# Samspillet mellom PSD2 og GDPR

*Hvorvidt det foreligger et behandlingsgrunnlag etter GDPR for betalingstjenesters behandling av silent party data*

Kandidatnummer: 87

Antall ord: 14429


JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

10.12.2020

# 1 Innholdsfortegnelse

# 1 Innledning

## 1.1 Problemstillingen og dens aktualitet

Utviklingen av finansteknologi (FinTech), og herunder betalingstjenester, har utfordret den tradisjonelle bankbransjen. Fra 2008 og frem til i dag har det skjedd betydelige endringer, og i dag kan andre aktører tilby finansielle tjenester som tidligere bare bankene kunne tilby. Eksempler på betalingstjenester som allerede er i bruk, er den norske betalingstjenesten Vipps, amerikanske PayPal og afrikanske M-pesa.[1] I tillegg har også Apple utviklet sin egen betalingstjeneste, Apple Pay, og Facebook har allerede lansert vennebetaling gjennom Messenger i enkelte land.[2]

Den raske teknologiske utviklingen førte til at første betalingstjenestedirektivet[3] fra 2009 ble utdatert. Behovet for å fylle hullene som var oppstått i regelverket og sikre juridisk klarhet var bakgrunnen for det reviderte betalingstjenestedirektivet (PSD2) [4] som trådte i kraft januar 2018.[5] PSD2 regulerer alle betalingstjenester innenfor EU, med formål om å legge til rette for innovasjon og for å sikre et høyt forbrukervernnivå. [6] Direktivet innførte noen store endringer. For det første, grunnprinsippet om at det er kunden som eier sine kontoopplysninger. Dette er en stor endring i finansbransjen ettersom det tradisjonelt har vært banken som eier kundenes kontoinformasjon. I tillegg ble nye betalingstjenesteytere underlagt regulering, såkalte tredjepartsaktører, og bankene ble pålagt å gi slike tredjepartsaktører tilgang til kundenes kontoopplysninger.

Den raske teknologiske utviklingen og det økte omfanget av deling av personopplysninger var også bakgrunnen for utarbeidelsen av personvernforordningen (GDPR) som trådte i kraft i

[1] Hernæs, "The Definitive Guide to Open Banking", (07.08.19)

[2] Datatilsynet, *Rapport om personlige finanser – hvordan utviklingstrekk i finanssektoren påvirker personvernet*, 2018, s. 7.

[3] Europaparlaments- og rådsdirektiv (EU) 2007/64/EF om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om opphevelse av direktiv 97/5/EF.

[4] Europaparlamentets- 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.

[5] PSD2 fortalepunkt 3 og 6

[6] PSD2 fortalepunkt 5

mai 2018. [7] Formålet med personvernforordningen er å tilrettelegge for en utvikling av den digitale økonomien, bidra til fri flyt av personopplysninger og samtidig gi forbrukerne mer kontroll over sine personopplysninger.[8] GDPR er utformet som et teknologinøytralt rammeverk slik at rettsakten kan anvendes på et bredt spekter av teknologier hvor personopplysninger blir behandlet.

Tredjepartsaktører må behandle personopplysninger for å yte sine tjenester overfor betalingstjenestebrukeren. Dette reiser spørsmål om hvor godt PSD2 og GDPR er harmonisert. Det følger av PSD2 artikkel 94 (2) at «behandling av personopplysninger i henhold til dette direktiv utføres i samsvar med [GDPR]».[9] Dette betyr at betalingstjenesteytere som opererer innenfor PSD2s anvendelsesområde, må sørge for at all behandling av personopplysninger er i samsvar med de krav til et rettslig grunnlag (behandlingsgrunnlag) som oppstilles av GDPR artikkel 6. 9 og 10, samt de alminnelige prinsippene nedfelt i artikkel 5. Uten et behandlingsgrunnlag etter GDPR vil betalingstjenestens behandling av personopplysninger være ulovlig.

Selv om utgangspunktet er at de to rettsaktene skal samsvare, har kravet til samspill i praksis ført til mye usikkerhet angående tolkningen av artikler under PSD2 og hvordan GDPRs bestemmelser skal anvendes på betalingstjenester. Et av spørsmålene som har oppstått i denne forbindelse, er behandling av såkalt silent party data.

Silent party data er personopplysninger som tilhører en person som ikke selv er bruker av betalingstjenesten. Begrepet «silent party data» er ikke et juridisk begrep, og det finnes ingen offisiell norsk oversettelse.[10] Oppgaven vil derfor bruke det engelske begrepet. Av hensyn til flyt og leservennlighet vil oppgaven oversette begrepet «The Silent Party» til «den utenforstående tredjepart» og bruke denne oversettelsen når det refereres til «The Silent Party».

[7] Europaparlamentets- 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]

[8] GDPR Fortalepunkt 7

[9] Ordlyden av bestemmelsen er «direktiv 95/46». Etter GDPR art. 94 skal alle referanser til 95/64 forstås som en referanse til GDPR. (Guideline 06/2020).

[10] Hverken Datatilsynet eller Språkrådet har kunnet gi noen veiledning rundt dette.

En utenforstående tredjepart kan være både en betaler og en betalingsmottaker. Dette kan illustreres med at Hilde overfører penger til Lars gjennom den fiktive betalingstjenesten Fun2Pay. For å kunne gjennomføre betalingen er det nødvendig for Fun2Pay å behandle Lars sine personopplysninger som kontonummer, adresse, fullt navn og betalingssummen som Hilde har overført.[11] Det foreligger ingen kontrakt mellom Lars og Fun2Pay, og hans personopplysninger er derfor silent party data. Ettersom Hilde er bruker av Fun2Pay, har tjenesten tilgang til hennes betalingshistorikk. På den måten vil Fun2Pay også kunne få tilgang til Lars sine personopplysninger dersom han utfører en betaling til Hilde.

Med de betalingstjenestene som foreligger i dag, for eksempel Vipps, er det ikke mulig å betale til en utenforstående tredjepart. Etterhvert som teknologien utvikles og flere aktører kommer på markedet, kan det tenkes at flere betalingstjenesteytere vil ønske å utvide sin funksjonalitet slik at det også er mulig å overføre penger til utenforstående tredjeparter. Oppgavens problemstilling er hvorvidt det foreligger et behandlingsgrunnlag etter GDPR som tredjepartsaktører kan bruke for å behandle silent party data, og eventuelt hvilket grunnlag dette er.

## 1.2 Rettskilder og metodiske utfordringer

Retten til personvern er nedfelt i EUs primærrett, nærmere bestemt i Den europeiske unions pakt om grunnleggende rettigheter [12] artikkel 8 nr. 1 og artikkel 16 nr. 1 i traktaten om Den europeiske unions virkeområde (TEUV).[13] Disse bestemmelsene utgjør hjemmelsgrunnlaget for GDPR.[14]

Oppgaven tar utgangspunkt i rettsaktene GDPR og PSD2. Dette er relativt nye rettsakter som trådte i kraft i 2018. Derfor er rettskildebildet tynt og bærer preg av manglende autoritative kilder. Rettsaktene er sekundærlovgivning, som betyr at de er en konkretisering av de

[11] Peeters, «Data Protection in Mobile Wallets», *European Data Protection Law Review*, nr. 1, 2020, s.64

[12] Charter of Fundamental Rights of the European Union 2000/C 364/01.

[13] The Treaty on the Function of the European Union (TFEU) 2012/C 326/01

[14] GDPR fortalepunkt 1

politiske mål som er nedfelt i EUs traktater, primærretten.[15]

GDPR ble vedtatt 27. april 2016 og erstatter det tidligere Personvernsdirektivet 95/46/EG.[16] For EUs medlemsstater trådte den nye forordningen i kraft 25. Mai 2018. GDPR er en forordning, hvilket betyr at den gjelder direkte i alle EU-medlemsland og er bindende i sin helhet, ord for ord, jfr. TEUV art. 288 (2). Forordninger er effektive rettsakter for rettsområder hvor det er viktig med en ensartet tolkning og praktisering av rettsakten i alle land.[17]

Etter GDPR art. 2 nr. 1 får forordningen anvendelse på «helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register». Ordlyden er generelt utformet og tilsier at anvendelsesområdet for forordningen favner vidt. Foruten unntakene som følger av art. 2 nr. 2, 3 og 4, får forordningen i praksis anvendelse på enhver informasjonsmengde som er systematisert på en måte som gjør det mulig å identifisere den registrerte.[18] I fortalepunkt 15 fremheves det at forordningen er utformet som et teknologinøytralt regelverk slik at anvendelsesområdet ikke er avhengig av hvilken teknikk som brukes. Konsekvensene av dette er at forordningen er vanskelig å omgå, i tillegg til at den gir fleksibilitet for rettsanvenderen. På den måten kan forordningens formål om å utvikle den digitale økonomien og bidra til fri flyt av personopplysninger realiseres. [19]

PSD2, Payment Service Directive 2, ble vedtatt 25. november 2015 og erstatter det første betalingstjenestedirektivet, PSD. For EU-medlemsstater trådte direktivet i kraft 13. januar 2018. Et direktiv får ikke umiddelbar virkning etter vedtakelse, men må inkorporeres i medlemsstatenes nasjonale rettssystem, jfr. TEUV art. 288 (3). PSD2 er et fullharmoniseringsdirektiv. Dette betyr at medlemsstatene har begrenset handlingsrom til å

[15] Odd Stemsrud, «*EØS-rett i et nøtteskall*», 1. utgave, Gyldendal, 2016, s. 69.

[16] 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 (EFT L 281 av 23.11.1995, s.31)

[17] Sejersted, Arnesen, Rognstad, Foyn, Kolstad, «*EØS-rett*», 3. utgave, Universitetsforlaget, 2014 s. 53

[18] Bergseng Skullerud, Rønnevik, Skorstad, Pellerud, «*Personopplysningsloven og Personvernforordningen (GDPR), kommentarutgave*», 1. utgave, Universitetsforlaget, 2019 s.138

[19] Ibid

endre eller gjøre tilføyelser ved inkorporering i nasjonal rett. Den nasjonale lovgivningen kan ikke fravike direktivets bestemmelser uten at direktivet selv åpner for det.

PSD2 får anvendelse på «betalingstjenester som ytes i Union», jfr. artikkel 2 nr. 1. Formålet med direktivet er å legge til rette for sikker elektronisk betaling gjennom å stille krav til effektivitet, gjennomsiktighet og et høyt forbrukervernnivå.[20] Elektroniske betalingstjenester er ifølge EU avgjørende for et velfungerende indre marked. I den forbindelse har EU ansett det som viktig å sørge for at brukerne av slike tjenester er godt beskyttet. Ved å tilrettelegge for økt konkurranse vil kostnadene for betalingstjenestene reduseres og gi forbrukerne bedre valgmuligheter.[21]

For at EU-lovgivning skal få virkning for EØS-land, må rettsaktene først innlemmes i EØS-avtalen. Etter EØS-avtalen art. 7 skal forordninger gjennomføres «som sådan» og direktiver gjennomføres i nasjonal rett på den måten nasjonale myndigheter bestemmer. I norsk rett er GDPR inkorporert gjennom personopplysningsloven som trådte i kraft 20. Juli 2018.[22] De offentligrettslige delene av PSD2 er foreløpig gjennomført i norsk rett ved endringer i finansforetaksloven og betalingssystemloven med tilhørende forskrifter.[23] I april 2020 la justis-og beredskapsdepartementet frem et forslag om ny finansavtalelov for å gjennomføre blant annet de privatrettslige delene av PSD2.[24]

Hverken norske eller svenske forarbeider er en formell rettskilde innenfor EU-retten. Likevel er forarbeidene en analyse av rettsområdet og gir uttrykk for hva en ekspertgruppe anser som gode tolkninger av rettsaktene og gode løsninger på rettslige problemer. Forarbeidene er derfor relevante for oppgaven som tolkningsbidrag og må anses for å ha rettskildemessige vekt på lik linje med juridisk litteratur.

[20] PSD2 fortalepunkt 5

[21] PSD2 fortalepunkt 7

[22] Lov av 15. Juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

[23] Jfr. Endringslov 23. November 2018 nr. 87. Lov om endringer i Finansforetaksloven mv. (andre betalingstjenestedirektiv)

[24] Prop. 92 LS (2019 - 2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. Mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014.

EU-retten er en autonom rettsorden som skal tolkes selvstendig og ensartet.[25] Gjennom rettspraksis har EU-domstolen utviklet tolkningsprinsipper for EU-retten. Det må først og fremst tas utgangspunkt i rettsaktens ordlyd. Ved uklarhet kan flere av de 24 offisielle språkversjonene sammenlignes. Videre kan det sees hen til EU-rettens autonome begreper, som brukes for å bidra til lik anvendelse og tolkning av EU-retten.[26]

Til slutt kan det legges en formålsrettet tolkning til grunn. Rettsaktens fortale er sentral for å klarlegge rettsakens overordnede formål eller formålet bak en konkret bestemmelse. Fortalen er ikke rettslig bindende, men presiserer rettsaktens innhold og er et utslag av begrunnelseskravet, jfr. TEUF art. 296. For tolkning av PSD2 og GDPR vil rettsaktenes fortale være sentral ettersom det foreligger få andre tungtveiende rettskilder.

Videre er rettspraksis fra EU-domstolen en sentral rettskilde innenfor EU-retten. Praksis fra EU-domstolen har ikke formell prejudikatsvirkning, men har blitt akseptert og fulgt av nasjonale domstoler og myndigheter som en autoritativ kilde.[27] EU-rettens dynamiske karakter og formålet om lik utøvelse av EU-retten tilsier at domstolens praksis har stor rettskildemessig vekt. Det foreligger imidlertid få rettsavgjørelser angående tolkningen av de ulike bestemmelsene i GDPR og PSD2. Ettersom GDPR i stor grad er en videreføring av det første personverndirektivet, vil flere avgjørelser fra før 2018 ha overføringsverdi.

Flere tidsskrifter og artikler omhandler problemstillinger i relasjon til GDPR og PSD2. Juridisk litteratur har begrenset rettskildemessig vekt, men i lys av det tynne rettskildebildet vil oppgaven i stor grad bruke litteratur for å belyse problemstillinger og gi tolkningsbidrag.

Uttalelser og retningslinjer fra Personvernrådet (European Data Protection Board) er viktige rettskilder. EDPB er opprettet i medhold av GDPR art. 68 og skal etter art. 70 være et uavhengig organ som skal sørge for lik anvendelse og tolkning av personvernforordningen innenfor EU. Organet består av representanter fra nasjonale datatilsyn og representanter fra European Data Protection Supervision (EDPS), EUs datatilsyn. Før ikrafttredelsen av GDPR het EDPB, Artikkel 29-gruppen. Ettersom GDPR viderefører flere av det tidligere

[25] C-135/15 *Nikiforidis v Greece*

[26] C-283/81, CILFIT *v Ministero della Sanita*, avsnitt 18, 19 og 20

[27] Sejersted m.fl. 2014 s.55.

personverndirektivets bestemmelser, er uttalelser fra Artikkel-29-gruppen fortsatt relevante rettskilder.

Retningslinjer og uttalelser fra EDPB er ikke rettslig bindende. Den faktiske rettskildemessige vekten er imidlertid stor, ettersom rådets kompetanse er direkte hjemlet i GDPR. Dessuten gir rådets retningslinjer og uttalelser uttrykk for en felles tolkning og anvendelse av reglene på tvers av landegrensene.[28] Mangelen på andre og mer tungtveiende kilder gjør at retningslinjene fra EDPB i praksis utgjør sentralt tolkningselement ved fastleggelsen av de nærmere reglene i GDPR og PSD2.

Problemstillinger rundt samspillet mellom PSD2 og GDPR ble først omtalt av EDPB i et brev fra 5. Juli 2018[29] i forbindelse med at et EU-parlamentsmedlem ønsket veiledning. I retningslinjene 06/2020[30] ble det gitt ytterligere veiledning rundt disse problemstillingene. Retningslinjene var ute på høring frem til 16. september.

Høringssvarene har liten rettskildemessig vekt. Likevel er det interessant å se hen til flere av høringssvarene som er skrevet av profesjonelle aktører og akademiske forskergrupper. Disse aktørene har verdifull innsikt i teknologien rundt en betalingstjeneste og faglig tyngde. Deres høringssvar kan dermed gi gode innspill og forslag til løsninger på problemstillinger som omtales i retningslinje 06/2020.

## 1.3 Avgrensning og fremstillingen videre

### 1.3.1 Avgrensninger

Oppgavens problemstilling er, som nevnt, hvorvidt det foreligger et behandlingsgrunnlag etter GDPR som tredjepartsaktører kan bruke for å behandle silent party data.

Problemstillingen er begrenset til å gjelde behandling av silent party data hvor betalingstjenesteyteren er en tredjepartsaktør. I retningslinje 06/2020 har EDPB avgrenset

[28] Datatilsynet, *Regelverk og verktøy, «Det europeiske personvernrådet»,* sist endret 19. 07. 2020 (lest 2. des. 20)

[29] EDPB, «*Letter regarding the PSD2 Directive»,* 5. juli 2018

[30] EDPB, «*Guideline 06/2020 on the interplay of the Second Payment Services Directive and the GDPR version 1.o»,* Adopted on 17. July 2020. Version for public consultation.

problemstilling på samme måte. Det betyr at samme problemstilling hvor andre aktører er betalingstjenesteytere jfr. PSD2 vedlegg 1, faller utenfor oppgavens rammer.

Behandling av personopplysninger krever hjemmel, et behandlingsgrunnlag, i GDPR. Oppgaven vil bare drøfte artikkel 6 og 9 som potensielle behandlingsgrunnlag for silent party data. Det avgrenses dermed mot opplysninger om straffedommer og lovovertredelser som krever behandlingsgrunnlag etter artikkel 10. Når det reises spørsmål om behandlingsgrunnlag etter artikkel 6 bokstav f, vil oppgaven avgrense mot tilfeller der den utenforstående tredjepart er et barn. I tillegg avgrenser oppgaven mot spørsmål om viderebehandling av silent party data jfr. art. 6 nr. 4.

For flere av behandlingsgrunnlagene som er opplistet i artikkel 6 og 9, kreves det et supplerende rettsgrunnlag i unionsretten eller medlemsstatens nasjonale rett. Ettersom oppgaven skrives fra et EU-rettslig ståsted, avgrenses det mot å drøfte hvorvidt det kan foreligge en rettslig forpliktelse i medlemsstaters nasjonale rett.

### 1.3.2 Fremstillingen videre

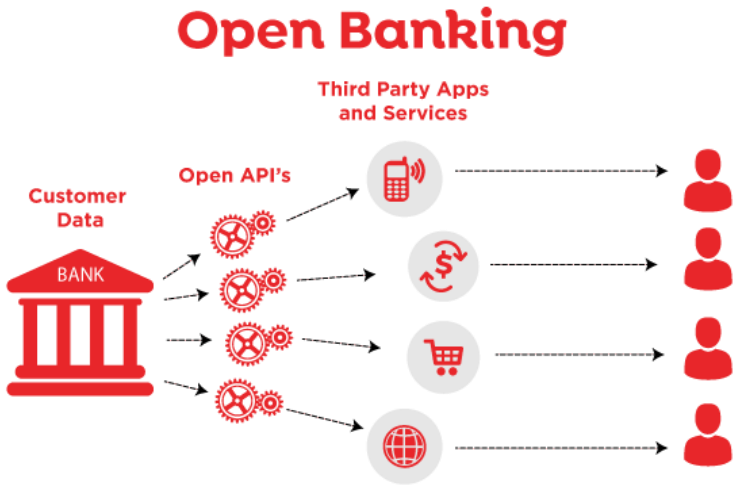
I det videre vil oppgaven først presentere PSD2 og GDPR. I del 2 vil oppgaven redegjøre for hvilke aktører som er regulert av PSD2 og deres funksjoner, samt regler for behandling av personopplysninger under PSD2. I del 3 vil oppgaven redegjøre for GDPR, herunder de alminnelige prinsippene for behandling av personopplysninger som følger av artikkel 5, en presentasjon av aktørene under GDPR og kravet til behandlingsgrunnlag etter artikkel 6 og 9.

Etter dette vil aktuelle behandlingsgrunnlag etter artikkel 6 og 9 drøftes. I del 4 vil oppgaven drøfte hvorvidt noen av behandlingsgrunnlagene etter artikkel 6 som kan anvendes for behandling silent party data. I del 5 vil oppgaven drøfte hvorvidt noen av behandlingsgrunnlagene etter artikkel 9 som kan være passende for silent party data som er sensitive opplysninger.

# 2 PSD2 – innovasjon og forbrukervern

Som nevnt i punkt 1.3, får PSD2 anvendelse på «betalingstjenester som ytes i Unionen», jfr. direktivets artikkel 2 nr. 1. For den videre fremstillingen er det hensiktsmessig med en redegjørelse av hvordan en betalingstjeneste fungerer, hvilke aktører som inngår i en betalingstjeneste og aktørenes ansvarsområder. Dette vil gjøres i punkt 2.1. I punkt. 2.2 vil oppgaven redegjøre for reguleringen av behandling av personopplysninger etter PSD2.

## 2.1 Aktørene i en betalingstjeneste og deres ansvarsområder




*Figur 1: Illustrasjon av «open banking»*[31]

PSD2 pålegger bankene å gi tredjepartsaktører tilgang til sine betalingssystemer, jfr. PSD2 artikkel 66 og 67.[32] Dette krever at bankene har et sett med åpne grensesnitt, API (Application Programming Interface), som gjør det mulig for betalingstjenestene å benytte bankens infrastruktur for å initiere betalinger og hente ut betalingstjenestebrukernes kontoinformasjon.[33] Dette omtales som Open Banking. Betalingstjenester som leveres av tredjepartsaktører, bygger sine tjenester på data og opplysninger som de får fra de tradisjonelle bankene.

[31] Ashirwada Dayarathne, *«WSO2 Open Banking to Cater Open Banking and PSD2 requirements»,* (22.10.19)

[32] Retningslinje 06/2020 a. 7 avsnitt 26.

[33] Øsebak, Horntvedt, «*Endrer risikobildet seg som følge av nye betalingsløsninger?*», (03.06.2019), Praktisk Økonomi og Finans 2019/2, Årgang 35 s. 122-131.

**Silent party data** er som tidligere nevnt, opplysninger som tilhører en person som ikke selv er bruker av den bestemte betalingstjenesten.[34] Oppgaven vil bruke «utenforstående tredjepart» når det refereres til «the silent party».

**Tredjepartsaktører** (Third Party Provider) ble introdusert som nye betalingstjenester under PSD2.[35] Dette er nærmere bestemt betalingsinitieringstjenester, jfr. vedlegg nr. 1 nr. 7 og kontoopplysningstjenester, jfr. vedlegg nr. 1 nr. 8. Tredjepartsaktørene har ikke direkte tilgang til betalingstjenestebrukerens kontoopplysningstjenester og er avhengig av å få tilgang til brukerens betalingskonto fra banken og bankens betalingssystem for å bygge sine tjenester. For å yte og gjennomføre betalingstjenester må tredjepartsaktørene ha tillatelse fra nasjonale myndigheter, jfr. art. 4 nr. 4 jfr. art. 11.

Den første tjenestetypen er **betalingsinitieringstjenester** (Payment Initiation Service Provider). Etter artikkel 4 nr. 15 er dette definert som «en tjeneste for å initiere en betalingsordre på anmodning fra betalingstjenestebrukeren med hensyn til en betalingskonto hos en annen betalingstjenesteyter.» Tjenesten fungerer ved at betalingstjenesten forespør banken om å initiere en betaling på vegne av betalingstjenestebrukeren.[36] Eksempler på betalingsinitieringstjenester er Vipps og PayPal.

Den andre tjenestetypen er **kontoopplysningstjenester** (Account Information Service Provider). Etter artikkel 4 nr. 16 er dette «en onlinetjeneste som skal gi samlede opplysninger om en eller flere betalingskontoer som betalingstjenestebrukeren har hos enten en annen betalingstjenesteyter eller hos mer enn én betalingstjenesteyter.» Gjennom bankens åpne grensesnitt kan kontoopplysningstjenesten gi en samlet oversikt over betalingstjenestebrukerens finansielle stilling.[37] Dersom betalingstjenestebrukeren har lån eller konto i flere banker, kan vedkommende få en samlet oversikt over disse i kontoopplysningstjenesten. Slike tjenester kan også for eksempel hjelpe forbrukeren med å sette opp budsjett og rådføring om hvordan han eller hun på best mulig måte kan investere sine midler for å oppnå et sparemål.

[34] Retningslinje 06/2020 s. 15 avsnitt 44.

[35] Oversettelse av Third Party Provider. Hentet fra Prop. 110 L (2017-2018) Endringer i finansforetaksloven mv. (andre betalingstjenestedirektiv) s. 11

[36] Retningslinje 06/2020 s. 6 avsn. 6

[37] PSD2 fortalepunkt 28

Brukeren av betalingstjenesten betegnes som **betalingstjenestebruker** (Payment Service User). Dette er definert som en «fysisk eller juridisk person som gjør bruk av en betalingstjeneste i egenskap av betaler, betalingsmottaker eller begge deler», jfr. art. 4 nr. 2.

## 2.2 Behandling av personopplysninger under PSD2

Kapittel 4 av PSD2 omhandler vern av personopplysninger og består av bare én bestemmelse – artikkel 94. Av artikkelens første ledd følger det at:

> *«formidling av opplysninger til fysiske personer om behandling av personopplysninger samt behandling av slike personopplysninger og enhver annen behandling av personopplysninger i henhold til dette direktiv skal utføres i samsvar med direktiv 95/46/EF, de nasjonale reglene som innarbeider direktiv 95/46/EF, og forordning (EF) nr. 45/2001.»* [38]

EUs intensjon om at PSD2 og GDPR skal harmonisere med hverandre er også presisert i PSD2s fortalepunkt 89:

> *«når personopplysninger behandles i henhold til dette direktiv, bør særlig det nøyaktige formål angis, relevant rettslig grunnlag, relevante sikkerhetskrav fastsatt i [GDPR] overholdes og prinsippene om nødvendighet, forholdsmessighet, formålsbegrensning, og forholdsmessig oppbevaringstid for opplysningene følges. Dessuten bør innebygd personvern og personvern som standardinnstilling inngå i alle databehandlingssystemer som utvikles og brukes innenfor rammen av dette direktiv.»*

Av artikkel 94 andre ledd følger det at «betalingstjenesteyteren skal bare hente, behandle og lagre personopplysninger som er nødvendige for å yte betalingstjenestene, med uttrykkelig samtykke fra betalingstjenestebrukeren».

EDPB har klargjort at et uttrykkelig samtykke etter PSD2 art. 94 (2) er et avtalerettslig samtykke, og dermed ikke det samme som et samtykke etter GDPR. Samtykke jfr. PSD2 art.

[38] Etter GDPR art. 94 skal alle referanser til 95/64 forstås som en referanse til GDPR.

94 (2) kan dermed ikke utgjøre et behandlingsgrunnlag for behandling av personopplysninger. Dette betyr at behandling av personopplysninger under PSD2 må ha et behandlingsgrunnlag som nedfelt i GDPR art. 6 og 9. [39]

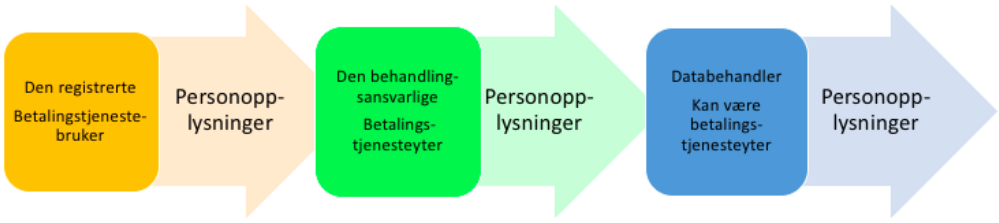
# 3 GDPR – den nye standarden for personvern

Som nevnt i punkt 1.2, er formålet med GDPR å verne fysiske personer i forbindelse med behandling av deres personopplysninger og legge til rette for fri utveksling av personopplysninger.[40] Anvendelsesområdet er teknologinøytralt utformet slik at forordningen kan anvendes på et vidt spekter av teknologi hvor behandling av personopplysninger er nødvendig. [41]

I det videre vil oppgaven gjøre rede for hvilke aktører som er involvert i behandlingen av personopplysninger, og hvordan aktørene overføres til betalingstjenester. Deretter vil de alminnelige prinsippene for behandling av personopplysninger i artikkel 5 presenteres i punkt 3.2. Til slutt vil det redegjøres for kravet til behandlingsgrunnlag i punkt 3.3.

## 3.1 Aktører under GDPR

Ved behandling av personopplysninger er det tre involverte aktører: *den registrerte, den behandlingsansvarlige og databehandleren.* Deres funksjoner og ansvarsområder er nærmere definert i GDPR artikkel 4.




*Figur 2: Behandling av personopplysninger.*

**Personopplysninger** er i GDPR artikkel 4 nr. 1 definert som:

[39] Retningslinje 06/2020 s. 14 punkt 3.3.

[40] GDPR art. 1 nr. 1

[41] GDPR fortalepunkt 15

> *«enhver opplysning om en identifisert eller identifiserbar fysisk person («**den registrerte**»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske personers fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet»* (min utheving)

Den registrerte er med andre ord den som personopplysningene omhandler. I en betalingstjeneste vil dette vær betalingstjenestebrukeren. Betalingstjenesteyteren kan behandle betalingstjenestebrukerens betalingskonto, fullt navn og adresse.[42] Dette er opplysninger om en identifisert fysisk person og er derfor personopplysninger etter art. 4 nr. 1.

Silent party data er personopplysninger som omhandler en utenforstående tredjepart. Ved spørsmål om behandling av silent party data vil den utenforstående tredjepart derfor være å regne som den registrerte.

I tillegg til den generelle definisjonen i art. 4 nr. 1 skiller GDPR ut **særlige kategorier av personopplysninger**. Dette er opplysninger som etter GDPR har et særskilt vern fordi behandling av dem kan skape en risiko for den registrertes grunnleggende rettigheter og friheter.[43] Etter artikkel 9 nr. 1 er særlige kategorier av personopplysninger opplysninger om:

> *«rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.»*

Det sentrale begrepet **«behandling av personopplysninger»** er et samlebegrep som omfatter «enhver operasjon eller en rekke operasjoner som gjøres med personopplysninger, enten automatiserte eller ikke», jfr. art. 4 nr. 2. Videre følger det av bestemmelsen at dette omfatter for eksempel lagring, innsamling, registrering eller sletting.

[42] Peeters 2020 s. 64

[43] GDPR fortalepunkt 51

**Den behandlingsansvarlige** er «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes», jfr. artikkel 4 nr. 7. Det er den behandlingsansvarlige som er ansvarlig for at kravene til behandling av personopplysninger følges, jfr. art. 5 nr. 2.

**Databehandleren** er etter art. 4 nr. 8 den som «behandler personopplysninger på vegne av den behandlingsansvarlige». En databehandler har som oppgave å sikre at personopplysningene behandles sikkert og konfidensielt. Databehandleren skal også bidra til at den behandlingsansvarlige oppfyller sine plikter etter GDPR.[44]

Anvendt på en betalingstjeneste vil hvem som er behandlingsansvarlig, og hvem som er databehandler, avhenge av hvordan betalingstjenesten er organisert.[45] Betalingstjenesteyteren vil alltid inneha rollen som behandlingsansvarlig, men kan i noen tilfeller påta seg rollen som databehandler i tillegg. Dersom en betalingstjeneste bruker en ekstern IT-tjeneste for å behandle personopplysninger, vil betalingstjenesteyteren være den behandlingsansvarlige og det innleide IT-selskapet være databehandleren.

## 3.2 Allmenne prinsipper for behandling av personopplysninger – artikkel 5

GDPR artikkel 5 inneholder prinsipper som er styrende for behandling av personopplysninger, og er i stor grad en videreføring av det tidligere personverndirektivets artikkel 6.[46] Prinsippene setter rammer for hvordan de øvrige bestemmelsene skal tolkes og anvendes.

For det første følger det av art. 5 nr. 1 (a) at personopplysninger skal *«behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte»*.

[44] Wessel-Aas, Ødegård, *Personvern – Publisering og behandling av personopplysninger,* 1. utgave, Gyldendal, 2018 s. 189.

[45] Retningslinje 06/2020 s. 7 punkt 12.

[46] Skullerud m.fl. (2019) s. 172.

At behandlingen skal være «lovlig», betyr at behandlingsansvarlig må ha et rettslig grunnlag for behandlingen etter artikkel 6 og eventuelt 9. Kravet til behandlingsgrunnlag i artikkel 6 og 9 vil bli nærmere redegjort for i punkt 3.3.

Kravet til en rettferdig behandling kan med rimelighet tolkes som at behandlingen må skje på en måte som er etisk og rimelig overfor den registrerte. EDPB har gitt en generell uttalelse om at rettferdighetskravet blant annet omfatter:

> *«recognizing the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller».*[47]

I tillegg har EDPB uttalt at behandling av personopplysninger blant annet ikke skal være diskriminerende, den skal være etisk forsvarlig og den behandlingsansvarlige må behandle personopplysningene på en måte som korresponderer med den informasjonen som er gitt til den registrerte.[48]

Kravet til at behandlingen skal skje «på en åpen måte», tilsier at behandlingen skal være transparent og gjennomsiktig. Dette vil oppnås dersom den registrerte får informasjon om behandlingen, jfr. art. 13 og 14, på en forståelig måte, jfr. art. 12.

For det andre skal personopplysninger kun «samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene (...)» jfr. art. 5 nr. 1 (b). Ordlyden tilsier at formålet med behandlingen må være konkret angitt, og at den registrerte må kunne forstå hva personopplysningene skal brukes til, slik at det er mulig å vurdere om behandlingen følger forordningens bestemmelser.

Etter dataminimeringsprinsippet i art. 5 nr. 1 (c) skal den behandlingsansvarlige tilstrebe å samle inn så få personopplysninger som mulig innenfor behandlingsformålet. I henhold til

---

[47] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, adopted October 8th 2019, avsn. 12.*

[48] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* adopted November 13th 2019, avsn. 64.

fortalepunkt 39, burde personopplysninger bare behandles dersom formålet ikke med rimelighet kan oppnås på en annen måte.

Videre følger det av art. 5 nr. 1 (d) at alle opplysninger som behandles skal være «korrekte og om nødvendig oppdaterte». Prinsippet om lagringsprinsippet kommer til uttrykk i art. 5 nr. 1 (e). Det følger av bestemmelsen at personopplysninger ikke skal lagres «i lengre perioder enn det som er nødvendig».

Prinsippet om integritet og konfidensialitet er nedfelt i art. 5 nr. 1 (f) hvor det følger at personopplysningene skal «behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene».

Det følger av art. 5 nr. 2 at «den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes». Dette nærmere konkretisert i art. 24, hvor det følger at «den behandlingsansvarlige gjennom egnede tekniske og organisatoriske tiltak [skal] sikre og påvise at behandlingen utføres i samsvar med denne forordning». I en betalingstjeneste vil dette ansvaret påhvile betalingstjenesteyteren.

## 3.3 Kravet til behandlingsgrunnlag

Som tidligere nevnt, oppstiller GDPR artikkel 5 nr. 1 (a) et krav om at enhver behandling av personopplysninger skal være «lovlig». Sammenholdt med art. 5 nr. 2 tilsier dette at den behandlingsansvarlige må kunne påvise et passende behandlingsgrunnlag etter GDPR artikkel 6 eller 9 for å kunne behandle personopplysninger på lovlig vis.

Av artikkel 6 nr. 1 følger det at «behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt (...)». Ordlyden tilsier at all behandling av personopplysninger må ha et behandlingsgrunnlag etter artikkel 6 nr. 1. I tillegg tilsier ordlyden at opplistingen av behandlingsgrunnlagene fra bokstav a til f er uttømmende.

For særlige kategorier av personopplysninger må behandlingen ha et behandlingsgrunnlag i artikkel 6 i tillegg til et supplerende behandlingsgrunnlag i artikkel 9 nr. 2. Utgangspunktet etter artikkel 9 første ledd er at all behandling av sensitive opplysninger er forbudt. Det oppstilles imidlertid ti unntak fra dette forbudet i artikkel 9 andre ledd.

Det første spørsmålet for den videre fremstillingen er hvorvidt det finnes et passende behandlingsgrunnlag etter artikkel 6 for behandling av silent party data som kan kategoriseres som *alminnelige* personopplysninger. Dette vil behandles i del 4. Spørsmålet for del 5 av oppgaven er hvilket supplerende behandlingsgrunnlag etter artikkel 9 nr. 2 som kan være passende av silent party data som er *sensitive* personopplysninger.

# 4 Behandling av silent party data – Artikkel 6

De alminnelige reglene for behandlingsgrunnlag fremgår av artikkel 6. Som tidligere nevnt, må enhver behandling av personopplysninger ha et behandlingsgrunnlag etter alternativene nedfelt i artikkel 6 nr. 1. Artikkel 29-gruppen har lagt til grunn at behandlingsgrunnlagene er likestilte. [49] Artikkelen lyder slik:

> «*behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:*
>
> *a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,*
>
> *b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,*
>
> *c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,*
>
> *d) behandlingen er nødvendig for å verne den registrertes eller en annen persons vitale interesser,*
>
> *e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,*
>
> *f) behandlingen er nødvendig knyttet til formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.»*

[49] Artikkel 29-gruppen, «*Opinion 15/2011 on the definition of consent*», Adopted on 13 July 2011, WP 187 s.7.

I det videre vil oppgaven drøfte hvorvidt noen av behandlingsgrunnlagene etter art. 6 nr. 1 som kan anvendes for behandling av silent party data.

## 4.1 Nødvendighetskravet

Med unntak av samtykkekravet, jfr. art. 6 (1) (a), oppstiller alle behandlingsgrunnlagene etter artikkel 6 et krav om at behandlingen av personopplysninger må være nødvendig.

Ordlyden av «nødvendig» tilsier at behandlingen av personopplysninger må være egnet til å oppfylle formålet med behandlingen. Etter fortalepunkt 39 følger det at «personopplysninger bør behandles bare dersom formålet med behandlingen ikke med rimelighet kan oppnås på en annen måte». Dette tilsier at nødvendighetskravet ikke kan tolkes som at behandlingsformålet er umulig å oppnå uten behandling av personopplysninger, men at behandlingen gjør det betydelig enklere å oppnå behandlingsformålet. Svenske myndigheter har lagt til grunn at nødvendighetsvilkåret vil være oppfylt så lenge behandlingen av personopplysninger vil medføre en merkbar forenkling av prosessen.[50]

I henhold til PSD2 artikkel 94 (2) skal betalingstjenesteytere bare behandle personopplysninger som er «nødvendig for å yte betalingstjenestene». Sammenholdt med GDPRs nødvendighetskrav tilsier dette at betalingstjenesteyteren kun burde behandle de personopplysningene som er nødvendig for å gjennomføre en betalingstransaksjon og for å gi den registrerte oversikt over sin finansielle stilling.

Overført til oppgavens tema reiser dette spørsmål om hvilke personopplysninger om den utenforstående tredjepart som er nødvendig for betalingstjenesteyteren å behandle for å kunne yte sin tjeneste.

Tredjepartsaktører kan bare behandle betalingsmottakerens navn, adresse og bankkonto der det foreligger et behandlingsgrunnlag.[51] I tillegg vil betalingstjenesteyteren ha tilgang til å

[50] SOU 1999:109 S.156 ref. Sören Öman, *Dataskyddsförordningen (GDPR) m.m., En kommentar,* 1. utgåva, Norstedts Juridik, 2019, s. 149.

[51] Peeters, 2020 s. 64; EDPS, *Opinion on payment services*, publisert 5. des. 2013, s. 2 avsn. 7.

behandle betalingssummen og friteksten tilknyttet betalingstransaksjonen.[52] Det vil være nødvendig å behandle de samme personopplysningene om den utenforstående tredjepart for at betalingstjenesteyteren skal utføre sine tjenester.

## 4.2 Samtykke jfr. art. 6 (1) (a)

Etter GDPR art. 6 nr. 1 (a) er behandlingen lovlig dersom «den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål».

En naturlig språklig forståelse av «samtykket» tilsier at den registrerte må godta å gi tilgang til sine personopplysninger ved å foreta aktiv handling. I GDPRs fortalepunkt 32 er det også fremhevet at et samtykke krever en tydelig handling som viser at den registrerte har godtatt behandling av sine personopplysninger. Det betyr at et stilltiende samtykke eller passivitet ikke er nok, og at standardinnstillinger fra nettleser, sosiale medier og lignende ikke er et gyldig samtykke etter GDPR.

Ettersom betalingstjenesteyteren ikke har behandlingsgrunnlag for å identifisere den utenforstående tredjepart etter art. 6 i utgangspunktet, kan ikke samtykke innhentes fra vedkommende. [53] Derfor kan ikke samtykke etter art. 6 nr. 1 (a) utgjøre et behandlingsgrunnlag for behandling av silent party data.

## 4.3 Nødvendig for å oppfylle en avtale jfr. art. 6 (1) (b)

Behandling av personopplysninger kan være lovlig dersom det er «nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse», jfr. GDPR art. 6 nr. 1 (b).

Ordlyden av «avtale som den registrerte er part i» tilsier at behandlingsgrunnlaget er myntet på avtaler der den person som opplysningene omhandler, også er part i avtalen. Behandling av silent party data kjennetegnes av at det ikke foreligger et avtaleforhold mellom den

[52] Österreichischer Sparkassenverband, *Response to EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR,* feedback reference: 06/2020-006, publ.14. september 2020, s. 2

[53] Retningslinje 06/2020, EDPB, s. 16

utenforstående tredjepart og betalingstjenesteyteren. Ordlyden åpner dermed ikke for at art. 6 (1) (b) kan tjene som behandlingsgrunnlag for behandling av silent party data.

## 4.4 Nødvendig for å oppfylle en rettslig forpliktelse jfr. art. 6 nr. 1 (c)

Etter GDPR art. 6 nr. 1 bokstav (c) kan personopplysninger behandles dersom det er «nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige». Spørsmålet er hvorvidt det finnes en rettslig forpliktelse for å behandle silent party data, jfr. art. 6 (1) (c).

Det nærmere innholdet av kravet til en rettslig forpliktelse er fastsatt i art. 6 nr. 3, hvor det følger at «grunnlaget for behandlingen nevnt i nr. 1 bokstav (c) (...) skal fastsettes i a) unionsretten eller b) medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt».

Videre følger det av art. 6 nr. 3 at «formålet med behandlingen skal være fastsatt i nevnte rettslige grunnlag (...)». En naturlig språklig forståelse av «fastsatt» tilsier at behandling av personopplysninger er en forutsetning for å oppfylle den forpliktelsen som det rettslige grunnlaget pålegger den behandlingsansvarlige. Denne tolkningen støttes av de norske forarbeidene til personopplysningsloven og juridisk teori.[54]

I tillegg følger det ytterligere krav av GDPRs fortalepunkt 41:

> *«når det i denne forordningen vises til et rettslig grunnlag eller et lovgivningsmessig tiltak, krever dette ikke nødvendigvis en regelverksakt vedtatt av et parlament (...) Nevnte rettslige grunnlag eller lovgivningsmessige tiltak bør imidlertid være tydelig og presist, og anvendelsen av det bør være forutsigbar for personer som omfattes av det, i samsvar med rettspraksisen til Den europeiske unions domstol («Domstolen») og Den europeiske menneskerettighetsdomstol».*

[54] Prop. 56 LS (2017 - 2018) Lov om behandling av personopplysninger (personopplysningsloven) s. 33-34; Skullerud m.fl. 2019 s. 187

Et rettslig grunnlag i unionsretten eller nasjonal rett må følgelig oppfylle to krav for å kunne utgjøre en rettslig forpliktelse etter GDPR art. 6 (1) (c). For det første må formålet med behandlingen fremgå av det rettslige grunnlaget. For det andre må det rettslige grunnlaget være tilstrekkelig tydelig og presist slik at anvendelsen fremstår som forutsigbar for personer som omfattes av det.

I sitt høringssvar til retningslinje 06/2020 foreslår forskningsgruppen Sprite+ at PDS2 kan utgjøre en rettslig forpliktelse, slik at GDPR art. 6 (1) (c) kan utgjøre behandlingsgrunnlag for silent party data:

> *«Articles 48, 49, 57, 58, 66 and 67 of the PSD2, for example, have clearly envisaged the scenarios where processing of the data concerning the silent payee is needed for the completion of the transaction, and have also specified the sole purpose of such processing. Once transposed into Member State laws, these provisions may provide a more predictable legal basis for uses of silent party data. (...)»* [55]

Som nevnt i punkt 1.2 har høringssvar i utgangspunktet liten rettskildemessig vekt, men i mangel på andre autoritative kilder er forslaget fra Sprite+ interessant. Sprite+ er en forskergruppe bestående av akademikere med ulik faglig bakgrunn fra fem engelske universiteter med det formål å forske på ulike sider ved den digitale økonomien. Gruppens faglige tyngde tilsier at deres forslag kan være en god løsning.

På bakgrunn av dette er det naturlig å reise spørsmål om hvorvidt artiklene 48, 49, 57, 58, 66 eller 67 i PSD2 hver for seg kan utgjøre en rettslig forpliktelse for å behandle silent party data, jfr. GDPR art. 6 (1) (c).

PSD2 er unionsrett og skal som et direktiv gjennomføres i nasjonal rett jfr. TEUV art. 288 (3). Ordlyden av art. 6 nr. 3 stenger derfor ikke for at PSD2 kan utgjøre en rettslig forpliktelse jfr. art. 6 (1) (c).

---

[55] Sprite + Future Payment Systems Working Group, «*Comments on the European Data Protection Board´s Guidelines 06/2020 on the interplay of the Second Payment Directive and GDPR*», publisert 16. september 2020, referanse: 06/2020-0039, United Kingdom

Det neste spørsmålet er om artiklene 48, 49, 57, 58, 66 eller 67 i PSD2 oppfyller kravene til en rettslig forpliktelse som følger av GDPR art. 6 nr. 3 og GDPRs fortalepunkt 41. Nærmere bestemt om artiklene forutsetter en behandling av silent party data og om de er tilstrekkelig tydelig og presist utformet. I det videre vil de artiklene som inneholder samme vilkår drøftes sammen.

### 4.4.1 PSD2 Artikkel 48, 49 og 57:

PSD2 artikkel 48 alternativ (a) omhandler opplysninger til betaleren etter mottak av betalingsordren. Av artikkelen følger det at:

> *«umiddelbart etter mottak av betalingsordren skal betalerens betalingstjenesteyter gi eller gjøre tilgengelig for betaleren, på samme måte som fastsatt i artikkel 44 nr. 1, følgende opplysninger med hensyn til sine tjenester: a) (...)* ***der det er relevant, opplysninger om betalingsmottakeren****».* (min utheving)

PSD2 artikkel 49 alternativ a) omhandler opplysninger til betalingsmottakeren etter gjennomføring. Det følger av artikkelen at:

> *«umiddelbart etter gjennomføring av betalingstransaksjonen skal betalingsmottakerens betalingstjenesteyter gi eller gjøre tilgjengelig for betalingsmottakeren (...) følgende opplysninger med hensyn til sine tjenester a)* ***en referanse som gjør det mulig for betalingsmottakeren å identifisere betalingstransaksjonen og****,* ***der det er relevant, betaleren****, samt eventuelle opplysninger som ble overført sammen med betalingstransaksjonen.*» (min utheving)

Av PSD2 artikkel 57 omhandler opplysninger til betaleren om enkeltstående betalingstransaksjoner. Det følger av artikkelen at:

> *«etter at beløpet for en enkeltstående betalingstransaksjon er debitert betalerens konto, eller når betaleren ikke bruker en betalingskonto, etter mottak av betalingsordren, skal betalerens betalingstjenesteyter uten unødig opphold og på samme måte som fastsatt i artikkel 51 nr. 1 gi betaleren alle følgende opplysninger a) (...)* ***der det er relevant****,* ***opplysninger om betalingsmottakeren****».* (min utheving)

Spørsmålet er om artiklene forutsetter en behandling av silent party data, jfr. GDPR art. 6 nr. 3 og om de er tilstrekkelig tydelig og presist utformet, jfr. GDPR fortalepunkt 41.

De tre artiklene åpner for at betalingstjenesteyteren skal kunne utgi «opplysninger om betalingsmottakeren» jfr. PSD2 art. 48 og 57 eller «en referanse som gjør det mulig for betalingsmottakeren å identifisere (...) betaleren» jfr. PSD2 art. 49.

Ordlyden er taus angående hvorvidt betaleren eller betalingsmottakeren som det utgis opplysninger om, må være bruker av betalingstjenesten eller ikke. Dersom betalingstjenesteyteren skal gi opplysninger om en betaler eller betalingsmottaker som ikke er bruker av den aktuelle tjenesten, forutsetter det behandling av silent party data. Ordlyden kan derfor tolkes som at artiklene tar høyde for behandling av silent party data, noe som trekker i retning av at formålet med behandlingen er fastsatt i det rettslige grunnlaget, jfr. art. 6 nr. 3. På den andre siden kan ordlyden også tolkes som at det er forutsatt at betaleren eller betalingsmottakeren er bruker. Ordlydens tvetydighet kan tale for at artiklene ikke er tydelige og presise nok, jfr. fortalepunkt 41.

Videre følger det av de tre artiklene at betalingstjenesteyteren skal oppgi opplysninger til betalingstjenestebrukeren om betaler eller betalingsmottaker, «der det er relevant». Ordlyden tilsier at betalingstjenesteyteren må foreta en konkret skjønnsmessig vurdering av om det er relevant å oppgi opplysninger om betaleren eller betalingsmottakeren til betalingstjenestebrukeren hver gang dette blir aktuelt. Det nærmere innholdet av «relevant» er imidlertid vanskelig å fastsette. Ordlyden åpner for en vid skjønnsmessig vurdering hvor en rekke momenter og hensyn kan være relevante. Det foreligger ingen tyngre rettskilder som kan belyse hvilke momenter og hensyn som vil være relevante for denne vurderingen. En vid skjønnsmessig vurdering kan føre til en vilkårlig anvendelse av artiklene, noe som i liten grad vil ivareta hensynet til forutberegnelighet. Dette trekker i retning av at artiklene ikke er tilstrekkelig tydelige og presise, jfr. fortalepunkt 41.

Argumentene trekker i retning av at PSD2 artikkel 48, 49 og 57 ikke er tilstrekkelig tydelige og presise for å kunne utgjøre en rettslig forpliktelse, jfr. GDPR art. 6 (1) (c). Det legges avgjørende vekt på vagheten i vilkåret «der det er relevant», samt at ordlyden i artiklene er tvetydig angående hvorvidt den part som det kan være aktuelt å utgi opplysninger om, må være bruker av betalingstjenesten eller ikke.

### 4.4.2 PSD2 Artikkel 58:

PSD2 artikkel 58 omhandler opplysninger til betalingsmottakeren om enkeltstående betalingstransaksjoner. Av artikkel 58 følger det at:

> *«etter at en enkeltstående betalingstransaksjon er gjennomført, skal betalingsmottakerens betalingstjenesteyter uten unødig opphold og på samme måte som fastsatt i artikkel 51 nr. 1 gi betalingsmottakeren alle følgende opplysninger:*
> *a)* ***en referanse som gjør det mulig for betalingsmottakeren å identifisere betalingstransaksjonen og betaleren****, samt eventuelle opplysninger som ble overført sammen med betalingstransaksjonen».* (min utheving)

Spørsmålet er om artikkelen forutsetter en behandling av silent party data, jfr. GDPR art. 6 nr. 3 og om den er tilstrekkelig tydelig og presist utformet, jfr. GDPR fortalepunkt 41.

Ordlyden av «skal betalingsmottakerens betalingstjenesteyter (...) gi betalingsmottakeren (...) en referanse som gjør det mulig for betalingsmottakeren å identifisere (...) betaleren» tilsier at betalingstjenesteyteren har en plikt til å utgi opplysninger om betaleren. En slik plikt forutsetter behandling av personopplysninger. Ordlyden trekker derfor i retning av at artikkel 58 er tilstrekkelig tydelig og presis, jfr. GDPRs fortalepunkt 41, og at formålet med behandlingen fremgår av det rettslige grunnlaget, jfr. GDPR art. 6 nr. 3.

På den andre siden er ordlyden av «betaleren» taus om hvorvidt den aktuelle betaleren må være bruker av tjenesten eller ikke. Ordlydens taushet kan tolkes som at artikkelen ikke stiller krav om at den aktuelle betaler eller betalingsmottaker er bruker av betalingstjenesten, og at artikkelen derfor forutsetter for behandling av silent party data jfr. art.6 nr. 3. Ordlyden kan imidlertid også tolkes som at det forutsettes at betaleren er bruker av betalingstjenesten. Ordlydens tvetydighet trekker i retning av at artikkel 58 ikke er tilstrekkelig tydelig og presis, jfr. fortalepunkt 41.

Argumentene trekker i retning av at PSD2 artikkel 58 ikke er tydelig og presis nok for å kunne utgjøre en rettslig forpliktelse, jfr. GDPR art. 6 (1) (c). Det må legges avgjørende vekt på at det er usikkert om artikkelen åpner for behandling av silent party data eller ikke.

### 4.4.3 PSD2 Artikkel 66 og 67:

PSD2 artikkel 66 regulerer tilgang til betalingskonto for betalingsinitieringstjenester. Av artikkelens første ledd følger det at:

> *«medlemsstatene skal sikre at en betaler har rett til å benytte en yter av betalingsinitieringstjenester for betalingstjenestene nevnt i vedlegg 1 nr. 7.»*

PSD2 artikkel 67 regulerer tilgang til betalingskonto for kontoopplysningstjenester. Av artikkelens første ledd følger det at:

> *«medlemsstatene skal sikre at en betalingstjenestebruker har rett til å benytte tjenester som gir tilgang til kontoopplysningene nevnt i vedlegg 1 nr. 8».*

Spørsmålet er om artiklene forutsetter en behandling av silent party data, jfr. GDPR art. 6 nr. 3 og om de er tilstrekkelig tydelig og presist utformet, jfr. GDPR fortalepunkt 41.

Ordlyden av «sikre at betaler har rett til å benytte en yter av betalingsinitieringstjenester» og «sikre at en betalingstjenestebruker har rett til å benytte [kontoopplysningstjenester]» forutsetter at betalingstjenesteyteren må behandle personopplysninger i forbindelse med en betalingstransaksjon eller for å kunne gi brukeren innsikt i sin finansielle stilling. Behandling av personopplysninger er avgjørende for at slike tjenester skal fungere.

Artikkel 66 er rettet mot en «*betaler*». For at en betalingsinitieringstjeneste skal kunne benyttes for sitt formål, nemlig å initiere betalinger på vegne av brukeren, er det nødvendig for tjenesten å ha tilgang til betalerens personopplysninger. Ordlyden av «betaler» indikerer derfor at artikkel 66 forutsetter behandling av *betalingstjenestebrukerens* personopplysninger, og avgrenser på denne måten for behandling av silent party data. Dette tilsier at artikkel 66 ikke forutsetter behandling av silent party data jfr. GDPR art. 6 nr. 3.

Bruken av ordet «kontoopplysningene» jfr. art. 67 gir også en klar indikasjon på at bestemmelsen sikter til opplysningene som tilhører betalingstjenestebrukeren, og ingen andre. «Kontoopplysningene» er nemlig skrevet i bestemt form og kommer etter at «betalingstjenestebrukeren» er nevnt. Det er følgelig naturlig å lese bestemmelsen slik at den forutsetter behandling av *de bestemte kontoopplysningene tilhørende*

betalingstjenestebrukeren. En naturlig forståelse av art. 67 avgrenser følgelig mot behandling av kontoopplysninger tilhørende en utenforstående tredjepart.

I forlengelse av dette er det verdt å bemerke at bestemmelsen kun bruker ordet «kontoopplysningene». Ordlyden i seg selv avgrenser dermed mot at bestemmelsen også skal kunne gi et rettslig grunnlag for å behandle øvrige personopplysninger. Som nevnt tidligere nevnt, kan *hvem* som betaler, *hvilken* betaling det er tale om og så videre, også utgjøre personopplysninger. Det har følgelig formodningen mot seg at art. 67 på generelt grunnlag forutsetter behandling av silent party data jfr. GDPR art. 6 nr. 3.

I henhold til EDPBs uttalelse i retningslinje 06/2020 pålegger PSD2 artikkel 66 (1) og artikkel 67 (1) en rettslig forpliktelse for bankene til å gi tredjepartsaktørene tilgang til betalingsbrukerens betalingskonto jfr. GDPR art. 6 (1) (c):

> *«In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISP´s and AISP´s services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case is Article 6 (1) (c) of the GDPR.».*

En slik behandling av personopplysninger fordrer at betalingstjenestebrukeren først registrerer seg hos den tjenesten det gjelder. Selv om art. 66 og 67 utgjør et rettslig grunnlag for bankenes plikt til å utlevere kontoopplysninger til tredjepartsaktørene, er det følgelig vanskelig å tolke bestemmelsene utvidende i så stor grad at tredjepartsaktørene også skal kunne behandle opplysningene til en utenforstående tredjepart i forbindelse med en betalingstransaksjon.

Det kan nevnes at formålet med PSD2 er å legge til rette for innovasjon og utvikling av det digitale betalingsmarkedet, og at behandling av silent party data vil legge til rette for utvikling av det digitale markedet ved å gjøre betalingstjenester mer attraktive og tilrettelegge for økt konkurranse. Formålet med PSD2 kan dermed i seg selv tale for en utvidende ordlydstolkning, men dette må klart anses som uholdbart. For det første er dette en drastisk utvidelse av ordlyden jfr. de nevnte momentene. I tillegg vil en slik tolkning medføre at

artiklene ikke er tydelige og presist nok utformet i henhold til kravet nedfelt i GDPRs fortalepunkt 41.

Uten tilgang til å behandle silent party data, vil betalingstransaksjoner bare kunne skje mellom brukerne av den aktuelle betalingstjenesten. Som nevnt i punkt 1.1, er det ikke mulig å gjennomføre en betaling til en utenforstående tredjepart med dagens betalingstjenester. Behandling av silent party data ikke er dermed avgjørende for at betalingstjenesten skal kunne yte sine tjenester. Dette tilsier at artikkel 66 og 67 ikke forutsetter behandling av silent party data, jfr. art. 6 nr. 3.

Samlet sett trekker argumentene klart i retning av at PSD2 art. 66 (1) og 67 (1) ikke kan utgjøre en rettslig forpliktelse for behandling av silent party data, jfr. GDPR art. 6 (1) (c).

### 4.4.4 Avsluttende bemerkninger

Etter en vurdering av artiklene 48, 49, 57, 58, 66 eller 67 i PSD2 trekker argumentene i retning av at artiklene ikke kan utgjøre en rettslig forpliktelse, jfr. GDPR art. 6 (1) (c). Det foreligger likevel argumenter for at artiklene kan utgjøre en rettslig forpliktelse, særlig hensett til formålet med PSD2 og at enkelte av artiklene ikke uttrykkelig avgrenser mot behandling av silent party data. På dette punktet er det behov for en nærmere avklaring, enten i domstolene eller av EDPB. I retningslinje 06/2020 har EDPB ikke behandlet hvorvidt PSD2 kan anvendes som et rettslig grunnlag for behandling av silent party data.

Ettersom artiklene 48, 49, 57, 58, 66 og 67 i PSD2 ikke kan sies å utgjøre en tydelig og presis rettslig forpliktelse for behandling av silent party data vil det være naturlig å se hen til om noen av de andre alternativene i GDPR art. 6 nr. 1 kan utgjøre et behandlingsgrunnlag.

## 4.5 Nødvendig for å verne vitale interesser jfr. art. 6 nr. 1 (d):

Etter GDPR artikkel 6 nr. 1 (d) kan personopplysninger behandles når det er «nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser». Spørsmålet er om behandling av silent party data er «nødvendig for å verne den registrertes (...) vitale interesser».

Ordlyden av «vitale interesser» tilsier interesser som er av fundamental og avgjørende betydning for den registrerte. Det nærmere innholdet av art. 6 nr. 1 (d) er presisert i fortalepunkt 46 hvor det fremgår at:

> «*Behandlingen av personopplysninger bør også anses som lovlig dersom den er nødvendig for å verne en interesse som er av avgjørende betydning for den registrerte eller en annen fysisk persons liv. (...) Noen typer behandling kan tjene både viktige allmenne interesser og den registrertes vitale interesser, f.eks. når behandlingen er nødvendig av humanitære årsaker, herunder for overvåking av epidemier og spredning av dem, eller i humanitære nødssituasjoner, særlig i forbindelse med naturkatastrofer og menneskeskapte katastrofer.*»

Eksemplenes karakter viser at behandlingsgrunnlaget er reservert for svært alvorlige situasjoner. Den høye terskelen som ordlyden oppstiller og de alvorlige eksemplene fortalen bruker, tilsier at det burde utvises varsomhet ved å anvende art. 6 nr. 1 (d) på andre situasjoner enn de som er brukt som eksempler.

I juridisk teori er det tatt til orde for at «vitale interesser» også kan omfatte vern av svært viktige økonomiske interesser fordi slike hensyn kan ha avgjørende betydning for den registrertes liv.[56] Ordlyden stenger ikke for en slik tolkning av bestemmelsen. I lys av den høye terskelen som eksemplene i fortalepunkt 46 taler for, er det naturlig å tolke bestemmelsen slik at dette må avgrenses til svært alvorlige økonomiske situasjoner.

En betalingstjenesteyter har økonomisk interesse i å kunne behandle silent party data. Det vil gjøre betalingstjenesten mer attraktiv på markedet og tilrettelegge for økt konkurranse. Slike interesser er imidlertid ikke av avgjørende betydning for den registrertes liv. Den høye terskelen som ordlyden og fortalepunkt 46 oppstiller, trekker i retning av at slike økonomiske interesser ikke kan være «nødvendig for å verne den registrertes (...) vitale interesser», jfr. art. 6 (1) (d).

Betalingstjenestebrukeren vil alltid kunne benytte seg av bankens betalingstjenester, uavhengig av om tredjepartsaktører kan behandle silent party data eller ikke. Dette illustrerer

[56] Skullerud m.fl. 2019, s. 181

at betaling gjennom en tredjepartsaktør ikke er av avgjørende betydning for den registrertes liv, og trekker i retning av at behandling av silent party data ikke er «nødvendig for å verne den registrertes (...) vitale interesser», jfr. art. 6 (1) (d).

Etter denne vurderingen legges det avgjørende vekt på at bankens betalingstjenester i alle tilfeller vil kunne brukes. Derfor vil det ikke medføre fare for den registrertes liv dersom betalingstjenesteyteren ikke kan behandle silent party data. Dette tilsier at behandling av silent party data ikke er «nødvendig for å verne den registrertes (...) vitale interesser», jfr. art. 6 nr. 1 (c).

## 4.6 Nødvendig for å utføre en oppgave i allmennhetens interesse jfr. art. 6 nr. 1 (e):

Etter GDPR art. 6 nr. 1 (e) kan personopplysninger behandles dersom det er «nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt». Videre følger det av art. 6 nr. 3 at «grunnlaget for behandling nevnt i nr. 1 bokstav (...) e) skal fastsettes i a) unionsretten eller b) medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt.»

Det første spørsmålet er hvorvidt behandling av silent party data kan være «nødvendig for å utføre en oppgave i allmennhetens»

En naturlig språklig forståelse av «oppgave i allmennhetens interesser» tilsier at oppgaven som uføres må ha et formål som kan ha samfunnsmessig betydning. Med andre ord må behandlingen komme en ubestemt krets av personer til gode, ikke en bestemt person eller virksomhet. Sammenholdt med ordlyden av «utøve offentlig myndighet» tilsier en kontekstuell tolkning at offentlige interesser er kjerneområdet for anvendelsen av art. 6 nr. 1 (e). Dette tilser at en «oppgave i allmennhetens interesser» kan være tilfeller hvor en privat virksomhet utfører oppgaver på vegne av det offentlige, for eksempel sykehjemstjenester. Forordningens fortale inneholder ingen nærmere konkretisering av vilkåret. I juridisk teori er det fremhevet at samfunnsnyttig statistikk og forskning også vil kunne oppfylle vilkåret. Eksempelvis kartlegging av barns kostholdsvaner. [57]

[57] Dag Wiese Schartum, *Personvernforordningen*, 1. utgave, Fagbokforlaget, 2020.

Dersom en tredjepartsaktør kan behandle silent party data vil det, som tidligere nevnt, føre til et mer effektiv og sømløst omsetningsliv. I tillegg vil det tilrettelegge for økt konkurranse mellom betalingstjenesteyterne på markedet. Dette kan tilsi at behandling av silent party data kan ha en samfunnsmessig funksjon og bidra til økonomisk utvikling.

Den kontekstuelle tolkningen av ordlyden tilsier som nevnt at oppgaver på vegne av det offentlige – eventuelt oppgaver som er i det offentliges interesse – er i kjernen av formålet med bestemmelsen. Behandling av silent party data befinner seg på ytterkanten av bestemmelsens anvendelsesområde. Selv om behandling av silent party data vil bidra til et mer effektivt og sømløst omsetningsliv, må det påpekes at bankenes betalingstjenester uansett vil kunne brukes for å gjennomføre betalinger. De positive sidene ved at tredjepartsaktører kan behandle silent party data fremstår følgelig ikke som å være tilstrekkelige for å anse vilkåret «allmenne interesser» som oppfylt.

Behandling av silent party data er følgelig ikke «nødvendig for å utføre en oppgave i allmennhetens interesser eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt» jfr. art. 6 nr. 1 (e). Derfor vil det ikke være nødvendig å vurdere om det finnes et passende rettslig grunnlag i unionsretten eller medlemsretten.

## 4.7 Berettiget interesse Art. 6 (1) (f):

Etter GDPR art. 6 (1) (f) kan personopplysninger behandles når behandlingen er:

> *«nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger (...)»*

Spørsmålet er om behandlingen av silent party data er «nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige og hvorvidt «den registrertes interesser eller grunnleggende rettigheter går foran og krever vern av personopplysninger».

Artikkelen inneholder tre kumulative vilkår. For det første må den behandlingsansvarlige eller den tredjeparten som ønsker tilgang til personopplysningene, ha en berettiget interesse. For det andre må personopplysningene være nødvendige for å kunne forfølge formålet med behandlingen. Det tredje vilkåret er at behandlingen av personopplysningene ikke skal krenke den registrertes grunnleggende rettigheter og friheter.

I GDPRs fortalepunkt 47 er det presisert at i vurderingen av om den behandlingsansvarlige har en berettiget interesse, må det tas hensyn til: *«de registrertes rimelige forventninger på grunnlag av forholdet mellom dem og den behandlingsansvarlige, f.eks. dersom den registrerte er kunde av den behandlingsansvarlige eller vedkommendes tjeneste (...)»*.

Overført til oppgavens tema tilsier fortaleuttalelsen at i vurderingen av hvorvidt betalingstjenesteyteren har en berettiget interesse i å behandle silent party data, må det tas hensyn til hva fremstår som rimelig sett ut ifra forholdet mellom betalingstjenesteyteren og den utenforstående tredjepart.

Et eksempel på anvendelse av art. 6 nr. 1 (f) er Rigas Satiksme-dommen.[58] En taxi hadde stoppet i veikanten for å slippe av en passasjer. I det passasjeren åpnet bildøren, kjørte en trikk fra selskapet Riga Satiksme forbi og trikkevognen ble skadet i sammenstøtet mellom bildøren og trikkevognen. Riga Satiksme ønsket å rette erstatningssøksmålet mot taxipassasjeren, men det nasjonale politiet ville imidlertid bare utlevere passasjerens navn og imøtekom ikke trafikkselskapets krav om å oppgi personnummer og adresse. Artikkel 6 nr. 1 (b) er en videreføring av artikkel 7 (f) i det forrige direktivet 95/46, og derfor har denne saken overføringsverdi.

For den videre drøftelsen er det verdt å bemerke at overført til GDPRs definisjon er betalingstjenesteyteren den behandlingsansvarlige, og den utenforstående tredjepart er å regne som den registrerte.

[58] Riga Satiksme *C-13/16, dom avsagt 4. mai 2017*

### 4.7.1 Har den behandlingsansvarlige som ønsker tilgang til personopplysningene, en berettiget interesse?

Det første vilkåret for å kunne behandle personopplysninger etter GDPR art. 6 (1) (f) er at den behandlingsansvarlige som ønsker tilgang til personopplysningene har en berettiget interesse. Spørsmålet er om tredjepartsaktøren som betalingstjenesteyter har en berettiget interesse i å behandle silent party data.

En naturlig språklig forståelse av «berettiget interesse» tilsier at formålet med å behandle opplysningene, må være rimelig, saklig og begrunnet. Ordlyden er vid og kan omfatte mange ulike typer behandlingsformål. Artikkel 29-gruppen har uttalt at for at en interesse skal være berettiget, må den være lovlig, konkret, reell og aktuell. [59] I Riga Satiksme-dommen kom EU-domstolen til at erstatningskravet var en slik berettiget interesse.

EDPB har uttalt at betalingstjenesteyterens interesse av å oppfylle en kontraktsbasert ytelse overfor betalingstjenestebrukeren kan være en berettiget interesse, jfr. art. 6 (1) (f):

> *«a lawful basis for the processing of these silent party data by PSIPs or AIPs – in the context of payment and account services under the PSD2 – could be the legitimate interest of a controller or a third party ex Article 6 (1) (f) to perform a contract with the service user. This means that the legitimate interest of the controller is limited and determined by the reasonable expectations of data subjects».*[60]

Uttalelsen tilsier at betalingstjenesteyteren kan ha en berettiget interesse i å yte en kontraktsbasert ytelse overfor betalingstjenestebrukeren. EDPB har videre påpekt at dette forutsetter at behandlingen er i tråd med de øvrige kravene til forholdsmessighet som følger av bestemmelsen.[61]

Betalingstjenesteyteren har en interesse i å behandle silent party data for å kunne tilby betalingstjenestebrukeren en forbedret tjeneste. Uten tilgang til å behandle silent party data,

---

[59] Artikkel 29-gruppen, *«Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC»,* Adopted on 9 April 2014, WP 217, se Annex 1 på s. 55.

[60] EDPB, *Letter regarding the PSD2 Directive*, 5 Juli 2018

[61] EDPB, Retningslinje 06/2020, avsnitt 46.

vil betalingstjenesten begrenses på den måten at betalingstransaksjoner bare kan skje mellom brukerne av den aktuelle betalingstjenesten. Med tilgang til å behandle silent party data, vil betalingstjenesten bli mer attraktiv på betalingstjenestemarkedet, det vil føre til økt konkurranse og et mer effektivt og sømløst omsetningsliv. Muligheten for å behandle silent party data vil være en viktig fordel for betalingstjenesten og for betalingstjenestemarkedet. Interessen fremstår derfor som saklig og rasjonell. Dette trekker i retning av at den behandlingsansvarlige har en berettiget interesse av å behandle silent party data, jfr. art. 6 (1) (f).

GDPRs fortale fremhever en rekke eksempler på behandlingsformål som kan oppfylle kravet til en berettiget interesse, jfr. Art. 6 nr. 1 (f). Av fortalepunkt 47-49 fremgår at eksempler på berettigede interesser kan være:

> *«behandling av personopplysninger som er strengt nødvendig for å forebygge bedrageri, (...) i forbindelse med direkte markedsføring (...), å overføre personopplysninger internt i konsernet med henblikk på interne administrative formål, (...). Behandling av personopplysninger (...) for å sikre nett-og informasjonssikkerheten (...).*

Fortalens bruk av eksempler må tolkes som at også andre lignende interesser kan anses som berettigede. Behandling av personopplysninger i forbindelse med direkte markedsføring er en økonomisk interesse. Det samme er betalingstjenesteyterens interesse i å tilby en forbedret tjeneste til sine brukere. Dette trekker i retning av at betalingstjenesteyteren har en berettiget interesse i å behandle silent party data jfr. art. 6 (1) (f).

Etter en denne vurderingen trekker argumentene i retning av at betalingstjenesteyteren har en berettiget interesse i å behandle silent party data. Det legges avgjørende vekt på at EDPB har uttalt at dette kan være en berettiget interesse, og at fortalen synes å åpne for at også andre økonomiske interesser kan anses som berettigede.

### 4.7.2 Vil personopplysningene kunne realisere formålet med behandlingen?

Det neste vilkåret for å behandle silent party data etter GDPR art. 6 (1) (f), er at personopplysningene som den behandlingsansvarlige ønsker tilgang til, må være nødvendige for å kunne forfølge formålet med behandlingen.

I Riga Satiksme-dommen uttalte EU-domstolen at behandling av personopplysninger må holdes til det strengt nødvendige. Uten behandling av silent party data vil det ikke være mulig å levere en tjeneste hvor betalingstjenestebrukerne kan gjennomføre betalinger til utenforstående tredjeparter. Dette viser at tilgang til silent party data vil realisere formålet med behandlingen.

### 4.7.3 Vil den registrertes grunnleggende rettigheter og friheter krenkes ved behandlingen?

Det siste vilkåret for behandling av silent party data jfr. GDPR art. 6 (1) (f) er at «den registrertes interesser eller grunnleggende rettigheter og friheter [ikke] går foran [den behandlingsansvarliges berettigede interesse] og kreve vern av personopplysninger.»

En naturlig språklig forståelse av ordlyden tilsier at den berettigede interessen må stå i et rimelig forhold til inngrepet i de registrertes personvern. Dette tilsier også at jo større konsekvenser behandlingen kan ha for personvernet, desto viktigere må den behandlingsansvarlige eller tredjeparts interesse være.[62]

I Riga Satiksme-dommen uttalte domstolen at dette avhenger av en konkret avveining av sakens motstridende rettigheter og interesser. EU-domstolen har uttalt at som en generell regel vil den registrertes rettigheter veie tyngre enn den behandlingsansvarliges økonomiske interesser.[63] I juridisk teori er det utarbeidet en ikke-uttømmende liste av momenter som vurderingen burde inneholde.[64]

Det første vurderingsmomentet er hvilke fordeler virksomheten kan oppnå ved behandling av de aktuelle personopplysningene, og hvor viktige disse fordelene kan være.

[62] Se for eksempel Wessel-Aas, Ødegaard, 2018 s. 149

[63] Artikkel 29-gruppen, «*Guidelines on the impltmentation of the court of justice of the european union judgement on «google Spain and inc a, agencia española de protección de datos (AEPB) and Mario Costeja González» C-131/12*, adopted on 26 November 2014, WP 225 s. 2, avsn. 2.

[64] Skullerud m.fl. 2019 s. 183; Datatilsynet, Veileder, *Behandlingsgrunnlag*, sist endret 08.08.19. (lest 7.12. 20)

Som tidligere nevnt, vil muligheten til å behandle silent party data medføre at betalingstjenesten blir mer attraktiv på betalingstjenestemarkedet, økt konkurranse og et mer effektivt og sømløst omsetningsliv. Dette illustrer at behandling av silent party data vil være en viktig fordel for betalingstjenesten.

På den andre siden er det mulig for betalingstjenesteyteren å tilby sine tjenester uten behandling av silent party data. Et eksempel på dette er betalingstjenesten Vipps, som kun tillater betalingstransaksjoner mellom betalingstjenestebrukerne. Dette trekker i retning av at fordelen for betalingstjenesteyteren ikke er av avgjørende betydning.

For det andre må det tas hensyn til den utenforstående tredjepersons personvern. Nærmere bestemt hvilken type personopplysninger det er aktuelt å behandle, hvordan personopplysningene vil behandles og hvilke konsekvenser behandlingen vil ha for den passive tredjepart.

Det fremgår av GDPRs fortalepunkt 7 at «fysiske personer bør ha kontroll over egne personopplysninger». Det utvikles stadig nye betalingstjenester og bruken av slike tjenester øker. Dersom betalingstjenester kan behandle silent party data, vil det medføre en risiko for at forbrukere mister kontroll over sine personopplysninger. GDPRs formål trekker dermed i retning av at hensynet til den utenforstående tredjeparts personvern burde gå foran betalingstjenesteyterens interesser.

På den andre siden følger det av PSD2 artikkel 4 nr. 32 at «for ytere av betalingsinitieringstjenester og ytere av kontoopplysningstjenester utgjør navnet på kontoeier og kontonummer ikke sensitiv betalingsinformasjon». Som nevnt i punkt 4.1, vil det være nødvendig for betalingstjenesteyteren å behandle den passive tredjeparts fulle navn, kontonummer og betalingssummen for å kunne gjennomføre en betaling. I henhold til PSD2s definisjon er ikke dette sensitiv betalingsinformasjon, noe som tilsier at det ikke vil ha store negative konsekvenser for den passive tredjepart om betalingstjenesteyteren kan behandle silent party data. Dette trekker i retning av at hensynet til den passive tredjeparts personvern ikke går foran betalingstjenesteyterens interesser.

Adresse er ikke nevnt i definisjonen i art. 4 nr. 32. Dette inngår imidlertid også i de personopplysningene som er nødvendig for å sikre at en overføring gjennomføres til riktig

betalingsmottaker, eller for å sikre at riktig betaler oppgis i betalingshistorikken. Adresse er heller ikke oppgitt i den uttømmende oppramsingen av sensitive opplysninger i GDPR artikkel 9 nr. 1. En antitetisk tolkning tilsier at adresse derfor ikke er en sensitiv personopplysning. Dette trekker også i retning av at behandling av at hensynet til den passive tredjeparts personvern ikke går foran betalingstjenesteyterens interesser.

Videre har både GDPR og PSD2 som formål å legge til rette for utvikling av det digitale marked.[65] Muligheten for betalingstjenesteytere til å behandle silent party data vil legge til rette for en utvikling av Unionens marked for digitale betalingsløsninger fordi det vil effektivisere betalingstjenestene og gjøre betalingstjenestene mer attraktive. Et enklere og mer effektivt omsetningsliv vil også være i den passive tredjeparts interesse ettersom dette vil gjøre pengeoverføring lettere. Hensynet til innovasjon og et mer effektivt omsetningsliv trekker i retning av at den passive tredjeparts grunnleggende rettigheter og interesser ikke går foran betalingstjenesteyterens berettigede interesser.

Det siste vurderingstemaet er tiltak for å minimere personvernkonsekvensene for den passive tredjepart. Dette kan innebære for eksempel at det er adgang til å reservere seg mot behandling av personopplysninger eller at betalingstjenestens systemer er utviklet på en måte som sikrer sikker behandling av personvern.

Det er usikkert om den utenforstående tredjepart vil få kunnskap om betalingstjenesteyterens behandling av vedkommendes personopplysninger. Den utenforstående tredjepart kan dermed ikke reservere seg mot behandlingen, og vil derfor være avhengig av at betalingstjenesten er utviklet slik at den ivaretar personvernet.

Det er den behandlingsansvarliges ansvar at de alminnelige prinsippene etter GDPR artikkel 5 nr. 1 overholdes, jfr. art. 5 nr. 2. For behandling av silent party data er det særlig prinsippene om formålsbegrensning, dataminimering og lagringsbegrensning som gjør seg gjeldende.

Prinsippet om formålsbegrensning er nedfelt i art. 5 (1) (b) og tilsier at personopplysninger må samles inn for et spesifikt formål og ikke viderebehandles i strid med det opprinnelige formålet. Etter artikkel 24 nr. 1 har den behandlingsansvarlige ansvar for å «gjennomføre

[65] Se f.eks. GDPR fortalepunkt 6 og PSD2 fortalepunkt 6.

egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.» Dette tilsier at den behandlingsansvarlige må sørge for at betalingstjenestens systemer må være utviklet på en slik måte at det ikke foreligger en risiko for at den utenforstående tredjeparts personopplysninger kan brukes på en annen måte enn det behandlingsformålet tilsier.

Lagringsprinsippet etter art. 5 (1) (e) tilsier at personopplysninger ikke må lagres lenger enn nødvendig. Et eksempel på en sikkerhetsmekanisme for betalingstjenestene er å sørge for at opplysningene om den utenforstående tredjepart ikke lagres for en lengre tidsperiode enn det som er nødvendig for å kunne være sikker på at transaksjonen er gjennomført til riktig betalingsmottaker eller betaler. Hvor lang tidsperiode som er tilstrekkelig for å oppnå dette formålet, er imidlertid vanskelig å stadfeste og krever teknisk kunnskap om betalingstjenester.

Dataminimeringsprinsippet er nedfelt i art. 5 (1) (c), og tilsier at det skal tilstrebes å samle inn så få personopplysninger som mulig innenfor formålet med behandlingen. Som EDPB også påpeker, vil et relevant sikkerhetstiltak være kryptering eller anonymising av silent party data.[66] Dette avhenger imidlertid av hva som er teknisk mulig å gjennomføre.

Etter en helhetsvurdering legges det avgjørende vekt på at betalingstjenesteyteren har en reell og rasjonell interesse i å oppfylle sin avtaleforpliktelse overfor den registrerte, og at de personopplysningene som det vil være nødvendig å behandle, ikke er av sensitiv karakter.

Behandling av silent party data vil dermed ikke medfører en betydelig negativ konsekvens for den utenforstående tredjeparts personvern. Dette trekker i retning av at art. 6 nr. 1 (f) kan brukes som et behandlingsgrunnlag for å behandle silent party data.

# 5 Behandling av silent party data – Artikkel 9

For å kunne behandle sensitive opplysninger, må den behandlingsansvarlige påvise både et behandlingsgrunnlag etter artikkel 6 og et supplerende behandlingsgrunnlag etter art 9 nr. 2.

[66] Retningslinje 06/2020 s. 15 avsn. 47.

For den videre fremstillingen forutsettes det at det foreligger et behandlingsgrunnlag etter artikkel 6 for tredjepartsaktørers behandling av sensitiv silent party data. Spørsmålet er om det finnes et passende supplerende behandlingsgrunnlag etter artikkel 9 nr. 2.

I den videre fremstillingen vil oppgaven i punkt 5.1 redegjøre for hvorvidt betalingstjenesteyteren kan unngå behandling av sensitive opplysninger, slik at det ikke er nødvendig med behandlingsgrunnlag i art. 9. I punkt 5.3 vil oppgaven drøfte hvorvidt behandlingsgrunnlag etter art. 9 nr. 2 (g) kan anvendes på behandling av silent party data som er sensitive opplysninger.

## 5.1 Hvorvidt betalingstjenesteyteren kan unngå behandling av transaksjoner med sensitive opplysninger

En finansiell transaksjon kan potensielt avsløre sensitive opplysninger om betalingstjenestebrukeren eller den andre part i transaksjonen. Dette kan avsløres ved en enkelt transaksjon, men også ved å se flere transaksjoner i sammenheng.

Angående betalingstjenesteyterens behandling av sensitive opplysninger har EDPB foreslått følgende løsning for tilfeller hvor det ikke kan påvises et passende behandlingsgrunnlag i art. 9 nr. 2:

> *«(…) In this case, technical measures have to be put in place to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points. In this respect, payment service providers may explore the technical possibilities to exclude special categories of personal data related to silent parties by TPPs.»* [67]

Med andre ord foreslår EDPB at i tilfeller hvor betalingstjenesteyteren ikke kan påvise et passende behandlingsgrunnlag, burde tjenesten installere en teknologi som kan filtrere bort transaksjoner som inneholder sensitive opplysninger. Dette reiser spørsmål om hvorvidt det er mulig for betalingstjenesteyteren å identifisere og skille ut transaksjoner som inneholder sensitive opplysninger. På den måten kan betalingstjenesteyteren unngå å behandle slike

[67] EDPB, Retningslinje 06/2020 s. 18 avsn. 57

opplysninger, som EDPB foreslår, og det vil ikke være nødvendig med et behandlingsgrunnlag etter art. 9 nr. 2.

Flere høringssvar har påpekt at forslaget fra EDPB er komplisert å gjennomføre i praksis. Alle transaksjoner kan potensielt inneholde sensitive personopplysninger. For å unngå å behandle slike transaksjoner må de først behandles, og dersom dette gjøres, er risikoen stor for at informasjonen som hentes fra en betalingstransaksjon, feiltolkes.

Den østerrikske sparebankforeningen, Österreichischer Sparkassenverband, påpeker i sitt høringssvar at hvor mye informasjon betalingstjenesteyteren får om betalingstransaksjoner, avhenger av hva betalingstjenestebrukeren skriver i friteksten og hvem som er betalingsmottaker.[68]

Til illustrasjon har noen kirker begynt å bruke betalingstjenesten Vipps ved innsamling av kollekt.[69] Religiøs overbevisning er et eksempel på en sensitiv personopplysning. En betalingstransaksjon til en kirke behøver ikke å være relatert til betalerens religiøse overbevisning. Det kan for eksempel være at et yngre familiemedlem har brukt Vipps for å overføre penger til kollekten på vegne av et eldre familiemedlem. Det kan også være at betaleren har gitt penger til et veldedighetsprosjekt i regi av en religiøs stiftelse. Eksemplet illustrerer hvordan en betalingstransaksjon kan tolkes på mange ulike måter.

Et annet eksempel er at en betaler skriver «sykehusregning 245» i fritekstfeltet ved en betalingstransaksjon. Dette behøver ikke å bety at det er betaleren selv som er syk og at betalingstransaksjonen derfor kan avsløre sensitive opplysninger om betalingstjenestebrukerens helse. Det kan være at regningen betales på vegne av et barn, en venn, ektefelle eller forelder. Österreichischer Sparkassenverband trekker også frem som eksempel at det tyske ordet «Krebs» kan tolkes som sykdommen kreft, stjernetegnet Krepsen, dyret kreps eller det kan være et etternavn.[70] Eksemplene illustrerer hvor vanskelig det er å identifisere betalingstransaksjoner som kan avsløre sensitive opplysninger om en betalingstjenestebruker.

[68] Österreichischer Sparkassenverband, 2020. s. 2

[69] E24, «Kirke innfører vipps-betaling av kollekt», 06. 03. 16, (lest 04. 11. 2020)

[70] Österreichischer Sparkassenverband, 2020 s. 3.

Österreichischer Sparkassenverband påpeker også i samme høringssvar at det ikke finnes en teknologi som vil gjøre det mulig å filtrere bort sensitive opplysninger slik som EDPB foreslår. FinTech-selskapet Trustly påpeker også i sitt høringssvar, at dersom en slik teknologi mot formodning skulle utvikles, vil den være for kostbar og medføre så stor ineffektivitet at det ikke vil lønne seg for betalingstjenesteyteren å benytte seg av den.[71]

Den store risikoen for feiltolkning av betalingstransaksjoner, og hensynet til at det ikke er mulig å utvikle en teknologi som kan filtrere bort sensitive opplysninger, tilsier at EDPBs forslag ikke er mulig å gjennomføre i praksis. Forslaget vil medføre store negative konsekvenser, noe som dessuten vil gå imot formålet med PSD2 om å legge til rette for innovasjon og utvikling av det digitale betalingstjenestemarkedet.[72] Det fremstår dermed nærliggende å legge til grunn at betalingstjenesteyteren må ha behandlingsgrunnlag både etter artikkel 6 og 9 for å kunne behandle silent party data.

## 5.2 Presentasjon av artikkel 9

Etter GDPR artikkel 9 første ledd er det i utgangspunktet forbudt å behandle personopplysninger om følgende:

> *«rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.»*

Etter andre ledd er det imidlertid opplistet følgende ti unntak fra forbudet i første ledd:

- Den registrerte har gitt et uttrykkelig samtykke, jfr. art. 9 (2)(a)
- Behandling for å oppfylle forpliktelser og utøve rettigheter innenfor arbeidsrett, trygderett og sosialrett, jfr. art. 9 (2)(b)
- Behandling for å verne den registrerte eller annen fysisk persons vitale interesser dersom vedkommende er ute av stand til å samtykke, jfr. art. 9 (2)(c)

[71] Trustly Group AB, *Response to EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR*, publisert 15. september 2020, tilbakemeldingsreferanse: 06/2020-0013.

[72] PSD2 fortalepunkt 6

- Behandlingen gjelder medlemmer eller tidligere medlemmer av en stiftelse med politisk, religiøst eller fagforeningsmessig formål og utføres av denne stiftelsen, jfr. art. 9 (2)(d).
- Behandling av opplysninger det er åpenbart at den registrerte har offentliggjort, jfr. art. 9 (2)(e).
- Behandling for å fastsette eller forsvare et rettskrav, jfr. art. 9 (2)(f).
- Behandlingen er nødvendig for viktige allmenne interesser, jfr. art. 9 (2)(g).
- Behandling i forbindelse med forebyggende arbeidsmedisin for å vurdere arbeidstakers arbeidskapasitet, jfr. art. 9 (2)(h).
- Behandlingen er nødvendig av allmenne folkehelsehensyn, jfr. art. 9 (2)(i).
- Behandlingen er nødvendig for arkivformål i allmennhetens interesse, jfr. art. 9 (2)(j).

Av de ti behandlingsgrunnlagene som følger av artikkel 9 annet ledd er det bokstav (g), «nødvendig for viktige allmenne interesser», som fremstår som det eneste mulige behandlingsgrunnlaget for sensitiv silent party data. Derfor vil de øvrige behandlingsgrunnlagene ikke gjennomgås nærmere.

## 5.3 Behandling er nødvendig av hensyn til viktige allmenne interesser jfr. art. 9 (2) (g)

Som nevnt i forrige punkt, fremstår art. 9 (2) (g) som det eneste mulige behandlingsgrunnlaget for behandling av sensitiv silent party data. Etter art. 9 (2) (g) kan sensitive personopplysninger behandles når:

> *«Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser»*

Spørsmålet er om behandling av silent party data kan være «nødvendig av hensyn til viktige allmenne interesser» og hvorvidt det kan påvises et rettslig grunnlag i unionsretten eller medlemsstatens nasjonale rett som oppfyller bestemmelsens krav.

For det første må det foretas en vurdering av om behandling av silent party data kan oppfylle viktige allmenne interesser. For det andre må det foreligge et rettslig grunnlag for slik behandling i unionsretten eller medlemsstatens nasjonale rett. Deretter må det foretas en vurdering av om det aktuelle rettslige grunnlaget oppfyller de kravene artikkelen oppstiller til proporsjonalitet, forenelighet med forordningens grunnleggende rettigheter og krav til å sikre tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

Artikkel 29-gruppen har uttalt at unntakene i den tidligere artikkel 8, som i all hovedsak er videreført i artikkel 9, skal tolkes begrensende, uttømmende og snevert.[73] For den videre vurderingen har dette den betydningen at behandlingsgrunnlagene opplistet i art. 9 nr. 2 skal tolkes begrensende og snevert, noe som også gjelder for art. 9 nr. 2 (g).

I retningslinje 06/2020 har EDPB uttalt at et uttrykkelig samtykke, jfr. art. 9 (2) (a), og viktige allmenne interesser art. 9 (2) (g) er de eneste mulige behandlingsgrunnlagene for behandling av sensitive personvernopplysninger i forbindelse med en betalingstjeneste. Art. 9 nr. (2) (a) kan ikke anvendes ved behandling av silent party data ettersom betalingstjenesteyteren ikke har behandlingsgrunnlag for å samle inn og behandle slike personopplysninger.[74]

Angående anvendelsen av art. 9 (2) (g), gir EDPB ingen nærmere veiledning enn følgende: «Payment services may process special categories personal data for reasons of substantial public interests, but only when all the conditions of Article 9 (2) (g) of the GDPR are met». Dette tilsier at den enkelte rettsanvender må vurdere hvorvidt vilkårene etter art. 9 (2) (g) er oppfylte.

### 5.3.1 Viktige allmenne interesser

Det første vilkåret etter art. 9 (2) (g) er at behandling av silent party data må være «nødvendig av hensyn til viktige allmenne interesser»

En naturlig språklig forståelse av «allmenne interesser» tilsier at formålet med behandlingen må være å oppfylle et samfunnsmessig behov. Ordlyden kan også tolkes som at behandlingen

[73] Artikkel 29-gruppen, *«working document on the processing of personal data relating to health in electronic health records",* adopted on 15 February 2007, WP 131 s. 8.

[74] Retningslinje 06/2020 s. 16 avsn. 49.

må være av interesse for den offentlig myndighet. I tillegg tilsier ordlyden av «viktige» at det er satt en høy terskel for hvilke allmenne interesser som kan begrunne behandling av sensitive personopplysninger. Dette underbygges av at behandlingsgrunnlagene er unntak fra forbudet nedfelt i art. 9 første ledd og Artikkel-29 gruppens uttalelse om at vilkårene skal tolkes strengt.

I den juridiske teorien har det blitt argumentert for at art. 9 (2) (g) er en sikkerhetsventil som åpner for behandling der ingen av de andre opplistede behandlingsgrunnlagene etter art. 9 nr. 2 gir grunnlag for behandling av personopplysninger, men hvor klart samfunnsmessige behov tilsier at enkelte personopplysninger må behandles.[75] Skullerud m.fl. bruker som eksempel at dersom GDPR var trådt i kraft i 2011, ville trolig 22. juli-kommisjonen hatt behandlingsgrunnlag etter art. 9 nr. 2 (g) for å få tilgang til ofrenes personopplysninger med det formål å gjennomføre granskningen etter terrorangrepet.[76]

Det følger av PSD2s fortalepunkt 5 at «fortsatt utvikling av et integrert indre marked for sikker elektronisk betaling (...) avgjørende for å støtte veksten i Unionens økonomi». I fortalepunkt 7 fremheves det at «[b]etalingstjenester er avgjørende for grunnleggende økonomiske og sosiale aktiviteters virkeområde». Behandling av silent party data vil, som tidligere nevnt, føre til enklere og mer effektiv pengeoverføring, noe som vil gjøre betalingstjenester mer attraktive og tilrettelegge for økt konkurranse mellom betalingstjenesteyterne. På denne måten kan behandling av silent party data ha en viktig samfunnsmessig funksjon og bidra til å utvikle det indre marked. Dette vil bidra til å styrke formålet med PSD2 og trekker i retning av at behandling av silent party data kan være nødvendig av hensyn til «viktige allmenne interesser».

Videre er det verdt å bemerke at det stilles en rekke sikkerhetskrav til betalingstjenesteyteren. Etter PSD2 artikkel 11 må alle betalingstjenesteytere ha tillatelse for å kunne yte betalingstjenester. Tillatelsen kan også trekkes tilbake dersom det er nødvendig, jfr. art. 13. I tillegg må alle alminnelige prinsipper etter GDPR art. 5 nr. 1 følges ved behandling av personopplysninger. Dette er tydeliggjort i art. 24 (1) hvor det fremgår at betalingstjenestens tjenester må ytes i samsvar med de krav som stilles etter forordningen og sørge for at

[75] Skullerud m.fl 2019, s. 211.

[76] Ibid.

tjenesten er oppdatert. Disse bestemmelsene viser at betalingstjenesteyteren er underlagt kontroll og kan sanksjoneres dersom kravene til sikkerhet ikke etterleves. Dette trekker i retning av at behandling av silent party data kan være nødvendig av hensyn til «viktige allmenne interesser».

På den andre siden fremgår det av GDPRs fortalepunkt 7 at «fysiske personer bør ha kontroll over egne personopplysninger». Den stadige utviklingen og økende bruken av betalingstjenester har den betydning at dersom betalingstjenestene kan behandle personopplysninger fra personer som ikke er brukere av tjenesten, vil det medføre en stor risiko for at forbrukere mister kontrollen over sine egne personopplysninger. Behandling av silent party data kan være i strid med et av formålene med GDPR, og trekker i retning av at behandling av silent party data ikke er nødvendig av hensyn til «viktige allmenne interesser».

I retningslinje 06/2020 påpeker EDPB at brudd på vernet av finansielle personopplysninger vil ha en alvorlig innvirkning av den registrertes liv.[77] Som illustrert i punkt 5.2, kan betalingstransaksjoner potensielt avsløre sensitive personopplysninger. Den store innvirkningen det kan ha på en persons liv dersom finansielle personopplysninger kommer på avveie, sammenholdt med den økte bruken og utviklingen av betalingstjenester, trekker til sammen i retning av at behandling av silent party data ikke er nødvendig av hensyn til «viktige allmenne interesser».

Som tidligere nevnt, tilsier ordlyden av bestemmelsen at det foreligger en høy terskel for anvendelse av art. 9 nr. 2 (g). Det er vanskelig å trekke noen konklusjoner om hvor den konkrete terskelen ligger, og om de fordelene behandling av silent party data kan medføre, når opp til den gitte terskelen. Ettersom EDPB selv har foreslått at art. 9 nr. 2 (g) kan anvendes som behandlingsgrunnlag for silent party data, kan dette imidlertid være avgjørende for å anse vilkåret som oppfylt.

[77] Retningslinje 06/2020 avsn. 68

### 5.3.2 Supplerende rettslig grunnlag i unionsretten eller medlemsstatens nasjonale rett

I tillegg til at behandlingen må være nødvendig av hensyn til en viktig allmenn interesse, må behandlingen av sensitive opplysninger ha en rettslig forpliktelse *«[...] i unionsretten eller medlemsstatenes nasjonale rett».*

I tillegg må den rettslige forpliktelsen «[...] *stå i et rimelig forhold til det mål som søkes oppnådd, være forenelig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser».*

Ordlyden tilsier at det må foretas en proporsjonalitetsvurdering av den plikt som følger av det rettslige grunnlaget i unionsretten eller medlemsstatens nasjonale rett og behandlingsformålet. I tillegg må den rettslige forpliktelsen være forenelig med den registrertes rettigheter etter forordningen og den burde gi angi konkrete tiltak for sikre disse. Dette avhenger av en konkret vurdering av det aktuelle rettslige grunnlaget.

Forordningen gir ingen veiledning om hvordan denne vurderingen skal gjøres eller hva som inngår som grunnleggende innhold i retten til personvern.[78]

Etter GDPR artikkel 6 stilles det, som tidligere nevnt i punkt 4.4, to krav til hva som kan utgjøre en rettslig forpliktelse. For det første må grunnlaget forutsette behandling av personopplysninger jfr. art. 6 nr. 3. For det andre må forpliktelsen være tilstrekkelig tydelig og presist, slik at anvendelsen av det rettslige grunnlaget er forutsigbar for den registrerte, jfr. GDPRs fortalepunkt 41.

En kontekstuell tolkning av GDPR artikkel 9 kan tale for at det må stilles strengere krav til hva som kan være egnet som rettslig grunnlag, enn kravet til rettslig grunnlag etter artikkel 6 nr. 3. Dette er også en naturlig konsekvens av at art. 9 nr. 2 (g) er et unntak fra hovedregelen om at sensitive opplysninger ikke skal behandles. Denne tolkningen støttes også av juridisk

[78] Öman, 2019 s. 251.

teori. Skullerud m.fl. påpeker at legalitetsprinsippet tilsier at kravet til rettslig grunnlag skjerpes for behandling av sensitive opplysninger.[79]

Svenske myndigheter har imidlertid sett det som lite sannsynlig at en rettslig forpliktelse som kan oppfylle kravene etter artikkel 6, ikke også er i tråd med de grunnleggende rettighetene som følger av forordningen.[80]

Som nevnt i punkt 1.3.1 avgrenser denne avhandlingen mot rettslige forpliktelser i medlemsstatens nasjonale rett. Det vises til diskusjon om hvorvidt PSD2 kan utgjøre et rettslig grunnlag, jfr. punkt 4.4.

# 6 Avsluttende refleksjoner

Oppgaven har undersøkt hvorvidt det foreligger et behandlingsgrunnlag etter GDPR som tredjepartsaktører kan bruke for å behandle silent party data, og eventuelt hvilket grunnlag dette er. Dette er gjort ved å gjennomgå og drøfte de alternativene for behandlingsgrunnlag som følger av GDPR artikkel 6 og 9.

Som nevnt tidligere, trådte GDPR og PSD2 i kraft i 2018. Derfor er rettskildebildet tynt og bærer preg av manglende autoritative kilder. Retningslinjene fra EDPB er dermed et sentralt tolkningselement ved fastleggelsen av de nærmere reglene i GDPR og PSD2.

Oppgavens drøftelse av hvorvidt det foreligger et behandlingsgrunnlag etter GDPR artikkel 6 og 9 for å behandle silent party data, viser at det er et stort behov for tydeligere og mer konkrete retningslinjer fra EDPB angående denne problemstillingen.

Kunnskap om teknologien rundt en betalingstjeneste er viktig for å kunne drøfte problemstillinger rundt samspillet mellom GDPR og PSD2. Problemstillingen som drøftes i punkt 5.1. illustrerer at innspill fra profesjonelle aktører er verdifulle og nødvendige for å klarlegge hvilke løsninger som lar seg gjennomføre. EDPB har i retningslinje 06/2020 uttalt at en betalingstjeneste må ha en måte å filtrere ut sensitive opplysninger på, mens aktører fra

[79] Skullerud m.fl 2019, s. 211

[80] Prop 2017/18:105 s.84 referert til i Öman, 2019 s. 251

bransjen påpeker at dette er umulig fordi det ikke finnes en slik teknologi, og fordi dette ikke vil være praktisk for betalingstjenestene dersom teknologien hadde fantes. Drøftelsen illustrerer også at det i dag ikke er mulig å behandle silent party data uten at den behandlingsansvarlige kan påvise et behandlingsgrunnlag etter både art. 6 og 9.

Videre er det behov for en avklaring fra EDPB av om PSD2 kan utgjøre en rettslig forpliktelse, jfr. art. 6 nr. 1 (c), herunder om artiklene 48, 49, 57 og 58 er ment å forutsette behandling av silent party data. I retningslinje 06/2020 har EDPB klart lagt til grunn at PSD2 art. 66 (1) og 67 (1) utgjør det rettslige grunnlaget for kontotilbyders plikt til å gi personopplysninger til tredjepartsaktører. Derfor er det interessant at EDPB ikke har nevnt noe om å bruke PSD2 som rettslig grunnlag for behandling av silent party data.

Behandling av silent party data etter art. 6 nr. 1 (f) reiser flere spørsmål om teknologi og hvordan betalingstjenesten faktisk er utviklet. Det er behov for innspill og avklaring fra betalingstjenesteytere eller andre aktører som har detaljkunnskap om hvor lenge det er nødvendig å lagre silent party data, og om det er nødvendig å lagre slike opplysninger i det hele tatt. I lys av de problemstillingene som reises, er det behov for en mer detaljert avklaring fra EDPBs angående hvordan art. 6 nr. 1 (f) best burde vurderes.

Til slutt er det behov for en avklaring av hvor terskelen for hva som kan anses som viktige allmenne interesser, jfr. art. 9 nr. 2 (g), burde settes. Hensynet til en ensartet anvendelse og tolkning av GDPR, tilsier at terskelen ikke burde settes av den enkelt rettsanvender, men at betalingstjenestemarkedet burde operere med en tilnærmet lik terskel. Uten en slik avklaring fra EDPB, vil det være for risikabelt å for dagens betalingstjenesteytere å behandle silent party data.

Som oppgaven viser, er det behov for avklaring og tydeliggjøring fra EDPB på flere punkter. Ved overtredelse av artikkel 5, 6 eller 9 kan et foretak ilegges et overtredelsesgebyr på opptil 20 millioner euro eller opptil 4 prosent av foretakets globale årsomsetning i forutgående regnskapsår, jfr. GDPR art. 83 (5) (a). Dette understreker at betalingstjenesteytere ikke kan operere i uvisshet, og et betalingstjenestemarked i stadig vekst har behov for avklaring.

# 7 Litteraturliste

## 1.1 EU-rett


| | |
|---|---|
| **TEUV** | Traktaten om Den europeiske unions virkeområde (TEUV), consolidated version of the Treaty on the Function of the European Union (TFEU), 26.10. 2012, 2012/C 326/01. |
| **Charter of Fundamental Rights** | Charter of Fundamental Rights of the European Union, 18.12.2000, 2000/C 364/01. |
| **Forordning (EU) 2016/679 [GDPR]** | Europaparlamentets- 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] |
| **Direktiv (EU) 2015/2366 [PSD2]** | Europaparlamentets- 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. |
| **Direktiv (EU) 2007/64/EF [Det første betalingstjenestedirektiv – PSD]** | Europaparlaments- og rådsdirektiv (EU) 2007/64/EF om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om opphevelse av direktiv 97/5/EF. |

### 1.1.1 Veiledninger og retningslinjer fra EDPB, Artikkel 29-gruppen og EDPS

| | |
|---|---|
| **Artikkel 29- gruppen** | *Working document on the processing of personal data relating to health in electronic health records,* adopted on 15 February 2007, WP 131 s. 8.<br><br>Tilgjengelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf |
| **Artikkel 29-gruppen, Opinion 15/2011:** | *Opinion 15/2011 on the definition of consent,* Adopted on 13 July 2011, WP 187 s.7.<br><br>Tilgjengelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf |
| **Artikkel 29-gruppen, Opinion 06/2014:** | *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC,* Adopted on 9 April 2014, WP 217<br><br>Tilgjengelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf |
| **Artikkel 29-gruppen** | *Guidelines on the impltmentation of the court of justice of the european union judgement on «google Spain and inc a, agencia española de protección de datos (AEPB) and Mario Costeja González C-131/12,* adopted on 26 November 2014, WP 225<br><br>Tilgjengelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf |

| | |
|---|---|
| **European Data Protection Board, Retningslinje 06/2020** | *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR version 1.o,* Adopted on 17. July 2020. Version for public consultation. |
| **European Data Protection Board, Brev 5. juli 2018** | *Letter Regarding the PSD2 Directive,* 5. juli 2018<br><br>Tilgjengelig her: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en |
| **European Data Protection Board, Retningslinje 4/2019** | *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* adopted on 13 November 2019. |
| **European Data Protection Board, Retningslinje 2/2019** | *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0,* adopted October 8th 2019. |
| **European Data Protection Supervisor, Opinion 2013** | *Opinion on Payment Services.* Publisert 5. des. 2013. *Opinion 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 2009/110EC and repealing Directive 2007/65/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions,*<br><br>Tilgjengelig her: https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf |

### 1.1.2 Høringssvar til retningslinje 06/2020:

| | |
|---|---|
| **Österreichischer Sparkassenverband** | *Response to EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR,* feedback reference: 06/2020-006*,* publisert 14. september 2020.<br><br>Tilgjengelig her: https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/austrian_savings_banks_association_response_to_edpb_psd2_gdpr_14_09_2020.pdf |
| **Trustly Group AB** | *Response to EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR,* feedback reference: 06/2020-0013, publisert 15. september 2020,<br><br>Tilgjengelig her: https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/trustly_response_to_edpb_consultation_on_interplay_between_psd2_gdpr_15092020.pdf |
| **Sprite + Future Payment Systems Working Group.** | *Response to EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR*, feedback reference: 06/2020-0039, publisert 16. september 2020.<br><br>Tilgjengelig her: https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/comments_on_edpb_guidelines_on_psd2_gdpr_-_final.pdf |

### 1.1.3 Rettspraksis fra EU-domstolen

- Dom av 4. mai 2017, Riga Satiksme, C-13/16, ECLI:EU:C:2017:336
- Dom av 18. oktober 2016, Nikiforidis, C-135/15, ECLI:EU:C:2016:774
- Dom av 6. oktober 1982, CILFIT, C-283/81, ECLI:EU:C:1982:335

## 1.2 Norske lover og forarbeider

| | |
|---|---|
| **Personopplysningsloven** | Lov av 15. Juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) |
| **Lov om endringer i Finansforetaksloven** | Endringslov 23. November 2018 nr. 87. Lov om endringer i Finansforetaksloven mv. (andre betalingstjenestedirektiv) |
| **Prop. 56 LS (2017 - 2018)** | Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernsforordning) i EØS-avtalen. |
| **Prop. 110 L (2017 - 2018)** | Endringer i finansforetaksloven mv. (andre betalingstjenestedirektiv) |

## 1.3 Juridisk litteratur

| | |
|---|---|
| **Dag Wiese Schartum** | *Personvernforordningen – en lærebok*, 1. utgave, Fagbokforlaget, 2020. |
| **Eirik Øsebak, Frank Horntvedt** | «Endrer risikobildet seg som følge av nye betalingsløsninger?», *Praktisk Økonomi og Finans 2019/2*, Årgang 35 s. 122-131. Publisert 03.06.2019. (lest 5. November) |

Tilgjengelig her: https://juridika.no/tidsskrifter/praktisk-økonomi-og-finans/2019/2/artikkel/øsebak

**Fredrik Sejersted, Finn Arnesen, Ole-Andreas Rognstad, Olav Kolstad** — *EØS-rett, 3.* utgave, Universitetsforlaget 2014.

**John Peeters** — «Data Protection in Mobile Wallets», *European Data Protection Law Review.*, nr. 1 2020 s.56 - 65, (lest 21. okt. 2020) DOI: https://doi.org/10.21552/edpl/2020/1/8

**Jon Wessel-Aas og Magnus Ødegaard** — *Personvern – Publisering og behandling av personopplysninger,* 1. utgave, Gyldendal 2018

**Odd Stemsrud** — *EØS-rett i et nøtteskall*, 1. utgave, Gyldendal, 2016

**Sören Öman** — *Dataskyddsförordningen (GDPR) m.m., En kommentar*, 1. utgåva, Norstedts Juridik, 2019.

**Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad, Marius Engh Pellerud** — *Personopplysningsloven og Personvernforordningen (GDPR), kommentarutgave*, 1. utgave, Universitetsforlaget, 2019

## 1.4 Det norske datatilsynet

**Datatilsynet** — Rapport, *Rapport om personlige finanser – hvordan utviklingstrekk i finanssektoren påvirker personvernet, 2018*, Datatilsynet.no (lest 15. september 2020)

Tilgjengelig her:

https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/fintech-og-personvern/

**Datatilsynet** Veileder, B*ehandlingsgrunnlag,* sist endret 08.08.19. (lest 7.12. 20) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/nodvendig-for-a-ivareta-legitime-interesser---interesseavveiing/

**Datatilsynet** "Det europeiske personvernrådet (EDPB)", sist endret 19.07.20 (Lest 2. Desember 2020) Tilgjengelig på: https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/

## 1.5 Internettadresser

- Christoffer Hernæs, «The definitive guide to Open Banking», publisert 7. August 2019, https://hernaes.com/2019/08/07/the-definitive-guide-to-open-banking/ (lest 5. nov. 2020)

- E24, «kirke innfører vipps-betaling av kollekt», publisert 12. mars 2016, https://e24.no/teknologi/i/vmBg8m/kirke-innfoerer-vipps-betaling-av-kollekt#:~:text=Kirken%20er%20den%20første%20i,MobilePay%2C%20som%20konkurrerer%20med%20Vipps, (Lest 4. november 2020)

- Illustrasjon av Open Banking: Ashirwada Dayarathne, *«WSO2 Open Banking to Cater Open Banking and PSD2 requirements»,* publisert 22.10.19