Hvordan GDPR påvirker plikten under PSD2 for kontotilbydere til å utlevere informasjon til fullmakttjenester

Kandidatnummer: 16

Antall ord: 14454

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.12.2019

Innholdsfortegnelse

Innholdsfortegnelse 1
1 Innledning 2
2 Introduksjon til PSD2 6
3 Introduksjon til GDPR 8
4 Behandlingsgrunnlag i GDPR 9
4.1 Generelt om behandlingsgrunnlag 9
4.2 Samtykke 10
4.2.1 Frivillig 11
4.2.2 Spesifikt 14
4.2.3 Informert 15
4.2.4 Utvetydig 16
4.3 Rettslig forpliktelse 17
5 Behandling av personopplysninger i PSD2 23
5.1 Generelt 23
5.1.1 Forholdet mellom PSD2 og GDPR 23
5.1.2 Hvilke data kan behandles under PSD2? 24
5.2 Samtykke som behandlingsgrunnlag i PSD2 25
5.2.1 Uttrykkelig samtykke 27
5.2.2 Dobbelt samtykke 32
5.3 Rettslig forpliktelse som behandlingsgrunnlag i PSD2 36
5.3.1 Artikkel 94 som rettslig grunnlag 37
5.3.2 Artikkel 66 og 67 som rettslig grunnlag 37
5.3.3 Artikkel 36 som rettslig grunnlag 39
6 Konklusjon 45
6.1 Virkningen av funnene for næringslivet 46
Litteraturliste 48

1 Innledning

Innovasjon og utvikling har preget betalingstjenester i lang tid. Fra de aller første bank- og kredittkortene, frem til minibanker og bank i butikk, deretter i form av nettbanker og mobilbanker. Innovasjonen innen betalingstjenester har vært preget av hvordan de tradisjonelle bankene, altså lisensierte tilbydere av bankkontoer og lån til offentligheten[1], har anvendt teknologi til å effektivisere transaksjoner mellom individer og bedrifter. Disse innovasjonene har skjedd internt i hver enkelt bank og vært formet av deres infrastruktur og brukergrensesnitt[2]. Kundene har dermed vært bundet til å anvende nettbanken eller mobilbanken til den kontotilbyderen de har bankkonto hos, og har derfor vært forhindret fra å fritt velge mellom ulike brukergrensesnitt på tvers av ulike kontotilbydere.

Fintech-bevegelsen handler om å bryte opp slike begrensninger for kundene og utfordre tradisjonelle banktjenester, ved å anvende digitale løsninger for å redusere friksjon eller ved å tilby helt nye løsninger. *Fintechs* kan være oppstartsselskaper, etablerte teknologiselskaper eller en avdeling/branch hos tradisjonelle kontotilbydere[3]. Det neste steget i denne utviklingen er *open banking*, hvor hovedformålet er økt konkurranse og større valgmuligheter for kundene. Med open banking prøver man å utfordre de tradisjonelle kontotilbyderne innen det siste monopolet, som er tilgang på bankkontoer. Open banking innebærer at lisensierte private selskaper og konkurrerende kontotilbydere gis tilgang til andre kontotilbyderes infrastruktur. Videre at de, med kundens godkjenning, kan få tilgang til kundens bankkonto og tilhørende kontoopplysninger for å tilby kunden skreddersydde, digitale tjenester[4].

Det første Payment Services Directive[5] skulle skape grunnlaget for et enhetlig marked i EU for betalinger, og skape tryggere og mer innovative betalingstjenester. Direktivet er nå erstattet av Payment Services Directive 2[6] (heretter kalt «PSD2»), som i større grad innebærer et steg i retning av å implementere tankegodset fra open banking, og legge til rette for at

[1] Av finansforetaksloven av 2015 § 2-7 defineres en «bank» som en virksomhet som har adgang «til å motta innskudd og andre tilbakebetalingspliktige midler fra allmennheten, å yte kreditt og stille garantier for egen regning og til å yte betalingstjenester.»
[2] Douglas W. Arner, Janos Barberis, Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm* (2016), side 1276-1286
[3] Ibid, side 1274-1276
[4] Christoffer Hernæs, "Open banking: An introduction" (2019), Hernæs er Chief Digital Officer i Sbanken
[5] Direktiv 2007/64/EF
[6] Europaparlaments- og Rådsdirektiv (EU) 2015/2366

fintechs kan få mulighet til å konkurrere mot de tradisjonelle kontotilbyderne[7]. Det nye direktivet ønsker å bidra til økt konkurranse ved å åpne opp for to fullmakttjenester, nemlig betalingsfullmakttjeneste[8] og kontoinformasjonstjeneste[9]. Disse tjenestene er ment å være et bindeledd mellom kunden og ulike kontotilbydere.[10]

Bakgrunnen for masteroppgavens problemstilling er at deler av PSD2 nylig er implementert i norsk rett ved forskrift om betalingstjenester av 2019[11], mens General Data Protection Regulation[12] (heretter kalt «GDPR») ble implementert sommeren 2018. Lovverkene regulerer begge flyten av data og har flere overlappende områder. Temaet for oppgaven er å undersøke harmoniseringen mellom PSD2 og GDPR.

En forutsetning for at de nyopprettede fullmakttjenestene skal fungere, er at de får tilgang til betalingskontoer hos kontotilbyderne, samt tilgang på kontoopplysninger knyttet til betalingskontoene. Kontoopplysninger vil i praksis alltid inneholde personopplysninger[13], slik at overføringen av kontoopplysninger til selskaper eller organisasjoner vil innebære behandling av personopplysninger iht. GDPR. Behandlingen vil derfor kreve et behandlingsgrunnlag jf. GDPR art. 6.

Oppgaven undersøker trepartsforholdet som oppstår mellom kunden[14], fullmakttjenesten og kundens kontotilbyder. Systemet som PSD2 legger opp til innebærer derfor at spørsmålet om overføring av personopplysninger kommer på spissen.

Utgangspunktet for masteroppgaven var et spørsmål som har blitt stilt i næringslivet – eksisterer det et krav til dobbelt samtykke i PSD2? Altså om det eksisterer et krav i PSD2 om at overføring av personopplysninger fra kontotilbyder til fullmakttjeneste, må bero på et samtykke fra kunden til kontotilbyderen[15]. Ved nærmere undersøkelser viste det seg at problemstillingen var noe for snever, og at oppgaven ville risikert å gå glipp av den større

[7] European Commission, ”Payment Services Directive: frequently asked questions” (2018), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793
[8] Se nærmere beskrivelse og definisjon av begrepet i oppgavens punkt 2
[9] Se nærmere beskrivelse og definisjon i oppgavens punkt 2
[10] Hernæs (2019)
[11] Forskrift om betalingstjenester, gitt i medhold av finansavtaleloven av 1999 § 9a
[12] Europaparlaments- og Rådsforordning (EU) 2016/679
[13] Se oppgavens punkt 3
[14] «Den registrerte» i GDPR sammenheng jf. GDPR art. 4(1)
[15] Jf. GDPR art. 6(1) a

helheten som spørsmålet er en del av. Jeg valgte derfor å ta et steg tilbake og å undersøke en mer overordnet problemstilling.

Hovedspørsmålet som masteroppgaven søker å belyse er derfor hvilke[t] behandlingsgrunnlag som kreves for at kontotilbyder skal kunne overføre kundens personopplysninger til fullmakttjenesten.

Under arbeidet med oppgaven fant jeg ut at samtykke og rettslig forpliktelse var de mest omstridte behandlingsgrunnlagene under PSD2, og oppgaven valgte derfor å prioritere behandlingen av disse. Av denne grunn velger oppgaven å avgrense mot de videre behandlingsgrunnlagene i GDPR art. 6.

PSD2 byr på en rekke interessante problemstillinger som enda ikke er avklart. Særlig i forholdet mellom sikkerhetsaspektene i PSD2 sammenlignet med regulering av informasjonssikkerhet, kan det tenkes flere spennende spørsmål. Denne oppgaven må derimot avgrense mot spørsmål om informasjonssikkerhet og reguleringen av sterk kundeautentisering i direktivet, da dette ville berettige en masteroppgave for seg selv. Videre vil oppgaven avgrense mot nærmere sammenlikninger av hendelsesrapportering i PSD2 og GDPR.

Hovedutfordringen med arbeidet med masteroppgaven har vært kildematerialet. Fagområdet preges av å være nytt og i stadig utvikling, og derfor er det mangel på kilder med dypere analyser av harmoniseringen mellom PSD2 og GDPR. I undersøkelsene til skrivingen har jeg ikke kommet over rettspraksis eller publisert litteratur som tar for seg oppgavens hovedproblemstilling, hverken i norsk, skandinavisk eller europeisk rett.

Likevel finnes det noen publiserte uttalelser og profesjonelle aktører som har stilt spørsmålstegn ved kompatibilitet mellom PSD2 og GDPR. Uttalelser fra European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB) og European Banking Authority (EBA) har vært med å nyansere bildet og avklare enkeltproblemstillinger. Materialet fra de profesjonelle aktørene tilbyr kommentarer til uttalelsene fra EU-organene, men har vært preget av en generell karakter. Oppgaven balanserer derfor mellom direktivet og forordningen i seg selv og uttalelser fra rettslige institusjoner, bransjepraksis i utvikling og litteratur knyttet til personvern. På grunn av at flere av spørsmålene mangler en endelig avklaring, har oppgaven prioritert å forklare bakgrunnen for problemstillingene og hvordan bakgrunnen påvirker forholdet mellom regelsettene.

Oppgaven undersøker en spisset problemstilling knyttet til et komplisert fagområde. Av denne grunn er det nødvendig å presentere sentral bakgrunnskunnskap, som en forutsetning for å forstå hovedproblemstillingen. Oppgaven vil derfor starte med å presentere direktivet og forordningen som utgjør fundamentet til oppgavens drøftinger. Oppgaven vil så foreta en presentasjon av behandlingsgrunnlagene samtykke[16] og rettslig forpliktelse[17].

For å komme til bunns i problematikken, er det nødvendig å undersøke hvordan personopplysninger behandles i direktivet og se nærmere på forholdet mellom direktivet og forordningen. Videre å finne ut hvor godt regelverkene er søkt harmonisert. Der det foreligger friksjon, vil oppgaven utforske hvilken betydning og effekt friksjonen får. Oppgaven vil deretter undersøke hvorvidt samtykke og/eller rettslig forpliktelse kan anvendes som behandlingsgrunnlag på overføringen av kundens personopplysninger mellom kontotilbyder og fullmakttjeneste. Til slutt vil oppgaven presentere en konklusjon og deretter vurdere hvilke konsekvenser de foregående drøftelsene får for norsk næringsliv. Dette danner omrisset for masteroppgaven.

[16] GDPR art. 6(1) a
[17] GDPR art. 6(1) c

2 Introduksjon til PSD2

Payment services directive 2 er et betalingsdirektiv som utvidere rekkevidden av gjeldende betalingstjenester og skjerper kravene til sikkerhet, ved å innføre krav om sterk kundeautentisering[18]. Payment Services Directive 2 trådte i kraft 25. november 2015, og opphevet dermed Payment Services Directive av 2007[19]. Det nye direktivet er inspirert av utviklingen innen fintech og open banking, og innebærer et steg i retning av tankene bak bevegelsene[20].

Måten direktivet ønsker å tenke nytt på, er ved å åpne opp for nye aktører innen leveranse av betalingstjenester. På denne måten skapes rom for den nye digitale økonomien. Disse nye aktørene er en betalingsfullmektig og en opplysningsfullmektig, som skal yte henholdsvis betalingsfullmakttjenester og kontoinformasjonstjenester[21].

Av PSD2 art. 4(15) fremgår det at «betalingsfullmakttjeneste»[22] er «en tjeneste for å initiere en betalingsordre på anmodning fra betalingstjenestebrukeren med hensyn til en betalingskonto hos en annen betalingstjenesteyter»[23].

En «betalingsfullmektig» [24] er definert som «en betalingstjenesteyter som utøver virksomhet som nevnt i vedlegg I nr. 7» i PSD2 art. 4(18). Av PSD2 vedlegg I nr. 7 fremkommer det utelukkende ordet «[b]etalingsinitieringstjenester».

Videre er en «kontoinformasjonstjeneste»[25] i PSD2 art. 4(16) definert som «en onlinetjeneste som skal gi samlede opplysninger om en eller flere betalingskontoer som

[18] På engelsk ”strong customer authentication” (SCA)
[19] European Commission, FAQ (2018)
[20] Hernæs (2019)
[21] Ibid
[22] I oversettelsen av PSD2 anvendes begrepet «betalingsinitieringstjeneste». Oppgaven velger heller å anvende den reviderte terminologien i forskrift om betalingstjenester 2019 § 2(7). Fra engelsk «payment initiation service» (PIS)
[23] Fra den uoffisielle norske oversettelsen av PSD2, tilgjengelig på https://lovdata.no/pro/static/NLX3/32015l2366.pdf
[24] I oversettelsen av PSD2 anvendes begrepet «yter av betalingsinitieringstjenester». Oppgaven velger heller å anvende den reviderte terminologien i forskrift om betalingstjenester 2019 § 2(5). Fra engelsk «payment initiation service provider» (PISP)
[25] I oversettelsen av PSD2 anvendes begrepet «kontoopplysningstjeneste». Oppgaven velger heller å anvende den reviderte terminologien i forskrift om betalingstjenester 2019 § 2(8). Fra engelsk «account information service» (AIS)

betalingstjenestebrukeren har hos enten en annen betalingstjenesteyter eller hos mer enn én betalingstjenesteyter».

Det følger av art. 4(19) at en «opplysningsfullmektig»[26] er «en betalingstjenesteyter som utøver virksomhet som nevnt i vedlegg I nr. 8». Av PSD2 vedlegg I nr. 8 fremkommer det utelukkende «[k]ontoopplysningstjenester»

Av art. 4(17) er «kontotilbyder»[27] definert som «en betalingstjenesteyter som tilbyr betalingskonto til og fører denne for betaler».

Formålet med PSD2 er å fremme den videre utviklingen av et enhetlig marked for elektroniske betalinger i Unionen, så forbrukere, handlende og andre markedsaktører kan nyte godt av alle fordelene med EUs indre marked iht. målsetningen om Europa 2020. For å nå dette formålet, samt skape større konkurranse, effektivitet og innovasjon på området for elektroniske betalinger, bør det forekomme rettssikkerhet og like vilkår som kan få ned transaksjonskostnader og priser for betalingstjenestebrukere[28].

For at fullmakttjenestene skal kunne yte tjenestene sine til kundene, behøver de tilgang til kontotilbyders infrastruktur[29] og tilgang til kundens betalingskonto hos kontotilbyder[30]. Tilgangen til kontotilbyders infrastruktur skal oppnås ved bruk av så kalte Application Programming Interface (API), eller programmeringsgrensesnitt på norsk.

Som et land som er helt i front når de kommer til bruk av digitale tjenester, vil PSD2 komme til å påvirke hverdagen til nordmenn flest, norske kontotilbydere og andre finansielle aktører. Allerede er alternative betalingstjenester som PayPal og Vipps merkevarer som er godt kjent, og PSD2 åpner for at enda flere kan komme. For norsk næringsliv byr derfor direktivet på nye muligheter, men også hodebry. PSD2 er ment å utfordre og forandre, og med forandring kommer også potensialet for konflikt.

[26] I oversettelsen av PSD2 anvendes begrepet «yter av kontoopplysningstjeneste». Oppgaven velger heller å anvende den reviderte terminologien i forskrift om betalingstjenester 2019 § 2(6). Fra engelsk «account initiation service provider» (AISP)
[27] Fra engelsk "account servicing payment service provider" (ASPSP)
[28] Se EDPS, *Resumé af udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse* (2013), side 1
[29] Se PSD2 art. 35
[30] Se PSD2 art. 36

3 Introduksjon til GDPR

General Data Protection Regulation trådte i kraft i EU fra 27. april 2016. Forordningen er implementert i norsk rett ved personopplysningsloven[31] § 1, og trådte i kraft i Norge fra 15. juni 2018. Bestemmelsen innebærer at oversettelsen som fremgår av vedlegg XI nr. 5e til EØS-avtalen, gjelder som norsk lov. Videre henvisninger til GDPR vil derfor være til den norske oversettelsen.

GDPR innebærer en videreføring og en videreutvikling av personverndirektivet[32] (heretter «DPD»). Av GDPR art. 94 fremgår det at enhver henvisning til DPD, skal regnes som en henvisning til forordningen.

Formålet til forordningen er «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger»[33] og sikre «[f]ri utveksling av personopplysninger i Unionen»[34].

Det følger av GDPR art. 4(1) at «personopplysninger» er definert som «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)». Videre at «en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator». Det eneste unntaket er dersom opplysningene er anonymisert, altså at opplysningen ikke kan brukes til å identifisere en fysisk person enten direkte eller indirekte.

Av denne grunn vil en kontoopplysning i PSD2 i praksis alltid være en personopplysning, siden opplysningene vil rette seg mot en fysisk person (kunden). Videre vil kontoopplysningene nettopp anvendes til å knytte kunden til en spesifikk betalingskonto.

Det fremkommer av GDPR art. 5 flere prinsipper for behandling av personopplysninger, nemlig «lovlighet, rettferdighet og åpenhet», «formålsbegrensning», «dataminimering», «riktighet», «lagringsbegrensning» og «integritet og konfidensialitet».

[31] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger
[32] Direktiv 95/46/EF
[33] GDPR art. 1(2)
[34] GDPR art. 1(3)

4 Behandlingsgrunnlag i GDPR

4.1 Generelt om behandlingsgrunnlag

All behandling av personopplysninger må oppfylle prinsippene i GDPR art. 5(1) bokstav a, om at personopplysninger skal behandles på en «lovlig, rettferdig og åpen måte». For at behandlingen skal være «lovlig» må behandlingen skje på bakgrunn av ett av behandlingsgrunnlagene i GDPR art. 6[35]. De ulike behandlingsgrunnlagene kan regnes som «nøklene» for å kunne behandle personopplysninger under GDPR. Uten et gyldig behandlingsgrunnlag, kan man ikke lovlig behandle personopplysninger. Dersom behandlingen omfatter særlige kategorier av personopplysninger, må ett av alternativene i art. 9 være oppfylt for at behandlingen skal være «lovlig»[36].

Av GDPR art. 6 følger det at de seks ulike behandlingsgrunnlagene er:

a) Samtykke
b) Nødvendig for å oppfylle en avtale
c) Rettslig forpliktelse
d) Nødvendig for å verne den registrertes vitale interesser
e) I allmennhetens interesse eller utøve offentlig myndighet
f) Berettiget interesse

Oppgaven vurderer at de behandlingsgrunnlagene som kan være anvendelige på oppgavens hovedspørsmål, er samtykke, rettslig forpliktelse og berettiget interesse.

Behandlingsgrunnlagene samtykke og rettslig forpliktelse er likevel de rettslige grunnlagene som det hersker mest usikkerhet om i forbindelse med PSD2. Av plasshensyn har oppgaven derfor valgt å prioritere å behandle disse to behandlingsgrunnlagene, og dermed avgrense mot de resterende, inkludert berettiget interesse.

I det videre vil oppgaven først presentere behandlingsgrunnlagene samtykke og rettslig forpliktelse generelt. Deretter vil oppgaven undersøke hvilke av de nevnte

[35] European Union Agency for Fundamental Rights (FRA) og Council of Europe (CoE), *Handbook on European data protection law* (2018), side 42
[36] Ibid

behandlingsgrunnlagene som er anvendelige som rettslig grunnlag for overføring av kundens personopplysninger fra kontotilbyder til fullmakttjenesten.

4.2 Samtykke

Det første behandlingsgrunnlaget i GDPR som skal klargjøres er samtykke. Det følger av GDPR art. 6(1) bokstav a at behandling av personopplysninger er lovlig dersom «den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål».

Av artikkelens ordlyd fremkommer det at den registrerte kan samtykke til at sine egne personopplysninger behandles. Artikkelen avgrenser dermed mot at man kan samtykke til behandling av andres personopplysninger. Unntak kan likevel tenkes i fullmaktsituasjoner, der personer er satt under vergemål eller for personer med foreldreansvar for barn, som samtykker på barnas vegne[37]. Ordlyden gir videre uttrykk for en formålsbegrensning. Samtykket må begrense seg til ett eller flere formål som må være konkretisert på samtykketidspunktet jf. også GDPR art. 5(1) bokstav b. Bruken av «har samtykket» indikerer at samtykket må være gitt før behandling av den registrertes personopplysninger igangsettes[38].

Et *samtykke* fra den registrerte er legaldefinert i GDPR art. 4(11) som:

> enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende.

Både art. 6(1) bokstav a og art. 4(11) er en videreføring fra henholdsvis DPD art. 7 bokstav a og DPD art. 2 bokstav h, med mindre språklige endringer[39]. Samtykke som behandlingsgrunnlag er dermed ingen nyvinning i GDPR. I forordningens fortale punkt 171 er forholdet mellom samtykke i DPD og GDPR søkt klargjort. Her fremgår det at dersom samtykke gitt iht. DPD, oppfyller vilkårene for samtykke i GDPR, så behøver ikke

[37] Se f.eks. GDPR art. 8(1) første setning annet punktum om barn under 16 års samtykkekompetanse
[38] Se også Article 29 Working Party (A29WP), *Guidelines on consent under regulation 2016/*679 (2017), side 17-18
[39] Originaltekst fra DPD art. 7 bokstav a: «den registrerte har gitt sitt utvetydige samtykke» og i DPD art. 2 bokstav h: ««den registrertes samtykke»: enhver frivillig, spesifikk og informert viljesytring om at den registrerte gir sitt samtykke til at personopplysninger om vedkommende blir behandlet»

behandlingsansvarlig å innhente nytt samtykke fra den registrerte. Samtykket fortsetter dermed å virke etter anvendelsesdatoen for forordningen, men vil gjelde med de rettigheter og vilkår som fremkommer av GDPR.

For at det skal foreligge et gyldig samtykke for behandling av den registrertes personopplysninger, følger det både av DPD og av GDPR fire kumulative vilkår som må være oppfylt. Samtykket må være:

- Frivillig
- Informert
- Spesifikt
- Utvetydig

Et tilleggsvilkår som ikke fremgår direkte av art. 4(11) eller art. 6(1) bokstav a, men som må innfortolkes, er et krav om at den registrerte innehar samtykkekompetanse. Dersom den registrerte ikke har mulighet til å samtykke i andre kontraktsforhold, er det heller ingen grunn til at den registrerte skal kunne samtykke til behandling av personopplysninger[40].

4.2.1 Frivillig

For det første må samtykket være frivillig. For at samtykket skal være frivillig må det foreligge et reelt valg for den registrerte på samtykketidspunktet. Dersom den registrerte føler seg presset, risikerer å bli manipulert, villedet eller møter negative konsekvenser fra behandlingsansvarlig om den ikke samtykker, vil samtykket være ugyldig. Samtykket vil heller ikke være gyldig om den registrerte ikke har mulighet til å trekke samtykket tilbake[41].

Et relevant spørsmål er her hvor terskelen for de negative konsekvensene ligger. Altså hvor mye den registrerte må tåle før samtykket regnes som ugyldig. Problemstillingen er ikke endelig avklart, men noen utgangspunkter kan presiseres. For det første vil det være en forskjell om det er en privat eller offentlig behandlingsansvarlig. Dersom behandlingsansvarlig er en offentlig aktør, skal det mer til for at samtykket anses som frivillig[42]. Mer om denne problematikken under. Dersom behandlingsansvarlig er en privat aktør, må man foreta en konkret vurdering av konsekvensene for den registrerte av ikke å

[40] FRA og CoE (2018), side 112-113
[41] GDPR art. 7(3) jf. fortalen 42 og A29WP (2017), side 6-7
[42] Ibid

samtykke. Hvor den registrerte kun går glipp av en mulighet, f.eks. et tilbud, et nyhetsbrev eller tidlig informasjon, uavhengig av øvrige tjenester fra den behandlingsansvarlige, så vil samtykket være gyldig[43]. I slike tilfeller er det klart at den registrerte har et valg om å samtykke til behandling av personopplysninger eller ikke. Derimot hvor den registrerte kun får tilgang til sterkt begrensede tjenester og mister sentral funksjonalitet, vil dette innebære negative konsekvenser for den registrerte av ikke å samtykke til behandling av personopplysninger[44].

Vanskeligere blir spørsmålet om negative konsekvenser hvor behandlingsansvarlig, f.eks. en butikkjede, tilbyr kundelojalitetskort med rabatter på butikkjedens varer, mot å registrere kundens kjøpsadferd. Kan rabattene eller fordelene av å være medlem bli så store at realiteten blir at den registrerte ikke har et reelt valg? Hva hvis den eneste måten den registrerte kan få tilgang til rabatter er gjennom kundelojalitetskortet? Vurderingen av hva som regnes som negative konsekvenser må derfor nyanseres. I begge eksemplene finnes det nok en terskel hvor fordelen av å være medlem blir så stor at kunden reelt sett blir presset til å tillate behandling av personopplysninger. Det vil naturligvis være en forskjell på om rabattene er på under 10% for de med kundelojalitetskort, enn om rabattene er på over 60%. I tilfellet hvor kundelojalitetskortet er den eneste kilden til rabatter, vil terskelen være lavere for å anse at kunden blir presset, enn hvor offentligheten blir tilbudt rabatter også utenom kundelojalitetskortet, men at disse rabattene f.eks. er lavere eller på andre varer[45]. Det er derimot vanskelig å si noe nærmere om hvor denne terskelen generelt ligger. Det må derfor foretas en konkret vurdering i det enkelte tilfellet.

Et annet viktig moment i vurderingen av om et samtykke er frivillig er hvorvidt det foreligger ubalanse i styrkeforholdet mellom partene. Det fremgår av fortalen punkt 43 at et samtykke ikke bør utgjøre et behandlingsgrunnlag om det er en «klar skjevhet mellom den registrerte og den behandlingsansvarlige …». Særlig at dette gjelder styrkeforholdet mellom den registrerte og en offentlig myndighet, dersom omstendighetene tilsier at det er usannsynlig at den registrerte ville samtykket frivillig[46]. Bakgrunnen for at det er problematisk at offentlig myndigheters behandling beror på samtykke, er at myndighetenes oppgave er å utøve makt og kontroll over de registrerte. Offentlige myndigheter skal fordele og forvalte begrensede

[43] Se A29WP (2017), side 11, eksempel 9
[44] Ibid, eksempel 8
[45] Se FRA og CoE (2018), side 145 og til dels A29WP (2017), side 11, eksempel 9 og 10
[46] GPDRs fortale 43

ressurser og ta hensyn til samfunnet som en større enhet. I denne prosessen er det lett for at hensynet til enkeltmennesket forsvinner og at dens rettigheter utfordres. I Article 29 Working Party (A29WP)[47] presiseres det derfor at andre behandlingsgrunnlag enn samtykke er mer egnet for offentlige myndigheter, som f.eks. art. 6(1) bokstav e om å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet. Likevel utelukkes det ikke helt at samtykke kan tjene som behandlingsgrunnlag, men da må det være klart at den registrerte har et reelt valg[48].

Også mellom den registrerte og arbeidsgiver kan det oppstå spørsmål om et samtykke er frivillig. I dette tilfellet vil det være usannsynlig at arbeidstaker kan gi samtykke til behandling uten å føle frykt eller en reell risiko for negative konsekvenser, som oppsigelse, utfrysning eller å bli forbigått i vurderingen av tilsetting til nye stillinger. Særlig dersom samtykket retter seg mot aktive oppfølgingssystemer på arbeidsplassen, som kameraovervåkning, timelogging, kontroll med taletid, eller å fylle ut vurderingsskjemaer. Majoriteten av behandling bør derfor bero på et annet behandlingsgrunnlag enn samtykke, som f.eks. nødvendighet for å oppfylle ansettelsesavtalen. Likevel betyr ikke dette at samtykke aldri kan være anvendelig i arbeidssituasjoner. Hvor arbeidsgiver f.eks. ønsker å lage en liste over de ansattes bursdager for å sende ut en felles hilsen, foreligger det ingen negative konsekvenser for den ansatte om den ikke samtykker. Samtykket vil derfor regnes som frivillig.

Et samtykket regnes ikke som frivillig avgitt dersom en behandlingsansvarlig anfører at den registrerte kan velge mellom å benytte deres tjenester, som krever samtykke for behandling av personopplysninger for andre formål enn de som er nødvendige, og en tilsvarende tjeneste tilbudt av en annen aktør. I et slikt tilfellet er det reelle valget helt avhengig av andre markedsaktører. Dersom alle markedsaktørene krever tilsvarende behandling som den første behandlingsansvarlige, vil det ikke eksistere et alternativ for den registrerte[49].

GDPR art. 7 vil bli nærmere gjennomgått under. Allerede nå kan det likevel nevnes at art. 7(4) påvirker forholdet mellom samtykke og kontrakt som behandlingsgrunnlag og vurderingen av om et samtykke regnes som frivillig avgitt. Det følger av art. 7(4) at det skal «tas størst mulig hensyn til blant annet om oppfyllelse av en avtale […] er gjort betinget av

[47] Nå henvist til som European Data Protection Board (EDPB) under GDPR
[48] A29WP (2017), side 6
[49] A29WP (2017), side 9-10

samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale.» Ordlyden tilsier at behandlingsansvarlig ikke kan kreve at den registrerte skal samtykke til ytterligere behandling, mot at behandlingsansvarlig skal oppfylle sin forpliktelse etter avtalen. Dette handler om at behandlingsgrunnlagene kontrakt og samtykke ikke skal sammenblandes. Det må derfor skilles mellom formålene som er nødvendig for oppfyllelsen av kontrakten, og andre formål som behandlingsansvarlig ønsker å behandle i tillegg[50]. Videre fremkommer det av A29WP at punkt (4) ikke er uttømmende[51].

4.2.2 Spesifikt

For det andre må samtykket være *spesifisert* for hvilket formål behandlingen utføres for. Hensynet bak vilkåret om spesifisering er at den registrerte skal få utøve kontroll over egne data og sikre gjennomsiktighet rundt hva den registrerte samtykker til. Vilkåret er nært knyttet til kravet om at samtykke må være *informert*[52].

Et sentralt moment i vurderingen av om et samtykke er spesifisert er hvorvidt behandlingsansvarlig har iverksatt tilstrekkelige tiltak mot formålsutglidning. Med andre ord om formålsbegrensningen er presis og konkret nok til å forhindre at behandlingsaktiviteten utvides over tid, slik at behandlingen til slutt omfatter mer enn hva den registrerte hadde intensjon om på samtykketidspunktet[53]. Vurderingsmomentet må ses i sammenheng med GDPR art. 5(1) bokstav b om at personopplysninger skal «samles inn for spesifikke, uttrykkelig angitte og berettigede formål». Behandlingsansvarlig må innhente nytt samtykke fra den registrerte dersom behandlingsaktiviteter, som kan påvirke formålet samtykket er gitt for, skal endres eller legges til på en måte som ikke er forutberegnelig for den registrerte på samtykketidspunktet[54].

Et annet moment er om samtykkeforespørslene er tilstrekkelig konkretisert, slik at den registrerte kan samtykke til separate forhold. Konkretiseringen skal forhindre at all behandling av personopplysninger samles under ett samtykke, på en måte som begrenser den registrertes innsikt i behandlingens omfang[55]. Samtykkeforespørslene må derfor knyttes til

[50] Ibid, side 8
[51] Ibid, side 5
[52] Ibid, side 11
[53] Ibid, side 11-12
[54] Se FRA og CoE (2018), side 147
[55] GDPRs fortale 42

hver enkelt behandlingsaktivitet og formål, slik at den registrerte faktisk kan velge hvilke behandlingsaktiviteter den ønsker å samtykke til, og hvilke den ikke ønsker, uten at tilgang til tjenesten blir nektet[56]. Behandlingsansvarlig må derfor skille mellom situasjonene hvor samme behandlingsaktivitet utføres for flere formål, og hvor flere behandlingsaktiviteter utføres for et enkelt formål. Det følger av fortalen 32 at behandling for ulike formål krever separate samtykker. Løsninger for oppdelt samtykke bør implementeres for å la den registrerte samtykke hver for seg til hvert enkelt formål, f.eks. ved at den registrerte elektronisk huker av en boks per formål. Oppdelingen av samtykkeforespørselen bør foregå på en måte som gir den registrerte bevissthet om hvilke alternativer som foreligger[57].

Et tredje moment er om samtykkeforespørselen klart skiller mellom informasjon som relaterer seg til å innhente samtykke for behandling av personopplysninger og informasjon om andre forhold. Det sentrale hensynet er her om den registrerte settes i stand til å forstå hva de separate samtykkene innebærer, og hvilken påvirkning dette får for den registrerte. Spesielt dersom enkelte av valgene er mer inngripende eller risikofylte enn andre, f.eks. ved overføring til tredjestater. På denne måten får den registrerte mulighet til å samtykke til behandling for de formål den registrerte aksepterer, samtidig som den registrerte blir gjort kjent med hva manglende samtykke for det enkelte formål innebærer. Denne informasjonen er essensiell for å forstå konsekvensene av de ulike valgene den registrerte foretar seg[58]. Problemstillingen har en naturlig sammenheng til vilkåret om at et samtykke må være *informert*.

4.2.3 Informert

For at et samtykke skal være gyldig må den registrerte være *informert*. Den registrerte bør minst kjenne den behandlingsansvarliges identitet og formålet med behandlingen av personopplysninger[59]. Det sentrale hensynet bak kravet om at et samtykke må være informert er å sikre den registrerte kontroll over egne personopplysninger. For at dette hensynet skal gjennomføres må det forekomme gjennomsiktighet i behandlingen av personopplysninger. Hensynet har en parallell til art. 5(1) bokstav a om at behandlingen skal skje på en «åpen måte» og den registrertes rett til informasjon på innsamlingstidspunktet i art. 13.

[56] A29WP (2017), side 10
[57] GDPRs fortale 43
[58] A29WP (2017), side 11-12
[59] GDPRs fortale 42

Forholdet til art. 13 påvirker også hvilken informasjon den registrerte bør få på samtykketidspunktet. I tillegg til den behandlingsansvarliges identitet og formålet med behandlingen[60], bør den registrerte informeres om hvilke typer personopplysninger som vil bli innsamlet og behandlet, retten til å trekke tilbake samtykket[61], informasjon om mulig bruk av automatiserte avgjørelser[62] og potensiell risiko ved overføring til tredjestat pga. manglende beslutning om tilstrekkelig beskyttelsesnivå[63]. En behandlingsansvarlig behøver ikke opplyse om hvilke databehandlere som vil få tilgang til personopplysningene, for at et samtykke skal være informert. Likevel bør behandlingsansvarlig informere om eventuelle felles behandlingsansvarlige.

Videre så kreves det at informasjonen holder en viss kvalitet. Informasjonen i samtykkeforespørselen bør fremgå på en «forståelig og lett tilgjengelig form» og være formulert på «et klart og enkelt språk»[64]. Med dette menes det at budskapet bør være egnet og tilpasset målgruppen, slik at den gjennomsnittlige person kan forstå det. Behandlingsansvarlige kan ikke gjemme seg bak lange personvernerklæringer som er vanskelig å forstå eller som er fullstappet av juridiske faguttrykk. Det er ingen krav til hvilket format informasjonen fremstilles på for den registrerte, så lenge den er klar og lett tilgjengelig. Dersom behandlingen særlig retter seg mot mindreårige, kreves det at informasjonen formuleres på en måte som mindreårige vil forstå[65].

Når samtykke kreves som del av en skriftlig kontrakt skal samtykkeforespørselen være lett å adskille fra øvrige forhold jf. art. 7(2). Videre kan det være behov for å behandle spørsmålet om samtykke i et eget separat dokument, dersom kontrakten inneholder mange aspekter som er irrelevante for vurderingen om samtykke for behandling av personopplysninger. Av fortalen 32 fremkommer det at informasjon som er relevant for avgjørelsen av om den registrerte skal samtykke eller ikke, eller samtykkeforespørselen i seg selv, ikke kan gjemmes blant generelle kjøpsvilkår eller «terms and conditions».

4.2.4 Utvetydig

[60] Ibid
[61] GDPR art. 7(3)
[62] GDPR art. 22
[63] GDPR art. 13(1) bokstav f og art. 45
[64] GDPRs fortale 42
[65] A29WP (2017), side 13-15

For det fjerde må samtykket fremgå av en «utvetydig viljesytring». Det følger av fortalen punkt 32 at et samtykke bør uttrykkes ved «en tydelig bekreftelse», som kan skje i form av en muntlig eller skriftlig erklæring. Den skriftlige erklæringen kan også være elektronisk. På nett kan samtykke utføres ved å huke av en boks, endre innstillinger, avgi en erklæring eller utføre en annen handling. Det sentrale er at den registrerte foretar et aktivt valg. Av denne grunn, utgjør ikke bokser som er huket av på forhånd, taushet, passivitet eller andre «opt-out» løsninger et gyldig GDPR-samtykke[66].

Det sentrale hensynet som vilkåret søker å oppfylle er at samtykke må gis på en måte som ikke reiser noen tvil om intensjonen til den registrerte[67]. Et samtykke kan derfor ikke innhentes i samme handling som når den registrerte aksepterer en kontrakt, de generelle kjøpsvilkårene eller «terms of service». En generell aksept av kjøpsvilkårene utgjør ikke en «tydelig bekreftelse» til å samtykke til behandling av personopplysninger[68].

Ytterligere krav til samtykket er presisert i GDPR art. 7. Artikkelen er ny i GDPR, og det var ingen tilsvarende artikkel i DPD. Av GDPR art. 7(1) fremgår det at den behandlingsansvarlige har bevisbyrden for at samtykke foreligger. Ikke nok med det, men den behandlingsansvarlige har også en plikt til å lagre dokumentasjon på at samtykke er avgitt[69]. Det følger av art.7(2) at samtykke til behandling av personopplysninger skal tydelig skilles fra andre forhold som avklares samtidig, som har en parallell til vilkåret om at samtykket må være *spesifikt*. Videre skal det være like enkelt å trekke tilbake et samtykke som å avgi et samtykke jf. art. 7(3). Artikkel 7(4) regulerer forholdet mellom samtykke og kontrakt. Forholdet ble behandlet under vilkåret om at samtykket må være *frivillig*.

4.3 Rettslig forpliktelse

Et aktuelt behandlingsgrunnlag i denne anledning er alternativet «rettslig forpliktelse» som følger av GDPR art. 6(1) bokstav c.

Behandlingsgrunnlaget innebærer at hvor behandlingsanvarlig er underlagt en lov som krever at denne skal behandle personopplysninger, så skal denne rettslige forpliktelsen til å behandle personopplysninger regnes som et behandlingsgrunnlag. Altså at behandlingsanvarlig ikke

[66] Se GDPR art. 7(2) og A29WP (2017), side 15-16
[67] FRA og Coe (2018), side 113
[68] A29WP (2017), side 16-17
[69] Se FRA og CoE (2018), side 143

behøver å innhente et samtykke, inngå en kontrakt eller forsøke å oppfylle et annet behandlingsgrunnlag for lovlig å behandle personopplysningene som den rettslige forpliktelsen krever.

I GDPR artikkel 6(1) bokstav c har behandlingsgrunnlaget kommet til uttrykk ved at behandling bare er lovlig dersom «behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige». Ordlyden er en videreføring av personverndirektivet artikkel 7 bokstav c.

Av artikkelens ordlyd fremgår det at behandlingen må være «nødvendig». En naturlig språklig forståelse tilsier et krav om årsakssammenheng mellom den rettslige forpliktelsen som påhviler den behandlingsansvarlige og behandlingen av personopplysninger. Behandlingen må bidra til å oppfylle den rettslige forpliktelsen. Dersom den rettslige forpliktelsen kan oppfylles uten å behandle personopplysninger, vil ikke den rettslige forpliktelsen være et gyldig behandlingsgrunnlag. Om det derimot kreves at behandlingen må være essensiell, altså at det er umulig å oppfylle den rettslige forpliktelsen uten behandling av personopplysninger, er mer usikkert.

Det britiske Information Commissioner's Office[70] har uttalt at behandlingen ikke må være essensiell, men at det er et krav om at behandlingen må være en rimelig og proporsjonal måte å oppfylle den rettslige forpliktelsen[71]. Videre gir *Personvern i informasjonssamfunnet* uttrykk for at «nødvendig» må vurderes opp mot omstendighetene og hvor sensitive personopplysningene som skal behandles anses å være[72].

Et annet sentralt spørsmål er hvilke vilkår som stilles til den «rettslige forpliktelsen».

Formål

Av GDPR art. 6(3) annen setning følger det at formålet med behandlingen av personopplysninger skal være fastsatt i nevnte rettslige grunnlag[73]. Altså at det rettslige

[70] Britisk tilsynsmyndighet for bl.a. personvern
[71] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/ (lest 31.10.2019)
[72] Se Dag Wiese Schartum og Lee A. Bygrave (2016), side 182
[73] Jf. fortalen pkt. 45

grunnlaget skal spesifisere hva behandlingen skal oppnå. Her er det verdt å nevne at ordlyden i forordningen er skjerpet til «skal», fra «bør» i fortalen punkt 45.

En formålsbegrensning er viktig fordi et slikt behandlingsgrunnlag kan oppleves inngripende for en registrert som ikke har mulighet til å motsette seg behandlingen.

Lov – unionsrett eller medlemsstatenes nasjonale rett

For å sikre at behandlingsgrunnlaget er underlagt demokratisk kontroll, kreves det at den rettslige forpliktelsen fremgår av lov. Slik forhindres at behandlingsgrunnlaget tillater for inngripende behandling overfor den registrerte eller at behandlingsgrunnlaget stiller urimelige krav til den behandlingsansvarlige.

Kriteriet til «rettslig forpliktelse» blir ytterligere presisert i GDPR art. 6 nr. 3, hvor det fremgår at grunnlaget for behandlingen skal fastsettes i enten unionsretten eller medlemsstatens nasjonale rett[74]. I forordningens fortale punkt 41 presiseres det at med «et rettslig grunnlag», kreves det «ikke nødvendigvis en regelverksakt vedtatt av et parlament». Det rettslige grunnlaget bør likevel være «tydelig og presist», og «anvendelsen av det bør være forutsigbar for personer som omfattes av det». Videre henvises det til rettspraksis fra EU-domstolen og Den europeiske menneskerettighetsdomstol.

Henvisningen innebærer at man ved vurderingen av om det rettslige grunnlaget er «tydelig og presist», må se hen til vurderinger av lovkravet i EMK art. 7. Lovkravet går ut på offentlige organers inngrep i noens private rettssfære, skal være hjemlet i lov[75]. Det er sikker rett at «nasjonal eller internasjonal rett» i EMK art. 7 omfatter mer enn lov vedtatt av et parlament, slik at også prejudikater i common law omfattes.

Uttalelsen i fortalen punkt 41, sett i sammenheng med vurderingen av EMK art. 7, innebærer at andre rettslige grunnlag kan tilfredsstille kravet til å danne en «rettslig forpliktelse». I norsk rett får dette betydning ved at også forskrift gitt i medhold av lov vil være et gyldig rettslig grunnlag.

[74] Jf. fortalen pkt. 40 og pkt. 41
[75] Andreas Føllesdal, Morten Ruud og Geir Ulfstein (2017)

For norsk rett har Schartum og Bygrave[76] argumentert for at det eksisterer to alternative måter å oppfylle kravet til rettslig grunnlag:

1. Hvor behandling av personopplysninger er direkte hjemlet i unionsretten eller nasjonal rett, eller

2. Hvor behandling av personopplysninger er klart forutsatt i unionsretten eller nasjonal rett.

Under alternativet «direkte hjemmel» nevnes til eksempel de mange tilfeller der det i lov, eller i forskrift gitt i medhold av lov, slåes fast at det skal opprettes registre, for eksempel selskapsregister, eiendomsregister eller gjeldsregister[77].

Alternativet «klart forutsatt» er interessant, da det åpner opp for behandling selv hvor dette ikke kommer direkte til uttrykk, men hvor behandling presumeres. Altså hvor rettsgrunnlaget selv ikke presiserer at det er behandling av personopplysninger bestemmelsen hjemler, men hvor rettsgrunnlaget stiller krav til behandlingsanvarlig som må løses ved behandling av personopplysninger.

Oppgaven finner grunn til å nevne at alternativet enda ikke er anvendt i rettspraksis eller vedtatt i lov. Likevel har alternativet gode grunner for seg, og forfatterne er autoritære kilder på personvernrettens område.

Et argument for alternativet er at det finnes bestemmelser som stiller krav som må løses ved behandling av personopplysninger, uten at dette eksplisitt kommer til uttrykk i bestemmelsen. I disse tilfellene er det gunstig å kunne tolke lovkravet utvidende slik at behandlingsgrunnlaget kommer til anvendelse. Alternativet ville vært at behandlingsgrunnlaget ville blitt betydelig uthulet eller et krav om at utallige lover måtte gjennomgå revisjon slik at de tydelig kunne formulere en direkte hjemmel for behandling av personopplysninger. En slik løsning ville vært lite ønskelig og innebåret betydelig merarbeid.

[76] Schartum og Bygrave (2016), side 180-181
[77] Ibid

Det kan være vanskelig å slå fast når en rettslig forpliktelse er «klart forutsatt» og det må derfor foretas en bred vurdering. Forfatterne oppstiller tre vurderingsmomenter som kan være klargjørende[78]:

g) Angivelse av aktuelle opplysningstyper

h) Er personvernspørsmål drøftet i forarbeidene?

i) Krav til forholdsmessighet

Aktuelle opplysningstyper bør nevnes i det rettslige grunnlaget for å begrense hvilken behandling grunnlaget åpner for. En slik begrensning er også naturlig sett i sammenheng med kravet til formålsbegrensning og at behandlingen må være «nødvendig». At de relevante opplysningstypene er beskrevet i grunnlaget er derfor et klart moment i retning av at det rettslige grunnlaget «klart forutsetter» at personopplysninger skal behandles.

Videre vil et sterkt moment være om det fremgår av grunnlagets forarbeider at personopplysninger skal behandles eller om behandling blir vurdert som en plausibel måte å oppfylle den rettslige forpliktelsen på. Taushet på dette området må vurderes konkret. I noen tilfeller kan det skyldes teknologisk utvikling, altså at behandling nå er en mer nærliggende metode for å oppfylle forpliktelsen enn når loven trådte i kraft.

Her som ellers i EU-retten stilles det krav til forholdsmessighet. Hvor behandlingen er inngripende overfor den registrerte, så taler mer for at hjemmelskravet skal tolkes strengt[79]. En usikkerhet her knytter seg til om forholdsmessighetsvurderingen også skal ta hensyn til momenter hos behandlingsansvarlig. Altså om det at et krav om behandlingen av personopplysninger er krevende, eller vil innebære betydelig merarbeid for behandlingsanvarlig å oppfylle, skal lede til en strengere terskel for at hjemmelskravet er oppfylt. Kravet til forholdsmessighet bør nok her forståes bredt, slik at også hensyn hos andre enn den registrerte kan være relevante.

Et sentralt moment i forholdsmessighetsvurderingen vil være hvor påregnelig eller klar den rettslige forpliktelsen vil være for den registrerte og behandlingsansvarlig, når forpliktelsen ikke direkte fremgår av det rettslige grunnlaget. Dersom den rettslige forpliktelsen er mer

[78] Ibid
[79] Ibid

avledet eller overraskende for den registrerte eller for behandlingsansvarlig, så taler dette imot at forpliktelsen er «klart forutsatt», og videre at kravet ikke er forholdsmessig. Resultatet vil i et slikt tilfelle være at kravet til behandling av personopplysninger bør fremgå direkte av det rettslige grunnlaget.

Det rettslige grunnlaget kan komme med ytterligere begrensninger og presiseringer enn hva som fremgår av GDPR for øvrig.

Av GDPR art. 6(3) andre setning andre punktum fremkommer at de nevnte rettslige grunnlag kan inneholde «særlige bestemmelser for å tilpasse anvendelsen av reglene i denne forordning». Med andre ord at den rettslige forpliktelsen kan inneholde begrensninger eller ytterligere presiseringer tilknyttet hvilke personopplysninger som kan behandles eller hvilke behandlingsaktiviteter som bestemmelsen hjemler. Altså at selv om det rettslige grunnlaget gir uttrykk for en mer begrenset adgang til behandling av personopplysninger enn GDPR for øvrig, vil dette fortsatt være i overenstemmelse med forordningen.

De tre momentene er bare et utgangspunkt i vurderingen av om den rettslige forpliktelsen er «klart forutsatt». Rekkevidden av behandling som tillates under hvert rettslige grunnlag må derfor tolkes konkret i hvert enkelt tilfelle.

5 Behandling av personopplysninger i PSD2

5.1 Generelt

5.1.1 Forholdet mellom PSD2 og GDPR

Det er beskrevet at PSD2 og GDPR har motstridende ambisjoner og målsetninger. Enklere sagt at regelsettene er på kollisjonskurs, ved at PSD2 krever deling av informasjon, mens GDPR ønsker å skjerme informasjon[80]. Forutsetningen for denne påstanden er at en ser bort ifra GDPRs ofte glemte andre formål – fri flyt av data i eurosonen[81]. Utgangspunktet er derfor at det skal foreligge harmoni mellom direktivet og forordningen. Begge regelsettene bygger på at det er kunden som eier sine egne data[82], og at kunden kan oppnå verdi fra dataene ved å selge eller overføre dataene til selskaper som kan anvende dataene til å tilby skreddersydde tjenester til kunden.

Personvern kommer opp som tema flere steder i PSD2. Tydeligst fremgår dette av kap. 4 med tittelen «vern av personopplysninger». Kapittelet inneholder kun én artikkel. Det følger av PSD2 art. 94(1) at «enhver annen behandling av personopplysninger i henhold til dette direktiv skal utføres i samsvar med direktiv 95/46/EF», også kjent som personverndirektivet. PSD2 har dermed en direkte henvisning til at personopplysninger skal forståes som i DPD.

Av GDPR art. 94(2) fremgår det at enhver henvisning til DPD skal forståes som en henvisning til forordningen. PSD2 inneholder derfor en indirekte henvisning om at personopplysninger skal behandles i tråd med GDPR.

Behandling av personopplysninger kan være aktuelt ved flere anledninger i trepartsforholdet som oppstår under PSD2. For det første ved opprettelsen av et kundeforhold mellom kunden og, enten fullmakttjenesten eller kontotilbyderen (initial behandling). For det andre ved tilfellet hvor kontotilbyder skal gi fullmakttjenesten løpende tilgang til betalingskontoer. I

[80] Se bl.a. ekspertuttalelse av advokat Niels Vandezande (2019), fra det internasjonale advokatkontoret Timelex, som spesialiserer seg innen IKT rett, https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr (lest 09.12.2019)
[81] Se GDPR art. 1(3)
[82] Bl.a. uttrykt ved retten til dataportabilitet i GDPR art. 20

dette tilfellet vil det være nødvendig å overføre personopplysninger mellom kontotilbyder og fullmakttjeneste. Det er overføringstilfellet som oppgaven vil undersøke nærmere i punkt 5.2 og 5.3.

5.1.2 Hvilke data kan behandles under PSD2?

En klar formålsbegrensning for hvilke personopplysninger som kan behandles under PSD2, fremkommer av art. 94(2). Her presiseres det at betalingstjenesteytere bare skal behandle personopplysninger som er «nødvendige for å yte betalingstjenestene».

I artikkel 66 og 67 gir PSD2 uttrykk for ytterligere begrensninger. Av art. 66(3) bokstav g fremgår det at betalingsfullmakttjenesten ikke skal «bruke, ha tilgang til eller lagre noen opplysninger for noe annet formål enn yting av [betalingsfullmakttjenesten] som betaleren uttrykkelig har anmodet om». Videre av bokstav e at betalingsfullmakttjenesten ikke skal «lagre følsomme betalingsdata[83] tilhørende betalingstjenestebrukeren». En tilsvarende begrensning for kontoinformasjonstjenestene fremgår av art. 67(2) bokstav f og e.

Spørsmålet blir deretter om hvilke data som er nødvendige.

Av EDPS sin uttalelse til PSD2[84] fremkommer det at betalingstjenester i det minste vil behandle personopplysninger som navn, bankkontonummer og innhold av kontrakter, som det er behov for å overføre mellom betaler og betalingsmottaker. Slike personopplysninger vil i alle tilfeller være «nødvendige».

Vanskeligere er det derimot med personopplysninger som personnummer, informasjon om lønninger og den registrertes kjøpsadferd, som kan bli behandlet av betalingstjenestene. I slike tilfeller må behandlingen nøye vurderes opp mot formålet, sånn at det ikke forekommer en uberettiget formålsutglidning. Det er likevel vanskelig å si noe nærmere om konkret hvilke

[83] Definert i PSD2 art. 4(32) som «opplysninger, herunder personlige sikkerhetsopplysninger som kan brukes til å utføre bedrageri. For ytere av [betalingsfullmakttjenester] og ytere av [kontoinformasjonstjenester] utgjør navnet på kontoeier og kontonummer ikke følsomme betalingsopplysninger»

[84] EDPS, *Opinion of the European Data Protection Supervisor* (2013), side 2. Full utgave av uttalelsen er bare tilgjengelig på engelsk, https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf

personopplysninger som kan, og ikke kan behandles under formålsbegrensningen, da det enda ikke foreligger rettspraksis på området.

Et annet spørsmål er hvorvidt PSD2 tillater viderebehandling av personopplysninger, f.eks. for markedsføring eller anbefaling av tilleggstjenester.

Det følger av art. 66(3) bokstav f at betalingsfullmakttjenesten ikke skal «anmode betalingstjenestebrukeren om andre opplysninger enn slike opplysninger som er nødvendige for å yte [betalingsfullmakttjenesten]». Denne ordlyden, sammenlignet med art. 66(3) bokstav g, er blitt tolket som at artikkelen ikke tillater viderebehandling for andre formål enn de som er nødvendige for levering av betalingstjenestene[85].

Et tilsvarende punkt som art. 66(3) bokstav f eksisterer derimot ikke i art. 67. Den eneste begrensningen her er som nevnt ovenfor art. 67(2) bokstav f, om at kontoinformasjonstjenesten ikke skal «bruke, ha tilgang til eller lagre noen opplysninger for noe annet formål enn yting av den [kontoinformasjonstjeneste] betalingstjenestebrukeren uttrykkelig har anmodet om, **i samsvar med bestemmelsene om vern av personopplysninger**» (min utheving). Punktet er altså påført en ekstra presisering sammenlignet med art. 66(3) bokstav g.

Eksperter på området argumenterer for at dersom denne distinksjonen mellom art. 66 og 67 skal ha en realitet, må forskjellen tolkes som at viderebehandling iht. GDPR er tillat for kontoinformasjonstjenester under art. 67[86].

Problemstillingen er ikke endelig avklart, og løsningen fremstår derfor som usikker. Av plasshensyn har oppgaven ikke anledning til videre å drøfte denne problemstillingen.

5.2 Samtykke som behandlingsgrunnlag i PSD2

[85] Scott McInnes og Lupe Sampedro, *EU: The interplay of PSD2 and GDPR – some select issues* (2019), forfatterne representerer Bird & Bird LLP, https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf, side 5
[86] Ibid

Samtykke er nevnt hele 33 ganger i PSD2 og fortalen. Samtykke holder altså en sentral funksjon i direktivet. Samtykkets sentrale funksjon i PSD2 bekreftes også av EDPS sin uttalelse[87].

Spørsmålet blir dermed om samtykke kan tjene som behandlingsgrunnlag for overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste.

Som det ble redegjort for i punkt 4.2, må et samtykke være «frivillig, spesifik[t], informert og utvetydig» for å være gyldig som behandlingsgrunnlag etter GDPR, jf. GDPR art. 4(11). Videre må samtykke være gitt av en som innehar samtykkeevne.

Hvorvidt det foreligger et gyldig samtykke, vil bero på situasjonen på samtykketidspunktet. Derfor kan det ikke allerede nå avgjøres om et samtykke til behandling av personopplysninger, gitt i medhold av PSD2, vil være gyldig som behandlingsgrunnlag etter GDPR. Det er derimot mulig å vurdere om forståelsen av et samtykke i PSD2 harmoniserer med forståelsen som legges til grunn i GDPR art. 4(11) jf. art. 6(1) bokstav a.

Det følger av PSD2 art. 94(2) at:

> Betalingstjenesteytere skal bare hente, behandle og lagre personopplysninger som er nødvendige for å yte betalingstjenestene, med uttrykkelig samtykke fra betalingstjenestebrukeren.[88]

Ordlyden tilsier at personopplysninger bare kan behandles av betalingstjenesteytere, altså bl.a. fullmakttjenester og kontotilbydere[89], dersom det foreligger et «uttrykkelig samtykke».

Bruken av «uttrykkelig» går igjen i art. 66 og 67 også. Det følger av art. 66(3) bokstav c at betalingsfullmakttjenesten skal «sikre at alle andre opplysninger om betalingstjenestebrukeren som innhentes i forbindelse med yting av [betalingsfullmakttjenester], bare oppgis til betalingsmottakeren og bare med betalingstjenestebrukerens uttrykkelige samtykke». Videre fremgår det av art. 66(3) bokstav g at betalingsfullmakttjenesten ikke skal «bruke, ha tilgang til eller lagre noen opplysninger for noe annet formål enn yting av

---

[87] Av EDPS (2013), side 6 fremkommer det at: "The provision of information about the processing of personal data in due time before requiring the payment service is all the more important as consent of the user is meant to play a central role …"

[88] Av den danske versjonen av artikkelen: «Betalingstjenesteudbydere må kun tilgå, behandle og opbevare personoplysninger, som er nødvendige for ydelse af betalingstjenester, med betalingstjenestebrugerens udtrykkelige samtykke.»

[89] Se PSD2 art. 4(11) jf. 1(1) bokstav d jf. 4(4)

[betalingsfullmakttjenesten] som betaleren uttrykkelig har anmodet om». Tilsvarende formuleringer anvendes også i art. 67, se bl.a. punkt (2) bokstav a om at kontoinformasjonstjenesten skal «yte tjenester bare på grunnlag av et uttrykkelig samtykke fra betalingstjenestebrukeren».

5.2.1 Uttrykkelig samtykke

Et spørsmål som raskt oppsto etter at PSD2 trådte i kraft var om «uttrykkelig samtykke» i PSD2 skulle forståes som i GDPR.

Av GDPR art. 9(2) bokstav a fremgår det at behandling av særlige kategorier av personopplysninger[90] er forbudt, dersom den registrerte ikke har «gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål». Behandlingsgrunnlaget regnes som mer krevende å oppfylle og gir uttrykk for en skjerpet terskel sammenlignet med et alminnelig GDPR-samtykke etter GDPR. Art. 6(1) bokstav a[91].

Det fremkommer av GDPR art. 9(1) at som særlige kategorier av personopplysninger, regnes:

> personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med de formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering …

Finansiell informasjon eller kundekontoopplysninger er dermed ikke ansett som en særlig kategori av personopplysninger i GDPR. Poenget uttrykkes eksplisitt i FRA og CoE (2018) i kapittelet om «financial data»[92].

Derimot i PSD2 art. 66 og 67 anvendes formuleringer som «følsomme betalingsdata tilhørende betalingstjenestebrukeren»[93] og «ikke anmode om følsomme betalingsopplysninger

[90] Tidligere omtalt som «sensitive» personopplysninger
[91] McInnes og Sampedro (2019), side 3
[92] På side 343 "… financial data are not considered sensitive data under Modernised Convention 108 or the General Data Protection Regulation …"
[93] Se PSD2 art. 66(3) bokstav e

knyttet til betalingskontoer»[94]. Tilsvarende i den danske oversettelsen hvor «følsomme betalingsdata» og «følsomme betalingsoplysninger» er brukt om de samme artiklene.

Ordlyden i artiklene tilsier at PSD2 legger til grunn at det kan eksistere finansiell informasjon som er «følsom» og som derav skal behandles som særlige kategorier av personopplysninger jf. GDPR art. 9.

Her foreligger det dermed ikke harmonisering mellom PSD2 og GDPR.

Dersom det legges til grunn at finansiell informasjon eller kundekontoopplysninger i PSD2 skal behandles som en særlig kategori av personopplysninger jf. GDPR art. 9, vil det skape dårlig harmoni mellom direktivet og forordningen[95]. Videre vil en slik løsning kunne skape usikkerhet knyttet til andre finansielle regelverk, hvor betalingsinformasjon eller kundekontoopplysninger ikke er ansett som en særlig kategori av personopplysninger iht. GDPR. Totalt sett vil løsningen innebære dårlig harmonisering, og skape usikkerhet knyttet til behandling av personopplysninger i finansielle forhold, om den mer krevende terskelen skulle legges til grunn på noe som etter forordningen ikke regnes som en særlig kategori av personopplysninger.

Den 16. februar 2018 mottok EDPB, da A29WP, et brev fra den nederlandske tilsynsmyndigheten om bl.a. problemstillingen knyttet til manglende harmonisering av «uttrykkelig samtykke». I brev av 5. juli 2018 fra EDPB[96] anføres en mulig løsning på konflikten. Her uttrykkes det bestemt at «[t]he concept of explicit consent under Article 94(2) of PSD2 […] is therefore not the same as (explicit) consent under the GDPR.»[97] Begrunnelsen som EDPB la til grunn var at «[t]he EDPB is of the view that the “explicit consent” referred to in Article 94 (2) of PSD2 is a contractual consent.»[98] Nærmere om virkningen av denne løsningen beskrives nedenfor. Rettskildeverdien til uttalelsene anses som høy, grunnet at EDPB holder en autoritær plassering innen europeisk personvernrett. Likevel foreligger det ingen rettspraksis på område, så uttalelsene forståes ikke som en endelig avklaring.

---

[94] Se PSD2 art. 67(2) bokstav e
[95] Se sammendrag fra EDPS (2013), hvor det bemerkes at «[m]ed hensyn til udtrykket »følsomme betalingsdata« i artikel 58 bør ordet »følsomme« udelades og udtrykket »betalingsdata« anvendes i stedet.»
[96] Se EDPB, *Letter regarding the PSD2 Directive* (2018), https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en
[97] Ibid, side 3-4
[98] Ibid

Løsningen som skisseres av EDPB legges til grunn i *EU: The Interplay of PSD2 and GDPR – some select issues* (2019)[99]. Her fremgår det at «uttrykkelig samtykke» i PSD2 ikke bør forståes som et GDPR (uttrykkelig) samtykke, på bakgrunn av at et GDPR-samtykke allerede er et komplisert behandlingsgrunnlag å oppfylle, at betalingsinformasjon ikke utgjør en særlig kategori av personopplysninger og at behandlingsansvarlig kan bero på et annet behandlingsgrunnlag, nemlig kontrakt. Videre støttes uttalelsen av bransjepraksis i *Reconciling Consent in PSD2 and GDPR* (2019), hvor det slås fast at uttalelsen fra EDPB ikke oppklarer alle spørsmål som er oppstått om forholdet mellom PSD2 og GDPR, men at den gir en velkommen oppklaring om at «uttrykkelig samtykke» i PSD2 er noe annet og noe forskjellig fra «uttrykkelig» samtykke i GDPR[100].

Hensynet til en alminnelig tolkning av artiklenes ordlyd står dermed i konflikt med hensynet til harmoni mellom direktivet og forordningen. Videre også i konflikt med hensynet til harmoni internt i EUs regulering av det finansielle markedet.

Til støtte for hensynet til artikkelens ordlyd, kan det nevnes at spørsmål rundt personvern ble kommentert av EDPS, se *Opinion of the European Data Protection Supervisor* (2013)[101] jf. PSD2s fortale 111. Dette innebærer at man ved arbeidet med PSD2 hadde tilgang til anbefalinger knyttet til hvordan personvern burde håndteres og reguleres i PSD2. Av denne grunn kan bruken av «uttrykkelig samtykke» forståes som et bevisst valg om at den skjerpede terskelen i GDPR art. 9 skal anvendes.

Likevel fremgår det av uttalelsen fra EDPS at det ble anbefalt at situasjonen rundt personvern skulle eksplisitt nevnes, slik at det ble klart hvordan personvern skulle forståes og behandles i direktivet. At spørsmålet om «uttrykkelig samtykke» har blitt så mye diskutert i ettertid, er en indikasjon på at anbefalingen om klarhet fra EDPS ikke ble tatt tilstrekkelig til følge. Videre ble det eksplisitt uttalt av EDPS at personvern i direktivet skulle forståes iht. «gældende databeskyttelseslovgivning»[102]. På tidspunktet for uttalelsen fra EDPS var gjeldende personvernlovgivning DPD, men det er sikker rett at en henvisning til DPD skal regnes som

[99] McInnes og Sampedro (2019), side 3 og 4
[100] Vandezande (2019)
[101] EDPS (2013)
[102] Sammendrag fra EDPS (2013), side 1

en henvisning til GDPR[103]. Momentene taler for at GDPRs forståelse av særlige kategorier av personopplysninger får forrang ved konflikt.

Et vektig argument til støtte for løsningen som ble presentert av EDPB, er at ett av EUs overordnede målsetninger er harmoni innen regulering av det interne markedet. Hensynet bak målsetningen er at individer og bedrifter møter tilsvarende regler uavhengig av hvilken medlemsstat de befinner seg i og hvilken EU regulering de tar utgangspunkt i. Det er et ønske om at lovgivingen skal være forutberegnelig for borgerne av Unionen.

Oppgaven finner grunn til å støtte løsningen som presenteres av EDPB, og anser at hensynet til harmoni er viktigere enn hensynet til en alminnelig tolkning av direktivets ordlyd. Det er derfor oppgavens forståelse at «uttrykkelig samtykke» i PSD2 ikke innebærer at de strengere vilkårene i GDPR art. 9(2) bokstav a, skal innfortolkes i direktivet.

Spørsmålet blir så hvordan PSD2 art. 94(2) videre skal forståes.

Det fremgår av brev fra EDPB, med henvisning til PSD2s fortale punkt 87, at:

> Payment services are always provided on a contractual basis between the payment services user and the payment services provider. […] In terms of the GDPR, the legal basis for the processing of personal data is Article 6 (1) (b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party.[104]

EDPB anfører dermed at avtalen mellom den registrerte og fullmakttjenesten, om utførelsen av betalingstjeneste, er det naturlige behandlingsgrunnlaget for initial behandling av personopplysninger i PSD2.

Videre argumenterer EDPB for hvordan PSD2 art. 94(2) nå skal forståes:

> This implies that Article 94 (2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and

[103] Se GDPR art. 94 jf. også EDPB (2018), hvor det eksplisitt nevnes på side 2 at referansen til DPD i PSD2 skal forståes som en referanse til GDPR.
[104] EDPB (2018), side 4

> have to explicitly agree to these clauses. […] The concept of explicit consent under Article 94(2) of PSD2 is therefore an additional requirement of a contractual nature[105]

Virkningen av løsningen som EDPB tar til orde for er at PSD2 art. 94(2) skal gis et innhold som strider mot den naturlige forståelsen av artikkelens ordlyd. Videre tolkes artikkelen til å omhandle og presisere et annet behandlingsgrunnlag enn det som følger av ordlyden. Altså forståes ikke art. 94(2) som et uttrykk for at samtykke (uttrykkelig eller ei), skal være det foretrukne behandlingsgrunnlaget for initial behandling av personopplysninger. Resultatet blir dermed at heretter vil kontrakt være det naturlige behandlingsgrunnlaget for initial behandling av personopplysninger i PSD2.

Likevel så uttales det av EDPB at samtykke fortsatt kan tjene som behandlingsgrunnlag under PSD2:

> Further processing of personal data for other purposes, not necessary for the performance of the contract, could be based on consent under Article 6(1) (a) GDPR, provided that the requirements and the conditions for consent laid out in Article 7 and Article 4 (11) GDPR are fully respected.[106]

Uttalelsen er knyttet til initial behandling av personopplysninger og ikke overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste. Det er derfor noe usikkerhet rundt hva løsningen vil bli.

Hovedspørsmålet som er blitt undersøkt under oppgavens punkt 5.2 er hvorvidt overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste kan bero på samtykke som behandlingsgrunnlag.

Det er på det rene at det ikke kan foreligge en kontrakt mellom kontotilbyder og fullmakttjeneste om behandling av den registrertes personopplysninger. Uttalelsen om at kontrakt vil være det viktigste behandlingsgrunnlaget treffer dermed ikke på den foreliggende problemstillingen.

[105] Ibid
[106] Ibid

Som nevnt ovenfor må bruken av «uttrykkelig» nyanseres i PSD2 når det kommer til behandling av personopplysninger. Likevel er det en kjensgjerning at art. 66 og 67 henviser spesifikt til samtykke.

Oppgaven tolker utsagnet fra EDPB som at samtykke vil kunne anvendes som behandlingsgrunnlag for overføringstilfellet, men at grunnlaget må utledes av GDPR art. 6(1) bokstav a jf. art. 4(11), og ikke av PSD2.

Det er oppgavens vurdering at samtykke vil være et aktuelt behandlingsgrunnlag for overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste.

5.2.2 Dobbelt samtykke

Et annet spørsmål som er oppstått er om det eksisterer et krav om dobbelt samtykke i PSD2. Med andre ord om kontotilbyder er forpliktet til å innhente eget samtykke fra kontoinnehaver for å overføre kundens personopplysninger til fullmakttjenesten.

Spørsmålet er oppstått som følge av at samtykke er eksplisitt nevnt i sentrale artikler som omhandler personopplysninger, bl.a. i PSD2 art. 94(2), 66 og 67. Samtykke er det eneste behandlingsgrunnlaget som nevnes i PSD2, foruten om i PSD2 art. 94(1), som omhandler en rettslig forpliktelse til å behandle personopplysninger for å forhindre betalingsbedrageri. Videre har samtykke ofte blitt sett på som det foretrukne behandlingsgrunnlaget, da det utledes direkte fra den registrerte. Et slik synspunkt fremmes bl.a. i forarbeidene til personopplysningsloven av 1998[107].

Som allerede nevnt, må derimot forståelsen av samtykke som behandlingsgrunnlag i PSD2 nyanseres, særlig referansen til «uttrykkelig». Likevel er samtykke nevnt hele 33 ganger i direktivet.

De fleste av disse henvisningene til samtykke knytter seg direkte opp mot betalingstransaksjoner, og det faktum at samtykke kreves for at en betaling kan gjennomføres. Forvirringen rundt samtykkets betydning i PSD2 skyldes nettopp dette, at samtykke tjener flere formål i direktivet.

[107] Se Ot.prp.nr. 92 (1998-1999) s. 108

Det er oppgavens forståelse at PSD2 opererer med to separate regimer for samtykke. Ett for samtykke som behandlingsgrunnlag og ett separat et for samtykke som mekanisme for autentisering av betalingstransaksjoner. Ved å se disse to ordningene for samtykke adskilt, begynner samtykke under PSD2 å gi mer mening.

Det er på det rene at en av de viktigste forutsetningene for at innføringen av fullmakttjenester skal fungere i praksis, er at de nye tjenestene har tillit blant kundene og tillit blant kontotilbyderne. Kunden ønsker ikke å gi tilgang til sin betalingskonto dersom den risikerer at fullmakttjenesten stikker av med innholdet. Tilsvarende så ønsker ikke kontotilbyder å gi fullmakttjenestene tilgang til sin infrastruktur, dersom det ikke foreligger klare garantier som sikrer kontotilbyder fra å lide et tap. Sikkerhetsaspektet har derfor hatt en nøkkelposisjon ved arbeidet med PSD2[108].

Det er ikke nok at fullmakttjenestene er lisensierte og at det iverksettes sikkerhetsrutiner. Det er også et behov for å kunne garantere at hver enkelt betalingstransaksjon er godkjent av kunden. Her kommer samtykke som mekanisme for godkjenning av betalingstransaksjoner inn.

Hvis art. 66 og 67 leses i denne sammenheng, er det klart at artiklene fokuserer mer på sikker gjennomføring og godkjenning av betalingstransaksjoner, enn på behandling av personopplysninger[109].

Videre er dette synlig i art. 64, som er den mest detaljerte reguleringen av samtykke i hele PSD2. Her benyttes ordet «samtykke» hele syv av de 33 gangene i direktivet. Overskriften til art. 64 heter «[s]amtykke og tilbakekalling av samtykke». Enhver kan falle for fristelsen å tenke at her er det snakk om behandling av personopplysninger, med en klar referanse til GDPR art. 7(3). Derimot så fremkommer det eksplisitt av punkt (1) at «[m]edlemsstatene skal sikre at en betalingstransaksjon anses som godkjent bare dersom betaleren har gitt sitt samtykke til å gjennomføre betalingstransaksjonen.» Videre av (2) annen setning «[d]ersom samtykke ikke foreligger, skal en betalingstransaksjon anses som uautorisert.» Selv behandlingen av tilbaketrekking omhandler ikke personopplysninger. Det følger av

[108] Se EBA, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (2018), side 1-2, hvor det beskrives at "the Directive conferred on the EBA the development of 12 technical standards and guidelines, to specify detailed provisions in relation to payment security, authorisation, passporting, supervision and more."
[109] Se bl.a. PSD2 art. 66(3) a, b og d, og art. 67(2) b og c jf. art. 97 og 98

artikkelens (3) at et samtykke kan trekkes tilbake av betaleren, frem til betalingsordren er mottatt av betalerens betalingstjenesteyter. Altså har den mest omfattende reguleringen av samtykke i direktivet fokus på sikring av krav til det å gjennomføre betalingstransaksjoner, ikke på vern av personopplysninger.

Det fremgår av artikkel 64, sammenlignet med forskrift om betalingstjenester § 5(2), at samtykke er den eneste akseptable måten i PSD2 for kunden å godkjenne at fullmakttjenesten overfører midler fra en betalingskonto til en annen.

Etter en helhetlig vurdering er min mening at samtykke som mekanisme for godkjenning av betalingstransaksjoner må ses separat fra samtykke som rettslig grunnlag for behandling av personopplysninger.

Dersom samtykke ses i denne snevrere betydningen, foreligger det flere argumenter som taler for at PSD2 åpner for at andre behandlingsgrunnlag kan anvendes på overføringen av personopplysninger mellom kontotilbyder og fullmakttjeneste.

For det første fremgår det av EBA at:

> where Account Information Services (AIS) or Payment Initiation Services (PIS) are provided to a payment service user (PSU) following a contract that has been signed by both parties, Account Servicing Payment Service Providers (ASPSPs) do not have to check consent. It suffices that AISPs and PISPs can rely on the authentication procedures provided by the ASPSPs to the PSU, when it comes to the expression of explicit consent[110]

Uttalelsen taler for at dersom fullmakttjenesten er autorisert etter PSD2 art. 11 og at betalingstransaksjonen er godkjent av kunden, så behøver ikke kontotilbyder be om bekreftelse på at gyldig samtykke foreligger.

Av art. 32(3) av delegert forordning (EU) 2018/389 fremkommer det at:

> obstacles may include, among others […] requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.

[110] EBA (2018), side 4

Ordlyden tilsier at dersom kontotilbyder ber om ekstra kontroll av samtykke eller ber om et ekstra (dobbelt) samtykke fra kunden, vil det kunne regnes som en hindring for ytingen av fullmakttjenester etter artikkelen.

Uttalelsen fra EBA og ordlyden i art. 32(3) taler mot at det eksisterer en forpliktelse til å innhente eget samtykke fra kontoinnehaver for å overføre kundens personopplysninger til fullmakttjenesten.

Videre foreligger det flere momenter som taler for at andre behandlingsgrunnlag enn samtykke får anvendelse på overføringstilfellet under PSD2. For det første kan det nevnes at selv om forarbeidene til personopplysningsloven av 1998[111] gav uttrykk for at samtykke var et foretrukket behandlingsgrunnlag, har synspunktet blitt diskutert og problematisert i bl.a. *Personvern i informasjonssamfunnet*[112], med videre henvisning til praksis fra personvernnemda[113]. Dersom det hersket noen tvil under DPD, er det nå på det rene at alle behandlingsgrunnlag i GDPR art. 6 er likestilte[114].

Dessuten var et av hovedpoengene under punkt 5.2.1, at EDPB anså kontrakt som et sentralt behandlingsgrunnlag ved initial behandling[115]. Selv om uttalelsen ikke direkte angikk overføringstilfellet, kan det tas til støtte for at andre behandlingsgrunnlag enn samtykke får anvendelse under PSD2. Brevet fra EDPB ble behandlet og kommentert i McInnes og Sampedro (2019)[116], uten at forfatterne fant grunn til å anse bruken av samtykke i direktivet som et forbud mot behandling på bakgrunn av andre behandlingsgrunnlag. Tvert om anså forfatterne det som nærliggende at «rettslig forpliktelse» i GDPR art. 6(1) bokstav c, kunne være et anvendelig behandlingsgrunnlag. Brevet ble også kommentert i *Reconsiling consent under PSD2* (2019)[117], hvor forfatteren støtter EDPBs vurdering av kontrakt som behandlingsgrunnlag, og stiller et åpent spørsmål ved om samtykke som behandlingsgrunnlag egentlig er nødvendig under PSD2.

[111] Se Ot.prp.nr. 92 (1998-1999) s. 108
[112] Se Schartum og Bygrave (2016), side 183-184
[113] Forfatterne skriver "[p]ersonvernnemda har uttalt at de anser de rettslige grunnlagene som likestilte, og at samtykke ikke representerer noen fast hovedregel etter loven.»
[114] Se f.eks. FRA og CoE (2018), side 142
[115] EDPB (2018), side 4
[116] Se rapportens side 3 og 4
[117] Se Vandezande (2019)

I EDPS sin uttalelse om PSD2[118] er det ikke nevnt noen begrensninger angående hvilke behandlingsgrunnlag som er aktuelle under PSD2. Uttalelsen kan derimot leses som at den åpner for behandling på bakgrunn av rettslig forpliktelse.

Etter en helhetsvurdering er min konklusjon at kontotilbyder ikke er forpliktet til å innhente eget samtykke fra kontoinnehaver for å overføre kundens personopplysninger til fullmakttjenesten. Med andre ord vil andre behandlingsgrunnlag enn samtykke kunne få anvendelse på tilfellet om overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste. Det er grunn til å understreke at det hefter en viss usikkerhet ved konklusjonen i mangel på rettslig avklaring av spørsmålet.

5.3 Rettslig forpliktelse som behandlingsgrunnlag i PSD2

Det følger av GDPR art. 6 (1) bokstav c at behandling bare er lovlig dersom «behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige».

Hovedspørsmålet som skal besvares i denne seksjonen er hvorvidt det foreligger en rettslig forpliktelse i PSD2 til å overføre personopplysninger fra en kontotilbyder til en fullmakttjeneste. Videre om et slikt rettslig grunnlag oppfyller vilkårene for å kunne tjene som behandlingsgrunnlag.

I oppgavens punkt 4.3 ble vilkårene for rettslig forpliktelse gjennomgått. Hovedmomentene kan oppsummeres i korte trekk ved at, for det første, behandlingen må være nødvendig. For det andre skal den rettslige forpliktelsen gi uttrykk for formålet med behandlingen. Videre at det rettslige grunnlaget kan inneholde begrensninger. Til slutt at den rettslige forpliktelsen enten må følge av en direkte hjemmel eller at den må være klart forutsatt.

I *EU: The interplay of PSD2 and GDPR – some select issues*[119] uttrykkes det at «rettslig forpliktelse» kan være et aktuelt behandlingsgrunnlag under PSD2. Rapporten gir derimot ikke noen nærmere drøftelse av om vilkårene nevnt ovenfor er oppfylt eller hvilken artikkel det rettslige grunnlaget utledes fra.

[118] Sammendrag fra EDPS, side 1-2
[119] McInnes og Sampedro (2019), side 4

Det første spørsmålet som må besvares er dermed hvilken artikkel i PSD2 som kan utgjøre et rettslig grunnlag for overføring av personopplysninger.

I punkt 5.1 gjennomgikk oppgaven hvordan PSD2 tilnærmer seg personvern og ved hvilke bestemmelser dette er kommet til uttrykk. De mest sentrale bestemmelsene er artikkel 94, 67, 66 og også 36.

5.3.1 Artikkel 94 som rettslig grunnlag

Et utgangspunkt for å lete etter et rettslig grunnlag er kapittel 4 av PSD2, med overskriften «Vern av personopplysninger». Artikkel 94(2) gir uttrykk for at «[b]etalingstjenesteytere skal bare hente, behandle og lagre personopplysninger som er nødvendige for å yte betalingstjenestene». Artikkelen gir dermed uttrykk for en generell formålsbegrensning og åpner for at personopplysninger kan behandles i direktivet. Av art. 94(1) følger det en direkte rettslig forpliktelse til å behandle personopplysninger for «forebygging, etterforskning og avsløring av betalingsbedrageri». Formålet er ikke forenelig med overføringstilfellet, hvor formålet er økt konkurranse og økt innovasjon knyttet til betalingstjenester.

Artikkel 94 gir dermed ikke uttrykk for en rettslig forpliktelse som må løses med overføring av kundens personopplysninger fra kontotilbyder til fullmakttjenesten.

5.3.2 Artikkel 66 og 67 som rettslig grunnlag

Artikkel 66 bærer overskriften «[r]egler for tilgang til betalingskonto for [betalingsfullmakttjenester]». Overskriften taler dermed for at artikkelen omhandler overføringstilfellet. Derimot fremkommer det av punkt 1 at «[m]edlemsstatene skal sikre at en betaler har rett til å benytte en yter av betalingsinitieringstjenester for betalingstjenestene nevnt i vedlegg I nr. 7». Ordlyden tilsier at artikkelen retter en forpliktelse mot medlemsstaten om å sikre at kunden har mulighet til å anvende en kontoinformasjonstjeneste. Artikkelen presiserer ikke nærmere hvordan kontoinformasjonstjenesten får tilgang til kontoopplysningene fra kontotilbyderen. Tilsvarende i art. 67.

Hverken art. 66 eller 67 gir uttrykk for en direkte forpliktelse til å overføre personopplysninger fra kontotilbyder til fullmakttjenesten.

Videre er det flere momenter som taler mot at artiklene «klart forutsetter» en rettslig forpliktelse til å overføre personopplysninger. For det første er art. 66 delt i fire[120], med forpliktelser rettet mot medlemsstatene, betaleren, betalingsfullmakttjenesten og kontotilbyderne. Hvis det var meningen at en forpliktelse til å overføre personopplysninger skulle innfortolkes, så ville det vært naturlig at forpliktelsen var plassert under kontotilbyders plikter eller betalingsfullmakttjenestens plikter. For det andre er behandling av personopplysninger eksplisitt nevnt under art. 66(3) bokstav f og g. Dersom det var intensjonen at punkt 1 skulle tjene som rettslig grunnlag for overføring av personopplysninger, ville det derfor være naturlig at dette kom tydeligere frem[121].

Det fremkommer derfor ikke en rettslig forpliktelse til å overføre personopplysninger fra kontotilbyder til fullmakttjeneste i PSD2 art. 66(1) eller 67(1).

En annen mulighet er PSD2 Art. 66(4) bokstav b. Punktet innebærer en forskjell mellom art. 66 og 67, da punktet ikke har en ekvivalent i art. 67. Av art. 66(4) bokstav b fremkommer det at kontotilbyderen skal «framlegge eller gjøre tilgjengelig […] alle opplysninger om gjennomføringen av betalingstransaksjonen» til betalingsfullmektigen. «Alle opplysninger» omfatter naturlig også kundens personopplysninger. Bokstav b gir dermed uttrykk for en direkte rettslig forpliktelse om å overføre personopplysninger og som inneholder en formålsbegrensning. Altså er alle vilkårene for at det skal foreligge en rettslig forpliktelse til å behandle personopplysninger oppfylt.

Spørsmålet som deretter oppstår, er knyttet til omfanget av forpliktelsen. Kan artikkel 66(4) bokstav b anses som en generell hjemmel for overføring av personopplysninger mellom kontotilbyder og betalingsfullmakttjenesten?

En slik tolkning er nok å strekke strikken for langt. Av bokstav b følger det at overføringen som hjemles må knytte seg til «gjennomføringen av betalingstransaksjonen». Ordlyden må ses i sammenheng med kapitteloverskriften om «godkjenning av betalingstransaksjoner», samt samtykke ved autorisering av betalingstransaksjoner. At forpliktelsen knytter seg direkte til betalingstransaksjoner, innebærer reelt sett en begrensing av adgangen til å behandle personopplysninger. Årsaken til denne begrensningen er at hver transaksjon ses individuelt i

[120] PSD2 art. 67 er tilsvarende delt i tre, med forpliktelser rettet mot medlemsstatene, kontoinformasjonstjenester og kontotilbyder
[121] Se tilsvarende i art. 67(2) f

PSD2. Forståelsen fremgår av samtykke- og autoriseringsregimet som er lovfestet i direktivet. Ses disse momentene i sammenheng innebærer det at adgangen til å overføre personopplysninger er basert på en transaksjon til transaksjons basis, noe som reelt sett betyr at hver overføring vil være autorisert og godkjent av kunden.

Resultatet blir dermed at bokstav b hjemler en begrenset overføring av personopplysninger tilknyttet hver enkelt transaksjon. Artikkel 66(4) bokstav b kan derfor ikke leses som en hjemmel for løpende overføring av personopplysninger mellom kontotilbyder og betalingsfullmektig.

5.3.3 Artikkel 36 som rettslig grunnlag

Det følger av artikkel 36 at «[m]edlemsstatene skal sikre at betalingsinstitusjonene har tilgang til kredittinstitusjonenes betalingskontotjenester på en objektiv, forholdsmessig måte som ikke innebærer forskjellsbehandling.» Videre fremkommer det av andre setning at «[t]ilgangen skal være tilstrekkelig omfattende til at betalingsinstitusjonene kan yte betalingstjenestene uhindret og effektivt.»

Innimellom formuleringene om likebehandling og effektivitet er det klart at det av artikkelen fremkommer et krav. Kravet går ut på tilgang til «kredittinstitusjonenes[122] betalingskontotjenester» og rettigheten innvilges «betalingsinstitusjonene[123]». Altså fremsetter artikkelen et krav om tilgang til betalingskontoer som skal være «tilstrekkelig omfattende».

Selv om begrepene i artikkel 36 fraviker noe fra begrepsbruken i direktivet for øvrig, gir altså artikkelen uttrykk for at kontotilbydere plikter å gi fullmakttjenestene og andre kontotilbydere tilgang til sine betalingskontoer.

Det neste spørsmålet er om artikkel 36 oppfyller vilkårene i GDPR art. 6(1) bokstav c til å virke som behandlingsgrunnlag for overføring av personopplysninger.

[122] Se PSD2 art. 1(1) a jf. Forordning (EU) 2013/575 art. 4(1). Her er «kredittinstitusjon» definert som «et foretak hvis virksomhet består i å motta fra offentligheten innskudd eller andre midler som skal betales tilbake, og å yte kreditt for egen regning»
[123] Se PSD2 art. 4(4) jf. 4(3) jf. Vedlegg I, om at begrepet «betalingsinstitusjon» omfatter både kontotilbyder og fullmakttjenester

For det første må det være nødvendig å behandle personopplysninger for å oppfylle den rettslige forpliktelsen. For at kontotilbyder skal kunne gi tilgang til betalingskontoer til fullmakttjenestene og andre kontotilbydere, så må de behandle personopplysninger. Kontotilbyder er avhengig av å kunne knytte den enkelte kunde til en konkret betalingskonto. Videre er det behov for å autentisere kunden, slik at fullmakttjenesten gir kunden tilgang til riktig konto. I tillegg må kontotilbyder overføre kontoopplysninger til fullmakttjenesten, for at denne skal kunne ta nytte av tilgangen til betalingskontoene. Disse kontoopplysningene vil naturlig også inneholde personopplysninger[124]. For at fullmakttjenesten skal kunne yte betalingstjenestene «uhindret og effektivt» er det dermed nødvendig å behandle personopplysninger.

Deretter er det et krav om formålsbegrensning i rettsgrunnlaget. Artikkel 36 første ledd andre setning gir uttrykk for at «tilgangen skal være tilstrekkelig omfattende til at betalingsinstitusjonene kan yte betalingstjenestene uhindret og effektivt». Behandlingen må derfor begrense seg til det som er nødvendig for å kunne «yte betalingstjenestene». Formålsbegrensningen må leses i sammenheng med begrensningene som fremkommer av art. 66 og 67[125], som retter seg spesifikt mot behandlingen av personopplysninger av fullmakttjenestene. I tillegg gir art. 94(2) uttrykk for en generell formålsbegrensning. Vilkåret om formålsbegrensning er derfor oppfylt.

Det tvilsomme vilkåret er hvorvidt den rettslige forpliktelsen er kommet til uttrykk direkte ved lov.

Det er klart at direktivet er omfattet av unionsretten og derfor har mulighet til å danne grunnlag for rettslige forpliktelser. Artikkel 36 kan likevel vanskelig leses som en direkte hjemmel for behandling av personopplysninger.

Det foreligger ikke noen nærmere begrunnelse for valget med å formulere en direkte hjemmel i art. 94(1) om svindel og ikke en direkte hjemmel for overføring mellom kontotilbyder og fullmakttjeneste. Det kan tenkes at i svindeltilfellet ville det være vanskelig å finne et annet behandlingsgrunnlag å støtte seg til, mens det i overføringstilfellet kan foreligge flere aktuelle behandlingsgrunnlag, se bl.a. overfor i punkt 5.2 om samtykke. Videre at man i arbeidet med

[124] Se punkt 3
[125] Se PSD2 art. 66(3) g hvor det fremgår at betalingsfullmakttjenesten ikke skal «bruke, ha tilgang til eller lagre noen opplysninger for noe annet formål enn yting av betalingsinitieringstjenesten som betaleren uttrykkelig har anmodet om». Tilsvarende i art. 67(2) f

direktivet derfor ikke ville ta et endelig standpunkt til hvilket behandlingsgrunnlag behandlingsanvarlig skal benytte, slik at behandlingsanvarlig har et reelt valg. En annen begrunnelse kan være at det i svindeltilfellet foreligger andre rettsgrunnlag som krever behandling, slik at behovet for harmonisering var klarere på tidspunktet for utarbeidelsen av direktivet.

Det foreligger dermed ikke en direkte hjemmel for behandling av personopplysninger i art. 36.

Spørsmålet videre er om den rettslige forpliktelsen er «klart forutsatt».

Av punkt 4.3, gjennomgått ovenfor, følger det at det skal foretas en bred vurdering for å avgjøre om den rettslige forpliktelsen er klart forutsatt. Videre at det foreligger tre vurderingsmomenter som bør avveies.

Det første vurderingsmomentet er hvorvidt det rettslige grunnlaget angir aktuelle opplysningstyper som kreves behandlet.

En viss beskrivelse av opplysningstyper følger av art. 36 første ledd andre setning ved at tilgangen til betalingskontoer hos kontotilbyder skal være «tilstrekkelig omfattende». Rent språklig vil en forståelse av «tilstrekkelig omfattende» innebærer at alle opplysningstyper som er nødvendige for å oppfylle formålet med å «yte betalingstjenestene uhindret og effektivt», vil være omfattet. Ved en slik tolkning er også personopplysninger omfattet. Bruken av «tilstrekkelig omfattende» bærer preg av at man i arbeidet med direktivet ikke ønsket å unnlate noen informasjonstyper, slik at artikkelen kunne gis en bred anvendelse.

Aktuelle opplysningstyper i artikkel 36 må også forståes i lys av begrensningene i artikkel 66 og 67, jf. redegjørelsen i punkt 5.1.2. Her er det spesifisert hvordan fullmakttjenestene kan behandle personopplysninger, samt hva formålet med behandlingen skal være. Det er derimot ikke konkretisert hvilke opplysningstyper som kan behandles.

Av sammendraget fra uttalelsen fra EDPS fremkommer det en viss klargjøring ved at det av uttalelsen fremgår at «[m]ed hensyn til udtrykket «tilstrækkelige midler til rådighed» i artikel 58 og 59 skal det gøres klart, at de oplysninger, der videregives til tredjeparten, kun bør bestå i et enkelt svar (»ja« eller »nej«) på spørgsmålet om, hvorvidt der er tilstrækkelige midler til

rådighet – og f.eks. ikke i en saldooplysning.»[126] Uttalelsen kan forståes som et uttrykk for dataminimering[127] og et eksempel på hvilke valg fullmakttjenestene kan foreta og hvilke opplysninger som er nødvendige for å yte betalingstjenestene.

Slik sett er det ikke direkte konkretisert hvilke opplysninger som kan behandles, men det er gitt en ramme og en begrensning for hvilke opplysningstyper som kreves behandlet. Artikkelen setter en i stand til å skille relevante opplysningstyper fra irrelevante opplysningstyper.

Det neste vurderingsmomentet er hvorvidt personvernspørsmål er drøftet i forarbeidene.

Av fortalen punkt 39 til artikkel 36 fremkommer det at «[f]or å gjøre det mulig for betalingstjenesteytere å yte betalingstjenester, er det et ufravikelig krav at de har mulighet til å åpne og opprettholde kontoer i kredittinstitusjoner. Medlemsstatene bør sikre at det gis tilgang til [kontoer i kredittinstitusjoner] på en måte som ikke innebærer forskjellsbehandling, og som står i forhold til det rettmessige mål den har til hensikt å nå. Selv om tilgangen kan være av grunnleggende art, bør den alltid være tilstrekkelig omfattende til at betalingsinstitusjonen kan yte sine tjenester uhindret og effektivt.» Personopplysninger er dermed ikke direkte nevnt.

I fortalen punkt 89 fremgår det derimot at «[n]år betalingstjenesteytere yter betalingstjenester, kan behandling av personopplysninger forekomme.» Uttalelsen kan tolkes som at man ved utarbeidelsen av direktivet var innforstått med at behandling av personopplysninger ville inntreffe ved å yte betalingstjenester. Videre at behandlingen kunne komme til å bero på andre behandlingsgrunnlag enn samtykke som er nevnt i art. 94(2).

Det er på det rene at personvernspørsmål ikke er drøftet i fortalen tilknyttet artikkel 36. Likevel er det heller ikke presisert noe som taler imot at artikkelen også åpner for behandling av personopplysninger. Som gjennomgått under vurderingen av nødvendighet vil det være behov for å overføre personopplysninger mellom kontotilbyder og fullmakttjeneste for å kunne gi tilgang til betalingskontoer. Behandling av personopplysninger kan derfor stå «i forhold til det rettmessige mål den har til hensikt å nå» jf. fortalen punkt 39.

[126] Sammendrag fra EDPS, side 2
[127] Dataminimering er et sentralt prinsipp i forordningen jf. GDPR art. 5(1) c

Vurderingsmomentet taler likevel ikke direkte for at artikkel 36 krever behandling av personopplysninger.

Det siste vurderingsmomentet stiller et krav til forholdsmessighet. Spørsmålet er om det er forholdsmessig at den rettslige forpliktelsen er klart forutsatt, altså implisitt, og ikke kommet direkte til uttrykk i det rettslige grunnlaget.

Som oppgaven behandlet under punkt 4.3, innebærer vurderingsmomentet at det skal foretas en konkret vurdering av hvor klar den rettslige forpliktelsen fremstår for de som rammes av den, både den registrerte og behandlingsansvarlig. Videre hvorvidt det er forhold i dette typetilfellet, ved de registrerte eller ved de behandlingsansvarlige, som taler mot at det aksepteres et lavere hjemmelskrav.

Det overordnede målet med artikkel 36 er ifølge overskriften å gi «[t]ilgang til kontoer i en kredittinstitusjon». Målsetningen er også en sentral funksjon i PSD2. Dersom fullmakttjenestene ikke får full tilgang til kontotilbyders betalingskontoer, på lik linje med kundene selv, vil det sette kraftige kjepper i hjulene for funksjonene som fullmakttjenestene er ment å fylle. Overføring av personopplysninger vil innebære en viktig del av tilgangen til betalingskontoer. At en sentral funksjon i direktivet vil bli styrket, taler for at man tillater et lempeligere hjemmelskrav.

Virkningen for den registrerte ved at man tillater et lavere hjemmelskrav, er at den registrerte får oppfylt forutsetningen for at den tok kontakt med fullmakttjenesten i utgangspunktet. Den registrerte har allerede samtykket til behandling eller inngått kontrakt hvor behandling er nødvendig, med både fullmakttjenesten og kontotilbyder hver for seg. Målet med å benytte seg av fullmakttjenesten er å forenkle kontakten med en eller flere kontotilbydere. At personopplysninger overføres mellom kontotilbyder og fullmakttjeneste er derfor ikke bare forutberegnelig for den registrerte, men også forventet. For den behandlingsansvarlige vil det innebære en forenkling dersom overføringen av personopplysninger til fullmakttjenestene kan skje på bakgrunn av en rettslig forpliktelse. I dette tilfellet vil kontotilbyder slippe å oppfylle et annet behandlingsgrunnlag, f.eks. det å innhente et nytt samtykke fra den registrerte. Altså taler dette for at kravet om overføring av personopplysninger er forutberegnelig for både den registrerte og for behandlingsansvarlig.

I fortalen punkt 89 er det presisert at «[n]år personopplysninger behandles i henhold til dette direktiv», så skal personvernprinsippene fastlagt i DPD følges. Henvisningen til DPD innebære en sikkerhetsgaranti for den registrerte, ved at den registrerte har mulighet til å påberope seg alle rettigheter etter DPD. Som det ble redegjort for i punkt 3, innebærer henvisningen til DPD en henvisning til GDPR.

Av EDPS sin uttalelse[128] fremgår det under EDPS sine anbefalinger at «[d]et bør udtrykkeligt præciseres i det foreslåede direktiv, at der kan finde behandling af personoplysninger sted, i det omfang det er nødvendigt for udførelsen af betalingstjenester.» Utsagnet kan tas til støtte for at rettslig forpliktelse som behandlingsgrunnlag vil være aktuelt og forholdsmessig. Videre at EDPS anbefalte at det ble opprettet en direkte hjemmel for behandling av personopplysninger i direktivet.

Etter en konkret vurdering så taler momentene om virkningen for den registrerte, virkningen for behandlingsansvarlig og EDPS sin anbefaling for at det er forholdsmessig at en rettslig forpliktelse klart forutsettes.

Delkonklusjonen blir dermed at det i artikkel 36 er «klart forutsatt» at det foreligger en rettslig forpliktelse.

Etter en helhetsvurdering er min hovedkonklusjon at det i PSD2 art. 36 foreligger en rettslig forpliktelse, som oppfyller vilkårene for å fungere som behandlingsgrunnlag, for kontotilbyder til å overføre kundens personopplysninger til fullmakttjenestene og/eller andre kontotilbydere. Oppgaven bemerker at det hefter en viss usikkerhet ved konklusjonen i mangel på rettslig avklaring av spørsmålet.

[128] Sammendrag fra EDPS, side 2

6 Konklusjon

Masteroppgaven har undersøkt hvorvidt samtykke[129] og/eller rettslig forpliktelse[130] kan anvendes som behandlingsgrunnlag for at kontotilbyder skal kunne overføre kundens personopplysninger til fullmakttjenesten. Måten oppgaven har vurdert problemstillingen på er ved å presentere behandlingsgrunnlagene, deretter undersøke hvordan behandlingsgrunnlagene er forstått og hvilken funksjon de fyller i PSD2

For det første har oppgaven funnet at samtykke kan tjene som behandlingsgrunnlag for overføringen av personopplysninger mellom kontotilbyder og fullmakttjeneste. Videre har oppgaven undersøkt om «uttrykkelig» samtykke i PSD2 skal forståes som en henvisning til GDPR art. 9, om behandling av særlige kategorier av personopplysninger. Oppgaven har funnet at dette ikke er tilfellet. Bruken av «uttrykkelig» samtykke i PSD2, skal derimot forståes som en kontraktforutsetning. Altså at formålene med behandling av personvern skal «uttrykkelig» reguleres av kontrakten, og at kunden «uttrykkelig» skal akseptere vilkårene i kontrakten, for at lovlig behandling kan foretas. Deretter har oppgaven kommet frem til at det ikke eksisterer et krav om dobbelt samtykke i PSD2. Med andre ord at kontotilbyder ikke er forpliktet til å innhente eget samtykke fra kontoinnehaver for å overføre kundens personopplysninger til fullmakttjenesten. Overføringen kan dermed bero på andre behandlingsgrunnlag enn samtykke.

For det andre har oppgaven undersøkt om det forekommer en rettslig forpliktelse til å overføre kundens personopplysninger mellom kontotilbyder og fullmakttjeneste. Oppgaven har funnet at en slik forpliktelse er «klart forutsatt» i PSD2 art. 36. Videre at det foreligger en begrenset rettslig forpliktelse til å overføre personopplysninger mellom kontotilbyder og fullmakttjenesten i forbindelse med autorisering av betalingstransaksjoner, i medhold av PSD2 art. 66(4) bokstav b.

Jeg finner grunn til å bemerke at flere av løsningene som fremgår av oppgaven enda er usikre. Direktivet og forordningen er fremdeles nye tilskudd til EU-retten, og av denne grunn vil flere avklaringer ventes i fremtiden. Denne oppgaven er neppe siste ord som blir sagt om forholdet mellom PSD2 og GDPR.

[129] GDPR art. 6(1) a
[130] GDPR art. 6(1) c

Angående norsk implementering av PSD2, ønsker oppgaven å poengtere at PSD2 art. 36 ikke er inkorporert ved forskrift om betalingstjenester av 2019. Dette innebærer at hjemmelen for tilgang til betalingskontoer, og artikkelen som klart forutsetter overføring av personopplysninger, ikke er inntatt i forskriften. Artikkelen er likevel inkorporert ved betalingssystemloven av 1999 § 6-1, som trådte i kraft 1. april 2019.

Oppgaven anbefaler at det i norsk rett, for det første, tas høyde for at fullmakttjenesters tilgang til betalingskontoer, vil innebære behandling av personopplysninger. For det andre, dersom det er ønskelig fra lovgivers side at overføringen av personopplysninger mellom kontotilbyder og fullmakttjeneste skal bygge på behandlingsgrunnlaget rettslig forpliktelse, anbefaler oppgaven at dette eksplisitt kommer til uttrykk i en egen bestemmelse. En slik løsning vil bidra til å redusere den tvilen som nå hersker rundt overføringstilfellet under PSD2.

6.1 Virkningen av funnene for næringslivet

Oppgaven har kommet frem til at både samtykke og rettslig forpliktelse er aktuelle behandlingsgrunnlag for overføring av personopplysninger mellom kontotilbyder og fullmakttjeneste.

Funnet får virkning for næringslivet ved at kontotilbydere dermed har et valg angående hvilket behandlingsgrunnlag de velger å overføre personopplysninger på bakgrunn av.

Overføringen kan bero på samtykke som behandlingsgrunnlag. Fordelen med denne løsningen er for det første at det er mindre risiko tilknyttet dette behandlingsgrunnlaget sammenlignet med rettslig forpliktelse. Altså at når samtykke er gitt av den registrerte og vilkårene for et gyldig samtykke er oppfylt, vil behandlingsansvarlig lovlig kunne overføre personopplysningene. Videre er behandlingsgrunnlaget fleksibelt, ved at behandlingsansvarlig kan tilpasse samtykkeforespørselen etter behov. For nye kunder kan samtykke til overføring av personopplysninger inntas i samtykkeforespørselen for initial behandling, forutsatt at det skilles ut som et eget punkt i forespørselen jf. vilkårene om at samtykke må være «spesifikt» og «utvetydig». Ulempen er derimot at vilkårene for at det skal foreligge et gyldig samtykke er strenge. Videre kan et samtykke etter omstendighetene være komplisert å innhente, både fordi man må lage digitale løsninger for innhenting av samtykke og fordi man må få den registrerte til faktisk å avgi samtykke. I overføringstilfellet foreligger det enda en utfordring,

siden det er stor sannsynlighet for at det allerede foreligger behandlingsgrunnlag for initial behandling. Dermed blir det snakk om å innhente et nytt samtykke for overføringstilfellet. Med andre ord at behandlingsansvarlig må innhente nytt samtykke fra alle foreliggende kunder. Løsningen er derfor kostnads- og arbeidskrevende. I tillegg må behandlingsansvarlig ta høyde for at et samtykke til enhver tid kan tilbakekalles.

Alternativet er at behandlingen beror på rettslig forpliktelse som behandlingsgrunnlag. Fordelen er her at behandlingsansvarlig ikke behøver å skape nye digitale løsninger eller oppsøke de registrerte for å innhente samtykke. Behandlingsansvarlig trenger kun å henvise til den rettslige forpliktelsen, foreta en vurdering av omfanget av forpliktelsen og angi hvilken behandling den anser som nødvendig for å oppfylle forpliktelsen. Slik sett er behandlingsgrunnlaget hverken kostnads- eller arbeidskrevende. Ulempen er derimot at den rettslige forpliktelsen ikke er endelig avklart. Det vil derfor være en grad av usikkerhet knyttet til den subjektive lovtolkningen hos den behandlingsansvarlige. Dette kan by på utfordringer ved en senere anledning dersom det kommer en avklaring som underkjenner at art. 36 gir uttrykk for en rettslig forpliktelse til å behandle personopplysninger. I et slikt tilfelle vil den foregående behandlingen gjort på bakgrunn av behandlingsgrunnlaget være ulovlig, og personopplysningene som er behandlet må følgelig slettes. En annen ulempe med behandlingsgrunnlaget er at det kun omfatter behandlingsaktiviteter som er helt nødvendige for å oppfylle den rettslige forpliktelsen. Eventuell viderebehandling for andre formål må derfor bero på et annet behandlingsgrunnlag.

Litteraturliste

Norske lover, forskrifter og forarbeider

Lov 25. juni 1999 om finansavtaler og finansoppdrag (finansavtaleloven)

Lov 17. desember 1999 nr. 95 om betalingssystemer m.v (betalingssystemloven)

Lov 10. mars 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven)

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Forskrift 18. februar 2019 om betalingstjenester (forskrift om betalingstjenester)

Ot.prp.nr. 92 (1998-1999) om lov om behandling av personopplysninger (personopplysningsloven)

EU forordninger og direktiver

Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet - DPD)

Europaparlaments- og rådsdirektiv 2007/64/EF av 13. november 2007 om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF samt oppheving av direktiv 97/5/EF (betalingstjenestedirektivet)

Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og verdipapirforetak og om endring av forordning (EU) nr. 648/2012

Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF (Payment Services Directive 2 – PSD2)

Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike

opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning – GDPR)

Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation

Uttalelser fra EU-institusjoner

Article 29 Working Party, *Guidelines on consent under regulation 2016/679*, i kraft fra 28. november 2017, sist endret 10. april 2018.

Den Europæiske Tilsynsførende for Databeskyttelse, *Resumé af udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om et forslag til Europa-Parlamentets og Rådets direktiv om betalingstjenester i det indre marked og om ændring af direktiv 2002/65/EF, 2006/48/EF og 2009/110/EF og om ophævelse af direktiv 2007/64/EF og til Europa-Parlamentets og Rådets forordning om interbankgebyrer for kortbaserede betalingstransaktioner* (2013), https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_ex_sum_da.pdf (lest 09.12.2019).

European Banking Authority, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (2018).

European Data Protection Board, *Letter regarding the PSD2 Directive* (2018), https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en (lest 09.12.2019).

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transaction* (2013), https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf (lest 09.12.2019).

Litteratur

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018 edition, Publications Office of the European Union 2018.

Føllesdal, Andreas, Morten Ruud og Geir Ulfstein, *Menneskerettighetene og Norge: Rettsutvikling, rettsliggjøring og demokrati*, Universitetsforlaget 2017.

Schartum, Dag Wiese og Lee A. Bygrave, *Personvern i informasjonssamfunnet: En innføring i vern av personopplysninger*, 3. utg., Fagbokforlaget 2016.

Arner, Douglas W., Janos Barberis og Ross P. Buckley, "The evolution of FinTech: A new post-crisis paradigm" Georgetown Journal of International Law (2016) 1271.

Christoffer Hernæs, "Open banking: An introduction", 7. august 2019, https://hernaes.com/2019/08/07/the-definitive-guide-to-open-banking/ (lest 09.12.2019).

European Commission, "Payment Services Directive: frequently asked questions", 12. januar 2018, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793 (lest 09.12.2019).

Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/ (lest 09.12.2019).

Lovdata.no, norsk oversettelse av Payment Services Directive 2, https://lovdata.no/pro/static/NLX3/32015l2366.pdf (lest 09.12.2019)

Niels Vandezande, "Reconsiling consent in PSD2 and GDPR", 22. mars 2019, https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr (lest 09.12.2019).

Scott McInnes og Lupe Sampedo, "EU: The interplay of PSD2 and GDPR – Some select issues", 1. februar 2019, https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf (lest 09.12.2019).