandle. Det er selvfølgelig veldig mye som går under radaren og som aldri blir oppdaget. På den andre siden så er jo en viktig grunn til innføringen av GDPR at myndighetene ønsker å holde Facebook, Google, Apple, Amazon og de andre store i tøylene. Det er klart at disse aktørene gjør litt som de vil fortsatt. Google ble varslet 50 millioner euro i Frankrike for brudd på GDPR og det stopper ikke Google fra å gjøre det de gjør. Det de driver med er tidvis brudd på GDPR. De har altfor vanskelig tilgjengelig informasjon om hvordan de behandler persondata og det veldig vanskelig for mennesker å finne ut av hva Google faktisk vet om dem. I tillegg hvis du har Anroidtelefon så er advertising automatisk satt på, og dette er ikke lov. Denne skulle vært av og du skulle selv satt den på dersom du ønsker

at Google skal samle inn data om deg og bruke i personalisert markedsføring. De er amerikanske og har en litt annen holdning til ting. Jeg mener at det først og fremst er Facebook og Google som myndighetene bør gå etter først fordi det blir vanskelig å forsvare hvorfor en norsk aktør skal bruke masse penger på etterlevelse av GDPR når Google og Facebook bare turer frem. Det må få konsekvenser for Facebook og Google også.

Tilleggsspørsmål: Hvor alvorlig må bruddet være før det blir ilagt sanksjoner?

Det er foreløpig lite praksis på dette. Bergen Kommune fikk jo æren av den første sanksjonen. De ble varslet en bot på 1,6 millioner kroner for svak personsikkerhet som gjorde det veldig enkelt å få ut informasjon og å logge seg inn på kommunens system. Boten er rekordhøy så langt i Norge. Det er klart at Datatilsynets holding er at det er i de alvorlige sakene at man gir sanksjoner, dette gis når de må. For eksempel ved veldig svak sikkerhet eller at det er store mengder persondata som rammes. Det er klart at for netthandelsaktører og hvis du har veldig dårlig sikkerhet, slik at uvedkommende får tak i e-post adresser som ligger inne, så er ikke dette noe som kvalifiserer til bøter isolert sett.

7. **Hvor godt håndheves loven?**

   Jeg vil si at den håndheves relativt godt. Datatilsynet har ressurser som er relativt på og de følger med. De har jo fattet vedtak også før GDPR og vi skal være klar over at GDPR er ikke så mange nye regler som kanskje media skal ha oss til å tro. For Norge sin del vil jeg si at 95% av GDPR-reglene er regler vi har hatt siden 2000. Datatilsynet har jo fulgt med i mange år og har fattet vedtak mot ulike sektorer og bransjer og pekt på hva som må forbedres og strammes opp.

8. **Dersom Google bryter loven, hva skjer? Er ikke de så store at de kan komme seg unna bøter på grunn av størrelse?**

   Det som skjer nå, det er at GDPR er jo et felles europeisk lovverk, som gjør at myndigheter i Europa koordinerer seg mot internasjonale aktører som Google. De koordinerer hvem som skal ta hvilken sak og det klages masse på Google, særlig i Irland hvor Google har sine hovedkontorer. Det er også levert inn klage på hele ad-tech industrien, altså at hele ad-tech industrien er ulovlig fordi folk vet ikke hvilke opplysninger som samles

inn og de har ikke sagt ja til det. Forbrukerrådet i Norge har også levert en klage på Google på at de benytter lokasjonsdata i apper selv om GPS er skrudd av. Denne saken ligger til behandling. Vi har denne saken i Frankrike der det er varslet en bot på 50 millioner euro på grunn av grunn på GDPR og advertisement i Android. Dette vil nok ta litt tid siden de ulike myndighetene koordinerer hvem som skal ta hvilke saker, men dette vil få konsekvenser for Google. De har ikke kommet seg unna, ikke på noen måte. Disse aktørene tjener så ufattelig mye penger at det ikke er gitt at selv større bøter er nok for å stoppe dem.

De er så store at de kan påvirke utfallet, med det mener jeg at de har ubegrensede ressurser til rådighet. De kan leie inn så mye advokathjelp de bare vil også kan de gjøre det så vanskelig for tilsynsmyndighetene som overhodet mulig. De kan påklage ethvert vedtak, som gjør at de får en ny runde og som krever masse jobb av tilsynsmyndighetene. Så ja, det er jo slik at dersom du er så stor og har så mye penger, vil du på mange måter kunne vanskeliggjøre saksbehandlingen. Du har ressurser til å slåss imot på absolutt alt, både juss og faktum og du tåler også nye rettsrunder. En mindre aktør vil ikke ha råd til dette og dersom en slik får Datatilsynet på nakken handler det om å bare gjøre som du får beskjed om. Det vil koste dem mye penger å eventuelt krangle på ting.

9. **I intervjuet med Komplett kommer det frem at det i noen tilfeller er uklart hvem som er «databehandler» og hvem som er «behandlingsansvarlig» og brukte Google som et eksempel. Kan du utdype dette?**

   Det er et veldig relevant innspill. Dette har vært et praktisk problem i næringslivet for alle parter i det siste. Det har vært mange unødvendige diskusjoner på dette om hvem det egentlig er som er databehandler her. Ofte er det slik at den som leverer en tjeneste til sluttbruker er behandlingsansvarlig. Det er egentlig ikke noe uklart i reglene hvem som er databehandler og ikke, det er bare at bedrifter har gjort veldig mye ut av det. Når det gjelder Google og en del andre aktører, så er det vanskelig å finne ut av hvem som databehandler og behandlingsansvarlig. Fordi det Google gjør er at de ofte både er en databehandler og en datainnsamler. For eksempel: Nettbutikken din går til et markedsføringsbyrå og de ønsker

re-targeting, sånn at folk som er inne på nettbutikken skal få reklame for dette når de går videre til Google. Dette betaler de Google for å få til og betaler kanskje også for Adwords. I en sånn situasjon så er utgangspunktet at Google er en databehandler, da de behandler data på vegne av nettbutikken. Problemet med Google er at de ofte gjør noe mer også, og det er her det blir vanskelig. Når du prøver å finne ut hva Google gjør og hvordan disse produktene fungerer og begynner å lese mye, så er det litt uklart. Du skjønner etter hvert at det kan være slik at Google tar vare på disse dataene og bruker de til andre formål. Cookies som Google samler inn gjennom nettsider tas da vare på og legges oppå en profil av personen som allerede ligger der som kan brukes for markedsføring for andre aktører senere. Da går Google over fra å være en databehandler til å være dataansvarlig. Da behandler de data for egne formål utover den bestillingen bedriften gjorde. Så Google er ofte begge deler også er de ikke noe flinke på å informere om når de er databehandler og når de er dataansvarlig, og det tror jeg de gjør med vilje. Det er vanskelig å avgjøre fordi du får ikke vite nok om hva de store aktørene som Facebook og Google gjør. Jeg synes Facebook er litt ryddigere når du kjøper Custom Audience tjenester og liknende. Sist jeg sjekket var de veldig klare på i sine vilkår at de er databehandler for deg og lover å slette kundelisten etter de har gjort matching mot sine medlemmer. Dette er bra, for da har vi en trygghet på at de opptrer som en databehandler og ikke noe mer.

Tilleggsspørsmål: Kan man være helt sikre på at data blir sletter dersom man ber om det?

Etter GDPR så har man rett til at opplysninger slettes, med mindre noe annet er hjemlet i loven og den retten gjelder mot alle bedrifter som måtte ha persondata om deg. For eksempel: Hadde du gått til skattemyndighetene og bedt de slette opplysningene de har om deg, så trenger de ikke gjøre dette fordi de har hjemmel i lov til å behandle dine data. Hvis du derimot går til Komplett og har kjøpt noen varer der, og ber dem slette opplysningene om deg, vil de måtte slette mesteparten av disse. Likevel kan data som er hjemlet i lov, for eksempel bokføringsloven, beholdes. Det er noen regler som gjør at de kanskje ikke må slette alt, men de må slette data som brukes til salg og markedsføring. Man kan aldri vite dette med sikkerhet, men min oppfatning er at bedriftene virkelig står på

for å etterleve lover og regler. Jeg tror du kan være sånn noenlunde sikker på at de sletter dataene dine når de skal. Bransjepraksis og GDPR-compliant er at personvernerklæringen skal være god og oversiktlig. Det skal være enkelt å få informasjon om retten din og uttrykke deg. Det skal være nok å kunne sende en mail til for eksempel Komplett der du ber om at de skal slette dataene de har om deg.

10. **Vi er fortsatt i startfasen av oppgaven, men ser at det ofte kan være selskaper som er knyttet sammen i leveransen av en vare til forbrukeren. Hvem sitter med det overordnede GDPR-ansvaret?**
    Veldig godt spørsmål, dette kommer veldig an på leveransekjeden. Her må man se på hvordan det er lagt opp, hvem som har kundekontakten og hvordan det er rigget. Det beste svaret er nok hvordan det er rigget. Eksempel: La oss si at du er mobilkunde hos Telenor, du har både mobil, IP-tv og internett fra Telenor. De leverer mobiltelefoni selv og har et samarbeid med Canal Digital som leverer deg kabel-tv. I tillegg har de en nummeropplysningsapp som de leverer selv, men henter numre fra 1881. I utgangspunktet er det slik at det er Telenor som er behandlingsansvarlige. Så viser det seg at leverandøren av kabel-tv heter Canal Digital AS, det er de som leverer kabel-tv, og da kan det være at du på et tidspunkt blir kunde av Canal Digital, helt avhengig av hvordan det er lagt opp. Da kan det være at Canal Digital blir behandlingsansvarlig for dine kundeopplysninger relatert til TV-biten, men Telenor er bare på mobiltelefoni. Så kommer dette også litt an på hvordan du oppfatter dette som kunde, hvorvidt du opplever at det er Canal Digital som leverer deg tv eller om det er Telenor. Det kommer an på hvordan det er rigget og det er mange gråsoner her. Det er klart at i det øyeblikket en leverandør som er en del av denne totale kjedeleveransen begynner å ha mye direkte kommunikasjon med deg, så taler mye for at det er de som er behandlingsansvarlige. Svaret på dette spørsmålet er at man må se på hvordan dette er satt sammen og hvordan det oppleves for deg som forbruker.
11. **Er det noen spesielle utfordringer knyttet til netthandelsbransjen, isåfall hvilke?**
    Jeg tror nok at det som definitivt er en utfordring for netthandelsaktører, men også andre aktører, er digital markedsføring med bruk av cookies og

generelt når man skreddersyr markedsføring etter data som er hentet inn. Dette er vanskelig av to grunner, både rettslig og faktisk. Det er veldig få som faktisk hvem hva som foregår her, hvilke data som samles inn, hvem som får de og hvor det blir av dem. Det er veldig få som egentlig har helt oversikt og det er dette som gjør det vanskelig rettslig. Det er vanskelig å vite hvordan du skal gjøre det rettslig når du egentlig ikke helt vet hva som foregår. Når du ikke vet hva som skjer, så er det helt umulig for deg å vurdere om det er lov eller ikke. Svaret er egentlig da at da er det ikke lov fordi du har ikke kontroll, og det skal du egentlig ha. Rettslig sett er det også litt vanskelig, for i tillegg til GDPR så har vi dette eldre e-com regelverket om Cookies. I reglene om Cookies er det slappere grad til samtykke enn det er for behandling av personopplysninger. Det er et slappere krav selv om Cookies også er personopplysninger. Man har altså to regelsett som ikke er like, som til dels overlapper hverandre. Etter å ha besøkt Zalando får man gjerne opp reklame fra dem i flere uker etterpå, og dette er faktisk lov. Jeg skal forklare hvorfor det er lov. I dems personvernerklæring så vil det stå at de benytter Cookies til det og det formålet, og de kan også da bruke denne dataen til å markedsføre personlig til deg. For at dette ikke skal være lov, så må man aktivt gå inn å skru av Cookies-funksjonen i nettleser eller på mobilen. De trenger altså ikke at man krysser av for ja eller nei, de trenger bare å gi informasjon om det. Du går så over til VG som da sjekker om det ligger noen markedsførings-cookies her, og du vil da få opp reklame fra Zalando på VG. Det er lov hvis man gjør det på den måten. Men slik det er i dag så samles det inn Cookies som videre kanskje sendes videre til Google og legges oppå en profil om deg som allerede eksisterer, da er man utenfor Cookie-reglene og innenfor GDPR. Da kreves det et frivillig samtykke for å kunne bruke disse. Da stilles det krav til at aktivt skal ha sagt «ja takk», hvis du velger å ikke aktivt trykke «ja takk», da har de ikke lov. Det er her Google er i så mange gråsoner.

12. **Hvordan påvirkes den digitale markedsføringen av GDPR? Hvordan var det før kontra nå?**

    Jeg jobber mye med digital markedsføring og det jobbes veldig mye med å lage veiledninger og bransjestandarder. Det er behov for at noen tar ansvar nå og vurderer de ulike Facebook og Google tjenestene og forteller

markedet at disse tjenestene kan bruke hvis du gjør sånn og sånn, disse er litt i en gråsone og til slutt hvilke som man bør styre unna. Jeg har også et inntrykk av at flere aktører nå holder på med å kartlegge hvilke Cookies som faktisk ligger på sin nettside. Dette gjorde man ikke så mye før og det kan ligge mange gamle Cookies fra gamle samarbeidspartnere som du ikke vet er der engang. Da vil de jo tracke brukeren din uten at du som nettstedinnehaver engang vet om det. Det blir også mye sånn advokatgreier på risikovurderinger, og hvorvidt man må slutte å bruke Google. Min vurdering er jo at slike kanaler kommer man ikke unna. Man har ikke sjanse til å komme utenom de store aktørene, Google er jo på mange måter internettet. De er annonsenettverkene. Man kommer ikke utenom det, så det man bør gjøre er å prøve å få kontroll over hva som faktisk skjer i den grad man greier det, og velge bort de tjenestene man har minst kontroll på. Det jobbes veldig mye med dette nå og alt dette med ad-tech, programmatisk og retargeting er en stor hodepine. Dette er fordi de fleste bedrifter ønsker jo å følge reglene, men det vanskelig når man ikke vet hva som skjer også har man denne uklarheten mellom Cookies-reglene og GDPR som også problematiserer.

13. **Er det forskjellige utfordringer blant store og små aktører? Hvilke?**
    Det spørs jo litt hva de driver med, i utgangspunktet har de jo de samme utfordringene. Du kan likevel se at den største forskjellen er kanskje at de små aktørene ikke har like mye ressurser til å jobbe med å få kontroll over hva som skjer. Det er enklere for de store aktørene å bruke mer ressurser på å få oversikt, gjøre det bedre, mer oversiktlig, gi ut informasjon og bruke penger på juridiske vurderinger. Jeg vil jo si at rent prinsipielt så er jo utfordringene de samme uavhengige om aktørene er store eller små. Når det er sagt så er jo en vesentlig forskjell at når man er stor aktør så har man mer personopplysninger og risikoen øker jo naturligvis i tråd med dette.
14. **Hvordan blir innholdskapsler og personalisering av markedsføring påvirket av GDPR?**
    Det blir jo påvirket. I første fase nå så har flere bedrifter valgt å tenke at Cookies er helt greit fordi det er det slappe regler på. Ofte er ikke dette riktig fordi disse cookiesene kan ofte være gamle og sende data videre til andre aktører som lagrer dem og bruker de på nytt. På denne måten er man da innenfor GDPR og utenfor Cookies-reglene. En del har da valgt å følge

Cookiereglene og basert seg på disse siden de kan det og tror at det er greit. Det som strekker seg frem nå og som er viktig det er å få trukket opp den grensen mellom GDPR og Cookies, men dette har jeg ikke sett noe til enda. Vurderingen som omhandler når man beveger seg fra Cookies og over til GDPR må trekkes og er enda uklar. Jeg har ikke sett Datatilsynet gjøre den vurderingen ordentlig foreløpig, men denne ville komme. For å gjøre det enda vanskeligere jobber også EU nå med et nytt regelverk som heter E-privacyforordningen, som blir som et slags «GDPR 2.0». Jeg vil tippe at dette regelverket blir vedtatt i 2019, og trer i kraft fra 2020. Dette kommer til å stramme inn Cookiereglene og kreve et mer GDPR-samtykke for også bruk av markedsføringscookies. Det vil si at det vil ikke være lov å bruke data til markedsføring og retargeting med mindre det kommer tydelig frem hva som skjer og man må aktivt samtykke til dette. Velger man å ikke samtykke eller å være passiv å ikke gjøre noen ting, vil det ikke lenger være lov å sette markedsføringscookies på utstyret ditt. Det blir en veldig stor endring, og den kommer ca. om to år.

15. **Hvor langt rekker cookies-reglene? Vi opplever at Norge er den «snille gutten i klassen», inntreden fra utenlandske aktører.**
    Det er helt riktig, Norge har slappere regler enn de andre landene. I Norge er det slik at dersom en nettbutikk gir beskjed om hva de bruker Cookies til, når og hvor det lagres og hvor lenge det lagres og at du ikke skrur av Cookies i nettleseren, så har nettbutikken lov til å gjøre dette. I noen land er det slik at det må poppe opp en boks nede i hjørnet som gir informasjon og brukeren må klikke ok eller les mer. I Norge er det ikke slik, da holder det med overnevnte.
16. **Ofte når man besøker nettbutikker, kommer det opp informasjon at nettsiden benytter innholdskapsler. Her kan man velge å trykke «ok» eller «les mer». Det kommer derfor ikke opp direkte om man godtar bruk av cookies eller ikke. Er dette innafor?**
    Ja, isolert sett så er det innafor etter norsk praksis. Så lenge denne informasjonen er lett tilgjengelig, gjennom for eksempel en egen Cookieerklæring eller Cookiepolicy, eller eventuelt om det står om Cookies i personvernerklæringen, så er det bra nok. Svaret isolert sett er derfor ja, dette er lov.

Vi hadde nylig et intervju med komplett om hvordan GDPR hadde påvirket dem. I det intervjuet kom det frem at de har brukt juridisk hjelp til å tolke regelverket. Da kom det frem at juristene ga generelle svar, og de mente det skyldes at juristene heller ikke var helt klar over hvordan de skulle tolke det.

17. Hvordan stiller du deg til denne påstanden?

For det første så tror jeg at den påstanden stemmer for en del jurister og advokater. Jeg tror på at Komplett har opplevd det som dette. Når det er sagt så er jobben til advokater også å ta avgjørelser når ting er vanskelig. Det jeg pleier å si er at vi må ta en posisjon. Når det gjelder netthandel og digital markedsføring, så må man ta juridisk risiko. Skal du være sikker på å ikke gjøre noe galt, så får du ikke gjort noen ting. Det som er viktig er å kartlegge og få kontroll på hvor stor risiko man tar. Det går an å gi konkrete svar, og jeg jobber med å gi konkrete svar hele tiden. De gangene det er vanskelig rettslig og faktisk og det er usikkert, så er det viktig å få frem at det er usikkert hvordan Datatilsynet vil se på det dersom de skulle komme på tilsyn. Det er alltid opp til bedriften å vurdere, men ofte er det slik at man ikke vet om man er innenfor, men har gode argumenter for at man er på riktig side av grensen. GDPR er såpass nytt at veien blir litt til mens man går. Det går ikke an å vite hvordan disse reglene vi bli forstått på en del områder, og en advokat må da vurdere og konkludere med hvorvidt dette kan være lov eller ikke basert på kilder (rettspraksis, lovverk). Ofte med GDPR kan man ikke være sikre fordi det ikke har vært prøvd før.

18. Hvordan har GDPR påvirket dere?

Det har hatt to konsekvenser for oss. For det første er jo vi også en bedrift som betyr at har måttet gjøre vår egen interne jobb med å skaffe dokumentasjon på egne interne kontroller og hvordan vi behandler personopplysningene. Tilsvarende har vi også oppdatert personvernerklæringer og gjort nye vurderinger av IT-systemer og rutiner. På den ene siden har vi måttet gjøre alt det andre som andre bedrifter også må gjøre. På den andre siden, som leverandør av advokattjenester, så har det vært et enormt trykk. Det var helt vilt i fjord, utrolig stort behov for

advokatbistand ved GDPR i fjord. Vi jobbet masse med det og det har vært mye i år også, men i fjord var det helt vilt.

19. **Mener du at Datatilsynet er for lite?**

    De har fått en del stillinger etter at GDPR ble innført. Det virker som for meg at de er store nok i Norge. De har fått til veldig mye og jeg tror de har nok ressurser til å håndheve dette i Norge. GDPR medfører jo også en del annet, blant annet har Datatilsynet en større plikt til å koordinere seg med andre myndigheter og de får også en viktigere rolle som nå skal inn når man lager bransjenormer. Det vil kreve masse ressurser av dem og det er ikke gitt at de har nok ressurser til å følge opp dette også. Når det kommer til å håndheve det vi har vært inne på i dag er min mening at de har tilstrekkelig med ressurser til å håndheve det.

20. **Andre områder som bør belyses?**

    Jeg ønsker å trekke frem at det er et stort behov for at noen kommer opp med noen kjøreregler, enten dette er myndigheter eller bransjeorganisasjoner. Noen må lage kjøreregler for hvordan man skal gå frem for å kjøpe digitale markedsføringstjenester som er helt innenfor lovverket. Det må opprettes en bransjenorm og flere må gå sammen. I virkeligheten er det ikke et alternativ å ikke kjøpe digital markedsføring. Det er vanskelig både juridisk og faktisk og virkeligheten er ikke i tråd med GDPR på dette punktet. Det er et stort behov for at bransjen (netthandel) går sammen for å lage noen kjøreregler. I forhold til Ad-tech har GDPR kommet for sent, det er rullende ball man ikke kan stoppe. I Norge kunne GDPR vært innført for 10 år siden (95% av reglene er allerede innført i Norge i 2010), men ikke nødvendigvis i andre europeiske land.

9.6. Forbrukertilsynet – Intervjuobjekt E

1. **Hva har GDPR betydd for den norske forbrukeren kontra tidligere personvernlover?**

   Mange av de grunnleggende prinsippene for forbrukeren, særlig dette med samtykke, er videreført med noe utbygging som følge av GDPR. I bunn og grunn er dette ting vi har de 20 siste årene med samtykke til behandling av personopplysninger, markedsføring og liknende. Det er helt klart at GDPR har satt et større fokus på forbrukerens rettigheter og økt oppmerksomheten rundt de grunnleggende kravene. Det er mye større oppmerksomhet rundt personvern enn det har vært tidligere, og mye av dette skyldes nok i stor grad sanksjonsregime. Det har også vært mye skrevet om i medier som også er med på å skape økt oppmerksomhet. Det er positivt fra forbrukeren at det skapes et større krav til etterlevelse fra bedrifter.

2. **Hvilke fordeler vil du si at GDPR har medført for norske bedrifter?**

   En svært viktig effekt er at man har større kunnskap om et regelverk som tidligere bare var for de spesielt interesserte. Veldig mange har bygget opp kompetanse om GDPR for å kunne gi gode råd. Det er enda flere som kan mye, og som kan gi gode råd vil jeg tro. Forhåpentligvis vil det derfor i neste omgang bli enklere for bedrifter å etterleve GDPR.

   Oppfølging: Hvilke fordeler vil du si at GDPR har medført for norske forbrukere?

   Det er litt tidlig å si i praksis. På dette tidspunktet i fjor ble det sendt ut masse mailer og informasjon. Det er klart at det har blitt tydeligere og bedre informasjon om innsamling og bruk av personopplysninger enn tidligere. Virksomheter skal ha kunnskap om dette og kunne ta gode valg basert på de opplysningene som samles inn.

3. **Kan man oppnå konkurransefortrinn ved å være GDPR-compliant? Eventuelt hvordan?**

   Generelt når vi møter bedrifter som er litt oppgitte over at vi stiller krav og diskuterer avtalevilkår, så er vi ofte inne på det at de kanskje ikke er helt enige, men at det kanskje vil være en god sak å kunne gå ut å si at man forholder seg til lover, regler og tilsynsmyndigheter. Det kan gi et konkurransefortrinn i form av at man gir et signal til omverden at man er

compliant og til å stole på. Spesielt kan det gi konkurransefortrinn sammenliknet med de virksomhetene som holder seg mer i risikosonen.

4. **Hvilke økonomiske gevinster kan det gi norske bedrifter ved å være GDPR-compliant?**

   Ved å implementere GDPR og sette et fokus på dette, vil man i stor grad kunne ha en trygghet dersom man har gjort en ordentlig, grunnleggende jobb og kan stole på at håndtering av personopplysninger foregår etter lovverket. På denne måten kan man også slippe å bruke veldig mye ressurser på dette og fokusere på andre områder i virksomheten. En annen viktig faktor er å slippe sanksjoner, men det er i de helt spesielle tilfellene.

5. **Hva vil du si er de viktigste konsekvensene som følge av GDPR?**

   Det har blitt større oppmerksomhet rundt temaet personvern og forhåpentligvis har det også blitt mer kunnskap, som igjen kan sørge for bedre etterlevelse av lover og regler

6. **Hvorfor lønner det seg for en virksomhet å ha kontroll på hvilke data man har?**

   Først og fremst slipper man å bruke masse tid og ressurser på at det dukker opp episoder der du må undersøke hva som har skjedd, gå ut med informasjon til de berørte partene, medieoppslag og liknende.

7. **Vi har sett «worst-case»-senarioer med for eksempel Cambridge Analytica. Tror du det er mulig for en norsk virksomhet å miste så mye omdømme at det fører til nedleggelse dersom de bryter med personvernreglene?**

   Forutsatt at det er en virksomhet som baserer seg på leads eller «data-broking» og det skjer på en måte som er i strid med regelverket, så kan dette skje. Egentic, et tysk firma, har blitt skrevet mye om i dagbladet og det ligger en sak inne på dem hos EU-domstolen. De henter angivelig inn samtykker gjennom konkurranser for eksempel der du kan vinne en Iphone, så samtykker man til å få spam av alle mulige aktører. Det venter en dom fra EU kan slå kroken på døra for hele denne typen virksomhet. Et annet selskap, riktignok dansk, EuroAd innhenter leads gjennom konkurranser der man samtykker til å bli kontaktet av 20-40 ulike firmaer. Mange som ikke står på listen i den opprinnelige konkurransen bruker også dette til å markedsføre.

8. **Vi har hittil sett få bøter i Norge, tror du dette skyldes at norske virksomheter er veldig gode på personvern eller har ikke Datatilsynet kapasitet til å følge opp alt? Eventuelt andre grunner?**
   Jeg tror at Datatilsynet er rundt 50-60 stykker som skal følge opp, håndheve og rådføre bedrifter med tanke på GDPR. Grunnen til at det hittil er varslet få bøter er nok fordi Datatilsynet ikke har kapasitet til å følge opp alt. Det er et enormt arbeid som Datatilsynet er satt til å gjøre og de har både offentlig og privat sektor. Primæransvaret ligger på bedriftene selv og det er neppe noen grunn til å tro at vi er bedre på personvern i Norge enn andre steder. Datatilsynet har fokusert veldig på å dette ut, holdt mange foredrag og lagd veiledninger. Datatilsyn i ulike land samarbeider, for eksempel mot Facebook og Google. Vi kan nok forvente en fase der det blir flere og flere saker etter hvert, og det vil komme flere bøter. Fortsatt mangler man en viktig bit med E-privacy-forordningen. Sannsynligvis vil denne bli vedtatt i løpet av høsten og tre i kraft fra januar 2021, forhåpentligvis. Det er mye lobbyisme fra tech-selskaper og medieselskaper. Planen var jo at også denne forordningen skulle vedtas samtidig som GDPR.
9. **Ifølge en analyse gjort av ATEA blant 611 norske bedriftsledere kommer det frem at kun 1/5 av dem hadde satt seg inn i den nye personloven. Undersøkelsen ble gjennomført i 2017. Hva er din oppfatning av kunnskapen om GDPR blant norske bedriftsledere i dag?**
   Min oppfatning er at kunnskapsnivået rundt GDPR og personvern har økt, og at det er mer kunnskap nå enn for tre-fire år siden.
10. **Ekom-loven avviker noe fra GDPR-lovverket. Kan dette gjøre det vanskelig å vite hvorvidt man er innenfor regelverket eller ikke?**
    Absolutt, dette vanskeliggjør problemstillingen. European Data Protection Board publiserte nå i mars en «opinion» der Datatilsynsmyndigheter fra forskjellige land kan stille spørsmål. Belgia hadde her et spørsmål om hvordan GDPR og cookies skal forstås med hverandre. I dag er det et direktiv som regulerer dette. Denne er oppe til forhandling nå og vil bli en forordning, som må implementeres i nasjonale lovverk. Vi har også mottatt en del henvendelser på dette området.

11. **Man ser stadig artikler om at datatilsyn i forskjellige land varsler bøter til de store selskapene som Google og Facebook. Blir det vanskelig for norske aktører å se hensikten med GDPR dersom de største aktørene fortsetter som før?**
    Jeg tror det vil være til stor hjelp når man ser at Google og Facebook får smell i store saker. Der smeller det virkelig og jeg tror etter hvert Google og Facebook må gjøre en del justeringer. Det er bare positivt at man får disse avklaringene og at norske aktører vil innrette seg etter dette.
12. **Gjennom tidligere intervjuer har vi fått vite at advokater tolker loven veldig forskjellig. Er GDPR generelt vanskelig å forstå? Er den utarbeidet for komplekst?**
    Jeg har vært på et foredrag der de fortalte at det var noen som gjorde en tekst-analyse av GDPR. Denne beregnet hvor lang høyere utdanning en gjennomsnittlig person ville trenge for å forstå denne lovteksten. Svaret viste at en gjennomsnittsperson bør ha 40 år i snitt med utdanning på høyskole eller universitetsnivå for å forstå teksten fullt ut og det er jo veldig få som har. Det er helt åpenbart at GDPR er vanskelig å forstå og at det fører til at folk har veldig ulike oppfatninger. European Data Protection Board forsøker å avklare og veilede. Man kan også stille spørsmål til EU-domstolen, men dette er en prosess som kan ta mange år.
13. **Det finnes foreløpig lite presedens på dette feltet. Hvordan kan en bedrift forsikre seg om at de etterlever alle lover og regler?**
    Jeg vil anbefale å følge med på veiledninger fra Datatilsynet. Det er fokus på å veilede og forklaring. Teksten i seg selv er veldig komplisert å sette seg inn i. Noen av tingene er riktignok veldig klare, som de grunnleggende prinsippene. Dette med samtykke for eksempel, det må kunne dokumenteres og trenger ikke være veldig komplekst og vanskelig hvis man har fokus på de overordnede tingene. Det er viktig å ikke gå seg bort i kompleksitet. Det er slik at ting i europeisk lovgivningsprosess ofte utformes litt mer komplekst enn nødvendig.
14. **Basert på tidligere intervjuer har vi fått vite at innføringen av GDPR har krevd veldig mye tid, penger og ressurser. Vil du si det er rettferdig at loven behandler alle likt, uavhengig av størrelse? Hvorfor/hvorfor ikke?**

Jeg har forståelse for at man må gjøre de samme tingene uavhengig av størrelse, men skjønner også at det kan oppleves som utfordrende. Det er det samme med regelverket vi håndhever, det må håndheves uavhengig av størrelse. Skal du drive forretningsvirksomhet så må du sette deg inn i grunnleggende lover og regler som angår deg og din virksomhet.

9.7. Cookie Information – Intervjuobjekt F

Innledningsvis holdt intervjuobjektet en presentasjon for å gi oss dypere innsikt i hvordan informasjonskapsler brukes og hvordan de er bygget opp. Vi har transkribert presentasjonen og det påfølgende intervjuet.

Presentasjon:

Presentasjonen er laget av et selskap som heter Cxense. Cxense er et selskap i mediebransjen som samler inn data og deler annonser.
Når man åpner en nettleser, så genereres det et skript. Et skript er en fil som inneholder kommandoer i et skriftspråk. Det sitter en komponent fra Cxense eller andre aktører i nettleseren som sjekker om det finnes informasjonskapsler fra før. Første gang man er inne på Facebook, Instagram o.l. settes det en informasjonskapsel som gir deg en ID. Det første skriptet gjør er å hente ut informasjonskapselen og finne ut hvem du er. Deretter sendes det et skript til en plattform som inneholder informasjon om eksempelvis URL, operativsystem, lokasjon osv. Dette er tekniske informasjonskapsler, som har til hensikt å bedre brukeropplevelsen.

Når man beveger seg ut på ulike tjenester, som for eksempel å abonnere på ulike tjenester, bruke nettsider og generell surfing - begynner vi å nærme oss persondata. Informasjonskapsler og persondata kan ses på som et puslespill. Hvis en brikke (en informasjonskapsel) alene eller sammen med andre kan fortelle hvem du er, så er det persondata. Dette vil typisk være geo-lokasjoner og IP-adresser. Persondata er ikke bare navn, fødsels- og personnummer, telefonnummer og adresse.

Cxense sporer ca. 1 milliard brukere, og aktører som VG, aftenposten og dagbladet bruker denne typen tjenester. De aller fleste nordmenn har flere enheter som iPhone, iPad og Smart-TV i hjemmene sine. Alle disse er koblet opp mot en plattform som henter ut informasjon om deg basert på hva du gjør på internett. Skriptene kjenner igjen din digitale ID og tilpasser derfor også reklamer basert på det du gjør på internett.

Eksempel på hva som skjer:
Et selskap ønsker å målrettet markedsføre et av sine produkter til potensielle kjøpere. De vil gjerne selge produktet til personer bosatt i Oslo, har en viss årslønn, formell utdannelse, er i aldersgruppen X til Y og er interessert i sykling eller seiling. Mao. man kan legge inn ulike parametere og markedsføre mot en gruppe mennesker man antar vil kjøpe produktet. Dette betyr at hver gang VG, kommer over en bruker som passer disse kriteriene, så vises reklame for det utvalgte produktet. Betalingsvilligheten for slik markedsføring er veldig høy, ettersom man skreddersyr hvem som får opp denne type reklame. Dette er også insentivet hos aktørene til å samle så mye informasjon som mulig om hver enkelt av oss.

I utgangspunktet så er det forskjellige ID som kommer fra ulike enheter. Telefonene er verstinger når det kommer til å dele persondata. IBM gjorde en analyse for noen år siden som ikke har endret seg. Undersøkelsen sier følgende:

- 82 % leser Device-ID
- 80 % sporer lokasjon
- 57 % sporer når man ringer
- 26 % leser hvilke apper man bruker
- 26 % lagrer brukerens SIM-kortnummer.

Alt som er gratis på internett og på applikasjon er laget på grunn av et formål, som er å samle inn kundedata. Det er for å hente inn data og selge videre.

Teknologien har kommet så langt at informasjonskapslene er så smarte at de klarer å koble sammen ulike ID på tvers av enheter til en felles ID. Det er ingen måte å gå rundt dette på, med mindre man ikke kobler til internett. Det er ikke nødvendigvis alt som er negativt. Det er dette EU prøver å ta tak i. Hele formålet med GDPR er å gi deg bedre kontroll på dine persondata. E-privacy regulerer mitt eierskap til data, mens GDPR regulerer bruken av persondata. Begge deler ender

opp med å kreve samtykke for å hente og dele videre data. GDPR og e-privacy kommer til å bli veldig samordnet.

Når man bruker internett så vil dette dukke opp i en slags blogg som viser alt du gjør på internett og deretter kan andre aktører kjøpe disse dataene. La oss ta et eksempel der en person har vært inne på internett og sett på et «BOSE-headset». Da kan SONY kjøpe disse dataene og neste gang man er inne på Facebook, så er det deres alternativ som kommer opp. Det spiller ingen rolle om man er på PC eller telefon, alt samles på et sted. All dataen blir lagret på profiler eller dimensjoner som er inndelt etter helse, økonomi og annet.

La oss ta et eksempel som omhandler kreft:
La oss si at et familiemedlem eller en i din omgangskrets har fått kreft. Da er det naturlig å søke rundt på internett for å tilegne seg mer informasjon om kreft. Det er tenkbart at en eller annen database, for eksempel Google, tenker at du når har sett så mye på kreft, at de huker av i boksen for kreft under din profil. Når man har fått kreft så begynner man å ordne opp i ting, som for eksempel livsforsikring. Da må man fylle ut en god del informasjon og forsikringsselskapet gjør en bakgrunnssjekk som de ikke har lov til gjennom et selskap på Cayman-øyene. De finner ut at du har kreft, men kan ikke si dette til deg. På bakgrunnen av informasjon så kan de øke prisen på livsforsikringen eller i verstefall avslå den.

Dette er kun et eksempel, men du kan være helt sikker på at dette skjer, også på andre områder. Om man ikke skal kunne bli sporet, må man gå på en enhet som ikke kan spores til deg som person.

En ansatt hos oss har funnet ut at en eller annen database har en ganske klar formening om hva som er hans favoritt tannkrem. Dette kommer av at han handler i en butikk og benytter kort eller trumf, som da profilerer brukeren hans. Grunnen til at trumf og andre fordelsprogrammer eksisterer er at de ønsker å profilere brukeren. De synes ikke det er så veldig stas å gi deg bonus. Verdien av det de klarer å samle inn om deg og matche opp mot alt annet er grunnen til at persondata er så verdifullt.

Dette er en kort innledning til informasjonskapsler og hvordan det fungerer. For å vise til et eksempel uten å nevne navn eller kilde, så har det vært en diskusjon på hvordan man kan bli valgt til stortingsrepresentant ved å bruke informasjonskapsler. Dette kan gjøres ved å sende politiske budskap til personer

basert på deres politiske mening. Politisk ståsted er klassifisert som sensitiv informasjon, men basert på «likes» på Facebook og andre steder, kan man likevel ganske enkelt se et mønster. La oss si at jeg stiller til valg for Høyre. Da sender jeg ut et budskap til en person som normalt stemmer arbeiderpartiet, og et annet budskap til en som stemmer SV. Ved å lage mange slike budskap, så kan en person ha et syn og en annen person et helt annet syn – også sørger man samtidig for å sende negative innspill om sin konkurrent. Er dette demokrati?

Intervju:

1. **Hva er informasjonskapsler og hva brukes det til?**
   En informasjonskapsel er en tekstfil. Den ligger i alle nettlesere i en egen katalog der det lagres millioner av informasjonskapsler av ulik karakter. For eksempel lager vi en egen informasjonskapsel som inneholder en «Consent-ID». Det vil si at når du har vært inne på vår nettside og gitt samtykke, så lagrer vi hva du har gitt samtykke til og husker det til neste gang du besøker oss. Samtidig så skriver vi til en ganske stor database, og i fjor samlet vi inn 6 milliarder samtykker, og der skriver vi Cookie-ID. Dette er ikke PII fordi den ikke kan settes sammen med andre og identifisere hvem du er. Det vi bruker den til er for å se om personen tidligere har avgitt samtykke. Cookies brukes til å lagre informasjon, både om «session», preferanser, innloggingsdetaljer og handlekurv.
2. **Hvordan kan en virksomhet samle inn data gjennom informasjonskapsler uten samtykke?**
   Det er fordi man ikke vet hva som foregår. Et nettsted bygges opp av elektroniske komponenter, også kalt legoklosser. Mye av det som ligger ute på nett er gratis. La oss si at jeg trenger en ny nettside også setter jeg sammen nettsiden med tjenestene til andre aktører – da har jeg ikke kontroll på hva som ligger i alle legoklossene.
3. **Har bruken av informasjonskapsler blitt påvirket av GDPR og eventuelt hvordan?**
   Når man deler persondata trår GDPR inn. Når data skal innhentes kreves det samtykke. Når persondata brukes til retargeting så er det en uenighet

om det kreves samtykke eller ikke. Jeg mener at man må innhente samtykke uansett. Jeg tror at dette kommer til å endre seg ganske klart når den nye e-privacyforordningen kommer. Når det kommer til informasjonskapsler og deling av persondata, så er mye mer som foregår enn hva folk flest er klar over. Loven sier at du som eier av et nettsted, må ta et ansvar. Du må vite hvem du deler data med, også må du gjøre en vurdering på hvorvidt det er så smart. Det må foreligge et samtykke om at du kan behandle denne dataen. Som eier av et nettsted, må man vurdere hva som er hensiktsmessig. Deling av persondata er greit så lenge man forteller hva du gjør og innhenter samtykke. En av tingene som gjør at det er mye misforståelser i Norge er at Ekomloven godtar samtykke der det kan settes en teknisk løsning og at en forhåndsinnstilling i nettleser på at brukeren godtar bruk av informasjonskapsler. Dette er langt utenfor etter vår mening. Det bør ikke være mulig å gå inn på et nettsted uten å godkjenne bruk av informasjonskapsler. Ofte er ikke bedriften selv klar over at de samler inn data og får ofte sjokk når de ser hva de deler av persondata.

4. **Kan databehandlere være sikre på hva som foregår, hvilke data som samles inn og hvor det blir av dataen ved bruk av informasjonskapsler?**

   Nei, det kan du i utgangspunktet ikke være sikker på. Det er her dette med databehandleravtaler kommer inn. Du må ha en databehandleravtale med de du deler data med og vite hva som skjer.

5. **Er det et brudd på GDPR dersom gamle informasjonskapsler ligger lagret på nettsiden, som videresendes til andre aktører og brukes i markedsføringsformål?**

   Ja, det er et brudd på GDPR-regelverket. Informasjonskapsler skal ikke kunne spore deg i mer enn 12 måneder og dette vil bli regulert i den nye e-privacyforordningen. Etter 12 måneder skal ikke informasjonskapselen lenger være aktiv og du må bekrefte samtykket på nytt.

6. **Det er en del uklarheter og relativt overlappende regelverk mellom informasjonskapsler og GDPR. Hvordan kan man vite hva som er lov og ikke?**

   Ekomloven ble oppdatert i 2013 og la på dette tidspunktet til paragrafen om informasjonskapsler. På dette tidspunktet var nok det beste å samtykke

i form av en forhåndsinnstilling i nettleseren. GDPR er veldig klar på at du som eier av et nettsted har det fulle ansvaret.

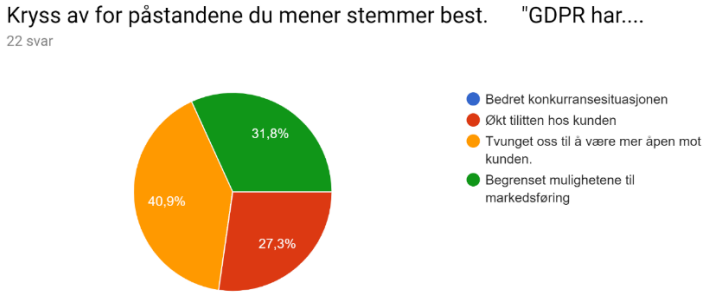
7. **Når beveger man seg fra Ekomloven og over til GDPR-lovverket?**
   Så fort persondata er involvert. Det vil flere nyanseforskjeller og tolkninger.
8. **Fører et overlappende regelverk til smutthull som kan være vanskelig for Datatilsynet å oppdage?**
   Jeg synes regelverket er klart, men det er klart at det oppstår noen uklarheter som kan føre til potensielle smutthull. Jeg synes folk lurer seg selv med tanke på at de ikke vil vite hvilke data de deler og med hvem. Vi ønsker å snu GDPR fra noe negativt til en positiv sak. Det skal bidra til å øke profilen din og fremstå som noe positivt.
9. **Hvilke informasjonskapsler er nødvendige for at en nettside skal fungere? Kan nettbutikker kreve at flere enn de helt nødvendige er på?**
   Man er nødt til å ha noen informasjonskapsler for at en nettside skal fungere. Det er mye tekniske informasjonskapsler som aldri skal dele persondata. Disse må også stå på for at en nettside skal fungere.
10. **Hvordan kan man vite hva som er lov og ikke ved bruk av informasjonskapsler for digital markedsføring?**
    Alle som behandler persondata må ha innhentet samtykke og kunne dokumentere det og hva som omfattes av samtykket. GDPR skiller ikke på plattform og det spiller ingen rolle om databehandlingen er frivillig er automatisk. Du må hele tiden kunne fortelle hva du gjør.
    Oppfølging: Tror du GDPR vil bli oppdatert kontinuerlig?
    Ja, jeg tror den vil bli kontinuerlig revidert på grunn av stadig ny teknologi. Hovedprinsippene kommer nok til å være der, men den vil nok bli regulert når man over tid finner ut hva som kan forbedres og ikke. Det vil nok bli noen tilpasninger i form av lovverk eller tillegg.

9.8. Kvantitativ spørreundersøkelse

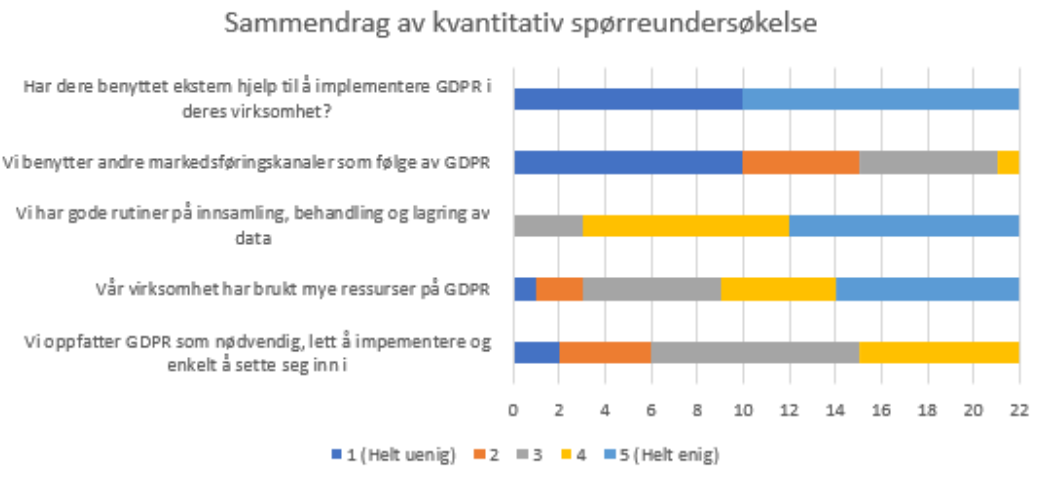
Spørsmål som ikke er inkludert i grafisk fremstilling:

Spørsmål 1:

Spørsmål 2:



Sammendrag/grafisk fremstilling av spørreundersøkelse:



9.9. Analyse av informasjonskapsler i samarbeid med Cookie Information

Analyse av bruk av informasjonskapsler på norske nettsteder

Powered by Cookie Information AS

1. **Bakgrunn/formål**

Det er flere risikoer man står ovenfor ved å ikke etterleve GDPR-lovverket. Intervjuobjekt F mener at en av de største utfordringene er bruken av informasjonskapsler. Det er mange virksomheter som ikke er klar over hvilke informasjonskapsler de benytter og deler unødvendig mye data med usikre tredjeparts land.

2. **Forklaring til analysen**

Analysen tar for seg en rekke aspekter som er verdt å belyse når det gjelder informasjonskapsler. Den tar blant annet for seg hvilke informasjonskapsler de selv opplyser at de bruker, og hvilke informasjonskapsler de faktisk benytter. Informasjonskapsler er delt inn i følgende kategorier: Nødvendige, funksjonelle, statistiske, markedsføring og uklassifiserte. Dette er ikke konfidensiell informasjon.

3. **Datagrunnlag**

Datagrunnlaget består av 48 norske netthandelsaktører, der vi har gått nærmere inn på fem av dem.

4. **Resultater**

- På de 48 undersøkte domenene er det plassert totalt 914 informasjonskapsler
- 211 informasjonskapsler for markedsføring
- Alle domenene hadde flere informasjonskapsler enn de har opplyst om.
- 178 av informasjonskapslene har en varighet over 12 måneder (Nytt samtykke skal innhentes hver 12. måned).
- Usikre tredjeland:
    - Russland
    - Kina (Hong Kong)
    - Virgin Islands

Utvalg av fem netthandelsaktører:

Netthandels-aktør		Kategorier av informasjonskapsler					Antall over 12. måneder	Maks år registrert
		Nødvendige	Funksjonelle	Statistiske	Markedsføring	Uklassifiserte		
Komplett.no	Opplyst (nett)	7	0	1	9	0	1	3 år
	Faktiske (CI)	5	2	4	5	16	2	2 år
	Avvik	**2**	**2**	**3**	**4**	**16**	**1**	
Fjellsport.no	Opplyst (nett)	7	2	3	10	0	3	2 år
	Faktiske (CI)	2	3	5	89	52	7	4 år
	Avvik	**5**	**1**	**2**	**79**	**52**	**4**	
Dressmykid.no	Opplyst (nett)	0	0	0	0	0	-	
	Faktiske (CI)	1	0	6	7	4	1	2 år
	Avvik	**-**	**-**	**-**	**-**	**-**	**1**	
SunKost.no	Opplyst (nett)	6	0	4	19	3	2	4 år
	Faktiske (CI)	3	1	4	28	8	2	4 år
	Avvik	**3**	**1**	**0**	**9**	**5**	**0**	
Zalando.no	Opplyst (nett)	19	0	15	56	0	-	
	Faktiske (CI)	3	1	2	15	23	3	10 år
	Avvik	**16**	**1**	**13**	**41**	**23**	**3**	

5. Kommentarer

Mange av de undersøkte nettsteder benytter i dag en løsning der de ikke opplyser (de vet heller ikke) hvilke cookies som settes og hvem nettstedet deler data med. Deretter sier man i noen tilfeller at «Vi bruker cookies», og oppfordrer brukeren til å gå inn i sin browser for å justere cookiesettingene i henhold til sine preferanser. Andel virksomheter som ikke har cookiebanner som informerer om informasjonskapsler eller vesentlige mangler ved cookiebanner er 95 %. Svært mange av nettstedene deler persondata om sine brukere (i mange tilfeller = kunder) og hva de gjør på nettstedet med ulike mottakere. Disse mottakere tilbyr disse dataene til høystbydende, noe som åpner for at konkurrerende virksomheter kan kjøpe tilgang til disse data, og målrette markedsføring på dette grunnlaget.

6. Utvalg:

Utvalget av netthandelsaktører som er med i analysen om informasjonskapsler:

1. Barnashus.no
2. Blush.no
3. Brandos.no
4. Braasport.no
5. CareofCarl.no
6. Cdon.no
7. Cg.no
8. Colorwool.no
9. Concretinterior.no
10. Coram.no
11. Designforevig.no
12. Dyrekassen.no
13. Elektroimportoren.no
14. Enklereliv.no
15. Europris.no
16. Fellekjopet.no
17. Getinspired.no
18. Gsport.no
19. Gullfunn.no
20. Helthjem.no
21. Hifiklubben.no
22. Kitchn.no
23. Kondomeriet.no
24. Lampehuset.no
25. Life.no
26. Ligthup.no
27. Maxbo.no
28. Mellymoon.no
29. Mobelringen.no
30. Motehus.no
31. Naturamed-pharma.no
32. No22.no
33. Organized.no
34. Rajapack.no
35. Sixbondstreet.no
36. Sjarmtroll.no
37. Skittfiske.no
38. Skomani.no
39. Slettvoll.no
40. Snushjem.no
41. Telenor.no
42. Tudos.no
43. Vitusapotek.no
44. Komplett.no
45. Fjellsport.no
46. Dressmykid.no
47. Zalando.no
48. Sunkost.no