Betalningsutredningen
Statens offentliga utredningar, Fi 2020:12

[Korrigerad version]

Skydd för betaldata på den svenska betalningsmarknaden

En översiktlig kartläggning av regleringen av personuppgifter och finansiell sekretess i relation till betaldata

Setterwalls Advokatbyrå, Niklas Follin och Andreas Löfholm [a]

SW416150422

[a] Rapporten är skriven på uppdrag av Betalningsutredningen. Författarna har självständigt ansvar för rapportens metod, analys och slutsats. De åsikter som uttrycks i denna rapport är författarnas egna.

PROMEMORIA

Skydd för betaldata på den svenska betalningsmarknaden - En översiktlig kartläggning av regleringen av personuppgifter och finansiell sekretess i relation till betaldata

SW41609611/6

STOCKHOLM / GÖTEBORG / MALMÖ
REG.NO: 556774-5772
SÄTE: STOCKHOLM

SETTERWALLS ADVOKATBYRÅ AB
STUREGATAN 10, STOCKHOLM
P.O BOX 1050, SE-101 39 STOCKHOLM

T: +46 8 598 890 00
STOCKHOLM@SETTERWALLS.SE
WWW.SETTERWALLS.SE

SETTERWALLS

SW4160961 1/6

Denna promemoria har upprättats av advokaterna Niklas Follin och Andreas Löfholm, Setterwalls Advokatbyrå, på uppdrag av Betalningsutredningen, genom huvudsekreterare Fredrik Wiklund Bystedt och utredningssekreterare Maia Drangel Wallbrand. Promemorian överlämnades till Betalningsutredningen den 3 december 2021.

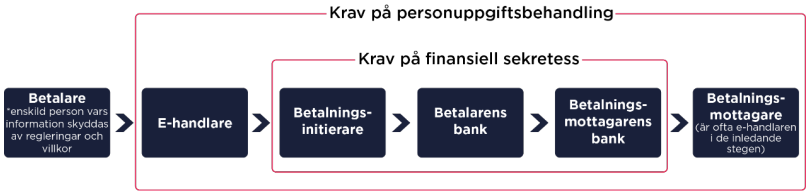
SETTERWALLS

1. Sammanfattning

Hantering av betaldata omfattas av både dataskyddslagstiftning samt lagstiftning om finansiell sekretess. Dessa regelverk innebär betydande krav och villkor för olika aktörers nyttjande av betaldata.

Reglerna om dataskydd och om finansiell sekretess kompletterar och överlappar varandra. Som framgår av bilden nedan är området för den finansiella sekretessen emellertid snävare.

Figur 1: Översikt över betaldata i ett förenklat betalflöde.



Vad gäller dataskyddslagstiftningen måste aktörer som behandlar betaldata i princip alltid uppfylla de krav som ställs enligt dataskyddsförordningen, bland annat innefattande att de måste ha ett på förhand tydligt angivet ändamål och en rättslig grund för sin personuppgiftsbehandling. Betaltjänstleverantörer måste dessutom, utifrån de krav som gäller med utgångspunkt i betaltjänstlagen, uppfylla särskilda krav för den personuppgiftsbehandling som sker i relation till betaltjänsterna. Dessa dataskyddsregler begränsar sammantaget möjligheterna att vidarenyttja betaldata för andra ändamål än utförande av betaltjänsterna.

Reglerna om finansiell sekretess skyddar uppgifter om en betalares eller betalningsmottagares betaldata, eftersom detta är uppgifter som typiskt sett inryms i en kunds mellanhavanden med ett finansiellt företag (till exempel en bank, betaltjänstleverantör eller utgivare av elektroniska pengar). Finansiella företag som omfattas av regler om finansiell sekretess måste säkerställa att enskildas förhållanden till det finansiella företaget inte obehörigen röjs och utlämnande av betaldata förutsätter således behöriga skäl för att vara tillåten. Den finansiella sekretessen berör i huvudsak tre parter: den enskilde som omfattas av det sekretessbelagda förhållandet, det finansiella företaget som känner till förhållandet och den tredje man som av någon anledning vill få del av uppgifter om förhållandet. Vid bedömning av om ett röjande är behörigt behöver man göra en intresseavvägning mellan dessa tre parters intressen. Den vägledning som finns avseende hur en sådan intresseavvägning ska utföras och bedömas är emellertid begränsad och leder ofta till osäkra bedömningar.

Aggregerad och helt anonymiserad betaldata omfattas varken av reglerna för finansiell sekretess eller av dataskyddslagstiftningen. Detta förutsätter dock att sådan data inte kan hänföras tillbaka till en enskild person. Aggregerad betaldata som inte avser en-

SETTERWALLS

skilda, såsom statistiska uppgifter avseende en större grupp individer, kan därför nyttjas i princip helt fritt och kan vidarenyttjas för andra ändamål eller säljas vidare till tredjeparter.

Sammantaget bedömer vi att det huvudsakliga sekretess- och dataskydd som finns avseende betaldata är förhållandevis gott. Det finns dock behov av att inom betalningsområdet ytterligare se över och förtydliga hur reglering av finansiell sekretess och dataskydd samspelar och ska tillämpas i ett modernt informationssamhälle. Överlappningen mellan de två områdena medför också ett behov av ökad samordning mellan tillsynsmyndigheterna. Beaktat de stora förändringar som skett på betalningsmarknaden med nya aktörer och ökad informationsspridning de senaste åren och den förväntat fortsatt starka utvecklingen på området bör det säkerställas att de aktuella regelverken även över tiden kan tillämpas på ett tydligt, effektivt och rättssäkert sätt.

SW4160961 1/6

SETTERWALLS

2. Bakgrund

2.1 Allmänt

Graden av digitalisering ökar kontinuerligt, såväl i samhället i stort som inom betalmarknaden. Med digitaliseringen kommer även en ökad mängd data som genereras i olika digitala processer och system samt ett ökat intresse för nyttja sådan data.

Digitaliseringen har inom finansbranschen gestaltat sig bland annat genom etableranden av nya företag och tjänster som verkar med innovativa nyttjanden av data, däribland betaldata. Det har även uppkommit nya koncept och regleringar som syftar till att öka möjligheterna för delning och vidareanvändning av betaldata, i synnerhet idéerna kring open banking[1] och reglerna i det andra betaltjänstedirektivet (PSD2)[2].

Det finns flera skäl till denna utveckling och varför man i vissa fall ser positivt på att öppna upp och tillåta vidarenyttjande av betaldata och finansiell data. Bland annat har man i lagstiftningsprocessen uttalat en ambition att åstadkomma en ökad innovation och konkurrens på finansmarknaden och en ökad makt för enskilda att kontrollera och ge tillgång till ”sin” data till andra aktörer (i vissa sammanhang benämnt som dataportabilitet).

Samtidigt förekommer skäl till att man ur andra perspektiv vill begränsa möjligheterna till att få tillgång till och vidarenyttja finansiell data. Sådana skäl avser ofta att man vill säkerställa en bibehållen integritet och konfidentialitet för den enskilde och för de finansiella system som hanterar data, trots ökad tillgång till data. Det kan också finnas intressen hos innehavare av större datamängder att värna sin egen kontroll över datan och därigenom värna sin egen marknadsposition - då datan kan har ett stort värde för innehavaren, både rent ekonomiskt (vilket man inte vill ge bort) och ett värde ur ett konkurrenshänseende. Dessa aspekter kan resultera i ett minskat möjliggörande av tillgång och vidarenyttjande av data.

Som ett exempel på det ökade värdet av data och dessa olika intressen har EU särskilt identifierat dataekonomin och värdet respektive skyddet av data som strategiska hörnpelare för den gemensamma inre marknaden och för EU:s övergripande arbete de kommande åren.[3] Likaså har den svenska regeringen identifierat värdet och betydelsen av data i en svensk datastrategi.[4] Såväl på Europeisk som på nationell nivå sker därför flera olika initiativ avseende nyttjande och skydd av data, både generellt och inom särskilda sektorer så som den finansiella sektorn[5].

[1] Begreppet open banking är inte tydligt definierat, men kan generellt beskrivas som *en process för banker och andra finansiella institutioner för att öppna upp tillgång till institutionens data för externa aktörers tillgång vidarenyttjande och vidaredelning*.
[2] Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden.
[3] En EU-strategi för data, EU-kommissionen, kommunicerad den 19 februari 2020.
[4] Data – en underutnyttjad resurs för Sverige: En strategi för ökad tillgång av data för bl.a. artificiell intelligens och digital innovation, Bilaga till beslut II 5 vid regeringssammanträde den 20 oktober 2021, I2021/02739.
[5] IMY Integritetsskyddsrapport 2020 s. 11 och 43: Se t.ex. genomförandet av andra PSD2, initiativet med e-kronan och EU:s datastrategi för att underlätta innovation och datadriven utveckling inom exempelvis den finansiella sektorn.

SETTERWALLS

2.2 Betalningsutredningens behov

En av Betalningsutredningens uppgifter är att analysera och kartlägga säkerhets- och integritetsaspekter av såväl privata som statliga digitala betalningssystem. Under arbetet med denna kartläggning har det dykt upp frågor kring vad den enskilde har för integritetsskydd vid genomförande av olika typer av betalningar hos olika typer av aktörer idag. Utredningen ser därför behov av att närmare utreda, utifrån gällande rätt, hur skyddet för den enskilde betalarens/betalningsmottagarens betaldata ser ut idag och vilka möjligheter olika aktörer på marknaden har att använda sig av sådan betaldata.

2.3 Setterwalls uppdrag

Setterwalls har uppdragits att göra en översiktlig och övergripande kartläggning av de ovan nämnda aspekterna utifrån gällande rätt, med fokus på personuppgiftsreglering och finansregulatoriska regleringen (primärt avseende finansiell sekretess) av betaltjänster.

Med begreppet betaldata avses i denna promemoria all information som följer med en betalning från en betalare, i tillämpliga fall via betalarens och betalningsmottagarens betaltjänstleverantörer, till en betalningsmottagare. Betaldata omfattar information som i tillämpliga fall enligt EU-förordningen 2015/847 om uppgifter som ska åtfölja överföringar av medel (till exempel namn och betalkontonummer för betalare och betalningsmottagare) samt annan information som behandlas vid en betalning, inkluderat information om institut eller aktörer som medverkar i betalningskedjan.

Betaldata kan således omfatta även sådana data som indirekt avser en person i betalningskedjan, även om det inte direkt avser själva betalningen. Detta kan röra sig om metadata[6], aggregerad data[7] eller annan information om den enskildes förhållanden. En följd av denna definition är att innehållet i begreppet betaldata kan variera, beroende på aktör och vilken behandling som sker.

Mot denna bakgrund har vi upprättat denna sammanställning och härvid uppställt följande huvudfrågeställningar att besvaras i promemorian:

(i) Vilka regelverk gäller för skydd och användande av betaldata och därtill relaterade personuppgifter?

(ii) Vilket huvudsakligt skydd respektive vilka huvudsakliga villkor gäller för användande av betaldata?

(iii) Hur får betaldata aggregeras/anonymiseras respektive hur får sådan aggregerad/anonym information användas?

Vi har i arbetet med denna promemoria utgått från ett typupplägg där betaldata delas mellan olika aktörer i en betalningskedja. Detta typupplägg avser en e-handelssituation

[6] Metadata avser information om annan data och kan i betalningssammanhang exempelvis avse information om avsändande bank, referensnummer till betalningen eller liknande uppgifter.
[7] Aggregerad data avser ihopsamlad data, t.ex. statistikuppgifter.

SETTERWALLS

med följande huvudsakliga aktörer: den enskilda betalaren[8], e-handlaren, betalningsinitieringsleverantör[9] (betaltjänstleverantör), betalarens bank, betalningsmottagarens bank och betalningsmottagaren. Till denna skara aktörer kan även ytterligare de tredjepartsleverantörer som definieras särskilt i betaltjänstlagen (betalningsinitieringstjänster - PISP och kontoinformationstjänster[10] – AISP) inkluderas. Vi berör de olika aktörerna i detta typupplägg där det är relevant för framställningen.

Det ska noteras att det finns ett mycket stort antal olika upplägg där betaldata används. Vår övergripande analys och slutsatser torde dock i huvudsak vara tillämplig även på sådana upplägg.

2.4 Avgränsningar

Promemorian riktas till en allmän läsarkrets som, även om den kan vara professionellt aktiv på området, inte har djupare kunskaper om de rättsliga reglerna avseende personuppgiftsskydd eller finansiell sekretess. Vår ambition är därför att ge en översiktlig bild av reglerna om skydd och villkor för vidarenyttjande av betaldata, samtidigt som vi gör lagom detaljerade nedslag i de tillämpliga reglerna.

På grund av denna begränsning kommer vi inte att beröra angränsande aktörer, behandlingar eller regleringar i någon större omfattning. Således kommer vi inte att gå in på exempelvis regleringar avseende marknadsföring eller konsumentskydd, vilket nyligen har uppmärksammats som en viktig aspekt avseende konsumentkrediter[11], eller på de bakomliggande aktörerna i betalkedjan som inte är primärt synliga för den enskilda (såsom de aktörer som hanterar clearing och avveckling). Vi kommer inte heller att behandla de krav och regler som gäller för andra personuppgiftsbehandlingar än de som anges häri, till exempel avseende behandling av relaterade uppgifter som inte utgör betaldata (vi kommer dock att beröra vissa aspekter i ett jämförande exempel avseende vidarenyttjande av personuppgifter).

SW41609611/6

[8] Även om analysen utgår från en fysisk person som enskild betalare så gäller dessa aspekter, åtminstone avseende finansiell sekretess, i viss mån även juridiska personers betalningar.
[9] En betalningsinitieringstjänst används för att initiera en betalningsorder på begäran av en användare som har ett betalkonto hos en betaltjänstleverantör, se definition i artikel 4.15 i PSD2 samt 1 kap. 4 § betaltjänstlagen.
[10] En kontoinformationstjänst är en tjänst som sammanställer information från olika betalkonton tillhörande en betaltjänstanvändare, se definition i artikel 4.16 i PSD2 samt 1 kap. 4 § betaltjänstlagen.
[11] Se t.ex. Svenska Dagbladets artikelserie om marknadsföring av konsumentkrediter, september-oktober 2021.

SETTERWALLS

3. Skydd och villkor för behandling av personuppgifter

3.1 Allmänt om dataskyddsförordningen

I denna del redogör vi för skyddet för den enskilde betalarens/betalningsmottagarens betaldata och vilka möjligheter olika aktörer på marknaden har att använda sig av sådan betaldata ur ett dataskyddsperspektiv.

Behandling av personuppgifter regleras i Sverige huvudsakligen genom EU:s dataskyddsförordning[12] (även känd som GDPR) samt de olika kompletterande regleringarna i svenska dataskyddslagen[13] och den svenska kompletteringsförordningen.[14] Därutöver finns det ett stort antal föreskrifter, rekommendationer, riktlinjer och vägledningar som utgetts av den svenska Integritetsskyddsmyndigheten (IMY) samt den Europeiska dataskyddsstyrelsen (EDPB) (och i viss mån inkluderat dess föregångare, artikel 29-gruppen). Dataskyddsförordningen är generellt tillämplig i det avseendet att den tillämpas på i princip all databehandling som innefattar behandling av personuppgifter.[15] Förordningen är samtidigt också mycket specifik i den bemärkelsen att regelverket innehåller mycket detaljerade regleringar om krav och villkor för hur personuppgifter får behandlas.

Det europeiska dataskyddet och tillhörande regleringar avseende personuppgiftsbehandling syftar till att skydda mänskliga rättigheter och grundläggande friheter, i synnerhet rätten till privatliv och integritet. Dataskyddsförordningen har två uttalade syften, dels att skydda fysiska personer vid behandling av deras personuppgifter, och på så vis stärka de enskildas rättigheter, dels att säkerställa ett fritt flöde av personuppgifter inom EU (vilket ska ses som en harmoniseringssträvan och inte ska missuppfattas som en ambition om obegränsad tillgång eller användande av personuppgifter).[16] Bestämmelserna i dataskyddsförordningen ska således ses som en skyddsreglering som kompletterar bland annat Europakonventionen[17], EU:s stadga om de grundläggande rättigheterna[18], Fördraget om Europeiska Unionens funktionssätt[19] och Regeringsformen.[20]

Dataskyddsförordningen är en generell lagstiftning som är allmänt tillämplig inom EU och EES. Förordningens regler kompletteras på olika sätt av nationell och unionsrättslig reglering genom antingen direkta hänvisningar till personuppgiftsregleringen eller mer indirekt, genom att den rättsliga grund som ska tillämpas för personuppgiftsbehandling enligt dataskyddsförordningen kan anges eller specificeras i annan lag. Detta innebär att lagstiftning som uppställer särskilda villkor avseende skydd eller föreskriver

[12] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[13] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[14] Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[15] Öman, Dataskyddsförordningen (GDPR) m.m. en kommentar, Norstedts juridik s. 65.
[16] Öman Dataskyddsförordningen s. 29. Se även skäl 1 och 2 dataskyddsförordningen och Törngren, m.fl., Juno kommentar till artikel 1 dataskyddsförordningen 13/3 2019.
[17] Se art. 8.1 i Europeiska konventionen om skydd för de mänskliga rättigheterna avseende rätt till respekt för privatliv och korrespondens.
[18] Se art. 8 i Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02) avseende skydd för personuppgifter.
[19] Se art. 16 i fördraget om Europeiska unionens funktionssätt (2012/C 326/01) avseende rätt till skydd av personuppgifter.
[20] Se 2 kap. 6 § i Regeringsformen avseende skydd mot intrång i den personliga integriteten.

särskilda åtgärder eller anger att dataskyddsreglerna ska tillämpas på specifika sätt således direkt eller indirekt får betydelse för hur dataskyddsreglerna sedan ska tillämpas. Ett exempel på sådan kompletterande reglering avseende behandling av betaldata är reglerna för anti-penningtvätt och sekretess, vilka både föreskriver att viss behandling ska ske (penningtvättskontroll) och uppställer särskilda begränsningar och villkor (lagstadgad och straffsanktionerad tystnadsplikt). Vi berör vidare samspelet mellan dataskyddsförordningen och betaltjänstlagen under avsnitt 3.3 nedan.

Eftersom dataskyddsförordningen tillämpas generellt gäller den i princip för samtliga aktörer som utför någon åtgärd med betaldata inom en betalningskedja (med undantag för den enskilde). De generella kraven i dataskyddsförordningen tillämpas också förhållandevis lika[21] på alla sådana aktörer, där eventuella skillnader i hur kraven tillämpas främst beror på skillnader i vilka behandlingar som utförs eller om det föreligger kompletterande lagstiftning som träffar aktörerna olika. Vi gör av denna anledning inte någon skillnad på de olika aktörerna i en betalkedja utan beskriver dataskyddsreglerna generellt i detta avsnitt.

Dataskyddsförordningen tillämpas på behandlingar av personuppgifter, så som dessa definieras enligt dataskyddsförordningen. Vilken reglering som tillämpas på innehållet i betaldata är således delvis beroende av om och i vilken grad informationen kan anses utgöra personuppgifter enligt dataskyddsförordningens definition.

Enligt artikel 4 i dataskyddsförordningen är personuppgifter definierade som uppgifter som *direkt* avser en fysisk person och uppgifter som *indirekt* kan hänföras till en fysisk person, alltså uppgifter genom vilka en person kan identifieras. Detta innebär att det antingen går att identifiera personen direkt genom uppgifterna[22] eller att personen går att indirekt identifieras genom användande av ”*hjälpmedel*”, vilket kan utgöras av ytterligare uppgifter eller tekniska hjälpmedel.[23] Det avgörande för om en fysisk person är identifierbar är om hjälpmedel med *rimlig sannolikhet* kan komma att användas för identifiering.

Vid bedömningen av om en person är identifierbar ska samtliga objektiva faktorer beaktas; innefattande såväl kostnader och tidsåtgång som tillgänglig teknik och den tekniska utvecklingen. Om det är rimligt sannolikt att en fysisk person kan identifieras med användande av ytterligare uppgifter eller tekniska hjälpmedel, beaktat den tillgängliga tekniken och de kostnader och arbetsinsatser som krävs för identifiering, så är det alltså fråga om personuppgifter.[24] Det krävs i praktiken inte mycket för att det ska anses möjligt att identifiera en person och således rör det sig ofta om personuppgifter, även i fall då informationen till synes kan verka avidentifierad.

Det krävs inte att innehavaren av personuppgifterna eller den som bestämmer över dessa har tillgång till alla uppgifter eller hjälpmedel som krävs för identifiering, utan

[21] Olika krav gäller dock enligt dataskyddsförordningen om en aktör agerar som personuppgiftsansvarig eller personuppgiftsbiträde (som är en slags underleverantörsroll enligt dataskyddsförordningen). Vi går dock inte in närmare på dessa aspekter.
[22] Detta avser huvudsakligen uppgifter som innehåller identifierare, såsom namn, personnummer, identifikationsnummer, onlineidentifikatorer eller faktorer som är specifika för personens identitet. Se vidare skäl 30 i dataskyddsförordningen.
[23] Alla tillgängliga hjälpmedel ska beaktas, se vidare skäl 26 i dataskyddsförordningen.
[24] Notera att denna sannolikhetsbedömning i praxis har visat sig vara lätt att uppfylla med följd av att det ofta är fråga om personuppgifter, se vidare nedan.

SETTERWALLS

det *räcker att någon annan har faktiska eller legala möjligheter att identifiera* de aktuella fysiska personerna. Som exempel kan anges att krypterade uppgifter, dynamiska IP-adresser[25], metadata, ofullständiga (hashade) kontokortsuppgifter eller numrerade resekort har ansetts utgöra personuppgifter.[26] Alltså kan uppgifter anses vara personuppgifter även om innehavaren av uppgifterna inte själv kan härleda identiteten.

Sammantaget innebär detta att definitionen av personuppgifter är mycket bred, vilket medför att dataskyddsreglerna tillämpas i mycket stor omfattning och över många olika områden. Som utgångspunkt kan det antas att större delen av all betaldata, inklusive metadata och kodade eller krypterade uppgifter, ska anses vara personuppgifter. Den enda sorts betaldata som med säkerhet kan sägas inte utgör personuppgifter är aggregerad betaldata som har anonymiserats på en sådan nivå att uppgifterna inte på något sätt går att härleda till en enskild person (detta kan dock vara svårt, se mer om anonymisering nedan).

Således utgör dataskyddsförordningen en grundläggande reglering för i princip all hantering av betaldata. Dataskyddsförordningens allmänna krav och villkor avseende skydd och nyttjande av betaldata ska således tillämpas på alla aktörer i en betalningskedja (med undantag för de enskilda individerna), oavsett om de agerar under finansiellt tillstånd eller inte - dock kan tillämplig finansreglering få följder på hur personuppgiftsreglerna tillämpas.

3.2 Villkor för personuppgiftbehandling

Dataskyddsförordningen innefattar omfattande krav och villkor avseende hur personuppgifter får behandlas. Vi kan inom ramen för denna promemoria inte belysa alla dataskyddsförordningens regler och krav vad avser personuppgiftsbehandling. Fokus kommer istället att vara på de viktigaste reglerna för skyddet för betaldata och reglerna som möjliggör för olika aktörer att använda sig av betaldata. De krav som vi således kommer att ta upp är dels att det måste finnas ett på förhand specifikt angivet ändamål avseende behandlingen (så kallad *ändamålsbegränsning*) och dels att det måste finnas specifik *rättslig grund* för behandlingen (utav de möjliga grunder som listas i dataskyddsförordningen).

Ändamålsbegränsning innebär ett krav att personuppgifter endast får behandlas enligt på förhand specificerade, uttryckligt angivna och legitima ändamål. Att ha ett tydligt utryckt ändamål är ett självständigt och nödvändigt steg inför en personuppgiftsbehandling - men kravet på ett på förhand angivet ändamål får också en indirekt inverkan på vilken rättslig grund som kan vara tillämplig, eftersom de rättsliga grunderna ofta är kopplade just till ändamålet med en behandling. Syftet med kravet på ett tydligt ändamål är att det ska på förhand vara klart för både den enskilde och den som behandlar uppgifterna vilka behandlingar som ska ske och varför (dessa måste också vara berättigade) samt att det inte ska vara möjligt att brett samla in personuppgifter för ändamål som man kommer på eller ändrar till först senare. En praktisk följd av detta är att ända-

SW41609611/6

[25] Dynamiska IP-adresser skiljer sig från vanliga IP-adresser i den bemärkelsen att adressen ändras vid varje anslutning till internet.
[26] Se t.ex. EU-domstolens domar i C-582/14 Breyer och C-434/16 Nowak.

SETTERWALLS

målsbegränsningen innebär ett tydligt hinder avseende oväntade, dolda eller otillbörliga vidarenyttjanden av personuppgifter och det utgör på så sätt en begränsning för hur betaldata kan vidarenyttjas.

Kravet på rättslig grund innebär att personuppgiftsbehandlingen måste stödjas på en av de rättsliga grunder som anges i dataskyddsförordningen, enligt en uttömmande uppräkning över vilka grunder som en personuppgiftsbehandling kan baseras på. Om det inte finns någon tillämplig rättslig grund för en viss personuppgiftsbehandling så får behandlingen således inte utföras. De rättsliga grunder som är av mest intresse för skyddet för betaldata och vilka möjligheter olika aktörer på marknaden har att använda sig av sådan betaldata är följande;

(i) om den registrerade har *samtyckt* till behandling, eller

(ii) om behandlingen görs för att *fullgöra ett avtal* mellan den registrerade och tjänsteleverantör, eller

(iii) om det föreligger en *rättslig förpliktelse* att behandla personuppgifterna i någon annan reglering än dataskyddsförordningen, eller

(iv) *den personuppgiftsansvariges eller en tredje parts berättigade intresse* av en behandling väger lika tungt som eller tyngre än den registrerades intresse av integritetsskydd (så kallad intresseavvägning).

Avseende samtycke till personuppgiftsbehandling uppställs flera krav som ska uppfyllas för att ett samtycke ska vara giltigt, särskilt: (a) samtycket ska vara frivilligt, specifikt, informerat och otvetydigt; och (b) samtycket ska vara möjligt att återkalla när som helst, varpå behandlingen som grundas på samtycket ska upphöra.[27] Samtycken som inte uppfyller dessa krav fullt ut är ogiltiga och kan inte användas som rättslig grund för personuppgiftsbehandlingen.

Dessa krav innebär bland annat att den enskilda inte får påverkas i sitt fria val att ge sitt samtycke eller drabbas av negativa konsekvenser om samtycke inte ges. En begäran om samtycke för personuppgiftebehandling måste kunna också kunna särskiljas från andra frågor och får inte buntas samman med andra godkännanden. Följaktligen innebär detta, som exempel, att allmänna villkor i vilka det anges att personuppgifter kommer behandlas och där det anges att det genom godkännande av villkoren sker ett samtidigt godkännande av personuppgiftsbehandlingen, inte kan utgöra ett giltigt samtycke för personuppgiftsbehandling. Samtycke kan inte heller ges som motprestation för en tjänst, där tjänsten inte levereras om samtycke inte ges.[28] Av dessa skäl är oftast andra grunder mer lämpliga för verksamheter som vill behandla personuppgifter.

Om personuppgiftsbehandling är nödvändig för att fullgöra ett avtal med den registrerade kan detta utgöra en rättslig grund för behandlingen så länge behandlingen är objektivt och strikt nödvändigt för fullgörandet av de centrala avtalsförpliktelserna. Denna rättsliga grund möjliggör således utförandet av de centrala åtgärder som omfattas av en avtalad tjänsteleverans, men den medger inte behandlingar som objektivt inte

[27] Artikel 7 i dataskyddsförordningen.
[28] EDPB riktlinjer 05/2020 om samtycke.

kan anses nödvändiga bara för att dessa kan ha angetts i avtalet. En leverantör kan således inte ensidigt föra in perifera behandlingar i avtalet och nyttja detta som en rättslig grund för denna behandling – vilket exempelvis kan innebära att vidarenyttjanden inte skulle kunna baseras på denna grund.[29] Att fullgöra avtalsförpliktelser torde vara den vanligaste grunden för den behandling som betaltjänsteleverantörer utför när de levererar sina tjänster, men den kan endast omfatta de behandlingar som då är centrala för leverans av betaltjänsten och kan inte omfatta eventuella andra behandlingar, såsom vidarenyttjande för marknadsföringsändamål.

Om en personuppgiftsbehandling är nödvändig för att fullgöra en rättslig förpliktelse som åligger den personuppgiftsansvarige kan detta utgöra en legal grund för personuppgiftsbehandlingen. Detta innebär att åtgärder som är förskrivna i lag eller som utförs för att uppfylla lagkrav kan göras med stöd av denna grund, till exempel personuppgiftsbehandlingar som görs i syfte att utföra kontroller för att uppfylla kundkännedom- och anti-penningtvättsregler. Denna grund omfattar endast den specifika behandlingen som krävs för att den ansvariga ska uppfylla de relevanta rättsliga förpliktelserna och angränsande behandlingar måste baseras på en annan rättslig grund.

Den som har ett berättigat intresse av att behandla personuppgifter kan göra detta om intresset för att behandlingen utförs väger tyngre än det enskilda integritetsintresset. Denna grund kräver att den personuppgiftsansvariga kan visa på en bedömning som bekräftar att intresset för ändamålet med behandlingen överväger den enskildes integritetsintresse. Behandlingen ska även vara legitim och nödvändig för att uppfylla det angivna ändamålet, varför detta måste tydligt anges på förhand (liksom är fallet för de övriga grunderna). Denna grund är vanlig för många olika behandlingar då den utgör en slags generalklausul och innefattar en något större grad av flexibilitet genom intresseavvägningen – dock finns det troligtvis en viss grad av överutnyttjande av grunden, då det är vanligt att man förlitar sig på en intresseavvägning utan att någon tillräcklig bedömning av de motstående intressena har gjorts. Exempel då en intresseavvägning kan användas som rättslig grund för personuppgiftsbehandling är vid direktmarknadsföring eller en e-handlares behandling för att förhindra bedrägerier (förutsatt att sådana behandlingar sker med tillräckligt beaktande av den enskildes integritetsintresse och med uppfyllande av övriga lagkrav).[30]

Sammanfattningsvis kräver varje behandling av personuppgifter att den personuppgiftsansvarige på förhand har definierat ett tydligt ändamål med behandlingen och kopplar detta ändamål till en giltig rättslig grund. Dessa krav begränsar möjligheterna till vidarenyttjanden för andra eller nya ändamål. Detta gäller även när eventuellt senare behandlingar sker av aktörer i senare led, till exempel avseende behandling av betaldata i en betalningskedja. I sådana fall måste de rättsliga grunderna och ändamålen med behandlingar som sker i senare led vara på förhand angivna (och förutsägbara) för den enskilda, innan behandlingarna påbörjas.

[29] EDPB riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade.
[30] Se IMY:s Integritetsskyddsrapport 2020 s. 55.

3.3 Särskilt om dataskyddsreglerna och skyddet av betaldata

Innehållet i betaldata kan vara båda värdefullt och integritetskänsligt, vilket innebär att flera olika intressen måste beaktas när denna information behandlas. Utöver de generella krav som dataskyddsförordningen uppställer för behandling av betaldata så förekommer även sektorspecifik reglering. En sådan för denna promemoria särskilt relevant särreglering utgörs av regleringen av betaltjänstleverantörer.

Betaltjänster regleras inom EU huvudsakligen genom det första respektive andra betaltjänstedirektivet (PSD1 och PSD2). Redan vid PSD1 ansågs det vara nödvändigt att särskilt och uttryckligen reglera betaltjänstleverantörernas möjlighet att behandla personuppgifter i samband med vissa specifika åtgärder: förebyggande, undersökning och avslöjande av betalningsbedrägerier. Dessa personuppgiftsregleringar implementerades sedan i 6 kap i lagen (2010:751) om betaltjänster (”betaltjänstlagen”). Genom PSD2 förtydligades sedan att ”betaltjänstleverantörer ska endast ha tillgång till, behandla och bevara sådana personuppgifter som är nödvändiga för tillhandahållande av betaltjänsterna, med uttryckligt medgivande från betaltjänstanvändaren”.[31] Dessa bestämmelser initierades sedan i 5 kap. 8 och 15 §§ betaltjänstlagen.

Eftersom reglerna i PSD2 och reglerna i dataskyddsförordningen överlappar och samspelar i stor omfattning har EDPB gett ut riktlinjer om förhållandet mellan dataskyddsförordningen och PSD2.[32] I dessa riktlinjer har EDPB särskilt fokuserat på den vidarebehandling som kan ske av tredjepartsleverantörer av betalningstjänster (alltså de tredjepartstjänster som definieras särskilt i PSD2: PISP och AISP) samt på annan behandling av personuppgifter för andra ändamål. Vi berör dessa aspekter närmare nedan.[33]

3.3.1 Vidarebehandling för tredjepartsleverantörer enligt PSD2

Enligt PSD2 föreligger det en rätt för PISP och AISP att få tillgång till och få använda information på betalkonton, förutsatt att ett uttryckligt medgivande för sådan behandling getts av kontoinnehavaren. När betaltjänstleverantörer får tillgång till uppgifter på ett betalkonto hos en kontoförvaltande betaltjänstleverantör (exempelvis en bank) sker huvudsakligen två behandlingar av personuppgifter:

(i) en personuppgiftsbehandling av den kontoförvaltande betaltjänsteleverantören när denna beviljar betaltjänstleverantören tillgång till personuppgifterna och,

(ii) en behandling då betaltjänstleverantören hanterar dessa personuppgifter för det angivna ändamålet.

Eftersom dataskyddsförordningens krav är tillämpliga måste personuppgiftsbehandlingen göras enligt kravet på rättslig grund och de övriga dataskyddsprinciperna.[34] Ändamålet för behandlingen är tillhandahållandet av tjänster enligt PSD2. Den kontoförvaltarende betaltjänsteleverantören kan i regel förlita sig på den rättsliga grunden att det föreligger en ”rättslig förpliktelse” att behandla personuppgifterna. Gällande tillhandahållare av betaltjänster så är det vanligt att dessa förlitar sig på att den rättsliga

[31] Se artikel 94.1 i PSD2.
[32] EDPB riktlinjer 6/2020.
[33] Vi utgår här från PSD2, eftersom EDPB:s uttalanden har gjorts i förhållande till direktivtexten. Slutsatserna är dock tillämpbara i samman utsträckning för den svenska implementeringen av PSD2 i betaltjänstlagen.
[34] EDPB riktlinjer 6/2020 p. 35.

grunden att behandlingen är nödvändig för att fullgöra ett avtal eller att vidta åtgärder som den registrerade begär.[35]

PSD2 uppställer ytterligare ett krav (utöver dataskyddsförordningens krav) vid behandling för tillhandahållande av betaltjänster, vilket är att personuppgiftsbehandling ska föregås av ett ”uttryckligt medgivande” av betaltjänstanvändaren. Enligt EDPB bör kravet tolkas i överensstämmelse med dataskyddsreglerna; den registrerade ska vid ingående av ett avtal med en betaltjänstleverantör få full kännedom om vilka personuppgifter som kommer att behandlas och det särskilda ändamålet för personuppgiftsbehandlingen och sedan godkänna dessa avtalsbestämmelser. Detta uttryckliga medgivande är enligt EDPB endast ett avtalsrättsligt godkännande av de villkor för personuppgiftsbehandlingen som ingås mellan betaltjänstleverantören och betaltjänstanvändaren. Medgivandet ska därför inte likställas med ett ”uttryckligt samtycke” i dataskyddsförordningen. Inte heller utgör ett uttryckligt medgivande någon ytterligare rättslig grund för personuppgiftsbehandling. Eftersom EDPB skriver att ett uttryckligt medgivande skiljer sig från ett uttryckligt samtycke bör inte en personuppgiftsansvarig utgå från att betaltjänstanvändaren har gett ett uttryckligt medgivande enligt PSD2 när denna har gett ett uttryckligt samtycke enligt dataskyddsförordningen och vice versa.[36]

Således måste betaltjänstleverantören alltså kunna påvisa att denna både har en rättslig grund för sin personuppgiftsbehandling och ett uttryckligt medgivande enligt PSD2.

3.3.2 Behandling av betaldata för andra ändamål

En av de centrala begränsningarna avseende behandling av betaldata är att personuppgifter i regel endast ska behandlas för det ändamål för vilket uppgifterna samlades in, i enlighet med ovannämnda princip om ändamålsbegränsning. Behandling av de personuppgifterna för andra ändamål än de ursprungliga är som utgångspunkt inte tillåten.

Betaltjänstleverantörer är relativt begränsade avseende deras möjlighet att behandla betaldata för andra ändamål än för de ändamål som uppgifterna samlades in. I PSD2 föreskrivs att den personuppgiftsbehandling som företas med stöd av direktivet är begränsad till tillhandahållandet av tjänsterna enligt PSD2, alltså för ändamålet att tillhandhålla den tjänst som betaltjänstanvändaren uttryckligen begärt.[37]

Personuppgifter som har samlats in för att tillhandahålla betaltjänster kan dock behandlas för andra ändamål i vissa särskilda fall: då ett samtycke getts eller om behandlingen tillåts i unionsrätten eller nationell rätt. Exempel på tillåten behandling är för uppfyllande av antipenningtvättsåtgärder eller i syfte att förebygga och avslöja bedrägerier i vissa fall, vilket har uttryckligen angetts som acceptabelt enligt betaltjänstlagen. Några nämnvärda möjligheter utöver detta att behandla betadata för andra ändamål torde inte finnas.[38]

[35] EDPB riktlinjer 6/2020 p. 14 och 36.
[36] EDPB riktlinjer 6/2020 s. 17 f.
[37] Artiklarna 66.3 g och 67.2 f i PSD2 reglerar att PISPs och AISPs vid tillhandahållandet av betaltjänsten inte får behandla uppgifter för andra ändamål än för att tillhandahålla den tjänst som uttryckligen begärs av användaren. Detta utrycks även i de ovannämnda bestämmelserna i betaltjänstlagen.
[38] EDPB riktlinjer 06/2020 p. 11 och 21-25 samt 4 kapitel 7 § Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism och 5 kapitel 4 § och 6 kap. betaltjänstlagen.

SETTERWALLS

3.4 Jämförande exempel: Vidarebehandling för annonsändamål

Ett område som på senare tid uppmärksammats som särskilt problematiskt ur ett dataskyddsperspektiv är det allmänt utbredda vidarenyttjandet av personuppgifter för annonsändamål i senare led. Detta är inte något som, såvitt är känt, förekommer i någon större omfattning i direkt samband med betaltjänster, men då det uppmärksammats förekomma i näraliggande avseenden och då det illustrerar svårigheterna med ett lagenligt vidarenyttjande tar vi kort upp dessa aspekter här.

En mycket stor del av den annonsering som sker online baseras på spårande av enskildas förehavanden på internet, exempelvis genom svepande insamling av data och tredjepartsinsamling av personuppgifter (där en annan aktör än den som den registrerade har en direkt relation till bearbetar personuppgifterna).[39]

Behandling av personuppgifter för sådan online-annonsering måste uppfylla kraven i dataskyddsförordningen. I verkligheten sker dock detta oftast i strid med flera grundläggande krav för personuppgiftsbehandlingen. Detta har under de senaste åren uppmärksammats av flera europeiska konsumentorganisationer och dataskyddsmyndigheter. I sin integritetsskyddsrapport från 2020 sammanfattar IMY situationen:

(i) Webbplatser spårar regelmässigt besökare, ofta med syftet att utföra riktad marknadsföring.

(ii) Merparten av denna digitala insamling av personuppgifter sker utan den registrerades vetskap.[40]

(iii) Dessa personuppgifter vidarebehandlas regelmässigt inom en annonsekonomi[41], vilket sker i mycket stor omfattning och oftast i strid med dataskyddsreglerna.

Mot denna bakgrund torde det vara vanligt att det i betalningssammanhang, främst i e-handelssituationer, förekommer sådana behandlingar för annonsändamål. Detta sker troligtvis utanför betaltjänsten och betalkedjan men kan förekomma i nära samband med betalningen. Som exempel kan det vara vanligt vid online-köp att spårning sker av vad konsumenten lägger i varukorgen och om de slutför köp för att sedan kunna skapa riktade annonser.[42] Konkurrensverket har i en rapport konstaterat att de flesta webbplatsbesök medför att en stor mängd tredjeparter samlar in data och spårar besöket, och att detta inkluderade webbplatsbesök inom såväl e-handel och som för bank och försäkringsbranschen.[43]

Det ska dock noteras att sådan behandling strikt sett troligtvis inte omfattar någon betaldata, utan omfattar istället andra data som kan genereras i samband med en betalning. Det vidarenyttjande som då eventuellt sker omfattas då primärt av dataskyddsförordningens krav och inte av de särregleringar som gäller för betaltjänsteleverantörer. I

[39] IMY Integritetsskyddsrapport s. 64.
[40] Se EDPB riktlinjer 05/2020 p. 81: EDPB förklarar att ett tyst godkännande av allmänna villkor inte godtas som ett samtycke enligt dataskyddsförordningen. Se även IMY Integritetsskyddsrapport s. 82: IMY refererar till norska konsumentsskyddsmyndighetens (Forbrukerradet) rapport Out of control, How consumers are exploited by the online adversiting industry, s. 23.
[41] IMY Integritetsskyddsrapport s. 64
[42] IMY Integritetsskyddsrapport s. 83 och Konkurrensverkets rapport 2020:4 s. 60 och 67 f.
[43] Stefan Larsson Dataekonomier - Om plattformar, tredjepartsaktörer och behovet av transparens på digitala marknader, Konkurrensverket uppdragsforskning rapport 2020:4.

SETTERWALLS

detta sammanhang har EDPB särskilt uppmärksammat avseende beteendestyrda online-annonseringar att grunden ”avtalsmässig nödvändighet”, vilket är den vanligaste grunden för behandling av betaldata för betaltjänster, inte utgör en rättslig grund för behandling av personuppgifter för beteendestyrd annonsering.[44] För sådant vidarenyttjande torde rättsliga grunden istället behöva vara ett uttryckligt samtycke. I den mån betaldata i något fall skulle vidarenyttjas för annonsändamål utan sådant samtycke, skulle det sannolikt ske i strid med dataskyddslagstiftningen. Vi känner dock inte till några indikationer på att sådant skulle vara vanligt förekommande.

[44] EDPB riktlinjer 2/2019 s. 14-15 och Norska Datatilsynet, beslut 20/02136-5.

SETTERWALLS

4. Banksekretess och annan finansiell sekretess

4.1 Allmänt om finansiell sekretess

För finansiella företag som hanterar betaldata gäller en lagreglerad sekretess - banksekretess eller annan finansiell sekretess - avseende företagens förhållande till dess kunder. Banksekretessen motiveras med att bankkunderna i regel har ett intresse av att deras personliga integritet och ekonomiska intressen (integritetsintresse) respekteras genom att den information som en bank har om deras privata och ekonomiska angelägenheter inte sprids.[45] Samma grunder kan åberopas även för den finansiella sekretessen som gäller för andra finansiella företag. Det ligger visserligen i de finansiella företagens intresse att värna om sekretessen för att upprätthålla kundernas förtroende för att de kommer att hålla deras uppgifter konfidentiella. Om svenska finansiella företag skulle brista i sin sekretess, kunde följden bli att kunder undviker att placera pengar hos dem med ett potentiellt utflöde av kapital från Sverige som följd, vilket skulle kunna få en allvarlig påverkan på landets kapitalförsörjning.[46]

Såvitt avser betaldata behandlar denna promemoria förenklat tre huvudsakliga typer av aktörer som omfattas av finansiell sekretess: banker, betaltjänstleverantörer och utgivare av elektroniska pengar.[47] Dessa benämns fortsättningsvis gemensamt för finansiella företag. Vi kommer i det följande vidare referera till finansiell sekretess när vi hänvisar till sådan sekretess som avser både banksekretess för kreditinstituts verksamhet och finansiell sekretess för betaltjänstverkssamhet eller utgivning av elektroniska pengar.

Banksekretessen finns reglerad i 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse (”LBF”). Enligt denna framgår att enskildas förhållanden till kreditinstitut inte obehörigen får röjas. Banksekretessens historia ur ett svenskt perspektiv går tillbaka så långt som till bankväsendets tidigaste skede när Rikets Ständers bank (sedermera Riksbanken) kom till år 1668 och finns angiven i den förordning genom vilket banken grundades. För privata banker finns den tidigaste lagsstiftningen om banksekretess från 1874. Lydelsen i dåvarande sekretessbestämmelsen var ”Enskildes förhållanden till banken må ej för allmänheten yppas” och uppvisar således stora likheter med den bestämmelse som gäller idag.[48]

Det finns även, såvitt är relevant för denna promemoria, regler om finansiell sekretess för bland annat betaltjänstverksamhet i 3 kap. 12 § betaltjänstlagen och för utgivare av elektroniska pengar i 3 kap. 12 § lagen (2011:755) om elektroniska pengar (”LEP”).[49] Dessa regler tar sin utgångspunkt i nämnda banksekretessreglering.

Förarbetsuttalanden och doktrin inom banksekretess och annan finansiell sekretess är begränsade. Doktrinen på området består i huvudsak av Per-Ola Janssons bok om

[45] Prop. 2002/03:139 Del 1 s 480.
[46] Jansson, s. 24.
[47] Fokus för denna utredning är som nämnts i inledningen de aktörer som är primärt synliga för den enskilde. Vi utreder inte den sekretess som är tillämplig för de aktörer som hanterar exempelvis clearing och avveckling.
[48] Jansson, s. 16-17.
[49] Det finns därutöver regler om finansiell sekretess för annan finansiell verksamhet. Dessa regler är dock inte relevanta för denna promemoria och lämnas därför därhän.

banksekretess och annan finansiell sekretess utgiven 2010[50], vilken anges vara en självständig bok, men ändå samtidigt moderniserad version av Håkan Nials bok Banksekretessen[51] utgiven 1987. Därutöver behandlas banksekretessen bland annat i några juridiska artiklar och viss branschkunskap delas även inom Bankföreningens banksekretessgrupp.

4.2 Skyddet för enskilda

Kärnan i banksekretess och annan finansiell sekretess är att de uppgifter om kundernas ekonomiska och andra förhållanden som finns hos finansiella företaget inte onödigtvis ska röjas för obehöriga. Bestämmelserna om sekretess ska skydda de enskilda kunderna oavsett om dessa är privatpersoner, företag eller offentligrättsliga subjekt, eller vem som helst som kan vara kund i ett finansiellt företag. Egenskapen att vara eller ha varit kund ska ges vidast möjliga tolkning. Alla som överhuvudtaget har haft något som kan uppfattas som en form av kundförhållande[52] till en bank eller annat finansiellt företag ska få skydd som sekretessbestämmelsen är avsedd att ge. Till kund ska i detta sammanhang även räknas till exempel en borgensman, eller någon annan som har en sådan relation till banken (eller det finansiella institutet) att uppgifter om honom eller henne förekommer i banken och vilken kan ha ett befogat intresse av att uppgifterna hålls hemliga. Kundbegreppet ska emellertid avse ett reellt förhållande i bankrörelsen och inte andra avtalsförhållanden mellan en bank och tredje man, exempelvis inte ett entreprenadförhållande.[53] Om inte något som helst kundförhållande förekommer eller har förekommit mellan en person och ett finansiellt institut, finns inget som konstituerar någon tystnadsplikt rörande personen. En banks rättsförhållanden till andra, till exempel anställda och hyresvärdar, omfattas således inte av sekretessen.[54]

När det gäller en kunds förhållanden till andra finansiella företag så omfattas detta inte av den finansiella sekretessen. När ett finansiellt företag får kännedom om en egen kunds förhållanden till ett annat finansiellt företag gäller emellertid den finansiella sekretessen alla förhållanden som på något sätt också rör den egna kundrelationen. Vid en strikt tolkning gäller den inte därutöver, vilket innebär att ett finansiellt institut i och för sig skulle vara berättigad att lämna upplysningar om sådan ”överskottsinformation” rörande en kunds förhållanden till ett annat finansiellt företag som går helt vid sidan om det egna kundförhållandet.[55] Det finansiella företaget bör dock trots detta inte upplysa om sina kunders förhållanden till andra finansiella företag.

Såvitt avser betaldata omfattar den finansiella sekretessen krav på betalarens och betalningsmottagarens betaltjänstleverantör att skydda betaldata avseende sina egna kunder. Därutöver bedömer vi att betaldata rörande motparten i transaktionen som inte utgör betaltjänstleverantörens egen kund ändå är sådana uppgifter där motparten har en sådan relation till det finansiella företaget att denne har ett ”befogat intresse av att de hålls hemliga” och att de därför också bör omfattas av finansiell sekretess. Detta in-

[50] Jansson, Per-Ola, *Banksekretess och annan finansiell sekretess,* Svenska Bankföreningen, 2010, se s. 8.
[51] Nial, Håkan, *Banksekretessen*, Svenska Bankföreningen, 5 uppl., 1987.
[52] Se vidare Jansson, s. 48-49.
[53] Jansson, s. 23 och 48.
[54] Prop. 2002/03:139 Del 1 s 477.
[55] Jansson, s. 53-54.

nebär till exempel att i den mån betalningsmottagarens betaltjänstleverantör får betaldata om betalaren så bör även denna omfattas av betaltjänstleverantörens sekretesskyldighet.

4.3 Förhållanden till kreditinstitut

Uttrycket ”*förhållanden till kreditinstitut*” omfattar upplysningar och uppgifter om en person som ett institut har eller har haft en kundrelation till. Tolkningen av vad som avses med förhållanden till ett kreditinstitut ska vara den vidast möjliga.[56] Alla uppgifter som rör en kunds mellanhavanden med banken (eller det finansiella institutet), oavsett om de är dokumenterade eller inte, är underkastade den finansiella sekretessen. Alla relationer bank - kund omfattas av sekretessregeln.[57] En förutsättning för att regeln om finansiell sekretess skall bli tillämplig är dock att det föreligger ett kontraktsförhållande i vid mening mellan institutet och en annan, fysisk eller juridisk, person.[58]

Eftersom den finansiella sekretessen förekommer i finansiell verksamhet, är det naturligt att uppgifter som skyddas av sekretessen i många fall gäller ekonomiska förhållanden, inte sällan med anknytning till betydelsefulla affärshemligheter. Att sådana uppgifter inte lämnas till obehöriga kan vara av mycket stor betydelse för de berörda kunderna. Med den mångfacetterade verksamhet som numera förekommer i de finansiella företagen, har dessa också tillgång till många andra slag av uppgifter om sina kunder. Dessa uppgifter kan vara lika känsliga som de strikt ekonomiska uppgifterna. Exempelvis kan de ha stor betydelse för kundernas integritet. Den finansiella sekretessen gäller emellertid alla uppgifter rörande en kund oavsett hur känsliga de kan antas vara generellt sett eller för den enskilde kunden.[59] Sekretessen gäller alla faktorer rörande relationen mellan banken eller det finansiella institutet och kunden av vad slag de än är, så länge de avser kundförhållandet. Inte heller information avseende att en person inte är kund hos ett finansiellt företag bör avslöjas i syfte att skydda den finansiella sekretessen.[60] Skulle kunden samtidigt ha en annan relation till det finansiella företaget gäller dock inte den finansiella sekretessen.[61]

Uppgifter om en betalares eller betalningsmottagares betaldata är uppgifter som typiskt sett inryms i en ”kunds mellanhavanden med” ett finansiellt företag och därför skyddas om regler om finansiell sekretess. Detta gäller enligt vår bedömning även såvitt avser information som till exempel betalningsmottagarens betaltjänstleverantör tagit del av om betalaren, vilken inte utgör dennes kund eftersom denne har ett befogat intresse av att de hålls hemliga. Sådana uppgifter får således inte lämnas ut av betalarens eller betalningsmottagarens betaltjänstleverantör utan behöriga skäl.

4.4 Obehörighetsrekvisitet

Den finansiella sekretessen berör i huvudsak tre parter: den enskilde som omfattas av det sekretessbelagda förhållandet, det finansiella företaget som känner till förhållandet och den tredje man som av någon anledning vill få del av uppgifter om förhållandet.

[56] Jansson, s. 49-50.
[57] Prop. 1986/87:12 s. 211.
[58] Prop. 2002/03:139 Del 1 s 478.
[59] Jansson, s. 23.
[60] Jansson, s. 53.
[61] Jansson, s. 51.

SETTERWALLS

Vid bedömning av om ett röjande är behörigt behöver man hitta en rimlig balans mellan dessa tre gruppers befogade intressen. Skulle tvekan råda om vad som gäller bör rekvisitet tolkas snävt så att sekretess gäller till dess någon omständighet tillkommer som medger att den kan brytas. Gränsdragningarna är många gånger svåra och förutsätter bedömning av bland annat ändamålet med utlämnade och prövning av hur uppgifterna behandlas efter ett eventuellt utlämnande.[62] . Den vägledning som finns avseende hur en sådan intresseavvägning ska utföras och bedömas är dessutom begränsad och leder enligt vår mening ofta till osäkra bedömningar.

I princip kan ett finansiellt företag behörigen röja uppgifter som omfattas av sekretess i fyra situationer: i) företaget kan lämna ut uppgifter till kunden själv, ii) företaget kan lämna ut uppgifter till annan om kunden har samtyckt till detta, iii) företaget kan lämna ut uppgifter om det är skyldigt att lämna ut uppgifter om en viss kund eller om sina kunder generellt sett på grund av krav på detta i lag eller i annat auktoritativt påbud, och iv) när någon sådan skyldighet inte finns, men när det ändå inte kan anses obehörigt att lämna upplysningar om kunden (”andra behöriga skäl”).[63]

Det finns inte utrymme inom ramen för denna promemoria att på ett uttömmande sätt beskriva de potentiella situationer som anges föregående stycke. I det följande ges emellertid ett antal exempel på situationer som bedömts vara särskilt relevanta att belysa såvitt avser betaldata.

Vid bedömning av om röjande får ske i fall då någon skyldighet att lämna ut uppgifter inte finns (andra behöriga skäl) blir den intresseavvägning som ska göras enligt ovan särskilt aktuell att tillämpa. Vid denna intresseavvägning kan det då finnas anledning att ta hänsyn till om sekretesskydd för uppgifterna också finns hos mottagaren, vilket kan vara fallet om mottagaren är ett annat finansiellt företag eller en myndighet i vars verksamhet sekretess gäller. Sekretesskydd hos mottagaren efter ett utlämnande får dock endast ses som ett stöd vid tolkningen i situationer när det samtidigt finns positiva skäl för ett utlämnande.[64]

Ett finansiellt företag kan under vissa förutsättningar ha rätt att lämna uppgifter om en kund till ett annat finansiellt företag. Det gäller i första hand när det följer av avtalet med kunden. I förarbetena till LBF anges att uppgiftslämnande anses tillåtet när det krävs för att banken skall kunna fullgöra kundens uppdrag.[65] Exempel på detta är när en stor kredit ska lämnas i samband med projektfinansiering eller annan företagsfinansiering. Då kan flera finansiella företag gemensamt utföra tjänsten och ge ett s.k. syndikerat lån. För bedömning av kundens kreditvärdighet, de ställda säkerheterna m.m. kan instituten behöva utbyta information om kunden och dennes förhållanden. Detta kan ske så långt det är nödvändigt för att den gemensamma tjänsten ska unna utföras.[66]

Såvitt avser betaldata lämnas uppgifter mellan betaltjänstleverantörer för att genomföra en betalning. Sådana uppgifter som betaltjänstleverantören har laglig skyldighet

[62] Jansson, s. 63.
[63] Jansson, s. 64.
[64] Jansson, s. 65.
[65] Prop. 2002/03:139 Del 1 s 478.
[66] Jansson, s. 185-186.

att tillse åtföljer betalningen framgår av förordning 2015/847[67] och utgör behörigt rö-jande på grund av denna skyldighet. Därutöver kan krav på betaldata föreligga enligt regler för de betalningsmeddelandestandarder betaltjänstleverantören har åtagit sig att följa inom ramen för ett visst betalsystem. Förutsatt att sådan information är nödvän-dig för att utföra betaltjänsten torde denna uppfylla krav på ”andra behöriga skäl”.

Enligt 4 kap. 9 § andra stycket 4 p. lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (”Penningtvättslagen”) finns också en möjlighet för bland an-nat banker, betaltjänstleverantörer och utgivare av elektroniska pengar att lämna upp-gifter sinsemellan som rör samma kund och samma transaktion och som bedöms (eller har bedömts) avseende om den utgör misstänkt för penningtvätt eller terrorismfinan-siering eller rapporterats till finanspolisen avseende detta. Detta förutsatt att verksam-hetsutövarna tillhör samma verksamhets- eller yrkeskategori och omfattas av skyldig-heter i fråga om tystnadsplikt och skydd för personuppgifter som följer av Penning-tvättslagen.

Möjligheten för finansiella företag att utbyta information för att motverka penningtvätt och finansiering av terrorism förutsätter således bland annat transaktionssamband. Ut-redningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism, SOU 2021:42, tar dock bland annat sikte på att utreda förutsättningarna för ett ökat infor-mationsutbyte. Utredningen konstaterar att bestämmelser om sekretess och annan tyst-nadsplikt utgör hinder för det informationsutbyte som behövs. Det föreslås därför att det ska införas en möjlighet till särskilt beslutad samverkan inom vilken uppgifter som omfattas av sekretess eller annan tystnadsplikt ska kunna utbytas genom en uppgifts-skyldighet. Sådan samverkan ska kunna beslutas när det, för att vidta åtgärder mot penningtvätt och finansiering av terrorism, finns särskilda skäl. De myndigheter som ingår i Samordningsfunktionen mot penningtvätt och finansiering av terrorism, Sveri-ges advokatsamfund och verksamhetsutövare enligt definitionen i Penningtvättslagen ska kunna ingå i en samverkan. En förutsättning för samverkan där verksamhetsutö-vare deltar är att åtminstone en myndighet deltar. Vidare föreslår utredningen att verk-samhetsutövare i större utsträckning med varandra ska kunna utbyta uppgifter som av-ser misstankar om penningtvätt och finansiering av terrorism om uppgifterna rör en transaktion som omfattar verksamhetsutövarna.[68]

Även utan särskild lagreglering såsom i Penningtvättslagen kan, utifrån en intresseav-vägning baserad på obehörighetsrekvisitet, uppgifter om en kund lämnas mellan finan-siella företag om synnerligen allvarlig brottslighet kan befaras vara riktad mot ett finan-siellt företags verksamhet i stort, till exempel i form av systematiska kreditbedrägerier eller systematiska försök att ta sig in i företagets datasystem. Det gäller i fall då frågan är så brådskande att en brottsutredning inte kan avvaktas.[69]

[67] Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006.
[68] Betänkande av utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism SOU 2021:42, s. 20-21.
[69] Jansson, s. 188.

SETTERWALLS

Uppgifter som har lämnats till polis eller åklagare med anledning av misstänkt bedrägeri i samband med tillhandahållande eller användning av betaltjänster får vidare enligt 6 kap. 5 § betaltjänstlagen delas mellan betaltjänstleverantörer och de som har ansvar för betalningssystem.

Vidare förekommer vid utbetalningar i vissa fall att kunder önskar att beloppet ska sättas in på kundens konto i en annan bank än den bank som fått uppdraget att utföra transaktionen. För att säkerställa att kundens uppgivna konto är korrekt, och därmed undvika att utbetalning sker till fel konto, kontaktar den utbetalande banken den andra banken där kontot finns för att få en bekräftelse att kontonumret är korrekt. Det torde inte finnas några hinder från banksekretessynpunkt att den kontohavande banken bekräftar dessa uppgifter. Detta dock under förutsättning att den utbetalande banken kan lämna upplysningar till den andra banken om såväl kontonummer som namn och personnummer på kontohavaren.

Det kan vidare förekomma att kunder ställer frågan till sin bank om vem som betalat in medel på kundens konto eller att en betalare ställer frågan om till vem som en betalning gått. Banken bör kunna medverka till att sådana frågor klarläggs. Banken får dock först bedöma att det rör sig om en berättigad förfrågan och kontrollera att det inte utgör ett obehörigt försök att få tillgång till betalningsmottagarens uppgifter.

4.5 Röjande

Förbudet att lämna ut uppgifter som täcks av finansiell sekretess omfattar inte förhållanden som redan har röjts. Information som är allmänt känd eller som kan inhämtas genom till exempel offentliga register eller i allmänt tillgängliga dokument, såsom prospekt, är redan röjt och omfattas därför inte av sekretessen. Ett finansiellt företag bör dock generellt vara försiktigt med att lämna ut uppgifter om sina kunder på den grunden att de redan är kända. Som vägledande regel bör detta kunna ske om det är till kundens förmån. Företaget bör emellertid inte lämna ut mer uppgifter än vad som redan har röjts.[70]

Från doktrin kan utläsas att alla förhållanden som kan identifieras som hörande till viss kund är skyddade av den finansiella sekretessen.[71] Någon närmre vägledning för när så är fallet, motsvarande vad som gäller inom personuppgiftsområdet, saknas emellertid inom området finansiell sekretess. Det torde i och för sig med viss försiktighet gå att beakta den vägledning som tillämpas inom personuppgiftsområdet avseende anonymisering och aggregering av data även för när ett förhållande till en viss kund ska anses föreligga.

4.6 Finansiell sekretess hos betaltjänstleverantörer

Enligt 3 kap. 12 § betaltjänstlagen gäller att den som är eller har varit knuten till ett betalningsinstitut eller en registrerad betaltjänstleverantör som anställd eller uppdragstagare inte obehörigen får röja eller utnyttja vad han eller hon i anställningen eller under uppdraget *i verksamheten med betaltjänster* har fått veta om enskildas förhållanden till institutet eller leverantören.

[70] Jansson, s. 50.
[71] Jansson, s. 51.

SETTERWALLS

Regleringen i 3 kap. 12 § betaltjänstlagen, vilken avser sekretess inom ramen för betaltjänstverksamhet enligt betaltjänstlagen, reglerar en skyldighet för den som är eller har varit knuten till ett betalningsinstitut eller en registrerad betaltjänstleverantör som anställd eller uppdragstagare. Till skillnad från regleringen i LBF träffar skyldigheten i betaltjänstlagen alltså inte själva institutet utan de enskilda personerna som är eller har varit knutna till detta[72]. Detta hindrar dock inte att det institut i vilket de är verksamma också kan vara ansvarigt i egenskap av deras principal eller till följd av avtalet med kund. Både banker och betaltjänstleverantörer agerar genom anställda eller uppdragstagare. I den praktiska verksamheten blir det därför dessa som tvingas iaktta sekretessen för banken eller betaltjänstleverantörens räkning. Den praktiska skillnaden i tillämpningen mellan de båda huvudtyperna av sekretessbestämmelser blir därför ur detta perspektiv obetydlig.[73] Däremot torde inte det finansiella företaget kunna göras ansvarigt genom ingripande från Finansinspektionen för en enskild anställds brott mot den finansiella sekretessen enligt 3 kap. 12 § betaltjänstlagen om inte företaget samtidigt bryter mot annan finansiell reglering, till exempel genom att ha bristfälliga interna regler och rutiner avseende finansiell sekretess.

Vidare är omfattningen av LBF:s sekretessbestämmelse bredare än motsvarande i betaltjänstlagen. LBF:s sekretessbestämmelse täcker in relationer avseende all verksamhet för kreditinstitutet mot kunder oavsett om det är inlåning, utlåning, betaltjänster eller andra produkter. Betaltjänstlagens sekretessbestämmelse omfattar emellertid endast betaltjänstverksamheten och således inte näraliggande verksamhet eller annan verksamhet som bedrivs av betalningsinstitutet eller den registrerade betaltjänstleverantören.

4.7 Finansiell sekretess hos utgivare av elektroniska pengar

Enligt 3 kap. 12 § LEP gäller att den som är eller har varit knuten till ett institut för elektroniska pengar eller en registrerad utgivare som anställd eller uppdragstagare inte obehörigen får röja eller utnyttja vad han eller hon i anställningen eller under uppdraget *i verksamheten med utgivning av elektroniska pengar eller betaltjänster* har fått veta om enskildas förhållanden till institutet eller utgivaren.

Enligt propositionen[74] till LEP motsvarar 3 kap. 12 § LEP motsvarande bestämmelse i betaltjänstlagen och avses ha samma innebörd. Det nämns vidare i propositionen att det i sammanhanget kan noteras att institut för elektroniska pengar och registrerade utgivare har möjlighet att bland annat tillhandahålla betaltjänster. Även utgivning av elektroniska pengar är en verksamhet som nära knyter an till tillhandahållande av betaltjänster. Tillhandahållande av betaltjänster är i sin tur en verksamhet som uppvisar likheter med verksamheten i kreditinstitut, som sysslar med omfattande betalningsförmedling.[75] Mot denna bakgrund ansågs det enligt förarbetena till LEP som lämpligt att

[72] Vi har inte återfunnit någon förklaring till denna diskrepans trots eftersökningar.
[73] Jansson, s. 21.
[74] Prop. 2010/11:124, s 139.
[75] Prop. 2009/10:220, s. 146.

SETTERWALLS

införa regler om tystnadsplikt för institut för elektroniska pengar och registrerade utgivare som motsvarar de regler som gäller för såväl betalningsinstitut och registrerade betaltjänstleverantörer som för kreditinstitut.[76]

4.8 Andra aktörer på betalmarknaden

I samband med betalningar behandlas betaldata i vissa fall även av andra aktörer än de som utför betalningen. Vid en betalning av varor på internet (en e-handelstransaktion) behandlar i normalfallet även säljaren uppgifter om betalaren som har erhållits från betalaren inför genomförandet av betalningen.

De uppgifter som behandlas av betalningsmottagaren kommer direkt från betalaren. Något röjande från betaltjänstleverantören kan således inte anses aktualiseras i det skedet. Behandlingen av denna betaldata av betalningsmottagaren omfattas inte av någon finansiell sekretess eftersom uppgifterna erhållits direkt från betalaren och utan inblandning av någon aktör som lyder under finansiell sekretess.

4.9 Betalare respektive betalningsmottagare

Betalare och betalningsmottagare är de parter som skyddas av reglering om finansiell sekretess, men dessa omfattas själv inte av skyldigheter enligt sekretessregleringen.

[76] Prop. 2010/11:124, s 89.

SETTERWALLS

5. Särskilt om anonymisering och aggregering av data

Användande av betaldata omfattas endast av dataskyddslagstiftningens krav i den mån den enskilda betaldatan utgör personuppgifter. Likaså täcks betaldata av finansiell sekretess endast om uppgifterna avser det finansiella företagets förhållande till kunden. Således omfattas rent anonym data inte av vare sig dataskyddslagens krav eller av reglerna för finansiell sekretess.

Det följer av dataskyddsförordningens definition att uppgifter som är helt anonyma och som inte går att hänföra till en fysisk person inte utgör personuppgifter. Sådana anonymiserade data faller utanför personuppgiftsregleringen och kan alltså nyttjas och vidarebehandlas i princip obegränsat. Således kan information som har sammanställts och aggregerats till den grad att den anonymiserats användas fritt, vilket medför att rent statistisk betaldata kan användas utan begränsningar så länge den verkligen är anonym. Exempel på sådan information är rent statistik, förutsatt att sådan information hålls på en sådan allmän nivå att enskilda eller mindre grupper av enskilda inte kan särskiljas.

Det ställs dock mycket höga krav för uppgifter ska anses vara anonymiserade. För att uppgifterna ska anses vara anonymiserade ska information vara *oåterkalleligen avidentifierad* – det ska alltså inte gå att åstadkomma eller återskapa kopplingen till en enskild person. Avgörande för om uppgifter utgör personuppgifter eller anonymiserad information är om den fysiska personen ”med rimlig sannolikhet” kan identifieras eller inte.[77] Det är för närvarande oklart hur pass oåterkallelig information måste förbli för att inte utgöra personuppgifter.[78]

Det har vid flera tillfällen visats att data som man trott ska vara anonym faktisk har kunnat användas för att identifiera enskilda fysiska personer[79] - med följd att sådan data ska anses utgöra personuppgifter. Som exempel kan tas att generell transaktionsdata har visats kunna identifiera enskilda personer genom analys av transaktionsmönster.[80] Även statistiska uppgifter har i vissa undantagsfall gått att hänföra till en så pass begränsad grupp av personer att detta ansetts utgöra personuppgifter, trots att de enskilda individerna inte framgick.

I sammanhanget ska det noteras att åtgärder som endast är tillfälliga, till exempel kryptering eller när identifierande uppgifter ersätts med unika identifikatorer/nycklar, inte innebär att informationen anses vara anonymiserad – sådana uppgifter anses istället vara pseudonymiserade[81], vilket alltjämt är personuppgifter som lyder under dataskyddsförordningens krav. Således täcks uppgifter som från den enskildes perspektiv

[77] Se skäl 26 i dataskyddsförordningen.
[78] EDPBs föregångare Artikel 29-gruppen har publicerat riktlinjer om anonymisering (WP 216) som uppställer ett närmast absolut krav på oåterkallelighet och därmed att det inte får finnas någon som helst risk för identifiering – dessa riktlinjer publicerades dock innan Dataskyddsförordningen trädde i kraft och de har inte antagits av EDPB. EDPB har angett att man planerar att under 2021/2022 ge ut uppdaterade riktlinjer om anonymisering.
[79] Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law, European Parliamentary Research Service, juli 2019, s. 22ff.
[80] European Parliamentary Research Service, s. 27.
[81] Art. 4, 5 p. dataskyddsförordningen.

SETTERWALLS

ofta kan uppfattas som avidentifierade, såsom delvis avidentifierade (hashade) uppgifter eller uppgifter som hänförs till ett alias, fortfarande av dataskyddsförordningens skydd och villkor.

Som nämnts under avsnitt 4.5 kan i doktrin utläsas att alla förhållanden som kan identifieras som hörande till viss kund är skyddade av den finansiella sekretessen. Någon närmre vägledning för när så är fallet, motsvarande vad som gäller inom personuppgiftsområdet, saknas emellertid inom området finansiell sekretess. I likhet med vad som gäller inom personuppgiftsområdet torde dock pseudonymiserade uppgifter om en kund till ett finansiellt företag utgöra förhållanden som kan identifieras som hörande till viss kund och därmed sådana uppgifter som skyddas av regleringen om finansiell sekretess.

Vad avser betaldata torde det i de allra flesta fall röra sig om uppgifter som direkt eller indirekt kommer att vara hänförligt till det finansiella företagets kunder eller en enskild person (till exempel uppgifter som kan hänföras till betalaren). Därför omfattas betaldata som huvudregel av dataskyddsförordningens villkor och krav samt av reglerna om finansiell sekretess. Om betaldata dock har sammanställts och anonymiserats fullt ut (utan att någon enskild kan härledas) så gäller inte dessa krav. Detta kan vara fallet för exempelvis rent statistisk betaldata som aggregerats till en sådan nivå att den endast visar på generella betal eller köpmönster över en större population. Sådan anonymiserad och aggregerad statistisk data kan användas i princip helt fritt för olika ändamål, inklusive vidareanvändning och försäljning till nya parter, utan att dataskyddslagstiftningen eller den finansiella sekretessen begränsar användningsmöjligheterna.

Det ska nämnas att själva aggregeringen och anonymiseringen är en åtgärd som i sig utgör en personuppgiftsbehandling enligt dataskyddsförordningen, varför det krävs att exempelvis laglig grund föreligger för en sådan åtgärd. I praktiken torde det dock vara relativt enkelt att säkerställa en laglig grund för en anonymisering, exempelvis genom en intresseavvägning, då det torde föreligga ett legitimt intresse av att skapa och nyttja sådana statistiska uppgifter i verksamheten och riskerna för den enskildes integritet torde vara minimala (förutsatt att uppgifterna faktiskt anonymiseras fullt ut).

SW4160961 1/6

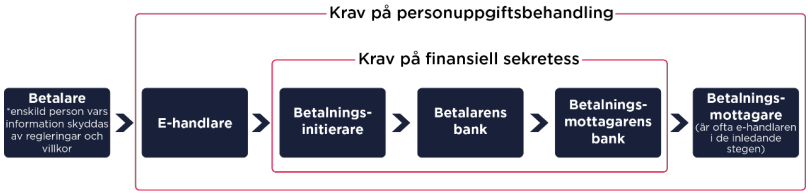
SETTERWALLS

6. Avslutande analys och kommentarer

6.1 Relationen mellan finansiell sekretess och dataskydd avseende betaldata

Reglerna om dataskydd och om finansiell sekretess kompletterar och överlappar varandra. Som framgår av bilden nedan är området för den finansiella sekretessen emellertid snävare. Kraven på finansiell sekretess är enbart tillämpliga på finansiella företag, som omfattas av sekretessreglering inom den finansiella rörelsen, samt den som är eller har varit knuten till ett finansiellt företag som anställd eller uppdragstagare.

Figur 1: Översikt över betaldata i ett förenklat betalflöde.[82]



6.2 Vilket skydd och villkor gäller för användning av betaldata

Behandling av betaldata förutsätter i sig en särskild försiktighet eftersom uppgifterna däri kan vara av känsliga för den enskilde och behandlingen kan således innebära en ökad risk för individens rättigheter och friheter.[83] Denna försiktighet tillgodoses i betalkedjan till viss del av att vissa aktörer omfattas av exempelvis finansiell sekretess. Andra aktörer i betalkedjan som betalningsmottagare och e-handlare omfattas inte av finansiell sekretess eller specifika regler avseende behandling av betaldata. Istället omfattas dessa aktörer av de allmänna och grundläggande kraven i dataskyddsförordningen.

Reglerna om finansiell sekretess och dataskydd är konstruerade på så vis att det som utgångspunkt är otillåtet att röja respektive behandla betaldata, om inte de villkor och förutsättningar som uppställs i reglerna uppfylls. För finansiell sekretess är det primära villkoret, för att uppgifter ska få delas till utomstående, att det föreligger ett *behörigt* röjande. För dataskydd gäller för att uppgifterna ska få behandlas att de omfattande kraven i dataskyddsförordningen (avseende bland annat giltigt ändamål och tillämplig rättslig grund) är uppfyllda. Olika aktörers möjlighet att på ett lagligt sätt använda sig av betaldata styrs och begränsas således klart genom dessa regleringar.

För anonymiserad och aggregerad betaldata gäller inte dessa regler utan sådan data kan nyttjas fritt, till exempel genom vidarenyttjande för andra ändamål eller delning eller försäljning av sådan data till andra aktörer. Ett sådant fritt nyttjande förutsätter

[82] Notera att denna bild är förenklad och att det kan förekomma såväl fler flöden som andra och mer komplexa strukturer än vad som anges nedan. Det ska också påpekas att det inom ramen för kraven på personuppgiftsbehandlingen förekommer andra regleringar som direkt eller indirekt kompletterar dataskyddsförordningen, inkluderat betaltjänstlagen (enligt vad som beskrivs i avsnitt 3.3 ovan) och även reglerna för finansiell sekretess. Bilden skulle således kunna göras betydligt mer komplex.
[83] Just risk för individens rättigheter och friheter är centralt för det europeiska dataskyddet, se närmare EDPB:s riktlinjer 6/2020 fotnot 30.

att inga enskilda ska kunna härledas utifrån sådan aggregerad betaldata. Om detta uppfylls är det enligt vår mening också rimligt att datan kan nyttjas fritt, men det gäller att man säkerställer att så är fallet. Som nämnt ovan är det i nuläget oklart vad som krävs för att uppnå anonymisering enligt dataskyddsförordningen. Här torde förväntade vägledningar från EDPB kunna bidra till att klargöra rättsläget.

6.3 Behov av mer vägledning inom området finansiell sekretess

På senare år, särskilt i samband med genomförandet av dataskyddsförordningen, har ett stort antal omfattande och detaljrika vägledningar avseende personuppgiftsbehandling upprättats, bland annat från EDPB och IMY. Dessa vägledningar har i stor utsträckning tagit hänsyn till den snabba tekniska utveckling som sker och den omfattande spridning av uppgifter det medför.

Förarbeten, doktrin och annan vägledning som finns avseende hur reglerna om finansiell sekretess ska tolkas är däremot begränsad och flera år gammal. Dessa vägledningar är huvudsakligen skrivna före de senaste årens tekniska utveckling och de är således inte anpassade till dagens komplexa digitala miljö. Detta försvårar en säker tolkning och juridiska analyser av gällande rätt för dagens digitala verksamheter.

Den begränsade vägledningen inom området finansiell sekretess blir särskilt tydlig när en jämförelse görs mellan olika grunder för behörigt röjande inom finansiell sekretess respektive rättsliga grunder för behandling av personuppgifter. Det saknas exempelvis en närmare vägledning för hur den intresseavvägning avseende om ett röjande är obehörigt eller ej ska utföras. Jämförelsevis finns inom personuppgiftsområdet mycket omfattande vägledningar avseende hur en sådan intresseavvägning ska göras och vad som då bör beaktas. Ett ytterligare exempel är grunden samtycke där det finns mycket vägledning inom personuppgiftsområdet avseende hur ett samtycke ska utformas medan vägledningen inom området finansiell sekretess även här är begränsad.

Sammanfattningsvis bedömer vi därför att den vägledning som finns inom området finansiell sekretess behöver uppdateras, förtydligas samt så långt möjligt samordnas med de vägledningar inom personuppgiftsområdet som det finns en naturlig anknytning till.

6.4 Tillsyn över behandlingen av betaldata

IMY har varit aktiv i sin tillsyn över personuppgiftskraven sedan dataskyddsförordningen trädde i kraft. Detta har i viss utsträckning omfattat tillsyn inom den finansiella sektorn, även om den tillsynen såvitt vi känner till inte har avsett några av de huvudsakliga aspekter som belysts i denna utredning. Några betydande påföljder har i dagsläget inte heller beslutats av IMY avseende finansbranschens aktörer.[84]

Avseende FI:s tillsyn känner vi inte till några betydande fall där myndigheten har ingripit mot aktörer till följd av bristande efterlevnad av regler om finansiell sekretess.[85]

[84] Jämförelse kan göras med sjukvården, en annan bransch men som likt betalmarknaden är föremål för omfattande särreglering, där IMY har gjort omfattande tillsyn vilket resulterat i beslut om betydande sanktionsavgifter.
[85] Det bör noteras att vi baserar detta på vår kunskap och erfarenhet av FI:s sanktionspraxis och att vi inte gjort en detaljerad genomgång av denna inom ramen för denna promemoria.

Eftersom dataskyddslagstiftningen och den finansiella regleringen överlappar innebär detta att IMY och FI har ett överlappande tillsynsansvar. IMY har i detta avseende efterfrågat en nära samverkan mellan myndigheter för att uppnå en harmoniserad reglering av personuppgifter inom olika samhällssektorer[86], exempelvis avseende initiativen på betaltjänstmarknaden och avseende incidentrapporteringar. I detta sammanhang har IMY framfört att det finns behov av samverkan med FI.[87] Även FI har framfört att överlappningar och ansvarsfördelning mellan myndigheterna bör klarläggas, särskild i de avseenden där FI utöver tillsyn som angränsar till personuppgiftsområdet.[88]

6.5 Behov utifrån den starka marknadsutvecklingen inom betaltjänster

Betaltjänstemarknaden har utvecklats kraftigt de senaste åren. Det har både skett en snabb teknisk utveckling samtidigt som det skapats många nya bolag med inriktning på betaltjänster (oftast sker detta i ett digitaliseringssammanhang, så kallad fintech). Detta kan bidra till en ökad innovation och konkurrens på marknaden, men samtidigt innebär nya affärsmodeller och ny teknikanvändning utmaningar vad gäller tillämpning och efterlevnad av de aktuella regelverken. Därtill kan många nya bolag, åtminstone i ett inledande skede, ha utmaningar med att skaffa den kompetens och de rutiner som krävs för att efterleva tillämpliga krav i en komplex verklighet.

Att regelverken i sig är komplexa bidrar till dessa utmaningar. En ökad samordning och förtydligande, enligt vad som nämnts ovan, kan enligt vår mening bidra till förbättrade möjligheter till en korrekt regelefterlevnad samtidigt som man tar till vara på utvecklingarna på betaltjänstemarknaden.

[86] IMY Integritetsskyddsrapport 2020 s. 19 och 43.
[87] IMY Integritetsskyddsrapport 2020 s. 43.
[88] Prop. 2017/18:77 s.296.