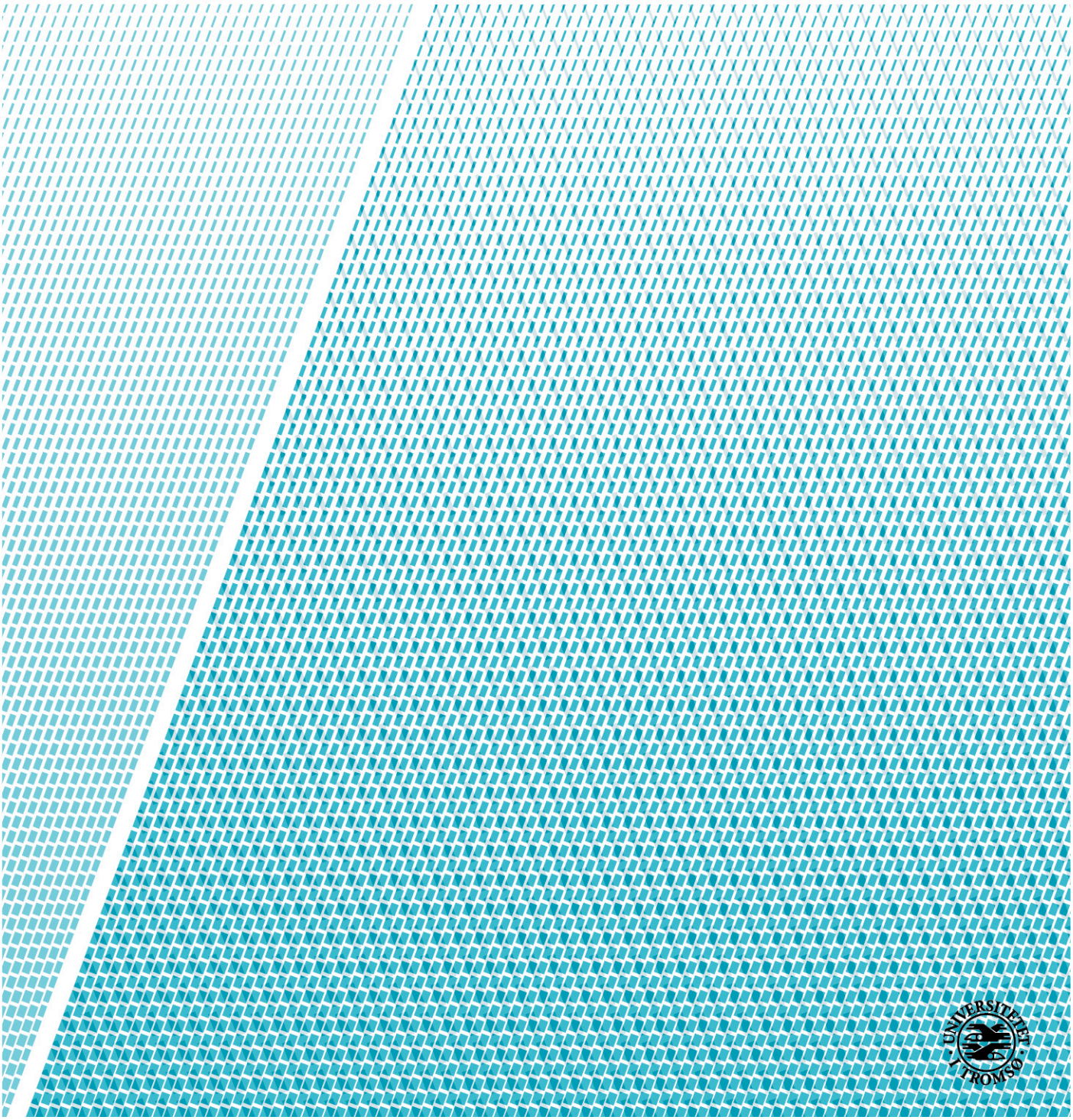
UiT
NORGES
ARKTISKE
UNIVERSITET

Det juridiske fakultet

# Samtykke til behandling av personopplysninger ved nedlastning og bruk av mobilapplikasjoner

**Emilie Langfjord**

*Liten masteroppgave i rettsvitenskap, våren 2018*



# Innholdsfortegnelse

# 1. Innledning

## 1.1 Tema og aktualitet

Temaet for oppgaven er samtykke som rettslig grunnlag for behandling av personopplysninger ved nedlastning og bruk av mobilapplikasjoner. Stadig flere er i besittelse av en smarttelefon. Undersøkelser viser at 99 prosent av alle nordmenn mellom 12 og 49 år har en smarttelefon.[1] På disse smarttelefonene lastes det ned en rekke applikasjoner. Det finnes millioner av applikasjoner å velge mellom hos de to store nettbutikkene App Store og Google Play. Applikasjonene tjener et bredt spekter av formål, blant annet nettlesing, kommunikasjon, underholdning, reise og bank. Det de fleste ikke er klar over er at de ved nedlastning og bruk av applikasjoner ofte gir fra seg personopplysninger om seg selv. Personopplysningene beskriver hvem de er og hva de gjør.[2] Tilbyderne av applikasjonene bygger på en forretningsmodell som utfordrer personvernet. Forretningsmodellen går ut på en byttehandel hvor gratistjenester utveksles mot personopplysninger. Personopplysninger har i løpet av de siste årene fått en enorm kommersiell verdi og blir blant annet omtalt som den nye oljen.[3] Det oppstår her en konflikt mellom tjenestetilbydernes ønske om å bruke personopplysningene kommersielt og brukernes interesse av å beskytte sitt privatliv.

Personopplysningsloven[4] bygger på en visjon om at den enkelte i så stor grad som mulig skal kunne bestemme og kontrollere bruken av opplysninger som gjelder seg selv.[5] En slik selvbestemmelsesrett er igjen en del av et mer generelt krav om personlig autonomi, som bunner i respekt for mennesket og dets egenverdi.[6] Det klareste uttrykket for denne selvbestemmelsesretten finner vi i personopplysningsloven § 8, som fastsetter samtykke fra den registrerte som ett av flere alternative rettslige grunnlag for behandling av personopplysninger.[7] Samtykke som hjemmel til behandling av personopplysninger vil

---

[1] Artikkel fra Medier24.no om Kantar TNSs måling av antall nordmenn med smarttelefoner: https://www.medier24.no/artikler/na-har-99-prosent-av-alle-mellom-12-og-49-ar-en-smarttelefon/366987
[2] Jon Bing, *Personvern i faresonen*, Oslo 1991 s. 10
[3] Lee A. Bygrave, *Data Privacy Law*, Oxford 2014 s. 4
[4] Lov 14. april 2000 nr. 31 om behandling av personopplysninger («personopplysningsloven»)
[5] Dag Wiese Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s. 178
[6] Lee A. Bygrave, *Selvbestemmelse til besvær?* Publisert i Spor (Kvartalsskrift utgitt av Datatilsynet) 2000 s.1
[7] Bygrave (2000) s. 1

kun bidra til å sikre den enkelte reell makt over sine personopplysninger dersom kravene som oppstilles for et gyldig samtykke etter personopplysningsloven § 2 nr. 7 er oppfylt.

## 1.2 Problemstilling

Ved installasjon og bruk av applikasjoner inngås en brukeravtale mellom brukeren og tjenestetilbyderen. Brukeravtalen inngås ved at brukeren avgir sitt samtykke. Ved å samtykke til inngåelse av denne avtalen aksepterer brukeren tjenestetilbyderens avtalevilkår og personvernerklæring. Samtykket kan avgis på flere måter. Det kan avgis ved klikk på et ikon i forbindelse med nedlastning av applikasjonen, klikk på et ikon etter at applikasjonen er lastet ned eller ved innlogging med en egen bruker etter at applikasjonen er lastet ned.

I realiteten innebærer samtykket at brukeren godtar den behandling av personopplysninger som fremgår av avtalevilkårene og personvernerklæringen. Vilkårene som oppstilles til et gyldig samtykke har som intensjon å sikre at den som samtykker selv har tatt direkte stilling til om den aktuelle behandlingen skal tillates. Undersøkelser viser imidlertid at svært få faktisk leser avtalevilkårene og personvernerklæringene, og at enda færre faktisk forstår hva de samtykker til.[8] Årsaken til dette er at avtalevilkårene og personvernerklæringene ofte er svært lange, i tillegg til at det brukes ord og uttrykk som er både lite konkrete og vanskelig å forstå. En kan dermed stille spørsmål om hvor reelle disse samtykkene er. Mye kan tyde på at samtykkealternativet her skaper en illusjon om et personvern som faktisk ikke eksisterer.

Problemstillingen denne oppgaven har som formål å svare på er hvorvidt den type samtykke som gis i forbindelse med nedlastning og bruk av mobilapplikasjoner oppfyller lovens krav om et frivillig, uttrykkelig og informert samtykke jf. personopplysningsloven § 2 nr. 7.

[8] Artikkel fra The Guardian om at brukere ikke leser vilkårene når de inngår brukeravtaler mv.: https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information

## 1.3 Rettskildebildet og metode

### 1.3.1 Innledning

Oppgaven er skrevet ut fra et rettsdogmatisk perspektiv. Den rettsdogmatiske metoden har som formål å klargjøre og systematisere gjeldende rett gjennom analyser av relevante rettskilder og relevant argumentasjon.[9] I punkt 1.3.2 til og med punkt 1.3.8 vil jeg redegjøre for de ulike rettskildene som er brukt for å løse oppgavens problemstilling, hvilke utfordringer som har oppstått og hvordan jeg har håndtert disse. Deretter i punkt 1.3.9 vil jeg redegjøre for de metodiske utfordringene som har oppstått knyttet til beskrivelsen av det faktiske grunnlaget for analysen.

### 1.3.2 Personopplysningsloven og dens forarbeider

Personopplysningsloven utgjør den sentrale loven på personopplysningsrettens område i norsk rett, og er utgangspunktet for løsning av oppgavens problemstilling.
I personopplysningsloven § 2 nr. 7 oppstilles vilkårene som må være oppfylt for at et samtykke skal være gyldig. Ordlyden gir imidlertid begrenset med informasjon om hvilke krav som må være til stede for at vilkårene kan anses å være oppfylt. Det har dermed vært nødvendig å gå til andre rettskilder for å kunne løse oppgavens problemstilling.

Det er utarbeidet flere lovforarbeider knyttet til personopplysningsloven.[10] Forarbeidene har til en viss grad bidratt til en nærmere forståelse av vilkårenes innhold. Det er særlig hentet argumenter fra Ot.prp.nr.92 (1998-1999).

### 1.3.3 Personverndirektivet og praksis fra EU-domstolen

EUs personverndirektiv 95/46/EF[11] ble i 1999 inntatt i avtalen om det europeiske samarbeid av 1992.[12] Som en følge av dette er Norge forpliktet til å vedta lovgivning i samsvar med personverndirektivet.[13] Personopplysningsloven er et resultat av denne plikten og

---

[9] Torstein Eckhoff og Jan E. Helgesen, *Rettskildelære*, 5. utgave, Oslo 2001 s. 15
[10] NOU 1997:19, Ot.prp.nr.92 (1998-1999) og NOU 2009: 1
[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data («personverndirektivet»)
[12] Avtale om Det europeiske økonomiske samarbeidsområde, 5. februar 1992 («EØS-avtalen»)
[13] EØS-avtalen artikkel 7

gjennomfører personverndirektivet i norsk rett. Da norsk personopplysningsrett i stor grad bygger på EUs personverndirektiv er direktivet en relevant og vektig kilde for tolkning av personopplysningsloven. Ved tolkning av personverndirektivet skal EU-domstolens tolkningsmetode legges til grunn. Som Arnesen og Steinvik uttaler er det mest fremtredende med EU-domstolen sin metode at formålsbetraktninger tillegges stor vekt, ikke sjeldent på bekostning av ordlyden, og at forarbeider og nasjonal praksis sjeldent tas i betraktning.[14]

De fleste bestemmelser i personverndirektivet har en parallellbestemmelse i personopplysningsloven.[15] Personopplysningsloven § 2 nr. 7 gjennomfører artikkel 2 bokstav h i personverndirektivet. Jeg viser til personverndirektivet der jeg mener det er av betydning for fastleggelsen av innholdet i vilkårene til gyldig samtykke.

Praksis fra EU-domstolene er en viktig kilde ved tolkning av personverndirektivet, og dermed også personopplysningsloven. EU-domstolen har i de senere år avsagt flere prejudisielle avgjørelser om tolkningen av direktivet.[16] Avgjørelser avsagt av EU-domstolen tillegges vesentlig vekt. Jeg har imidlertid kun funnet en dom avsagt fra EU-domstolen av relevans for oppgaven. Denne er brukt for å belyse vilkåret om et informert samtykke.

### 1.3.4 Rettspraksis

Jeg har ikke funnet Høyesterettspraksis som er relevant for tolkningen av personopplysningslovens vilkår til et gyldig samtykke. Jeg har heller ikke funnet relevant underrettspraksis. Mangelen på relevant rettspraksis kan forklares ut fra at de fleste saker som gjelder personvern behandles og avgjøres av Personvernnemnda. Det har vært utfordrende å redegjøre for temaet uten å kunne vise til rettspraksis, da rettspraksis er en tungtveiende rettskilde.

### 1.3.5 Praksis fra Personvernnemnda og Datatilsynet

På personopplysningsrettens område er praksis fra Personvernnemnda og Datatilsynet en

[14] Finn Arnesen og Are Steinvik, Internasjonalisering og juridisk metode, Oslo 2009 s. 24
[15] Line M. Coll og Claude A. Lenth, *Personopplysningsloven*, Oslo 2000 s. 20
[16] Thomas Olsen, *Personvernøkende identitetsforvaltning*, artikkel i Complexserien 2015 s. 27

aktuell rettskilde. Hvor stor vekt praksis fra forvaltningen kan tillegges er relativt. Ifølge Eckhoff avhenger vekten av «hvor utbredt, fast og varig» vedkommende praksis er, samt hvorvidt praksisen skriver seg fra organer som anses å ha «særlig kyndighet på vedkommende felt».[17]

Personvernnemnda er et uavhengig forvaltningsorgan som avgjør klager over Datatilsynets avgjørelser.[18] Personvernnemnda består av syv medlemmer som oppnevnes for fire år. Lederen og nestlederen oppnevnes av Stortinget, mens de øvrige fem medlemmene oppnevnes av Kongen.[19] Medlemmene innehar særskilt kompetanse og sakkyndighet på personopplysningsrettens område. På grunn av at det finnes beskjedent med rettspraksis på området, i tillegg til at nemnda består av medlemmer med særskilt kompetanse, har avgjørelser truffet av Personvernnemnda blitt tillagt en viss rettskildemessig vekt. Dette gjelder spesielt hvor avgjørelsene gir uttrykk for en fast og konsistent praksis. Praksis fra nemnda har blitt anvendt i oppgaven for å belyse kravene til et frivillig og uttrykkelig samtykke.

Datatilsynet er også et uavhengig forvaltningsorgan.[20] Datatilsynet har som oppgave å føre tilsyn med at reglene i personopplysningsloven etterleves av de som behandler personopplysninger. Samtidig skal Datatilsynet gi råd og veiledning både til de som skal behandle personopplysninger og til de som er registrert i et personregister.[21] Avgjørelser fattet av Datatilsynet vil være en relevant kilde på personopplysningsrettens område. Men jeg har ikke funnet noen avgjørelser som har relevans for løsning av oppgavens problemstilling.

### 1.3.6 Uttalelser fra Artikkel 29-gruppen

Et betydningsfullt organ innen EU er Artikkel 29-gruppen.[22] Artikkel 29-arbeidsgruppen er et selvstendig rådgivende EU-organ som er opprettet med hjemmel i personverndirektivet

---

[17] Eckhoff og Helgesen (2001) s. 233
[18] Personopplysningsloven § 43 første ledd
[19] Personopplysningsloven § 43 annet ledd
[20] Personopplysningsloven § 42 første ledd
[21] Artikkel fra Kommunal- og moderniseringsdepartementets om Datatilsynet og Personvernnemnda, https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/datatilsynets-og-personvernnemndas-saksbehandling/id2340093/
[22] Working Party on the Protection of Individuals with regard to the Processing of Personal Data – heretter «Artikkel 29-gruppen»

artikkel 29. Deres oppgave er å gi råd til Kommisjonen om ulike problemstillinger vedrørende personopplysningsvern. Gruppen har gitt flere rådgivende uttalelser som berører oppgavens tema og jeg har valgt å bruke disse i min fremstilling. Det er imidlertid viktig å være oppmerksom på at deres uttalelser kun er veiledende og at deres uttalelser derfor ikke er rettslig bindende. Det er likevel viktig å understreke at gruppen er svært kompetent, og som Schartum og Sætre påpeker har deres uttalelser preg av å være utfyllende retningslinjer med et innhold som på mange måter innebærer mer detaljert og utfyllende standpunkt til rettsspørsmål enn det som fremkommer av direktivteksten og fortalen.[23] Selv om uttalelsene og anbefalingene ikke er rettslig bindende, må de likevel kunne anses å ha relevant betydning. I fravær av andre mer tungtveiende rettskilder har deres uttalelser blitt tillagt en viss rettskildemessig vekt.

### 1.3.7 Juridisk teori

En rettsanvender er ikke bundet av den juridiske teorien. Teorien kan verken fastsette generelle regler eller avgjøre konkrete saker, men den beskriver gjerne hva som etter forfatterens mening er gjeldende rett, og den kan gi begrunnede anbefalinger de lege ferenda.[24] Juridisk teori vil normalt ikke bli tillagt vesentlig vekt, men den vil likevel kunne tillegges en viss vekt i de tilfeller den gir uttrykk for en fast rettsoppfatning.[25]

Juridisk teori har i vesentlig grad influert oppgaven. Det er særlig hentet argumenter fra boken «Personvern i informasjonssamfunnet» skrevet av Dag Wiese Schartum og Lee A. Bygrave og artikkelen «Samtykke til å behandle personopplysninger i offentlig forvaltning» av Dag Wiese Schartum og Kjetil Wick Sætre.

### 1.3.8 Den kommende personvernforordningen

De siste årene har det pågått en omfattende revisjon av EUs regelverk på personvernfeltet, noe som har resultert i at en ny personvernforordning[26] vil erstatte det nåværende

---

[23] Dag Wiese Schartum og Kjetil Wick Sætre, *Samtykke til å behandle personopplysninger i offentlig forvaltning*, artikkel i Complexserien 2016 s. 37
[24] Olav Torvund, *Å studere jus*, Oslo 1996 s. 253
[25] Nils Nygaard, *Rettsgrunnlag og standpunkt*, 2. utgave, Oslo 2012 s. 105
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC («personvernforordningen»)

personverndirektivet. Forordningen vil tre i kraft 25. mai 2018. På grunn av EØS-avtalen vil Norge være pålagt å vedta ny lovgivning i samsvar med den kommende forordningen. I den forbindelse foreslår Justis- og beredskapsdepartementet i sin proposisjon av 23. mars 2018 en ny personopplysningslov som vil avløse gjeldende personopplysningslov.[27] Det foreslås videre at personvernforordningen gjøres til norsk lov gjennom en inkorporasjonsbestemmelse i § 1 i den nye loven.[28] Det gjøres oppmerksom på at grunnet forsinkelser i EØS-komiteen og interne prosedyrer i Liechtenstein vil ikke forordningen tas inn i EØS-avtalen før tidligst 1. juli. Det betyr at ny personopplysningslov tidligst vil kunne settes i kraft i juli i år.

Ved gjennomføring av direktiver står nasjonale myndigheter mer fritt, da et direktiv gir større rom for nasjonale myndigheter til å bestemme form og midler.[29] En forordning skal på sin side gjøres til nasjonal rett som sådan, noe som betyr at de skal oversettes ordrett til norsk og gjennomføres uten forandring av ordlyden.[30] Den kommende forordningen vil dermed snevre inn handlingsrommet for norske myndigheter. Forordningen åpner unntaksvis for nasjonale tilpasninger også etter forordningen, men kun der hvor dette fremgår uttrykkelig.[31] Forordningen åpner ikke for å fastsette generelle nasjonale regler om samtykke, og forordningen vil dermed gi uttrykk for hvordan den kommende personopplysningslovens vilkår til et gyldig samtykke sannsynligvis blir.[32]

Personvernforordningen utgjør ingen grunnleggende brudd med nåværende direktiv, men vil likevel medføre noen endringer og ytterligere presiseringer av enkelte vilkår. I oppgaven er personvernforordningen brukt for å se om denne vil bidra til en enklere praktisering og forståelse av kravene til et gyldig samtykke. Siden forordningen ikke har trådt i kraft knytter det seg noen særskilte problemstillinger til å bruke den som rettskilde. Det foreligger naturlig nok ingen rettspraksis, og det finnes begrenset med rettskilder for øvrig som direkte belyser hvordan reglene i forordningene er å forstå.

---

[27] Prop. 56 LS (2017-2018) s. 7
[28] Prop. 56 LS (2017-2018) s. 7
[29] EØS-avtalen artikkel 7 bokstav b
[30] EØS-avtalen artikkel 7 bokstav a.
[31] Personvernforordningen fortalepunkt 8
[32] Prop. 56 LS (2017-2018) s. 31 og Personvernforordningens fortalepunkt 8 jf. artikkel 6.

### 1.3.9 Det faktiske grunnlaget for analysen

Som Torvund uttaler er det vanskelig å foreta en rettslig analyse uten at man kjenner til analysens gjenstand.[33] En stor utfordring i dette arbeidet har vært å finne ut av og beskrive det faktum som skal analyseres. På grunn av begrensninger i både tid og omfang har jeg ikke foretatt noen uttømmende empirisk undersøkelse av situasjonen knyttet til nedlastning og bruk av norske applikasjoner. Det er likevel enighet i juridisk teori om at det ikke alltid er nødvendig å foreta omfattende empiriske analyser som grunnlag for en rettslig analyse.[34] Torvund uttaler blant annet at det for rettslige analyser ofte vil være «tilstrekkelig å konstatere hvilke fenomener som forekommer eller kan forekomme» og at «det typiske i en rettslig analyse vil være at man stiller opp idealtypiske situasjoner som så underkastes en rettslig analyse».

Beskrivelsen av den faktiske situasjonen knyttet til nedlastning og bruk av norske applikasjoner bygger dels på en rapport fra Datatilsynet med tittelen «Hva vet appen om deg?», dels på egne undersøkelser av en gruppe applikasjoner. For nedlastning av applikasjonene har jeg brukt en Iphone 6 s som er knyttet til operativsystemet iOS og en Samsung Galaxy S7 som er knyttet til operativsystemet Android. Applikasjonene er lastet ned fra nettbutikkene App Store og Google Play. Jeg har valgt ut applikasjoner som er mye brukt og som tilbyr ulike typer tjenester. Applikasjonene jeg har valgt er VG (nyhetstjeneste), Vipps (banktjeneste), Yr (værtjeneste), RuterBillett (reisetjeneste), Norsk tipping (spilltjeneste), Norli e-bok (e-boktjeneste) Æ (matvarehandeltjeneste) og Finn (markedsplasstjeneste). Etter nedlastning har jeg analysert applikasjonenes brukeravtaler og personvernerklæringer. Der hvor applikasjonen har krevd særskilt innlogging etter nedlastning, har jeg opprettet bruker og logget inn. Analysene ble foretatt i mars 2018 og det tas dermed forbehold om at tjenestetilbyderne kan ha endret sine brukeravtaler og personvernerklæringer i ettertid.

---

[33] Olav Torvund, *Betalingsformidling i et rettslig perspektiv*, Otta 1993 s. 30, Mads Bryde Andersen, *IT-retten*, 2. udg., København 2005 s. 105-107, Olsen (2015) s. 22

[34] Torvund (1993) s. 47

## 1.4 Avgrensninger

Oppgaven avgrenses til å behandle installasjon og bruk av norske mobilapplikasjoner. Avgrensningen begrunnes i spørsmålet om personopplysningslovens geografiske virkeområde. Tjenestetilbyderne som er ansvarlig for norske applikasjoner er å anse som etablert i Norge slik at personopplysningsloven kommer til anvendelse.[35] Behandling av utenlandske applikasjoner ville kunne ført til kompliserte spørsmål knyttet til hvilken jurisdiksjon applikasjonens håndtering av personopplysningene hører under. Det bemerkes at den kommende personvernforordningens geografiske virkeområde er utvidet.[36] Det betyr at når forordningen inkorporeres i norsk rett vil problemstillingen bortfalle.

Videre avgrenses oppgaven mot behandling av personelle krav til samtykke. Personopplysningsloven inneholder ingen bestemmelse om hvem som kan avgi gyldig samtykke. Hvilke personelle krav som må være oppfylt utgjør dermed en problemstilling i seg selv, da det kan reises spørsmål om hvorvidt mindreårige, demente eller psykisk utviklingshemmede o.l. kan samtykke til registrering og bruk av personopplysninger. Videre kan det reises spørsmål om representasjon. Det er hverken tid eller ordmessig plass til å behandle problemstillingen innen rammen av oppgaven. I oppgaven forutsettes det at samtykkekompetanse foreligger.

Oppgaven avgrenses også mot å behandle samtykke som rettslig grunnlag til behandling av sensitive personopplysninger.[37] Personopplysningsloven stiller strengere krav til behandling av sensitive personopplysninger.[38] For det første må det foreligge et gyldig samtykke etter personopplysningsloven § 8, i tillegg må det foreligge et gyldig samtykke etter personopplysningsloven § 9. På grunn av begrensninger i tid og omfang blir ikke samtykke som rettslig grunnlag til behandling av sensitive personopplysninger behandlet.

Til sist avgrenses det mot behandling av avtalerettslige og forbrukerrettslige regler.

---

[35] Personopplysningsloven § 4
[36] Personvernforordningen artikkel 3 nr. 2 bokstav a og b
[37] Personopplysninger som anses sensitive etter loven, gjelder opplysninger om rasemessig eller etnisk bakgrunn; politisk, filosofisk eller religiøs oppfatning; at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling; helseforhold; seksuelle forhold; og medlem- skap i fagforeninger jf. personopplysningsloven § 2 nr. 8
[38] Coll og Lenth (2000) s. 28

Behandlingen ville i så fall blitt for omfattende. Det vil likevel knyttes noen kommentarer til avtaleloven i den rettslige analysen i kapittel 4.

## 1.5 Fremstillingen videre

Oppgaven er delt inn i fire kapitler, foruten innledningen.

Det er vanskelig for en leser å følge en rettslig analyse uten å gjøres kjent med analysens gjenstand. I kapittel 2 redegjøres det derfor kort for hvordan den faktiske situasjonen rundt nedlastning og bruk av applikasjoner er.

Kapittel 3 er ment som et innføringskapittel forut for den rettslige analysen i kapittel 4. I kapittel 3 gis det en oversikt over rettslige utgangspunkter og sentrale begreper det er nødvendig at leseren kjenner til.

I kapittel 4 fremgår den rettslige analysen av vilkårene som stilles til samtykke som et gyldig rettslig behandlingsgrunnlag etter personopplysningsloven § 8 jf. § 2 nr. 7. Vilkårene vurderes i lys av den type samtykke som avgis ved installasjon og bruk av applikasjoner. Med andre ord er dette kjernen i fremstillingen.

Avslutningsvis i kapittel 5 gis det et svar på oppgavens problemstilling. Det gjøres også noen betraktninger vedrørende veien videre.

# 2. Hvordan er den faktiske situasjonen?

## 2.1 Innledning

Formålet med kapittel 2 er å gi en kort beskrivelse av den faktiske situasjonen rundt nedlastning og bruk av applikasjoner. I punkt 2.2 vil det redegjøres for hvorfor applikasjonene innhenter opplysninger om brukeren. Deretter i punkt 2.3 vil det gis en oversikt over hvilke opplysninger de undersøkte applikasjonene innhenter om brukeren. Oversikten antas å gi et bilde av hvilke opplysninger som typisk innhentes om brukere ved nedlastning og bruk av applikasjoner.

## 2.2 Hvorfor samler applikasjonene inn opplysninger om brukeren?

Det er som regel nødvendig for tjenestetilbyderne å innhente opplysninger om brukeren for at tjenesten skal kunne leveres. Opplysningene bidrar også til å gjøre tjenestene mer effektive og personaliserte.[39] Disse opplysningene blir imidlertid også ofte brukt til andre formål enn det som er nødvendig og tjenlig for tjenestens funksjonalitet. Årsaken til sistnevnte er at tjenestetilbyderne bygger på en forretningsmodell som forutsetter stadig mer overvåkning av brukerne.[40] Modellen baserer seg på at de fleste tjenester tilbys gratis mot at tjenestetilbyderen samler inn store mengder informasjon om brukeren.[41]

Opplysninger om brukerne anses som en vare som danner grunnlag for inntekt slik at tjenestene kan finansieres. Tilgang til opplysninger om brukerne gir mulighet for innsikt i deres behov, interesser og vaner. Opplysninger om brukerne har dermed stor verdi som inntektskilde ved salg til aktører som driver med reklame og markedsføring. Desto flere opplysninger aktørene får tak i, jo bedre forutsetninger har de for å skreddersy og personalisere markedsføringen.

---

[39] Bernard Enjolras, *Big data og samfunnsforskning*, artikkel Idunn.no 2014
[40] Datatilsynets rapport med tittelen «Personvern tilstand og trender» (2016) s. 13
[41] Datatilsynets rapport med tittelen «Personvern tilstand og trender» (2016) s. 13

Dette betyr at slike tjenester i realiteten ikke er gratis, da brukeren betaler med opplysninger om seg selv.

## 2.3 Hvilke opplysninger innhenter applikasjonene?

### 2.3.1 Innledning

Alle applikasjonene undersøkt i oppgaven innhenter opplysninger om brukerne. De innhenter imidlertid både ulike opplysninger og ulikt antall opplysninger. Dette kan blant annet forklares ut fra at det er tale om ulike typer applikasjoner som har ulike formål med sine tjenester.

Opplysningene blir nedenfor inndelt i kategorier. Årsaken til dette er at innhentingen rent teknisk kan være komplisert. Eksempelvis kan lokasjonsopplysninger innhentes på flere måter. Én applikasjon kan innhente GPS- opplysninger mens en annen innhenter IP-adresse, men begge vil falle inn under kategorien «lokasjonsopplysninger».

### 2.3.2 Lokasjonsopplysninger

Lokasjonsopplysninger er opplysninger som forteller hvor en telefon befinner seg rent geografisk.[42] Denne type opplysning kan være svært følsom da folk flest er svært knyttet til sin telefon og som regel bærer denne med seg til enhver tid. En oversikt over hvor vedkommende har oppholdt seg vil kunne gi detaljert innsikt i privatlivet til brukeren. Det vil eksempelvis være mulig å finne ut av hvor vedkommende bor og arbeider.

Tilgang til lokalisering kan være nødvendig for å tilby en tjeneste som har som formål å angi ting i nærheten, for eksempel været, eller for å kunne gi en veibeskrivelse ut fra brukerens posisjon til et gitt mål, for eksempel veien til nærmeste café.

[42] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011) s. 15

### 2.3.3 Kontaktliste

En kontaktliste kan bestå av mange forskjellige informasjonselementer. Det vanligste innholdet i en kontaktliste er kontaktdatanavn, telefonnummer og e-postadresse.[43] En kontaktliste kan også inneholde informasjon om fødselsdatoer, ansettelsesforhold og familie- og vennerelasjoner.[44] En kontaktliste kan dermed fortelle mye om brukeren og dens forhold til verden rundt seg.[45] Men den kan også fortelle mye om andre, noe som i seg selv kan være problematisk.

Tilgang til kontaktliste og adgang til å bruke telefonens kontakter kan være nødvendig ved bruk av applikasjoner som innebærer kommunikasjon med andre.

### 2.3.4 Identifiserende opplysninger

Identifiserende opplysninger er opplysninger som gjør at man kan gjenkjenne en enkeltperson. Typiske identifiserende opplysninger er: navn, adresse, mobilnummer, e-postadresse, IMEI-nummer[46], kredittkortinformasjon og kontonummer.[47]

Identifiserende opplysninger kan være nødvendig for at tjenestetilbyderen skal kunne verifisere reelle brukere og opprette kommunikasjon med brukeren. Hvor grundig dette må gjøres er avhengig av hvilken type tjeneste det er tale om.

### 2.3.5 Adferdsopplysninger

Med adferdsopplysninger siktes det til opplysninger om bruken av den aktuelle tjenesten. Ved å se på hva brukeren foretar seg over tid får tjenestetilbyderne innsyn i brukerens interesser og preferanser. Adferdsopplysninger er nødvendig dersom tjenestetilbyderen skal personalisere sine tjenester, slik at den enkelte tjeneste blir spesielt tilpasset brukeren. Videre kan de være nødvendig for å avdekke uønsket atferd.

---

[43] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011) s. 16
[44] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011) s. 16
[45] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011) s. 17
[46] IMEI står for International Mobile Equipment Identity og kan kalles for mobiltelefonens fingeravtrykk. Det er en internasjonal standard for merking av mobiltelefoner ved å gi dem et unikt serienummer. https://www.tek.no/artikler/dette_er_imei-koden/7597
[47] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011) s. 16

# 3. Personopplysningsloven – rettslige utgangspunkter og sentrale begreper

## 3.1 Innledning

I kapittel 3 vil det gis en oversikt over sentrale elementer i personopplysningsloven som det er viktig å ha kunnskap om med hensyn til den rettslige analysen i kapittel 4. Kapitlet er ment som et innføringskapittel.

I punkt 3.2 vil det redegjøres for personopplysningslovens anvendelsesområde. Videre i punkt 3.3 vil de ulike aktørene som får sine forhold regulert av personopplysningsloven bli presentert. Til sist i punkt 3.4 gis den en kort fremstilling av personopplysningslovens krav om hjemmel for behandling av personopplysninger. I tillegg vil det redegjøres kort for forholdet mellom samtykke og avtale som behandlingsgrunnlag.

## 3.2 Lovens saklige virkeområde

Personopplysningsloven har som formål å beskytte enkeltindivider mot at deres personvern blir krenket gjennom behandling av personopplysninger.[48] Loven har et vidt saklig virkeområde, og kommer i utgangspunktet til anvendelse ved all elektronisk behandling av personopplysninger jf. personopplysningsloven § 3 første ledd bokstav a. Så lenge behandlingen skjer elektronisk stilles det ingen krav til hvordan opplysningene er organisert.[49] Skal loven komme til anvendelse må det skje en behandling av personopplysninger. Innholdet i begrepene «personopplysning» og «behandling av personopplysninger» må dermed fastslås.

Begrepet «personopplysning» er definert i personopplysningsloven § 2 nr. 1 som «opplysninger og vurderinger som kan knyttes til en enkeltperson». Ut fra en naturlig språklig

[48] Personopplysningsloven § 1
[49] Schartum og Bygrave (2016) s. 151

forståelse av bestemmelsens ordlyd må to kumulative vilkår være oppfylt for at noe kan anses som en personopplysning. Det må for det første foreligge opplysninger eller vurderinger om en enkeltperson. For det andre må disse opplysningene kunne knyttes til en enkeltperson.

I proposisjonen fra departementet fremgår det at begrepet «enkeltperson» kun omfatter fysiske personer.[50] Opplysninger om juridiske personer faller dermed som utgangspunkt utenfor lovens anvendelsesområde.[51]

Definisjonen er i utgangspunktet svært vid med tanke på hvilken type informasjon som kan anses som en personopplysning jf. «opplysninger og vurderinger». Det forutsettes imidlertid at det kan etableres en sammenheng mellom informasjonen og en bestemt person jf. «knyttes til en enkeltperson». Med andre ord må det kunne skje en identifisering. Som utvalget påpeker i NOU 2009: 1, må det fastslås hvilken type informasjon som kan muliggjøre identifikasjon av personer.[52] Informasjon som er direkte knyttet til en person vil alltid være omfattet, eksempelvis navn eller personnummer. Men også informasjon som indirekte er knyttet til en person vil omfattes, for eksempel IP-adresse, IMEI- nummer, telefonnummer, bostedsadresse, bilregistreringsnummer og yrkestittel.

Artikkel 29-gruppen har i Opinion 13/2011 lagt til grunn at lokasjonsdata fra smarttelefoner må betraktes som en personopplysning.[53] I en annen uttalelse, Opinion 2/2010, uttaler Artikkel 29-gruppen at opplysninger om bruksmønster ved bruk av tjenester også må anses som personopplysning. De begrunner uttalelsen med at opplysninger om bruksmønster vanligvis er knyttet til en IP-adresse eller andre unike enhetsidentifikatorer som kan knyttes til en person eller en liten gruppe.[54] Schartum og Bygrave ser ut til å være enige med Artikkel 29-gruppen, da de har uttalt at hvorvidt bruksmønsterinformasjon vil bli regnet som personopplysning avhenger av om tilknytningen til en bestemt person er tilstrekkelig sikker.[55] En telefon er for de fleste svært personlig og brukes gjerne kun av eieren. Tilknytningen til personen vil dermed være relativ sikker. Det fremgår uttrykkelig i den kommende personvernforordningen at både lokasjonsdata og bruksmønsterinformasjon er å anse som

---

[50] Ot.prp.nr.92 (1998-1999) s. 101
[51] Ot.prp.nr.92 (1998-1999) s. 101
[52] NOU 2009: 1 s. 47
[53] Opinion 13/2011 s. 20
[54] Opinion 2/2019 s. 9
[55] Schartum og Bygrave (2016) s. 139

personopplysninger.[56]

Ved indirekte koblinger mellom opplysninger og personen må gjerne flere opplysninger bringes på det rene før koblingen kan fastslås. Det er ikke noe vilkår for at opplysningene skal anses som personopplysning at en på et gitt tidspunkt vet hvilken person det foreligger opplysninger om. Det er tilstrekkelig at det er mulig å identifisere vedkommende. Likevel er ikke enhver fjern mulighet tilstrekkelig. Dersom innsatsen som skal til for å knytte en person til en opplysning er betydelig kan det være at opplysningen faller utenfor begrepet.[57]

Ut fra det ovennevnte er det klare utgangspunktet at samtlige av de opplysningene som applikasjonene undersøkt i oppgaven innhenter jf. punkt 2.3 er å anse som «personopplysninger».

Begrepet «behandling av personopplysninger» er definert i personopplysningsloven § 2 nr. 2 som «enhver bruk av personopplysninger». Som eksempler nevnes «innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter». En naturlig språklig forståelse av bestemmelsens ordlyd tilsier at behandlingsbegrepet er svært vidt. Proposisjonen taler også for en vid forståelse av begrepet. Det fremgår her at «behandling av personopplysninger» omfatter «enhver formålsrettet håndtering av personopplysninger».[58] Det betyr at alle typer handlinger som kan tenkes utført med personopplysninger i utgangspunktet vil omfattes.

På bakgrunn av dette vil tjenestetilbydernes registrering, bruk og viderebruk av personopplysninger ved nedlastning og bruk av applikasjoner anses som behandling av personopplysninger.

---

[56] Personvernforordningen artikkel 4 nr. 1 og fortalepunkt 30
[57] Schartum og Bygrave (2016) s. 139
[58] Ot.prp.nr.92 (1998-1999) s. 102

## 3.3 De sentrale aktørene

I personopplysningsloven er det særlig tre sentrale aktører som står i fokus ved behandling av personopplysninger. Dette er den «behandlingsansvarlig[e]», den «registrert[e]» og «databehandler[en]». Det må være registrerte personer og en behandlingsansvarlig dersom loven skal komme til anvendelse.[59] Databehandlere er aktuelle aktører, men må ikke nødvendigvis forekomme.[60]

Den «behandlingsansvarlig[e]» er ifølge personopplysningsloven § 2 nr. 4 «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes». I proposisjonen fra departementet fremgår det at den behandlingsansvarlige er den som har «bestemmelsesrett over personopplysningene».[61] Ifølge forarbeidene kan den behandlingsansvarlig være en fysisk eller en juridisk person.[62] Det forutsettes imidlertid at subjektet har sivilprosessuell partsevne.[63] Den behandlingsansvarlige pålegges en rekke plikter etter loven, blant disse er å sørge for at gyldig og korrekt innhentet samtykke foreligger.[64]

Behandlingsansvarlig ved behandling av personopplysninger i forbindelse med installasjon og bruk av mobilapplikasjoner vil ofte være selskapet som leverer applikasjonen. Den behandlingsansvarlige omtales som «tjenestetilbyder» i denne oppgaven.

Den «registrert[e]» er i personopplysningsloven § 2 nr. 6 definert som «den som en personopplysning kan knyttes til». En naturlig språklig forståelse av «registrert» synes å forutsette at det kun dreier seg om personer som det er lagret eller registrert opplysninger om fra før. Ordlyden er dermed noe misvisende. Hvorvidt en person skal anses som registrert beror på om personopplysningene som behandles kan knyttes til vedkommende eller ikke.[65] Med andre ord vil betydningen av «personopplysning» og «behandling av

---

[59] Schartum og Bygrave (2016) s. 158
[60] Schartum og Bygrave (2016) s. 158
[61] Ot.prp.nr.92 (1998-1999) s. 102
[62] Ot.prp. nr. 92 (1998-99) s. 102-103 og NOU 1997: 19 s. 132-133
[63] Ot.prp. nr. 92 (1998-99), s 102 og NOU 1997: 19 s. 133
[64] Personopplysningsloven § 11første ledd
[65] Coll og Lenth (2000) s. 66

personopplysninger» bli bestemmende for hvem som er å anse som registrert.[66]

En bruker som laster ned og tar i bruk de tjenestene applikasjonene tilbyr er å anse som «registrert». Den «registrert[e]» omtales i oppgaven som «bruker».

En «databehandler» er definert i personopplysningsloven § 2 nr. 5 som «den som behandler personopplysninger på vegne av den behandlingsansvarlige». Databehandleren er typisk en juridisk person, gjerne et firma, men kan også være en fysisk person.[67] En databehandler er kun en aktuell aktør dersom denne blir oppdragstaker hos den behandlingsansvarlige (tjenestetilbyderen) og har som oppgave å behandle personopplysninger på dennes vegne. Med utviklingen innenfor informasjonsteknologi har det blitt vanlig at firma utfører behandling av data, herunder personopplysninger, på vegne av andre selskaper.[68] Årsaken til dette er at disse firmaene ofte har bedre kompetanse, bedre teknologi eller er mer kostnadseffektive.[69]

## 3.4 Krav om hjemmel ved behandling av personopplysninger

### 3.4.1 Hjemmelskravet

I norsk rett gjelder det et alminnelig krav om hjemmel for rettslige beslutninger og enkelte faktiske handlinger. Den som vil fastsette rettslige beslutninger som binder andre må kunne vise til et hjemmelsgrunnlag som rettsordenen anerkjenner. Eng kaller dette for kompetansegrunnsetningen.[70]

Personopplysningsloven § 8 jf. § 11første ledd bokstav a kan sies å være en presisering av hjemmelskravet på personopplysningsrettens område, da det her oppstilles et alminnelig krav om hjemmel ved behandling av personopplysninger. Personopplysningsloven § 8 fastsetter tre

---

[66] Schartum og Bygrave (2016) s. 159
[67] Schartum og Bygrave (2016) s. 173
[68] Jan Sandtrø, *Databehandlers behandling av personopplysninger*, artikkel Idunn.no 2016
[69] Sandtrø (2016)
[70] Svein Eng*, Begrepene «kompetanse» og «gyldighet» i juridisk argumentasjon,* Tidsskrift for rettsvitenskap ISSN 0040-7143, 1990 s. 647

alternative behandlingsgrunnlag. Det må enten foreligge samtykke fra den registrerte, en lovhjemmel eller at behandlingen av personopplysningene er å anse som nødvendig for å fremme visse formål eller virkninger som er angitt i § 8 bokstav a til f.

Behandlingsgrunnlaget må foreligge før personopplysningene blir behandlet for at behandlingen skal kunne anses som lovlig.

### 3.4.2 Forholdet mellom samtykke og avtale som behandlingsgrunnlag

Samtykke er det mest praktiske behandlingsgrunnlaget ved nedlastning og bruk av applikasjoner, og er det behandlingsgrunnlaget som behandles i oppgaven. Det er likevel verdt å merke seg at det kan foreligge et annet behandlingsgrunnlag i tillegg til samtykke. Særlig aktuelt er avtale som behandlingsgrunnlag. Etter personopplysningsloven § 8 bokstav a kan personopplysninger behandles dersom behandlingen er «nødvendig for å oppfylle en avtale med den registrerte». En naturlig språklig forståelse av bestemmelsens ordlyd tilsier at det er et vilkår at brukeren og tjenestetilbyderen har inngått en avtale som krever behandling av personopplysninger, og at avtalen ikke kan oppfylles uten at personopplysningene behandles.

Det er åpenbart en likhet mellom avtale som behandlingsgrunnlaget og samtykke som behandlingsgrunnlag, men det er også en del ulikheter. Avtalealternativet innebærer en avtaleaksept og forutsetter at behandling av personopplysninger er nødvendig for å gjøre noe som brukeren selv ønsker.[71] En slik aksept kan betegnes som et «samtykke», men personopplysningslovens vilkår for et gyldig samtykke kommer ikke til anvendelse ved avtaleinngåelse etter § 8 bokstav a.[72] Aksepten som gis er med andre ord ikke beskyttet av vilkårene som skal sikre at brukeren selv har tatt direkte stilling til om den aktuelle behandlingen av personopplysningene skal tillates.[73] Vurderingen av hvilke personopplysninger og til hvilke formål det er nødvendig å behandle opplysningene overlates til tjenestetilbyderen. Tjenestetilbyderen må vurdere hva som er nødvendig, og dermed lovlig å behandle, ut fra den inngåtte avtalens formål.[74] Dersom tjenestetilbyderen ønsker å behandle

[71] Schartum og Sætre (2016) s. 18
[72] Schartum og Sætre (2016) s. 18
[73] Olsen (2015) s. 364
[74] Schartum og Bygrave (2016) s. 181

personopplysninger utover det som er nødvendig for oppfyllelse av avtalen kreves det et supplerende grunnlag for behandlingen.

Når det gjelder behandling av personopplysninger til kommersiell bruk, har Artikkel 29-gruppen uttalt i Opinion 06/2014 at slik behandling neppe kan anses som nødvendig for å tilby en tjeneste og dermed oppfylle en avtale.[75] Det betyr at dersom tjenestetilbyderne skal ha adgang til å bruke personopplysninger til kommersielle formål må de ha grunnlag for dette i et annet behandlingsgrunnlag. Det mest naturlige er at det innhentes et samtykke fra brukeren.

På bakgrunn av dette vil tjenestetilbyderne kunne registrere og behandle de personopplysningene som er nødvendige for oppfyllelsen av avtalen med brukeren med grunnlag i avtalealternativet. Dette gjelder flere av applikasjonene undersøkt i forbindelse med oppgaven. Eksempelvis må Æ-appen med grunnlag i avtalen ha rett til å behandle telefonnummeret til brukeren. Uten telefonnummeret vil ikke tjenesten kunne tilbys brukeren og avtalen vil ikke kunne oppfylles. Men for bruk av personopplysningene til kommersielle formål må tjenestetilbyderne ha grunnlag i samtykke fra brukeren. Tjenestetilbyderne velger dermed ofte å innhente samtykke fordi de kan da foreta en mer utstrakt bruk av personopplysningene.

[75] Opinion 06/2015 s. 18 og s. 45-46

# 4. Hvilke vilkår stilles for et gyldig samtykke?

## 4.1 Innledning

Et samtykke er etter definisjonen i personopplysningsloven § 2 nr. 7 en «frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv». Det er altså tre kumulative vilkår som må være oppfylt for at et samtykke skal være gyldig.

I det følgende kapittelet vil det gjøres rede for innholdet i de tre vilkårene. I lys av vilkårene vil det bli drøftet om den type samtykke som gis i forbindelse med installasjon og bruk av applikasjoner oppfyller disse. Det vil også gis noen korte bemerkninger til avtalelovens krav til gyldig aksept, for å se hvorvidt personopplysningsloven gir et større vern enn de generelle reglene som fremgår av avtaleloven.

## 4.2 Frivillig

### 4.2.1 Innledning

Det første vilkåret som må være oppfylt for at behandling av personopplysninger skal kunne baseres på samtykke, er at samtykket må være avgitt «frivillig».[76] En naturlig språklig forståelse av «frivillig» tilsier at brukeren selv må bestemme at han ønsker å samtykke til tjenestetilbyderens bruk av hans personopplysninger. Ordlyden gir imidlertid ingen holdepunkter for hva et frivillig samtykke faktisk er. Et nærliggende spørsmål er hvilke forhold som kan medføre at et samtykke ikke er å anse som frivillig.[77]

En aksept etter avtalerettslige regler må også være frivillig. Det gjelder med andre ord et generelt krav om frivillighet i norsk avtalerett.[78]

---

[76] Samsvarer med personverndirektivets vilkår i artikkel 2 bokstav h jf. «freely»
[77] Schartum og Sætre (2016) s. 58
[78] Lov 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer («avtaleloven») §§ 28 og 29

Vilkåret om frivillighet vil videre belyses ved å trekke frem forhold som gjør at et samtykke ikke kan anses å være frivillig. Fremstillingen er delt inn i fire deler: «tvang og negativ påvirkning», «negative konsekvenser og sanksjoner», «tilbaketrekking av samtykke» og «behandling av personopplysninger som ikke er nødvendig»

### 4.2.2 Tvang og negativ påvirkning

Det følger av proposisjonen fra departementet at et samtykke ikke kan være avgitt «under noen form for tvang fra den behandlingsansvarlige eller andre».[79] Det er åpenbart at dersom en bruker utsettes for tvang fra tjenestetilbyderen eller andre, vil ikke vilkåret om frivillig samtykke være oppfylt. Artikkel 29-gruppen har drøftet vilkåret i Opinion 15/2011, og ifølge gruppen innebærer vilkåret at det heller ikke må ha forekommet noen form for negativ påvirkning fra andre i forbindelse med avsigelsen.[80] Som eksempler nevnes å skremme eller lure en person til å samtykke til at det blir behandlet personopplysninger om vedkommende.

Videre i Opinion 15/2011 presiserer Artikkel-29 gruppen kravet til frivillighet ved å gjengi en av sine tidligere uttalelser. Artikkel 29-gruppen uttaler her at den intellektuelle kapasiteten til den som samtykker vil være et vektig moment i vurderingen av hvorvidt et samtykke er å anse som frivillig.[81] Alle mennesker er forskjellige og noen blir lettere påvirket enn andre. Grensen for når et samtykke ikke er å anse for frivillig vil dermed kunne variere fra person til person, og må vurderes konkret i hvert enkelt tilfelle.

Ved nedlastning av applikasjoner er ikke tvang og negativ påvirkning særlig aktuelt, men det kan likevel ikke ses bort fra at tjenestetilbydere tar i bruk virkemidler som bidrar til en form for psykisk negativ påvirkning. Et eksempel er RuterBillett-appen som etterspør samtykke til behandling av personopplysninger etter at applikasjonen er lastet ned og klar for bruk. Det påpekes samtidig at applikasjonen ikke vil fungere optimalt dersom brukeren ikke samtykker.

---

[79] Ot.prp. nr. 92 (1998-1999) s. 103-104
[80] Opinion 15/2011 s. 12
[81] Opinion 15/2011 s. 13

Ved at tjenestetilbyderen påpeker dette vil brukeren påvirkes i negativ retning.

### 4.2.3 Negative konsekvenser

Personvernnemnda har i flere av sine avgjørelser gitt uttrykk for at et samtykke ikke må være påvirket av frykt for eventuelle negative konsekvenser av at samtykket ikke gis. I Personvernnemndas avgjørelse «Securitas», som gjaldt blant annet adgangen til å gjennomføre rusmiddelkontroll av ansatte i Securitas, legges det til grunn en streng fortolkning av vilkåret frivillig. Selv om arbeidsgiveren uttrykte at nektelse av å utføre kontrollen ikke ville få følger for ansettelsesforholdet, uttalte Personvernnemnda at det «for den enkelte likevel [vil] være nærliggende å oppleve at det vil kunne få konsekvenser for vedkommendes arbeidsforhold».[82] Nemnda kom frem til at behandling av personopplysninger innhentet ved testene ikke kunne skje med grunnlag i samtykke. I avgjørelsen «Sentralt låneregister», som gjaldt hjemmelsgrunnlaget for opprettelse av et sentralt låneregister, uttalte nemnda at «det er åpenbart at hvis samtykke stilles som vilkår for at en lånesøknad skal behandles, vil det ikke være avgitt med det krav til frivillighet som stilles i personopplysningsloven».[83] Personvernnemnda kom frem til at et slikt låneregister måtte etableres med hjemmel i lov. På bakgrunn av dette ser det ut til at Personvernnemnda oppstiller strenge krav til når et samtykke kan anses å være frivillig.

Det ser ut til at Artikkel 29-gruppen også legger til grunn en streng fortolkning av vilkåret. I den allerede omtalte Opinion 15/2011 uttaler gruppen at bortfall eller redusert kvalitet på en tjeneste som følge av at en bruker ikke vil avgi sitt samtykke, kan medføre at samtykket ikke kan anses å være frivillig.[84] Såkalte «take-it-or-leave-it»-løsninger vil være problematiske, da de innebærer at brukeren må samtykke til behandling av personopplysninger for å kunne ta i bruk tjenesten som tilbys. Slike løsninger er utbredt og flere av tjenestetilbyderne undersøkt i oppgaven tar i bruk denne typen løsning.

Her skiller kravet til frivillighet seg fra det generelle kravet til frivillighet etter avtaleretten. Etter personopplysningsloven oppstilles det et strengere krav. Personopplysningsloven gir

---

[82] PVN-2005-06 (Securitas)
[83] PVN-2003-01 (Sentralt låneregister)
[84] Opinion 15/2011 s. 13

dermed et større vern enn det avtaleloven gjør på dette punkt.

En må imidlertid spørre seg om Personvernnemnda og Artikkel 29-gruppen legger til grunn en for streng fortolkning av vilkåret. Det bør kunne settes saklige og rimelige vilkår om at det må gis samtykke til bruk av personopplysninger ved innvilgelse av en tjeneste, uten at det skal medføre at samtykket ikke kan anses å være frivillig. Öman og Lindblom ser ut til å legge til grunn en mer liberal fortolkning av vilkåret knyttet til negative konsekvenser.[85] Ifølge Öman og Lindblom bør frivilligheten vurderes ut fra hvorvidt tjenesten kan anses som nødvendig i dagens samfunn eller for den enkelte.[86] Dersom tjenesten ikke er nødvendig vil det neppe være problematisk at tjenesten forutsetter samtykke fra brukeren. Er tjenesten derimot nødvendig vil en vurdering av samtykkets frivillighet bero på om det finnes andre tjenestetilbydere som tilbyr en alternativ tjeneste uten at det settes krav om samtykke. Finnes det ingen reelle alternative muligheter vil det tale for at samtykket ikke kan være frivillig.

Blume har også uttrykt tvil om et frivillighetsvilkår som tolkes for strengt.[87] Ifølge Blume må vilkåret tolkes strengt i de tilfeller det er tale om tvang eller hierarkiske relasjoner, men at det utover slike tilfeller må settes en grense for hvor strengt vilkåret kan tolkes.[88] Når det gjelder tilfeller hvor brukeren vil samtykke fordi han ønsker å motta en tjeneste, mener Blume at samtykket bør anses som frivillig selv om tjenesten ikke kan mottas uten at vedkommende samtykker.[89]

Grensen mellom beskyttelse av brukernes personvern og samtykke som aktuelt behandlingsgrunnlag er komplisert. Ved en streng fortolkning av vilkåret gis brukeren en sterk beskyttelse av sitt personvern. Samtidig mister samtykke en del av sin betydning fordi det skal så mye til for at samtykket oppfyller vilkåret. På mange måter vil brukeren da fratas adgangen til samtykke, noe som også kan fremstå som umyndiggjørende.

Legges det til grunn en for streng fortolkning kan ikke et samtykke anses som frivillig i de

---

[85] Se Olsen (2015) som henviser til Sören Öman og Hans-Olof Lindblom, Personuppgiftslagen, 3. uppl., Stockholm 2007, s. 93
[86] Se Olsen (2015) som henviser Öman og Lindblom (2007) s. 93
[87] Peter Blume, *Konsumenterne og persondatabeskyttelse i Norden*, København 2000 s. 17-18 og Peter Blume, *Persondata rettslige grundfigurer*, 1. utg., København 2017 s. 66
[88] Blume (2017) s. 66
[89] Peter Blume, *Databeskyttelsesret*, 4. utg., København 2013 s. 17-18

tilfeller det ikke er mulig å ta i bruk en applikasjon, uten at brukeren må samtykke til behandling av personopplysninger. De aller fleste av tjenestene som tilbys via applikasjoner kan ikke anses som nødvendige, noe som taler for at det ikke er urimelig overfor brukeren at han ikke får ta i bruk tjenesten uten å samtykke. Videre er applikasjonene ofte gratis, og legges det til grunn en for streng fortolkning vil det medføre at slike gratistjenester ikke kan forbli gratis. Som følge av dette vil ikke brukeren ha mulighet til å bruke sine personopplysninger som en forhandlingsressurs.

Et aktuelt spørsmål er videre hvordan kravet til frivillighet stiller seg ved en endring av brukeravtalen eller personvernerklæringen. Tjenestetilbyderne forbeholder seg ofte retten til å ensidig endre disse. Ved en eventuell endring vil brukeren måtte avgi sitt samtykke på nytt for å kunne fortsette sin bruk av tjenesten. Det vil utgjøre en negativ konsekvens dersom brukeren ikke vil kunne fortsette sin bruk av tjenesten dersom han ikke samtykker til de nye vilkårene. På dette tidspunktet kan vedkommende ha brukt tjenesten i lang tid og den kan ha blitt en del av brukerens hverdag. Eksempelvis er RuterBillett-appen en del av hverdagen til mange mennesker som oppholder seg i Oslo og omegn. Dersom brukeren av RuterBillett-appen ikke ønsker å samtykke til de nye vilkårene vil han måtte gå over til et fysisk reisekort. Et fysisk reisekort er på mange måter mindre praktisk, da brukeren eksempelvis må oppsøke Ruters servicekontor eller bestemte utsalgssteder for å fylle på kortet. Det er en vesentlig forskjell på å ta i bruk en ny tjeneste og det å fortsette bruk av en tjeneste. Terskelen for å ikke samtykke vil være høyere når det er tale om å fortsette bruk av en tjeneste. Dette taler for at det bør stilles strengere krav til når et samtykke kan anses som frivillig ved tale om fortsatt bruk.

### 4.2.4 Tilbakekall av samtykke

Artikkel 29-gruppen har i Opinion 15/2011 uttalt at vilkåret om frivillig samtykke står i sammenheng med muligheten til å trekke samtykket tilbake. Det finnes ingen uttrykkelig bestemmelse i hverken personopplysningsloven eller personverndirektivet som gir brukeren rett til å tilbakekalle sitt samtykke. Det følger imidlertid av proposisjonen til departementet at det er klart at det finnes en slik rett.[90]

[90] Ot.prp.92 (1998-1999) s. 104

Artikkel 29-gruppen mener at muligheten til å trekke samtykket tilbake uten at det oppstår negative følger indikerer at samtykket er frivillig.[91] Trekkes et samtykke tilbake, forutsatt at det ikke foreligger et annet behandlingsgrunnlag, mister tjenestetilbyderen retten til å både innhente nye personopplysninger og til å fortsette behandlingen av opplysningene som allerede er samlet inn.[92] Retten til å tilbakekalle samtykket kan ses i sammenheng med personopplysningslovens visjon om selvbestemmelse. En bruker bør ha mulighet til å endre sin mening, og et samtykke vil ikke fortsette å være frivillig dersom brukeren på et senere tidspunkt ikke ønsker å tillate behandlingen av personopplysningene. Adgangen til å trekke tilbake samtykke vil dermed kunne utgjøre et moment i vurderingen av hvorvidt samtykket er å anse som frivillig.

Brukeravtalen eller personvenrerklæringen til alle applikasjonene undersøkt i oppgaven gir informasjon om brukerens adgang til å trekke sitt samtykke og hvordan dette utføres.

Retten til å trekke et samtykke tilbake fremgår klart og tydelig i den kommende forordningens artikkel 7 nr. 3. Ifølge forordningens fortalepunkt 42 skal kravet om frivillighet ikke anses å være oppfylt dersom den registrerte ikke er i stand til å trekke tilbake et samtykke uten at det er til skade for vedkommende. Det fremgår dermed uttrykkelig av forordningen at frivillighet og adgang til å trekke tilbake samtykke står i sammenheng, og at adgang til å trekke tilbake samtykket settes som krav for at vilkåret om frivillig samtykke skal være oppfylt.

### 4.2.5 Behandling av personopplysninger som ikke er nødvendige

Ifølge mine undersøkelser forutsetter flere av tjenestetilbyderne at brukeren samtykker til behandling av personopplysninger som ikke er nødvendige for tjenestens funksjon. Et eksempel er VG-appen som innhenter og behandler brukerens lokasjonsopplysninger. I personvernerklæringen begrunner tjenestetilbyderen innhentingen med ønsket om å presentere brukeren værvarslet der han befinner seg. Formidling av informasjon om været er ikke hovedfunksjonen til VG-appen og kan ikke anses som nødvendig for tjenestens funksjon. Et annet eksempel er Norli e-bok-appen som innhenter lokasjonsopplysninger fra brukere av

[91] Opinion 15/2011 s. 13
[92] Schartum og Bygrave (2016) s. 180

operativsystemet Android. Av deres brukeravtale fremgår det ingenting som kan forklarer innhentingen. Videre kan det neppe antas at lokasjonsopplysninger er nødvendig for å tilby salg av e-bøker på en applikasjon.

I den kommende personvernforordningens artikkel 7 nr. 4 fremgår det at det i vurderingen av om et samtykke er avgitt frivillig, skal tas størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfyllelse av avtalen. Bestemmelsen ser dermed ut til å snevre inn tjenestetilbydernes mulighet til å kreve samtykke til bruk av personopplysninger som ikke er nødvendig for å tilby tjenesten. Artikkel 29-gruppen har uttalt i Guidelines on Consent under Regulation 2016/679 at formålet med bestemmelsen er å hindre at samtykke til bruk av personopplysninger kan brukes som motytelse ved inngåelse av en avtale.[93] At det skal tas «størst mulig» hensyn taler imidlertid for at bestemmelsen ikke kan tolkes absolutt. Men Artikkel 29-gruppen har i ovennevnte uttalelse gitt uttrykk for at adgangen til å gjøre unntak er svært begrenset.[94]

En kan spørre seg om bestemmelsen vil medføre en for streng tolkning av vilkåret om frivillig samtykke. Større vern for brukeren er positivt, men bestemmelsen vil også medføre negative konsekvenser. For det første vil samtykke som behandlingsgrunnlag i en rekke tilfeller miste sin relevans. Er personopplysningene nødvendige for å oppfylle en avtale vil like gjerne avtale som behandlingsgrunnlag etter forordningens artikkel 6 nr. 1 bli brukt. For det andre vil brukeren miste muligheten til å bruke egne personopplysninger som en forhandlingsressurs ved at samtykke ikke lengre vil kunne brukes som en motytelse til en tjeneste. For det tredje vil bestemmelsen medføre at tjenestetilbydere ikke lengre kan tilby tjenestene gratis, fordi de vil miste mye av sitt inntektsgrunnlag ved å ikke kunne innhente andre personopplysninger enn de som er nødvendige for tjenestens funksjon.

Det må også kunne antas at «minimalitetsprinsippet» som kommer til uttrykk i både dagens lovgivning og den kommende forordningen tar sikte på å beskytte brukeren mot urimelige tjenestetilbydere, og vil fange opp situasjoner som bestemmelsen tar sikte på å beskytte

---

[93] Guidelines on Consent under Regulation 2016/679 s. 9
[94] Guidelines on Consent under Regulation 2016/679 s. 10

brukeren fra.[95]

Det kan i det minste fastslås at personvernforordningen artikkel 7 nr. 4 vil bidra til å utdype hva det skal tas hensyn til i vurderingen av om et samtykke er frivillig. Det vil bli spennende å se hvordan bestemmelsen blir tolket i praksis.

## 4.3 Uttrykkelig

### 4.3.1 Innledning

Det neste vilkåret som må være oppfylt for at behandling av personopplysninger skal kunne baseres på samtykke, er at samtykket er avgitt «uttrykkelig». En naturlig forståelse av ordlyden innebærer at samtykket skal gis ved en tydelig handling som klart markerer at det er brukerens intensjon å gi tillatelse. Etter personverndirektivet er det et vilkår at samtykket er «specific».[96] En tolkning av «specific» tilsier at samtykke etter direktivet skal angis på en klar og presis måte. Dette taler for at det stilles krav om at det fremgår klart at brukeren samtykker, men også hva det samtykkes til. I Opinion 02/2013 uttaler Artikkel 29-gruppen at samtykket skal gi uttrykk for brukerens vilje, i tillegg til at det skal fremgå klart hvilke personopplysninger og hvilken behandling det samtykkes til.[97] Det ser dermed ut til at direktivet stiller strengere krav enn personopplysningsloven. I proposisjonen fra departementet fremgår det imidlertid at vilkåret om uttrykkelig samtykke etter personopplysningsloven ikke bare stiller krav om en klar og utvetydig handling, men at det også er et krav at det fremgår klart «hvilke behandlinger samtykket omfatter og hvilke behandlingsansvarlige det er rettet til».[98] Personopplysningsloven og direktivet er dermed i samsvar også her.

Dette betyr at vilkåret om uttrykkelig samtykke inneholder to krav. For det første er det krav til hvordan samtykkeerklæringen skal komme til uttrykk. For det andre er det krav til

---

[95] Se personopplysningsloven § 11 første ledd bokstav d, personverndirektivet artikkel 6 nr. 1 bokstav c og personvernforordningen artikkel 5 nr. 1 bokstav c
[96] Personverndirektivet artikkel 2 bokstav h
[97] Opinion 02/2013 s. 15
[98] Ot.prp.92 (1998-1999) s. 103

samtykkets innhold og rekkevidde.[99]

Den videre fremstillingen av vilkåret om uttrykkelig samtykke deles inn i «krav til samtykkeerklæringen» og «krav til samtykkets innhold og rekkevidde».

### 4.3.2 Krav til samtykkeerklæringen

Ifølge proposisjonen fra departementet stilles det ingen formkrav til hvordan samtykket fra brukeren skal gis, og samtykket kan derfor gis både muntlig, skriftlig og elektronisk.[100]

Skal et samtykke gis ved en tydelig handling tilsier dette at samtykket må utgjøre en aktiv handling. I NOU 1997:19 er det lagt til grunn at et passivt eller stilltiende samtykke ikke er tilstrekkelig, det samme gjelder et samtykke avgitt gjennom konkludent atferd.[101] Personvernnemnda ser ut til å ha den samme oppfatningen av kravet. I Personvernnemndas avgjørelse «Ung i Norden» var spørsmålet hvorvidt et foreldresamtykke kunne avgis passivt.[102] Personvernnemnda uttalte her at «personopplysningsloven åpner ikke for passivt samtykke». Videre ble det uttalt at «når kravet til samtykke er at det skal være «uttrykkelig» er det bare det aktive samtykke som kan godtas».

Etter avtalerettslige regler oppstilles det ingen krav til uttrykkelig samtykke, og avtaler kan dermed inngås ved konkludent atferd. Kravet til uttrykkelig samtykke gir dermed her større beskyttelse for brukeren sammenlignet med de generelle avtalerettslige reglene.

Artikkel 29-gruppen har i Opinion 2/2010 vurdert hvorvidt det er en tilstrekkelig løsning at brukeren har mulighet til å reservere seg mot behandlingen av personopplysningene etter at tjenesten er tatt i bruk.[103] En slik løsning innebærer med andre ord at brukeren aktivt må endre innstillingene i tjenesten etter nedlastning for å hindre behandlingen. Gruppen anser en slik løsning for problematisk da folk flest forholder seg passivt til den standardløsningen en tjeneste leveres med. Et annet moment er at de fleste ikke har nok kunnskap til å forstå

---

[99] Olsen (2015) s. 352
[100] Ot.prp.92 (1998-1999) s. 103
[101] NOU 1997:19 s. 186
[102] PVN-2010-09 (Ung i Norden)
[103] Opinion 2/2010 s. 15

nødvendigheten av å endre innstillingene. Det å ikke motsette seg kan ikke sidestilles med å samtykke. Gruppen er derimot åpne for at en motsatt løsning, hvor innstillingene i utgangspunktet er satt til ingen deling av personopplysninger, oppfyller kravet til uttrykkelig samtykke. [104] En bruker må da aktivt gå inn og endre innstillingene for at personopplysningene skal deles. Brukeren vil i den forbindelse måtte foreta en vurdering av hvorvidt han ønsker å dele personopplysningene eller ikke, og kravet til aktivt samtykke må anses å være oppfylt.

Samtykkehandlingen ved nedlastning og bruk av applikasjoner er som nevnt i innledningens punkt 1.2 former for elektronisk samtykke, gjennom klikk på et ikon eller innlogging med registrert bruker. Slike handlinger anses å oppfylle lovens krav til samtykkeerklæringen.

Det er den behandlingsansvarlige som har bevisbyrden og som må sannsynliggjøre at det foreligger et samtykke. Dette fremgår allerede av gjeldende rett, men vil bli uttrykkelig fastslått i artikkel 7 nr. 1 i den kommende forordningen. Det stilles ingen krav etter den nåværende lovgivningen om at samtykket må være dokumentert. Det vil imidlertid være enklere å sannsynliggjøre et samtykke dersom dette er avgitt skriftlig, enten på papir eller elektronisk. Med forordningen vil det stilles strengere krav til dokumentasjon. I artikkel 5 nr. 2 fremgår det at den behandlingsansvarlige må påvise at det er gitt samtykke.

### 4.3.3 Krav til samtykkets innhold og rekkevidde

Som nevnt skal det også klart fremgå av samtykket hva brukeren samtykker til. Kravet må blant annet ses i sammenheng med formålsbestemthetsprinsippet som kommer til uttrykk i blant annet personopplysningslovens § 11 første ledd bokstav b.[105] Dersom det er flere formål med behandlingen skal det gå klart frem hvilke formål det samtykkes til. I sammenheng med dette er det naturlig at samtykket også gir uttrykk for hvilke personopplysninger brukeren tillater at blir behandlet til de ulike formålene. Videre er det viktig at samtykket uttrykker hvem brukeren tillater at behandler personopplysningene, og at det dermed fremgår av samtykket hvem tjenestetilbyderen er. Kravet som stilles til samtykkets innhold og rekkevidde bidrar til at brukeren må ta stilling til eget personvern, og sikrer i større grad et

[104] Opinion 2/2010 s. 16
[105] Olsen (2015) s. 352- 353

bevisst samtykke.

Artikkel 29-gruppen uttaler i Opinion 02/2013 at det å kun krysse av i en boks eller trykke på et ikon ikke kan anses som tilstrekkelig fordi samtykket ikke kan være en slik generell aksept.[106] Gruppen mener at en tilnærming hvor brukerne bes om å godta et lengre sett av vilkår ikke utgjør et spesifikt samtykke.[107] Skal samtykket være gyldig må brukeren kunne avgi sitt samtykke for hver type personopplysning og til hvert enkelt formål. I praksis kan dette gjøres ved at tjenestetilbyderne tar i bruk en løsning hvor de ulike personopplysningene og de ulike formålene presenteres hver for seg, og brukeren gis mulighet til å krysse av for de opplysninger og formål vedkommende godtar at blir behandlet.

Samtykket i forbindelse med nedlastning og bruk av applikasjoner innhentes ved at brukeren må godta et lengre sett av vilkår, herunder vedrørende behandling av personopplysninger, i ett og samme trykk. Denne typen samtykke er ikke å anse i overensstemmelse med kravet til samtykkets omfang og rekkevidde.

I den kommende forordningen er kravet til samtykkets innhold og rekkevidde presisert. Av forordningens artikkel 7 nr. 2 fremgår det at samtykke til bruk av personopplysninger ikke kan inntas som en del av vilkårene for en tjeneste. Det betyr at en bruker ikke kan samtykke til behandlingen av personopplysningene samtidig som han aksepterer vilkårene for tjenesten. Dette vil presisere at samtykke til å behandle personopplysninger ikke er det samme som en generell avtaleinngåelse. I forordningens fortalepunkt 32 fremgår det at det må gis samtykke til alle formålene dersom behandlingen har flere formål. Forordningen vil følgelig bidra til en presisering av hvordan tjenestetilbydere må tilrettelegge sine tjenester ved innhenting av samtykke, for å oppfylle vilkåret om uttrykkelig samtykke.

---

[106] Opinion 02/2013 s. 15
[107] Opinion 02/2013 s. 15

## 4.4 Informert

### 4.4.1 Innledning

Det tredje vilkåret som må være oppfylt for at behandling av personopplysninger skal kunne baseres på samtykke et at samtykket er «informert».[108] En naturlig språklig forståelse av «informert» tilsier at brukeren skal gis informasjon om relevante faktiske forhold.[109] Tilstrekkelig og god informasjoner er avgjørende for at brukeren skal kunne foreta et bevisst valg vedrørende hvorvidt han ønsker å avgi sitt samtykke eller ikke. Ordlyden sier imidlertid lite om hvilken informasjon som skal gis eller når og hvordan denne skal formidles. Forarbeidene bidrar heller ikke til særlig større klarhet, og det fremgår her kun at det skal gis tilstrekkelig informasjon slik at vedkommende vet hva han samtykker til.[110]

I juridisk teori er det derimot enighet om at det i utgangspunktet er grunn til å gi informasjon om de samme forhold som den behandlingsansvarlige skal informere om ved innsamling av personopplysninger etter personopplysningsloven § 19.[111] Bestemmelsen angir informasjonsplikten den behandlingsansvarlige har når opplysningene samles inn direkte fra den registrerte. Informasjonsplikten må tolkes i lys av samtykkesituasjonen, noe som blant annet vil medføre at det også må informeres om andre forhold enn de som uttrykkelig fremgår av personopplysningsloven § 19. Det må samtidig understrekes at hva som skal til for at et samtykke er å anse som avgitt på et informert grunnlag må vurderes konkret.[112]

Fremstillingen av informasjonskravet er videre inndelt i seks deler: «informasjon om hva det samtykkes til», «informasjon om mulige konsekvenser av behandlingen», «annen informasjon som kan styrke brukerens stilling», «kontaktinformasjon», «tidspunktet informasjonen gis» og

---

[108] Samsvarer med personverndirektivets vilkår i artikkel 2 bokstav h jf. «informed».
[109] Schartum og Bygrave (2016) s. 178
[110] Ot.prp.92 (1998-1999) s.104, NOU 1997:19 s. 186 og NOU 2009:1 s. 44
[111] Jon Bing, *Samtykke til behandling av personopplysninger i arbeidsforhold*, artikkel lovdata.no 2009 s. 57 og Schartum og Sætre (2016) s. 61
[112] Olsen (2015) s. 356

«måten informasjonen gis».[113]

### 4.4.2 Informasjon om hva det samtykkes til

For å ha mulighet til å ivareta sitt personvern må brukeren få informasjon om hva det samtykkes til. Informasjon er dessuten en forutsetning for berettiget tillit, og dersom brukeren skal samtykke til tjenestetilbyderens behandling må han ha tillitt til at personopplysningene behandles på en god måte. Det er derfor viktig at brukeren får informasjon om hva som er formålet med behandlingen av personopplysningene (§ 19 bokstav b), hvilke opplysninger som vil bli behandlet og hvem opplysningene eventuelt vil bli delt med (§ 19 bokstav c).

Vilkåret om informert samtykke må videre ses i sammenheng med vilkåret om uttrykkelig samtykke. Dersom et samtykke skal kunne anses å være uttrykkelig kan det ikke være av generell karakter, men det må fremgå klart og tydelig hva det samtykkes til jf. punkt 4.3.3. Et uttrykkelig samtykke forutsetter dermed at brukeren har fått informasjon som kan sette han i stand til å avgi et slikt uttrykkelig og spesifisert samtykke. Med andre ord kan heller ikke informasjonen som gis være for generell.

Skal brukeren få informasjon om hva han samtykker til må han for det første få informasjon om *formålet* med behandlingen av personopplysningene. Det betyr at det skal informeres om hva personopplysningene vil bli brukt til. Plikten til å informere om formålet henger sammen med formålsbestemthetsprinsippet i personopplysningsloven § 11 b. Tjenestetilbyderen har etter § 11 bokstav b plikt til å fastsette et bestemt formål for hver behandling av en personopplysning som han planlegger. Videre av § 11 bokstav b følger det at personopplysningene bare kan benyttes til de formål tjenestetilbyderen på forhånd har fastsatt. Formålet setter dermed en klar ramme for hva personopplysningene kan brukes til.

Det fremgår av proposisjonen at formålsangivelsen må være «tilstrekkelig konkret og avgrenset til at det skaper åpenhet og klarhet om hva behandlingen skal tjene til.»[114] Generelle og vage formål er uheldig fordi brukeren vil ha vanskelig for å forstå hvorfor og hvordan personopplysningene blir behandlet. Det samme gjelder svært vide behandlingsformål, de vil

---

[113] Inndelingen er inspirert av Schartum og Sætre (2016) s. 60-71
[114] Ot.prp.nr.92 (1998-1999) s. 113-114

lett medfører at brukeren mister kontroll over hvordan personopplysningene vil bli brukt.

På den annen side er det forståelig at tjenestetilbyderne har behov for å finansiere sine tjenester, og at de av den grunn ønsker å behandle så mange personopplysninger som mulig til så mange formål som mulig. Slik behandling oppnås gjerne ved bruk av vage og vide formålsangivelser. Som Blume uttaler må det vises forståelse for at tjenestetilbyderne har legitime kommersielle behov, og at det av den grunn må aksepteres at personopplysninger har en varelignende verdi.[115] I proposisjonen fremgår det imidlertid at hensynet til privatlivets fred må tillegges betydelig vekt i avveiningen mot kommersielle interesser.[116] Dette taler for at brukerens mulighet for forutberegnelighet og kontroll over egne personopplysninger går foran tjenestetilbydernes kommersielle interesser.

I flere av brukeravtalene og personvernerklæringene undersøkt i forbindelse med oppgaven fremgår ikke behandlingsformålene tilstrekkelig konkret, og dette gjør det vanskelig å forstå hva tjenestetilbyderne bruker personopplysningene til. Brukeravtalene og personvernerklæringene er utformet på en måte som gir tjenestetilbyderne stort spillerom til å utnytte personopplysningene som samles inn. Behandlingsformål som går igjen i flere av brukeravtalene og personvernerklæringene er at brukeren skal gis en «best mulig opplevelse» eller å «forbedre tjenestene». Slike formålsangivelser blir for vage, og det blir vanskelig for brukeren å forstå hva tjenestetilbyderne faktisk vil bruke personopplysningene til. Det er også et problem at tjenestetilbyderne forsøker å «pakke inn» det faktiske ved å knytte positive assosiasjoner til behandlingen.

Videre er det viktig at brukeren får informasjon om *hvilke personopplysninger* tjenestetilbyderen vil samle inn og behandle for det angitte formålet. Informasjonsplikten fremgår ikke direkte av personopplysningsloven § 19, men står i sammenheng med at det skal gis informasjon om formålet. Skal en bruker kunne vurdere hvorvidt han ønsker å samtykke til et behandlingsformål må han vite hvilke personopplysninger tjenestetilbyderen har tenkt å behandle. Det er derfor liten tvil om at også denne informasjonen skal gis.

Ifølge Schartum og Sætre kan det neppe anses å være et fast krav om at hver og en

---

[115] Blume (2017) s. 170
[116] Ot.prp.nr.92 (1998-1999) s. 109

opplysningstype skal fremgå eksplisitt av informasjonen.[117] Dersom det er tale om flere typer kan det være tilstrekkelig å angi grupper av opplysningstyper, slik som «lokasjonsopplysninger» eller «kontaktopplysninger.[118]

I de aller fleste av brukeravtalene og personvernerklæringene som er undersøkt kommer det klart og tydelig frem hvilke personopplysninger som vil bli samlet inn og behandlet. Norli e-bok-appen er den eneste som ikke presiserer hvilke personopplysninger som innhentes. I brukeravtalen står det at de vil innhente «personopplysninger du gir til oss». Denne formuleringen gir ikke brukeren god nok oversikt over hvilke personopplysninger som samles inn, fordi brukeren ikke alltid er klar over hvilke opplysninger han gir fra seg.

Til slutt er det av vesentlig betydning for brukeren å bli informert om mulig *utlevering av personopplysninger til andre*. Selv om brukeren tillater at en tjenestetilbyder samler inn og behandler hans personopplysninger, er det ikke sikkert vedkommende ønsker at andre skal få tilgang til opplysningene. Samtykker brukeren til slik utlevering risikerer han at hans personopplysninger blir delt eller solgt til aktører som bruker opplysningene til blant annet markedsføring.

På grunn av at samtykket skal innhentes før behandlingen finner sted, har det ved avgivelsen av samtykket ikke skjedd noen faktisk overføring av opplysninger til tredjeparter. Det kan dermed være tilfelle at opplysningene ikke vil bli overført til andre. Det relevante er imidlertid at det opplyses om hvem opplysningene potensielt kan bli utlevert til, om det skjer eller ikke er irrelevant. Tjenestetilbyderen kan bare utlevere personopplysninger til tredjeparter brukeren har samtykket til. Derfor bør tjenestetilbyderen på forhånd foreta grundige vurderinger av hvem han ønsker å dele informasjonen med.[119]

Deling med tredjeparter er i dag svært vanlig. Tredjeparter kan deles inn i mange grupper, blant annet reklametilbydere, analyseselskaper og andre som i utgangspunktet tilbyr tjenester til aktøren.[120] Flere av applikasjonene undersøkt i oppgaven deler personopplysninger med

---

[117] Schartum og Sætre (2016) s. 64
[118] Schartum og Sætre (2016) s. 64
[119] Schartum og Sætre (2016) s. 65
[120] Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011)

tredjeparter. VG-appen og Finn-appen deler begge adferdsopplysninger med «andre selskaper i Schibsted Media Group[121]». I personvernerklæringene fremgår det imidlertid ikke hvilke selskaper dette faktisk er. Det kan ikke forutsettes at en alminnelig bruker vet hvilke selskaper som inngår i denne gruppen. VG-appen deler også i noen tilfeller brukerens personopplysninger med sine «samarbeidspartnere». En alminnelig bruker vil ikke ha kjennskap til hvilke samarbeidspartnere det her er tale om.

### 4.4.3 Informasjon om konsekvenser

Et naturlig spørsmål i forbindelse med vilkåret om informert samtykke er hvorvidt brukeren skal informeres om hvilke konsekvenser det kan ha for hans personvern at han samtykker. Hverken personopplysningsloven eller personverndirektivet gir svar på dette spørsmålet.

NOU: 1997: 19 og en uttalelse fra Artikkel 29-gruppen kan på den ene siden tas som inntekt for at det skal gis slik informasjon. Utvalget uttalte i sin utredning at brukeren skal «forstå hva erklæringen gjelder, og hvilke konsekvenser denne får eller kan få».[122] Artikkel 29- gruppen har i sin Opinion 15/2011 uttalt at konsekvensene av å gi et samtykke bør komme til uttrykk.[123]

På den annen side er ikke kravet om konsekvensinformert samtykke videreført i senere forarbeider. I tillegg uttaler gruppen kun at det «bør» komme til uttrykk, og de oppstiller ikke et absolutt krav. Som Schartum og Sætre påpeker vil et krav om konsekvensinformert samtykke dessuten henge dårlig sammen med andre deler av personopplysningsloven.[124] Etter personopplysningsloven §§ 13 til 15 har den behandlingsansvarlige en rekke plikter til å etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å sikre brukerens personopplysninger. Et ytterligere moment er at brukeren uansett vil kunne gjøre seg opp en mening om personvernkonsekvenser ved å bli informert om hvilke personopplysninger som innhentes, behandlingsformålene og utlevering til tredjeparter. Dette taler for at det i utgangspunktet ikke er noe krav om at informasjon om konsekvenser skal gis.

---

[121] Schibsted ASA er et norskbasert internasjonalt mediekonsern, https://snl.no/Schibsted_ASA
[122] NOU 1997:19 s. 186
[123] Opinion 15/2011 s. 17
[124] Schartum og Sætre (2016) s. 66

Hvor det derimot foreligger en særskilt grunn til å tro at en ikke kan være sikker på at behandlingen vil tilfredsstille sikkerhetsmessige krav, kan det rimeligvis stilles krav om at brukeren informeres om eventuelle konsekvenser.[125]

Ingen av brukeravtalene eller personvernerklæringene undersøkt i oppgaven inneholder informasjon om hvilke konsekvenser det å avgi samtykke til innhenting av personopplysninger kan innebære. Alle applikasjonene, bortsett fra Norli e-bok-appen, informerer derimot om hvordan de ivaretar sikkerheten.

I forordningens fortalepunkt 63 fremgår det at informasjon om konsekvensene bør fremgå. Forordningen vil dermed ikke medføre noen endring i praksis, da det fortsatt ikke oppstilles et krav om konsekvensinformert samtykke jf. «bør».

### 4.4.4 Annen informasjon som kan styrke brukerens stilling

Tjenestetilbyderen skal informere brukeren om annen informasjon som gjør brukeren i stand til å anvende sine rettigheter etter loven på best mulig måte jf. personopplysningsloven § 19 bokstav e. I proposisjonen fremgår det at den behandlingsansvarlige har plikt til å gi ytterligere informasjon dersom dette må til for at den registrerte skal kunne bruke sine rettigheter på best mulig måte.[126] Som eksempel i personopplysningsloven § 19 bokstav e nevnes informasjon om innsynsrett og retten til å kreve retting. Eksemplifiseringen er ikke ment som en uttømmende regulering jf. ordlyden «som f.eks.».

I sammenheng med samtykke er informasjon om muligheten til å tilbaketrekke et samtykke relevant for styrking av brukerens stilling. Denne informasjonen er viktig fordi adgang til å trekke et samtykke gir brukeren mulighet til å stoppe behandlingen av personopplysningene dersom han endrer sin mening. Det er likevel ikke et krav om at det informeres om denne

[125] Schartum og Sætre (2016) s. 66
[126] Ot.prp.nr.92 (1998-1999) s. 119

adgangen.[127] Hvorvidt informasjon om adgangen til å trekke tilbake samtykket er gitt eller ikke vil imidlertid, som påpekt i punkt 4.2.4, kunne virke inn som et moment i vurderingen.

Alle applikasjonene undersøkt i oppgaven gir informasjon om adgangen til å trekke samtykket.

### 4.4.5 Kontaktinformasjon

Det kreves også at det gis informasjon om navn og adresse til tjenestetilbyderen og dens eventuelle representant jf. personopplysningsloven § 19 bokstav a. Formålet er å gi brukeren informasjon om hvem som gis adgang til å behandle personopplysningene. Et annet formål er å gi brukeren informasjon om hvem han kan kontakte dersom han har spørsmål vedrørende innsamlingen av personopplysningene. Når det er tale som store selskaper med flere avdelinger oppstår det spørsmål om hvor spesifikk informasjonen må være. På bakgrunn av at brukeren skal informeres om hvem han kan kontakte bør det stilles krav om en viss konkretisering.

Alle applikasjonene undersøkt i oppgaven gir tilstrekkelig informasjon vedrørende tjenestetilbyderens kontaktinformasjon.

Det er svært vanlig at tjenestetilbyderne benytter seg av databehandlere. Databehandlere behandler personopplysninger på vegne av den behandlingsansvarlige. Bruk av databehandlere medfører dermed at personopplysningene også gjøres kjent for andre enn kun tjenestetilbyderen. Dette er informasjon som kan være relevant for brukeren å få før han avgir sitt samtykke, og er dessuten av betydning for tillitsforholdet mellom brukeren og tjenestetilbyderen. Loven oppstiller ingen direkte krav om at brukeren skal gis informasjon om bruk av databehandlere, da slik involvering ikke kommer inn under informasjonsplikten etter personopplysningsloven § 19 bokstav c.[128] Tjenestetilbyderen bør likevel vurdere å informere om dette.

---

[127] Schartum og Sætre (2016) s. 67
[128] Schartum og Sætre (2016) s. 68

De fleste brukeravtalene og personvernerklæringene undersøkt i oppgaven informerer om bruk av databehandlere, men de sier ikke noe om hvem disse er.

### 4.4.6 Tidspunktet informasjonen skal gis

Etter personopplysningsloven § 19 første ledd skal informasjonen gis før samtykket blir avgitt jf. «først informere». I proposisjonen fremgår det at «noe av formålet med bestemmelsen er å sørge for at den registrerte har nok informasjon om behandlingen til å avgjøre om han eller hun vil gi fra seg opplysninger når dette er frivillig».[129] Det må altså legges til rette for at brukeren blir tilstrekkelig informert før eller samtidig med at brukeren kan samtykke. Dette er også fastslått av EU-domstolen.[130] Det betyr at informasjonen redegjort for i punkt 4.4.2 til og med 4.4.5 skal gis før eller i forbindelse med at brukeren kan avgi sitt samtykke.

I Opinion 02/2013 har artikkel 29-gruppen uttalt at informasjon i forbindelse med nedlastning og bruk av applikasjoner må gjøres tilgjengelig før brukeren laster ned applikasjonen, det vil si i nettbutikken.[131] Finnes ikke informasjonen i nettbutikken må informasjonen gis når applikasjonen er nedlastet og den åpnes første gang. Sistnevnte kan imidlertid være problematisk da innhenting av personopplysninger ofte skjer allerede ved nedlastning.

Alle applikasjonene, bortsett fra Norli e-bok-appen, har en link til sine brukeravtaler eller personvernerklæringer i App Store og Goole Play. For Æ-appen fungerer derimot ikke linken. I applikasjonene som krever særskilt innlogging etter nedlastning presenteres det en link til brukeravtalen eller personvernerklæringen også ved innlogging. De fleste av applikasjonene har i tillegg brukeravtalene og personvernerklæringene lett tilgjengelige i selve applikasjonen.

I forordningens fortalepunkt 61 fremgår det at informasjonen bør gis den registrerte på tidspunktet for innsamlingen av personopplysninger fra vedkommende. Forordningen vil dermed bidra til en uttrykkelig presisering av tidspunktet informasjonen skal gis.

---

[129] Ot.prp.nr. 92 (1998-99) s. 119
[130] Sak C-397/01 (Pfeiffer-saken)
[131] Opinion 02/2013 s. 22-23

### 4.4.7 Måten informasjonen formidles

Det finnes ingen bestemmelser i hverken personopplysningsloven eller personverndirektivet som direkte stiller krav til hvordan informasjonen skal formidles til brukeren. Det kan dermed ikke utledes noen absolutte krav eller grenser for hvordan informasjonen skal fremgå.[132] Det må likevel kunne forutsettes at informasjonen gis med et slikt innhold og på en slik måte at det legges til rette for individuelle og personlige valg.[133]

Informasjonen bør for det første ikke ha et større omfang enn at den som blir bedt om å samtykke faktisk har mulighet til å sette seg inn i det som står. For mye informasjon blir ofte uoversiktlig, noe som gjør at det blir vanskelig å sette seg inn i og forstå informasjonen. Informasjonen bør derfor gjøres så kort og konkret som mulig.

I forbindelse med sin kampanje «#appfail»[134] lastet Forbrukerrådet ned brukeravtaler og personvernerklæringer til applikasjonene på en gjennomsnittlig smarttelefon. Forbrukerrådet kom frem til at en gjennomsnittlig bruker må forholde seg til over 250 000 ord. Denne mengden tekst overstiger lengden til det nye testamentet og det ville tatt brukeren over 24 timer å lese disse høyt.[135] Kampanjen viser at det er et reelt problem at informasjonen som presenteres er for omfattende. Når det blir så mye informasjon er det nærmest umulig for en bruker å sette seg inn i innholdet. Som en følge av dette er det vanskelig for brukeren å ta bevisste valg med hensyn til eget personvern, og det ender ofte med at han samtykker uten å egentlig vite hva det samtykkes til.

Informasjonen bør for det andre ha et slikt innhold som gjør at brukeren kan forstå hva som faktisk fremgår. Det kan nok ikke oppstilles noe krav til individualisering av informasjonen, og plikten må antas å gjelde på et generelt nivå.[136] Det skal dermed tas utgangspunkt i hva en alminnelig bruker vil forstå.

Skal informasjonen være forståelig må den formuleres på en klar og tydelig måte. Juridiske

---

[132] Schartum og Sætre (2016) s. 69
[133] Rettsdata.no, lovkommentar (16) til personopplysningsloven § 2 nr. 7, Dag Wiese Schartum, 18.10.2012
[134] Forbrukerrådet satte vinteren 2016 i gang en kampanje hvor de undersøkte og analyserte populære mobilapplikasjoner. Formålet med kampanjen var å finne ut hvorvidt forbruker- og personvernet var ivaretatt.
[135] Artikkel fra Forbrukerrådet om omfanget av applikasjonsvilkår: https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/
[136] Blume (2013) s. 141

eller tekniske ord og uttrykk som ikke brukes i dagligtalen bør unngås. Når en tjeneste retter seg mot norske brukere bør informasjonen være skrevet på norsk. Det kan videre være hensiktsmessig å ta i bruk pedagogiske virkemidler som eksempler og gjentakelse.

Ingen kan tvinges til å bli informert, det må derfor antas at uansett hvor pedagogisk og konkret informasjonen utformes, vil det alltid være brukere som ikke ønsker å benytte seg av opplysningene.[137] Det relevante er imidlertid at den som ønsker å sette seg inn i behandlingen av personopplysningene får mulighet til å gjøre det.

Felles for flere av brukeravtalene og personvernerklæringene til applikasjonene undersøkt i oppgaven er at de inneholder mye tekst og er dermed tidkrevende å sette seg inn i. Videre brukes det et noe komplisert språk, herunder tekniske og juridiske ord og uttrykk.
Dette gjelder likevel ikke for samtlige av applikasjonene. Enkelte av tjenestetilbyderne formidler informasjonen på en oversiktlig måte til tross for mye tekst. Ved bruk av gode overskrifter, god struktur og spørsmålsstillinger presenteres informasjonen på en måte som gjør at brukeren får kontroll over informasjonen. Et eksempel er Norsk Tipping-appen som tar i bruk informative overskrifter og i tillegg presenterer et kort sammendrag hvor det viktigste fremgår.

I den kommende forordningen er måten informasjonen skal formidles på presisert. Etter forordningens artikkel 12 nr. 7 fremgår det at informasjonen skal presenteres på en forståelig, lettlest og meningsfull måte.

[137] Blume (2013) s. 155

# 5. Avslutning og veien videre

Formålet med oppgaven har vært å gi et svar på hvorvidt den type samtykke som gis i forbindelse med nedlastning og bruk av mobilapplikasjoner oppfyller vilkårene til et gyldig samtykke etter personopplysningsloven § 2 nr. 7. For at et samtykke skal være gyldig må tre kumulative vilkår være oppfylt. Samtykket må være frivillig, uttrykkelig og informert. Vilkårene har som formål å sikre brukere reell makt over egne personopplysninger, ved at det skal legges til rette for at brukerne kan ta bevisste og selvstendige valg vedrørende deling av sine personopplysninger.

Det foreligger flere rettskilder med relevans for fastsettelsen av innholdet i vilkårene til et gyldig samtykke. Det er derimot få av rettskildene som kan tillegges vesentlig vekt. På bakgrunn av den rettslige analysen i kapittel 4 må det likevel kunne fastslås at den type samtykke som gis ved nedlastning og bruk av personopplysninger ikke alltid lever opp til lovens krav. Det er særlig vilkårene om uttrykkelig og informert samtykke som skaper utfordringer. Brukernes personvern er dermed under press i møte med den kommersielle utnyttelsen av personopplysninger. Jeg mener det er flere årsaker som ligger bak.

For det første mener jeg det er enkelte svakheter ved lovgivningen. I alle tre vilkårene foreligger det flere krav som vanskelig kan utledes av ordlyden. Innholdet i vilkårene bør i større grad presiseres i bestemmelsens ordlyd. Den kommende personvernforordningen vil bidra til et mer moderne regelverk som i større grad er tilpasset den omfattende digitaliseringen samfunnet bærer preg av. Forordningens bestemmelser om samtykke vil gi større klarhet og presisjon rundt de ulike vilkårene. Det kan dermed se ut til at den kommende forordningen er et steg i riktig retning. Et nytt regelverk vil imidlertid ikke løse alle problemene.

For det andre må reglene i større grad etterleves av tjenestetilbyderne. Dårlig etterlevelse henger naturligvis sammen med svakhetene ved lovgivningen. Forhåpentligvis vil dette bli bedre med den kommende forordningen. Tjenestetilbyderne må i større grad legge til rette for at brukerne kan foreta bevisste og informerte valg. De må i den forbindelse tilstrebe større åpenhet rundt egen praksis og heve kvaliteten på informasjonen som gis til brukerne. Brukerne skal forstå hvorfor og hvordan personopplysningene blir behandlet. Det kan ikke

forventes at enhver bruker vil forstå eller ønsker å forstå, men det må legges til rette for de som prøver. Tjenestetilbyderne må også legge til rette for at brukerne kan avgi sitt uttrykkelige samtykke. De må tilby brukerne en løsning som gjør at det kan samtykkes til de ulike personopplysningene og behandlingsformålene hver for seg, slik at brukerne gis mulighet til å kun samtykke til behandling av de personopplysninger og behandlingsformål de selv ønsker.

Forhåpentligvis vil godt personvern i større grad bli et konkurransefortrinn. Dersom det ikke tilrettelegges for god informasjon vedrørende hvordan personopplysningene blir brukt, vil brukere heller etterspørre tjenester som gir denne informasjonen. At brukere føler seg trygge og ivaretatt er også en forutsetning for videre vekst og utvikling av digitale tjenester.[138] Dette kan tale for at det er hensiktsmessig å få utarbeidet en felles standard på området. Etter forordningen kan det se ut til at dette også er et mål. I forordningens artikkel 40 fremgår det blant annet at de nasjonale myndighetene skal oppmuntre til utarbeiding av felles adferdsnormer.

For det tredje er det behov for å øke brukernes bevissthet. De færreste reflekterer rundt eget personopplysningsvern. Brukerne kan ikke forvente å få både totalbeskyttelse og tilgang til gratistjenester. Det må dermed til en viss grad forventes at myndige personer forstår at tjenestene faktisk ikke er gratis. De har et eget ansvar som de må ta på alvor. Problemet er antagelig at innsamling av personopplysninger med formål om å bruke opplysningene kommersielt er såpass nytt. Folk flest har derfor foreløpig ikke et bevisst nok forhold til bruken av egne personopplysninger som byttemiddel. Dette vil sannsynligvis endre seg i løpet av tiden fremover. Avsløringene om grov personvernsvikt hos Facebook i mars 2018 har allerede bidratt til økt oppmerksomhet rundt temaet. Skandalen gikk ut på at data fra mange millioner Facebook-brukere ble innhentet og brukt i politisk sammenheng. Som et resultat av dette ble Facebook-sjefen Mark Zuckerberg innkalt til åpen høring hos den amerikanske Kongressen.[139] Dette viser at personvernet i møtet med den digitale verden blir tatt på alvor.

---

[138] Artikkel fra Forbrukerrådet om krav til forbrukervennlige apper: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/10-krav-til-forbrukervennlige-apper-2/

[139] Artikkel fra NRK.no om Mark Zuckerbergs høring hos den amerikanske Kongressen: https://www.nrk.no/norge/dette-er-sporsmalene-zuckerberg-unngikk-a-svare-pa-1.14004352

Som Bygrave påpeker vil det kunne være effektivt med systematiske kampanjer for å opplyse brukerne om betydningen av personvernet for deres integritet som enkeltindivider og for samfunnslivet generelt.[140] Videre kan det være hensiktsmessig å innta personopplysningsvern som en del av undervisningen på grunnskolen, slik at det offentlige skolesystemet også pålegges et visst ansvar.

[140] Lee. A Bygrave, *Personvern som lettvekter*, Forsker og formidler - festskrift til Erik Magnus Boe på 70-årsdagen, Oslo 2013.

# Kildeliste

**Lovgivning:**


| | |
|---|---|
| 1918 | Lov 31. mai 1918 nr. 4 om avsluting av avtaler, fuldmagt og om ugyldige viljeserklæringer (Avtaleloven) |
| 1992 | Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS- loven) |
| 2000 | Lov 14. april 2000 nr. 31 om behandling av personopplysninger (Personopplysningsloven) |


**Internasjonale rettsakter:**


| | |
|---|---|
| EØS-avtalen | Avtale om Det europeiske økonomiske samarbeidsområde, 5. februar 1992 (EØS-avtalen), |
| Personverndirektivet | Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (personverndirektivet). |
| Personvernforordningen | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repeal- ing Directive 95/46/EC (General Data Protection Regula- tion) |

**Forarbeider:**

| | |
|---|---|
| NOU 2009: 1 | Individ og integritet - personvern i det digitale samfunnet |
| NOU 1997:19 | Et bedre personvern - forslag til lov om behandling av person- opplysninger |
| Ot.prp.92 (1998-1999) | Om lov om behandling av personopplysninger |
| Prop.56 LS | Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen |

**Forvaltningspraksis:**

| | |
|---|---|
| PVN-2003-01 | «Sentralt låneregister» |
| PVN 2005-6 | «Securitas» |
| PVN-2010-09 | «Ung i Norden». |

**Avgjørelser fra EU-domstolen:**

| | |
|---|---|
| Sak C-397/01 (Pfeiffer) | Pfeiffer, Roith, Süβ, Winter, Nestvogel, Zeller, Döbele in joined Cases C-397/01 to C-403/01, ECLI:EU:C:2004:584 |

**Litteratur:**

| | |
|---|---|
| Andersen (2005) | Mads Bryde Andersen, *IT-retten*, 2. udg. (København 2005) |

| | |
|---|---|
| Arnesen og Steinvik (2009) | Finn Arnesen og Are Steinvik, *Internasjonalisering og juridisk metode – særlig om EØS-rettens betydning i norsk rett* (Oslo 2009) |
| Bing (1991) | Jon Bing, *Personvern i faresonen* (Oslo 1991) |
| Bing (2009) | Jon Bing, *Samtykke til behandling av personopplysninger* (Lovdata.no 2009) |
| Blume (2000) | Peter Blume, *Konsumenterne og persondatabeskyttelse i Norden* (København 2000) |
| Blume (2013) | Peter Blume, Databeskyttelsesrett, 4. utg. (København 2013) |
| Blume (2017) | Peter Blume, Persondata retlige grundfigurer – Streijftog i den nye persondataret (København 2017) |
| Bygrave (2000) | Lee A. Bygrave, *Selvbestemmelse til besvær?* (Publisert i Spor (Kvartalsskrift utgitt av Datatilsynet) 2000) |
| Bygrave (2013) | Lee A. Bygrave, *Personvern som lettvekter*, del av Forsker og formidler, festskrift til Erik Magnus Boe på 70-årsdagen 17. April 2013 (Oslo 2013) |
| Bygrave (2014) | Lee A. Bygrave, *Data Privacy Law - An International Perspective* (Oxford 2014) |
| Coll og Lenth (2000) | Line M. Coll og Claude A. Lenth, *Personopplysningsloven – en håndbok* (Oslo 2000 s. 20) |
| Eckhoff og Helgesen (2001) | Torstein Eckhoff og Jan E. Helgesen, *Rettskildelære*, 5. utgave (Oslo 2001) |
| Eng (1990) | Svein Eng, *Begrepene «kompetanse» og «gyldighet» i juridisk argumentasjon* (Tidsskrift for rettsvitenskap ISSN 0040-7143 1990) |

| | |
|---|---|
| Enjolras (2014) | Bernard Enjolras, *Big data og samfunnsforskning: nye muligheter og etiske utfordringer* (Idunn.no 2014) |
| Nygaard (2012) | Nils Nygaard, *Rettsgrunnlag og standpunkt*, 2. utgave (Oslo 2012) |
| Olsen (2015) | Thomas Olsen, *Personvernøkende identitetsforvaltning* (Senter for rettsinformatikk, Complexserien 2016) |
| Öman og Lindblom (2007) | Sören Öman og Hans-Olof Lindblom, *Personuppgiftslagen*, 3. uppl. (Stockholm 2007) |
| Sandtrø (2016) | Jan Sandtrø, *Databehandlers behandling av personopplysninger* (Idunn.no 2016) |
| Schartum og Bygrave (2016) | Dag Wiese Schartum og Lee. A Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave (Bergen 2016) |
| Schartum og Sætre (2016) | Dag Wiese Schartum og Kjetil Wick Sætre, *Samtykke til å behandle personopplysninger i offentlig forvaltning,* (Senter for rettsinformatikk, Complexserien 2016) http://www.complexserien.net/sites/complexserien/files/CompLex_2-16_web.pdf |
| Torvund (1993) | Olav Torvund, *Betalingsformidling i et rettslig perspektiv* (Otta 1993) |
| Torvund (1996) | Olav Torvund, *Å studere jus – innføring i privatrett grunnfag*, (Oslo 1996) |


**Uttalelser fra Artikkel 29-gruppen:**


Artikkel 29-gruppen, opinion 2/2010 on Online Behavioural Advirtising.

Artikkel 29-gruppen, opinion 13/2011 on Geolocation services on smart mobile devicess

Artikkel 29-gruppen, opinion 15/2011 on the definition of consent.

Artikkel 29- gruppen, opinion 02/2013 on apps on smart devices

Artikkel 29-gruppen, opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller

Artikkel 29-gruppen, Guidelines on Consent under Regulation 2016/679

**Internettartikler:**

Artikkel fra The Guardian med tittel «Will you read this article about terms and conditions? You really should do», link: https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information
[Sitert: 9.april 2018]

Artikkel fra Medier24.no med tittel «Nå har 99 prosent av alle mellom 12 og 49 år en smarttelefon», link: https://www.medier24.no/artikler/na-har-99-prosent-av-alle-mellom-12-og-49-ar-en-smarttelefon/366987
[Sitert: 9.april 2018]

Artikkel fra Kommunal- og moderniseringsdepartementets med tittel «Datatilsynet og Personvernemndas saksbehandling», link: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/datatilsynets-og-personvernnemndas-saksbehandling/id2340093/
[Sitert: 9.april 2018]

Artikkel Forbrukerrådet med tittelen «250, 000 words of app terms and conditions», link: https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/
[Sitert: 9.april 2018]

Artikkel fra Forbrukerrådet med tittelen «10 krav til forbrukervennlige apper», link: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/10-krav-til-forbrukervennlige-apper-2/
[Sitert: 9.april 2018]

Artikkel fra Tek.no med tittel «Dette er IMEI-koden», link:

https://www.tek.no/artikler/dette_er_imei-koden/7597
[Sitert: 9.april 2018]

Artikkel fra Storenorskeleksikon.no med tittel «Schibsted ASA», link:
https://snl.no/Schibsted_ASA
[Sitert: 9.april 2018]

Artikkel fra NRK.no med tittelen «Dette er spørsmålene Zuckerberg unngikk å svare på», link: https://www.nrk.no/norge/dette-er-sporsmalene-zuckerberg-unngikk-a-svare-pa-1.14004352
[Sitert: 1. mai 2018]

**Datatilsynet:**

Datatilsynets rapport med tittelen «Hva vet appen om deg?» (2011), link:
https://www.datatilsynet.no/globalassets/global/regelverk-skjema/veiledere/app_rapport_dt2011.pdf
[Sitert: 9.april 2018]

Datatilsynets rapport med tittelen «Personvern tilstand og trender» (2016), link:
https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Personvern-Tilstand-og-trender-2016.pdf
[Sitert: 1.mai 2018]

**Rettsdata:**

Rettsdata.no, lovkommentar (5) og (16) til personopplysningsloven § 2, Dag Wiese Schartum (2012), link:
www.rettsdata.no
[Sitert: 9.april 2018]