IMY. Integritetsskydds myndigheten

Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet

Slutrapport från Integritetsskyddsmyndighetens regulatoriska sandlåda om dataskydd

Diarienummer
IMY-2024-14275

Datum
2025-05-19

Diarienummer:
IMY-2024-14275

Datum:
2025-05-19

Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet

Innehållsförteckning

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Sammanfattning

- **Integritetsskyddsmyndigheten (IMY) har under hösten 2024 och våren 2025 genomfört sitt fjärde projekt i myndighetens regulatoriska sandlåda.** Med regulatorisk sandlåda avser IMY fördjupad vägledning om hur dataskyddsregelverket bör tolkas och tillämpas. Kännetecknande för arbetssättet är att IMY tillsammans med den aktuella verksamheten identifierar de rättsliga frågor som vägledningen ska fokusera på. Vägledning ges därefter muntligt vid flera tillfällen under några månaders tid i form av workshops eller andra dialogbaserade former. Arbetet utmynnar i en publik rapport där resonemang och bedömningar sammanfattas för att möjliggöra ett lärande för fler.

- **I projektet ”Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet” har SEB, Swedbank, Handelsbanken och Nordea deltagit.** Målet har varit att utreda om det finns rättsliga förutsättningar, utifrån dataskyddsregelverket, för banker att dela vissa uppgifter om potentiella, befintliga och avvisade/avslutade kunder mellan varandra. Syftet är att motverka och förhindra att banker utnyttjas för penningtvätt, terroristfinansiering och bedrägerier genom att flagga och pinga dessa kunder i ett gemensamt system. En kund kan bara flaggas om den uppfyller någon av bankernas överenskomna bakomliggande orsaker för när en individ kan anses innebära en förhöjd risk för penningtvätt, terroristfinansiering och/eller bedrägeri.

- **För de uppgifter som bankerna avser att dela med varandra inom ramen för projektet tänker de sig två olika alternativ.** I det första alternativet (alternativ 1) delar bankerna endast information om huruvida en viss individ är flaggad i systemet. Den enda information som delas är individens namn, personnummer och om individen är flaggad i systemet eller inte. I det andra alternativet (alternativ 2) delar bankerna samma information som i alternativ 1, samt information om den bakomliggande orsaken till flaggningen, det vill säga den specifika grund som har lett till bedömningen att individen anses ha en förhöjd riskprofil. En flaggning i systemet utgör endast en indikator på förhöjd risk som kan föranleda behov av ytterligare åtgärder för kundkännedom.

- **Vägledningen i projektet har fokuserat på huvudsakligen två rättsliga frågeställningar**. Utöver dessa frågeställningar finns andra juridiska frågor som behöver beaktas, men som inte analyserats inom ramen för projektet.

- **Fråga 1. Kan flaggning i sig utgöra uppgift om lagöverträdelser enligt artikel 10 i dataskyddsförordningen?** I projektet har IMY tittat på frågan om delningen av uppgifter mellan bankerna i projektet enligt alternativ 1 respektive alternativ 2 ovan faller in under begreppet behandling av personuppgifter om lagöverträdelser. IMY anser inledningsvis att den delning som bankerna önskar göra typiskt sett utgör en behandling enligt dataskyddsförordningen. IMY finner vidare att det inte går att utesluta möjligheten att sammankoppla flaggningen med en uppgift om lagöverträdelser enligt artikel 10 i dataskyddsförordningen.

- **Fråga 2. Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för att dela uppgifter enligt alternativ 1 eller alternativ 2 inom ramen för en annan banks kundkännedomsprocess och riskbedömning?** IMY har i projektet bedömt frågan om det finns en rättslig grund enligt artikel 6.1 i dataskyddsförordningen för bankernas tilltänka delning av personuppgifter om lagöverträdelser. IMY har utrett tillämpligheten av den rättsliga grunden rättslig

förpliktelse (artikel 6.1 c), allmänt intresse (artikel 6.1 e) och berättigat intresse (artikel 6.1 f). IMY:s samlade bedömning är att den tilltänkta delningen av personuppgifter inte kan anses vara nödvändig för att uppfylla en rättslig förpliktelse som följer av lag eller förordning, vare sig enligt penningtvättslagen, betaltjänstlagen eller någon annan författning i svensk rätt. IMY konstaterar också att uppgifterna att bekämpa penningtvätt och finansiering av terrorism enligt penningtvättslagen, och att bekämpa bedrägeri enligt betaltjänstlagen, kan betraktas som uppgifter av allmänt intresse (artikel 6.1 e), samt att dessa uppgifter av allmänt intresse kan ligga till grund för viss personuppgiftsbehandling som får ske med stöd av särskilda bestämmelser i penningtvättslagen och betaltjänstlagen. IMY finner dock att mycket talar emot att bankerna skulle kunna stödja den tilltänkta delningen av personuppgifter om lagöverträdelser på den rättsliga grunden uppgift av allmänt intresse, vilket främst beror på att det inte finns lagligt stöd för den delning som bankerna önskar att genomföra inom ramen för detta projekt. Slutligen konstaterar IMY även att bekämpning av penningtvätt och finansiering av terrorism enligt penningtvättslagen, samt bekämpning av bedrägeri enligt betaltjänstlagen, kan utgöra berättigade intressen. IMY finner dock att en grundläggande förutsättning för tillämpningen av den rättsliga grunden berättigat intresse (artikel 6.1 f) är att det berättigade intresset som en personuppgiftsansvarig, eller en tredje part, vill uppfylla kan anses vara legitimt. Detta förutsätter i sin tur att intresset är lagligt, det vill säga att det inte strider mot gällande rätt. Mot bakgrund av banksekretessen i banklagen samt sekretessbestämmelserna i penningtvättslagen och betaltjänstlagen, är IMY:s bedömning att det framstår som svårt för bankerna att grunda den tilltänkta delningen av personuppgifter om lagöverträdelser på den rättsliga grunden berättigat intresse. IMY anser att det sannolikt behövs lagändringar för att möjliggöra den delning av personuppgifter om lagöverträdelser som bankerna önskar genomföra inom ramen för det aktuella projektet.

Integritetsskyddsmyndighetens regulatoriska sandlåda om dataskydd

Med regulatorisk sandlåda avser Integritetsskyddsmyndigheten (IMY) **fördjupad vägledning om hur dataskyddsregelverket bör tolkas och tillämpas**. Inget undantag ges från reglerna i dataskyddsförordningen eller dess kompletterande lagstiftning utan vägledningen baseras på gällande rätt.

Kännetecknande för arbetssättet är att:

- IMY och innovationsaktörerna tillsammans identifierar de rättsliga frågor som vägledningen ska fokusera på,
- vägledning ges muntligt vid flera tillfällen under några månaders tid i form av workshops eller andra dialogbaserade former, och
- resonemang och bedömningar från vägledningen sammanfattas och publiceras i en rapport för att möjliggöra lärande för många.

1. Inledning

Ekonomisk brottslighet utgör idag ett allvarligt och växande samhällsproblem i Sverige och beräknas kosta samhället upp till 150 miljarder kronor årligen.[1] Detta omfattar en rad olika typer av brottsliga aktiviteter såsom penningtvätt, finansiering av terrorism, skattebrott, sanktionsbrott, bedrägerier samt mutor och otillbörlig påverkan. Omkring 130 miljarder kronor beräknas tvättas årligen i det finansiella systemet i Sverige.[2]

Utvecklingen av den ekonomiska brottsligheten har varit snabb och de aktörer som bedriver sådan verksamhet har blivit alltmer sofistikerade och svårupptäckta. Polisens uppskattningar visar att över 62 000 personer är involverade i organiserad brottslighet. Många av dem verkar internationellt och använder sig av gränsöverskridande metoder.[3]

Banker och andra finansiella institut spelar en central roll i bekämpningen av ekonomisk brottslighet. Trots att antalet misstankerapporter till finanspolisen har ökat med över 300 procent under de senaste sex åren är mörkertalet kring den här typen av brottslighet fortfarande stort.

Detta projekt, som har bedrivits inom IMY:s regulatoriska sandlåda, har haft som syfte att utforska om vissa personuppgifter om kunder kan delas mellan banker för att motverka ekonomisk brottslighet. Fokus har legat på att bedöma de dataskyddsrättsliga förutsättningarna för att kunna dela information om individer som anses utgöra en förhöjd risk för viss typ av ekonomisk brottslighet.

[1] Den kriminella ekonomin, Polismyndigheten, Polisregion Stockholm, Regionkansliet, Operativ Verksamhetsstyrning, september 2024, s. 4.
[2] Ibid, s.20 f.
[3] Lägesbild över aktiva gängkriminella i Sverige, Polismyndigheten, Polisregion Stockholm, Regionkansliet, Operativ Verksamhetsstyrning, september 2024, s. 6 f.

2. Projektet ”Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet”

2.1. Projektets deltagare

I projektet har följande banker deltagit:

- Svenska Handelsbanken AB
- Nordea Bank Abp
- Skandinaviska Enskilda Banken AB (SEB)
- Swedbank AB

I denna rapport kommer bankerna ovan att tillsammans benämnas som ”bankerna”.

2.2. Projektets mål

Projektets mål har varit att utreda om det finns rättsliga möjligheter, utifrån dataskyddsregelverket, för banker att dela vissa uppgifter om potentiella, befintliga och avvisade/avslutade kunder[4] mellan varandra. Syftet är att motverka och förhindra att banker utnyttjas för penningtvätt, terroristfinansiering och bedrägerier genom att flagga dessa kunder i ett gemensamt system. Bankernas vision är att även andra banker ska kunna delta i samarbetet.

2.3. Rättsliga frågeställningar

Bankerna har tillsammans med IMY enats om att fokusera på följande rättsliga frågeställningar i det aktuella projektet:

- Kan flaggning[5] i sig utgöra uppgift om lagöverträdelser enligt artikel 10 i dataskyddsförordningen[6]?

- Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för en bank att inom ramen för en annan banks kundkännedomsprocess och riskbedömning:

  1. dela förekomst av flaggning avseende potentiella, befintliga och avvisade/avslutade kunder

  2. dela förekomst av flaggning tillsammans med information om den bakomliggande orsaken till flaggningen?

[4] Begreppet ”kund” definieras i 1 kap. 8 § p. 4 lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism som ”den som har trätt eller står i begrepp att träda i avtalsförbindelse med sådan verksamhetsutövare som avses i denna lag”.
[5] Företeelsen att en av bankerna har flaggat en potentiell, befintlig eller avvisad/avslutad kund med anledning av att en förhöjd risk för penningtvätt, terroristfinansiering och/eller bedrägerier bedöms föreligga enligt de mellan bankerna särskilt överenskomma bakomliggande orsaker för flaggning. Se vidare avsnitt 3.
[6] 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).

2.4. Avgränsningar i projektet och annan upplysning

Detta projekt har fokuserat på frågor relaterade till delning av vissa särskilda kunduppgifter mellan banker. I projektet har det dock inte utretts hur ett IT-system som kan hantera den tilltänkta delningen av kunduppgifter mellan bankerna skulle kunna utformas eller användas. Det bör också understrykas att den tilltänkta behandlingen, det vill säga den avsedda delningen av vissa kunduppgifter mellan bankerna, inte sker idag.

Frågor som ligger utanför IMY:s verksamhetsområde har inte analyserats utöver vad som har krävts för rapportens frågeställningar. Det ska noteras att Finansinspektionen är behörig tillsynsmyndighet enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen), lagen (2010:751) om betaltjänster (betaltjänstlagen) och lagen (2004:297) om bank- och finansieringsrörelse (banklagen). Detta innebär bland annat att frågan om huruvida banksekretess föreligger mellan bankerna i relation till den tilltänkta delningen av vissa kunduppgifter endast har berörts inom ramen för frågan om huruvida det kan finnas rättslig grund enligt dataskyddsregelverket. Finansinspektionen har informerats och hållits löpande underrättad om projektet.

IMY:s föreskrifter IMYFS 2024:1[7] om behandling av personuppgifter som rör lagöverträdelser är inte tillämpliga på den tilltänkta delningen av kunduppgifter mellan bankerna eftersom delningen inte avser kontroller mot så kallade sanktionslistor. IMY kommer därför inte att beröra dessa föreskrifter inom ramen för denna rapport.

IMY noterar att det finns pågående lagstiftningsinitiativ som bland annat berör delning av information mellan privata aktörer, såsom exempelvis banker, som kan komma att påverka svensk rätt och möjligheterna för delning.[8] I denna rapport har IMY dock utgått från nu gällande rätt.

[7] Beslutade den 27 september 2024. Föreskrifterna rör bland annat i vilka fall andra än myndigheter får behandla personuppgifter om lagöverträdelser. Ett exempel på ett sådant fall följer av 6 § i föreskrifterna, där det framgår att företag under Finansinspektionens tillsyn får behandla personuppgifter om lagöverträdelser för kontroller av vissa kategorier av registrerade mot så kallade sanktionslistor under vissa närmare beskrivna omständigheter. En sådan omständighet är om behandlingen är nödvändig för att efterleva penningtvättslagen, andra föreskrifter på finansmarknadsområdet eller regelverk på det området utfärdade av utländska myndigheter, EU-organ eller mellanstatliga organisationer. I IMY:s vägledning till IMYFS 2024:1, Vägledning – föreskrifter om behandling av personuppgifter som rör lagöverträdelser, framgår att exempel på föreskrifter och regelverk som avses i 6 § är bland annat regelverk utfärdade av U.S. Department of the Treasury - Office of Foreign Assets Control, rekommendationer från Financial Action Task Force, samt riktlinjer från den europeiska tillsynsmyndigheten European Banking Authority.

[8] Se exempelvis den föreslagna artikel 75 i den kommande Europaparlamentets och rådets förordning (EU) 2024/1624 av den 31 maj 2024 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, som öppnar upp för ett större informationsutbyte mellan olika verksamhetsutövare under översyn av relevanta tillsynsmyndigheter. Se även Finansdepartementets promemoria ”Övervaknings- och rapporteringsskyldighet för clearingbolag” där det föreslås att clearingbolag ska vara skyldiga att övervaka transaktioner, lämna uppgifter om misstänkta transaktioner till banker och rapportera misstänkt penningtvätt eller finansiering av terrorism till Polismyndigheten.

3. Beskrivning av projektet

Bankerna önskar att dela vissa kunduppgifter mellan varandra i syfte att motverka och förhindra att de utnyttjas för penningtvätt, terroristfinansiering och bedrägerier. Tanken är att bankerna ska genomföra detta samarbete på egen hand, utan att involvera brottsbekämpande myndigheter eller tillsynsmyndigheter. Den planerade delningen är tänkt att ske genom att bankerna ”flaggar” potentiella, befintliga och avvisade/avslutade kunder som bedöms kunna utgöra en förhöjd risk avseende penningtvätt, finansiering av terrorism eller bedrägerier i ett IT-system som övriga banker har tillgång till. Övriga banker har då, inom ramen för det egna kundkännedomsarbetet, möjlighet att söka efter en potentiell eller befintlig kund i systemet genom att ”pinga” systemet om kunden. Varje bank bedömer själv när det är nödvändigt att pinga en individ mot systemet. Om den potentiella eller befintliga kunden har flaggats av en annan bank, indikerar det att den pingande banken kan behöva vidta utökade åtgärder för kundkännedom eftersom individen då kan anses ha en förhöjd riskprofil.

3.1. Vad är en banks kundkännedomsprocess?

För att försvåra och motverka ekonomisk brottslighet måste verksamhetsutövare[9] som bedriver bank- eller finansieringsrörelse enligt penningtvättslagen ha goda kunskaper om sina kunder och kundernas affärer och transaktioner (även känt som Know-Your-Customer, KYC). Det är för att förhindra att verksamhetsutövaren utnyttjas för penningtvätt eller finansiering av terrorism. Utan tillräcklig kundkännedom får inte verksamhetsutövaren etablera eller upprätthålla en affärsrelation eller utföra en transaktion för kundens räkning, enligt 3 kap. 1 § penningtvättslagen. Med ”tillräcklig kundkännedom” avses tillräcklig kännedom om en kund för att dels kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen, dels kunna övervaka och bedöma kundens aktiviteter och transaktioner.

Vilka åtgärder som vidtas för att uppnå kundkännedom ska utgå från kundens riskprofil, det vill säga vilken risk kunden representerar när det gäller penningtvätt eller finansiering av terrorism, utifrån verksamhetsutövarens allmänna riskbedömning. Den allmänna riskbedömningen inkluderar, enligt 2 kap. 1 § penningtvättslagen, en bedömning av hot och sårbarheter kopplat till verksamhetsutövarens produkter, tjänster, kunder, distributionskanaler och geografiska marknader, men också en bedömning av risken hos den enskilda individen. Det handlar bland annat om att vidta åtgärder för att säkerställa en individs identitet på distans, inhämta uppgifter om syftet med affärsförbindelsen och omfattningen av kundrelationen. Detta underlag ligger sedan till grund för att bestämma individens riskprofil. Om det framkommer faktorer som tyder på hög risk ska verksamhetsutövaren, enligt 3 kap. 16 § penningtvättslagen, vidta skärpta åtgärder för kundkännedom.[10]

Skyldigheten att inhämta och bedöma uppgifter om en kund gäller inför att affärsförbindelsen mellan kunden och verksamhetsutövaren inleds men också löpande

[9] Definitionen av ”verksamhetsutövare” enligt 1 kap. 8 § p. 8 penningtvättslagen är ”en fysisk eller juridisk person som utför verksamhet som omfattas av denna lag”.
[10] I EBA:s riktlinjer ”Riktlinjer enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 för kundkännedom och de faktorer som kreditinstitut och finansiella institut bör beakta vid bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser och enstaka transaktioner (riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism) som upphäver och ersätter riktlinjerna JC/2017/37om åtgärder för utökad kundkännedom”, beskrivs exempel på åtgärder som kan behöva vidtas för utökad kundkännedom i p. 4.64.

under hela affärsförbindelsen. Löpande uppföljning innebär, enligt 3 kap. 13 § penningtvättslagen, att verksamhetsutövaren ska följa upp pågående affärsförbindelser och övervaka kundens transaktioner och andra aktiviteter i syfte att säkerställa att verksamhetsutövarens kundkännedom är aktuell och tillräcklig för att hantera risken för penningtvätt och finansiering av terrorism. Om en verksamhetsutövare, vid inledningen av en affärsförbindelse eller under den löpande uppföljningen, får skälig grund att misstänka att kunden ägnar sig åt penningtvätt eller finansiering av terrorism, ska detta enligt 4 kap. 3 § penningtvättslagen rapporteras till finanspolisen. Verksamhetsutövaren kan även göra en polisanmälan om det finns misstanke om brott. Att göra en sådan anmälan är dock inte ett uttryckligt krav enligt penningtvättslagen.

Vid misstanke om bedrägeri har en betaltjänstleverantör[11], såsom en bank, inte någon skyldighet att behandla personuppgifter enligt betaltjänstlagen. Banken får däremot behandla personuppgifter om det exempelvis är nödvändigt för att granska betalningstransaktioner, enligt 6 kap. 1 § betaltjänstlagen. Banken får då behandla uppgifter om identitet och unika beteckningar som identifierar en viss person som en betaltjänstanvändare. Enligt 6 kap. 4 § får banken föra register som endast får innehålla namn och person-, samordnings- eller organisationsnummer, betalkontonummer eller motsvarande, unika beteckningar som identifierar en viss person som en betaltjänstanvändare, och övriga uppgifter som framkommit vid granskningen av betalningstransaktioner. Om misstanke om bedrägeri kvarstår efter närmare analys får uppgifterna rapporteras till polis eller åklagare, men det föreligger inte någon sådan skyldighet enligt betaltjänstlagen.

3.2. Flaggning av en kund

Flaggning skulle, enligt det planerade upplägget, innebära att en eller flera av bankerna markerar en potentiell, befintlig eller avvisad/avslutad kund som en individ med förhöjd risk i systemet. Att en individ registreras i bankernas gemensamma system skulle alltså innebära att denne ”flaggas”. Syftet med flaggningen är att informera andra banker om att personen bedömts ha en förhöjd riskprofil. På så sätt skulle andra banker kunna vidta nödvändiga kundkännedomsåtgärder innan en eventuell affärsförbindelse inleds. Åtgärder skulle också kunna behöva vidtas löpande under kundförhållandet, om det krävs för att säkerställa tillräcklig kundkännedom.

Den bank som flaggar en individ i systemet ska inte få kännedom om huruvida någon annan bank också har flaggat samma individ. Vidare ska ingen information delas mellan bankerna om vilken bank som gjort en sökning i systemet.

En bank ska inte få flagga en individ godtyckligt, utan endast om individen uppfyller särskilda kriterier som bankerna gemensamt har beslutat ska gälla för flaggning. Dessa kriterier som beskrivs närmare i avsnitt 3.5 nedan fungerar som indikatorer på att individen har en förhöjd riskprofil.

3.3. Pingning av en kund

Pingning skulle innebära att en bank skickar en förfrågan till systemet för att få fram information om huruvida någon annan bank har bedömt att den aktuella kunden förknippas med en förhöjd risk för penningtvätt, terroristfinansiering och/eller bedrägeri. Genom att skicka en förfrågan till systemet om huruvida en viss person,

[11] För en fullständig definition av begreppet ”betaltjänstleverantör”, se 1 kap. 3 § betaltjänstlagen.

med namn och personnummer, finns i systemet kan banken få information om individen har flaggats av en annan bank. När en bank skickar en sådan förfrågan benämns det i rapporten som att banken ”pingar” de andra bankerna. En pingande bank ska inte få kännedom om vilken bank som kan ha flaggat individen. Vidare ska det inte vara möjligt att ta reda på vilken som är den pingande banken, det vill säga den bank som har sökt efter en individ i systemet. Varje bank bestämmer själv när den skickar en pingning till systemet inom ramen för sin egen kundkännedomsprocess. Pingningen är alltså inte tänkt att ske automatiskt.

3.4. Beskrivning av den tilltänkta delningen i systemet

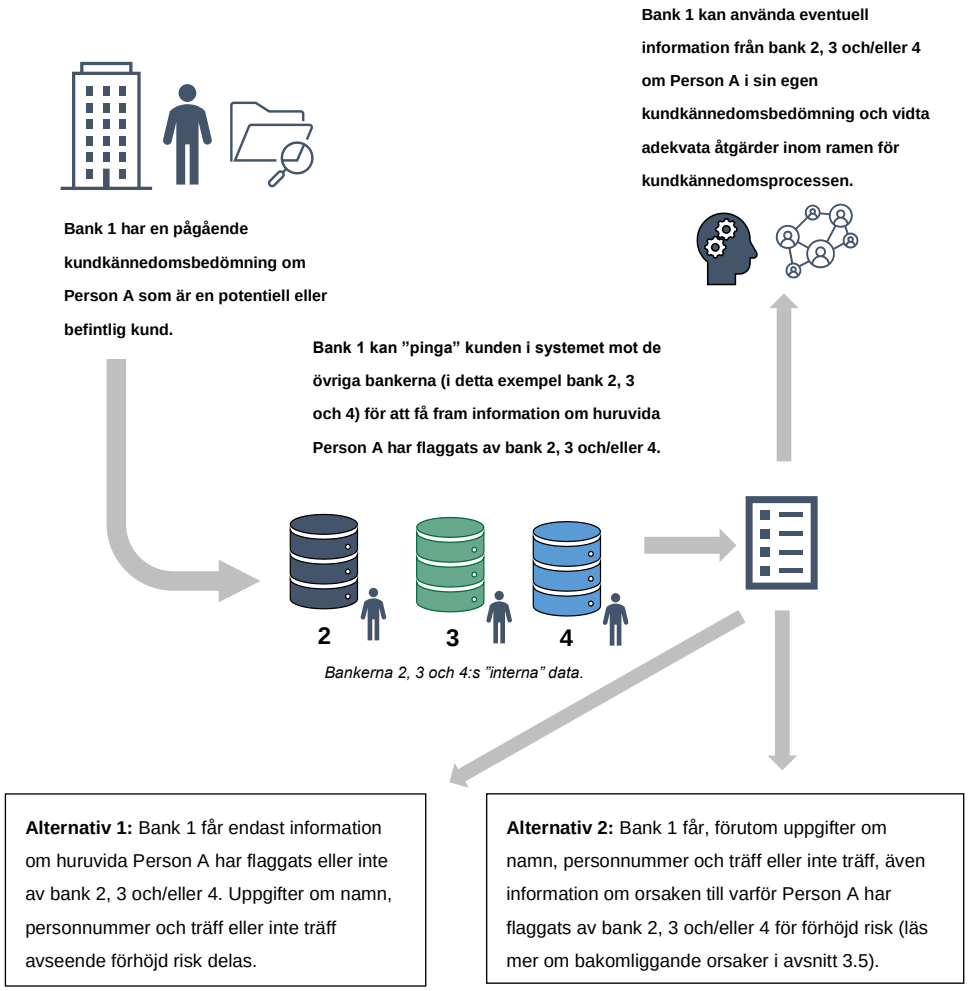
För de uppgifter som bankerna avser att dela med varandra inom ramen för projektet tänker de sig två olika alternativ.

I det första alternativet (alternativ 1) delar bankerna endast information om huruvida en viss individ är flaggad i systemet eller inte. Den enda information som delas är individens namn, personnummer och om individen är flaggad i systemet eller inte. Bankerna delar inga ytterligare uppgifter mellan varandra. Om flera av bankerna har flaggat en och samma individ visas ändå bara en flagga i systemet, utan att det framgår vilka eller hur många av bankerna som har gjort flaggningen.

I det andra alternativet (alternativ 2) delar bankerna samma information som i alternativ 1, det vill säga namn, personnummer och information om individen är flaggad i systemet eller inte. Utöver detta delar bankerna även information om den bakomliggande orsaken till flaggningen, det vill säga den specifika grund som har lett till bedömningen att individen har en förhöjd riskprofil. Om en individ har flaggats på flera olika grunder visas en separat flagga för varje orsak. Om däremot flera banker har flaggat individen av samma orsak visas endast en flagga för just den orsaken, oavsett hur många av bankerna som har gjort flaggningen.

Enligt reglerna om kundkännedom behöver bankerna vidta skärpta åtgärder för kundkännedom om det framkommer faktorer som tyder på en förhöjd risk kopplat till en kund. Varje bank som efter en pingning noterar att en individ är flaggad i systemet behöver därför även fortsättningsvis göra sin egen riskbedömning. En flaggning i systemet ska inte i sig innebära att en individ kan avfärdas som kund, utan detta fungerar endast som en indikator på att banken kan behöva vidta ytterligare åtgärder för kundkännedom. Varje bank kommer alltså att behöva göra sin egen bedömning av kunden och därefter bestämma kundens riskprofil. Värderingen och vilka åtgärder som banken väljer att vidta när banken får kännedom om att individen är flaggad i systemet kan därmed skilja sig från bank till bank.

Flödeskartan nedan illustrerar hur informationen är avsedd att delas mellan bankerna enligt alternativ 1 respektive alternativ 2.



3.5. Vilka uppgifter önskar bankerna dela med varandra?

Varje bank som har deltagit i projektet hämtar idag in sin egen kund- och transaktionsdata. Informationen samlas in från olika register och databaser som tillhandahålls av externa leverantörer och används för att få en bättre bild av kunden och dennes aktiviteter. Därutöver inhämtar bankerna information direkt från kunden genom exempelvis frågeformulär. Den samlade informationen används sedan för bankernas interna kundkännedomsprocess. För att ytterligare motverka penningtvätt, terroristfinansiering och bedrägerier önskar bankerna också kunna dela vissa kunduppgifter i syfte att utröna om en viss individ bedömts ha en förhöjd riskprofil av en annan bank.

Förhöjd risk föreligger när en bank gör, eller har gjort, bedömningen att en *potentiell*, *befintlig eller avvisad/avslutad kund*, är förknippad med en förhöjd risk för penningtvätt, finansiering av terrorism och/eller bedrägeri.

De faktorer som inom projektet leder till att en potentiell, befintlig eller avvisad/avslutad kund flaggas av en bank i systemet listas nedan. Dessa bakomliggande orsaker är

endast tänkta att delas med den pingande banken i alternativ 2 i enlighet med den ovan beskrivna flödeskartan. En kund flaggas i systemet om kunden har:

1. rapporterats av banken till Polismyndigheten eller Åklagarmyndigheten för misstänkt bedrägeri enligt 6 kap. 5 § betaltjänstlagen

2. rapporterats av banken till Polismyndigheten för misstänkt penningtvätt (inklusive är en så kallad möjliggörare[12] eller målvakt[13]) enligt 4 kap. 3 § penningtvättslagen

3. rapporterats av banken till Polismyndigheten för misstänkt terroristfinansiering enligt 4 kap. 3 § penningtvättslagen

4. polisanmälts av banken eller av en extern part[14] för misstänkt penningtvätt, terroristfinansiering eller bedrägeri

5. polisanmälts av banken eller av en extern part i egenskap av möjliggörare[15] eller misstänkt insider vid penningtvätt, terroristfinansiering eller bedrägeri

6. polisanmälts av banken eller av en extern part i egenskap av målvakt[16] vid penningtvätt, terroristfinansiering eller bedrägeri

7. nekats att bli kund eller avslutats som kund på grund av att en bank, efter en intern bedömning enligt penningtvättslagen, har identifierat förhöjd risk för penningtvätt, terroristfinansiering eller bedrägeri.

Alla bakomliggande orsaker enligt ovan relaterar till förhöjd risk för penningtvätt, terroristfinansiering eller bedrägeri. De utgör gemensamma faktorer som bankerna har kommit överens om och är tänkta att ge en indikation till den pingande banken om att en viss individ är förknippad med en förhöjd risk.

Att en kund har rapporterats av en bank innebär att någon av de banker som använder systemet har lämnat uppgifter till finanspolisen med anledning av misstänkt bedrägeri, penningtvätt eller terroristfinansiering kopplat till individen. Att en kund har polisanmälts av banken eller en extern part innebär att antingen någon av bankerna som deltar i samarbetet eller en extern part, till exempel en annan bankkund, har polisanmält kunden i fråga och att banken därefter, efter egen utredning, bedömt att det finns fog för anmälan. Om banken däremot bedömer att anmälan saknar grund, eller att anmälan inte påverkar kundens riskprofil, flaggas kunden inte i systemet.

---

[12] Se exempelvis följande källor för definition av "möjliggörare": BRÅ, och Polismyndigheten, "Lägesbild över aktiva gängkriminella i Sverige", februari 2024.
[13] Se exempelvis följande källor för definition av "målvakt": Polismyndigheten.
[14] Extern part i detta sammanhang kan exempelvis vara en kund till banken som har polisanmält en annan kund, eller någon annan som kontaktar banken och informerar om att en polisanmälan har gjorts mot en kund till banken. En bank kan också få information från en myndighet, till exempel Polismyndigheten, om att en extern part har polisanmält en kund. Varje bank ska därefter bedöma relevansen av en sådan polisanmälan och avgöra om den medför en förändrad riskbild för kunden, det vill säga om den indikerar en förhöjd risk. I sådant fall kan det finnas behov av en uppdaterad eller utökad KYC (kundkännedom) för den aktuella kunden, vilket i sin tur kan motivera att kunden flaggas i systemet.
[15] Se till exempel följande källor för definition av "möjliggörare": BRÅ och Polismyndigheten.
[16] Se till exempel följande källor för definition av "målvakt": Polismyndigheten.

4. Kan flaggning utgöra uppgift om lagöverträdelser enligt artikel 10 i dataskyddsförordningen?

Mot bakgrund av att de bakomliggande orsakerna enligt punkterna 1–7, som beskrivits i avsnitt 3.5 ovan, kan vara relaterade till uppgifter om brott, blir det relevant att utreda om dessa uppgifter kan anses utgöra uppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen. Detta får även betydelse för frågan om rättslig grund för behandlingen.

4.1. Vilka typer av personuppgifter omfattas av artikel 10?

Behandling av personuppgifter som rör fällande domar i brottmål och personuppgifter som rör lagöverträdelser som innefattar brott och därmed sammanhängande säkerhetsåtgärder regleras i artikel 10 i dataskyddsförordningen. Enligt denna bestämmelse får behandling av sådana uppgifter endast ske under kontroll av en myndighet eller då behandlingen är tillåten enligt EU-rätten eller medlemsstaternas nationella rätt, förutsatt att lämpliga skyddsåtgärder fastställs för de registrerades rättigheter och friheter. Vidare får ett fullständigt register över fällande domar i brottmål enbart föras under kontroll av en myndighet.

Personuppgifter om lagöverträdelser kan delas in i två kategorier: dels uppgifter som är kopplade till rättsliga förfaranden, dels uppgifter om misstankar om brott där något rättsligt förfarande inte har inletts.

4.2. Rättsliga förfaranden

Av EU-domstolens dom i målet GC m.fl. [17] följer att information om ett rättsligt förfarande som inletts mot en fysisk person utgör brottsuppgifter, oberoende av om det brott som personen åtalats för faktiskt har styrkts eller inte under domstolsförfarandet.[18] EU-domstolen har således bedömt att uppgifter om att det inletts en förundersökning eller en rättegång i ett brottmål omfattas av skyddet i artikel 10. IMY har bedömt att detta gäller även en uppgift om att en fysisk person har polisanmälts, eftersom ett rättsligt förfarande därmed har inletts.[19]

Enligt IMY:s bedömning följer av EU-domstolens dom i målet GC m.fl. att artikel 10 även omfattar uppgifter om att en fysisk person tidigare har varit föremål för ett rättsligt förfarande utan att det meddelats en fällande dom. [20] Detta innebär att till exempel uppgifter om en nedlagd förundersökning eller en friande dom i ett brottmål omfattas av skyddet i artikel 10.

4.3. Misstankar om brott utan att ett rättsligt förfarande har inletts

Frågan om huruvida uppgifter om misstankar om brott utanför rättsliga förfaranden omfattas av begreppet ”lagöverträdelser” saknar vägledande praxis från EU-

[17] GC m.fl. (Borttagande av länkar till känsliga uppgifter) C-136/17, EU:C:2019:773.
[18] GC m.fl. C-136/17, EU:C:2019:773, punkt 72.
[19] IMY:s beslut 2021-05-03 i dnr DI-2021-1856.
[20] Se vidare IMY:s rättsliga ställningstagande IMYRS 2021:1 – Rättsliga förfaranden s. 14.

domstolen. Det finns heller inte något tydligt svar på frågan i beslut eller vägledning från den Europeiska dataskyddsstyrelsen (EDPB).

IMY har bedömt att uttrycket ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen – i avvaktan på praxis från EU-domstolen eller tydlig vägledning från EDPB – bör ges samma innebörd som motsvarande uttryck i den numera upphävda personuppgiftslagen (1998:204).[21] Vägledning finns i detta avseende att hämta i svensk praxis, särskilt i ett avgörande från Högsta förvaltningsdomstolen (HFD), det så kallade TankStopp-målet.[22] Här berörde HFD frågan om uppgifter om misstankar om brott kan anses utgöra uppgifter om lagöverträdelser.

Målet rörde en databas där företag och privatpersoner kunde se uppgifter om misstänkta bensinsmitningar (det vill säga fall där någon tankat bensin utan att betala för sig). Uppgifterna omfattade registreringsnummer på de inblandade fordonen samt eventuella beskrivningar av händelseförloppet. En av huvudfrågorna i målet avsåg om denna typ av uppgifter utgjorde personuppgifter om lagöverträdelser enligt personuppgiftslagen, särskilt eftersom databasen omfattade uppgifter om misstänkta lagöverträdelser. HFD fann att registrering av uppgifter om fordon som förekommit i samband med obetalda tankningar utgjorde en behandling av personuppgifter om lagöverträdelser eftersom det rörde sig om påstådda brott, även om något rättsligt förfarande ännu inte inletts.

Mot bakgrund av detta avgörande har IMY bedömt att uppgifter om att en fysisk person har, eller kan ha, begått ett visst brott utgör personuppgifter om lagöverträdelser även i fall där något rättsligt förfarande inte har inletts.[23]

Frågan om vilka uppgifter som omfattas av brottsmisstankar har också behandlats i förarbetena till lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) där följande anges:

”Frågan om i vilken utsträckning brottsmisstankar omfattas av begreppet lagöverträdelser som innefattar brott har varit föremål för diskussion. Datalagskommittén menade att en uppgift om att någon har eller kan ha begått stöld otvivelaktigt utgör en uppgift om lagöverträdelse, även om det inte finns någon dom beträffande brottet. Uppgifter om faktiska iakttagelser om en persons handlande kunde dock enligt Datalagskommittén inte rimligen anses som uppgifter om lagöverträdelser i alla de fall handlandet kan innebära en lagöverträdelse (SOU 1997:39 s. 380). Högsta förvaltningsdomstolen har i det s.k. TankStopp-målet (HFD 2016 ref. 8) uttalat att registrering av uppgifter om fordon som förekommit i samband med obetalda tankningar ska anses innefatta en behandling av personuppgifter om lagöverträdelser som innefattar brott i den mening som avses i personuppgiftslagen. Utredningen har mot denna bakgrund, i avsaknad av klargörande EU-rättslig praxis, bedömt att misstankar om brott bör omfattas av artikel 10 i dataskyddsförordningen i samma utsträckning som de gör enligt personuppgiftslagen.”[24]

[21] Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen, s. 15.
[22] HFD 2016 ref. 8.
[23] HFD 2016 ref. 8. s. 3 ff. Se även avsnittet ”IMY:s rättsliga ställningstagande” nedan.
[24] Prop. 2017/18:105, s. 98 f.

IMY:s praxis

I det så kallade BankID-beslutet[25] från IMY (då Datainspektionen) från 2020 beviljades ett antal banker tillstånd att behandla uppgifter om lagöverträdelser genom att använda en gemensam spärrlista för BankID. Denna lista skulle upprättas av bankerna i syfte att förhindra bedrägerier och missbruk av BankID-tjänsten genom att blockera individer som utnyttjade tjänsten på ett otillåtet sätt. Spärrlistan innehöll endast personnummer och utgångsdatum för spärrarna, utan att avslöja skälen bakom dem. Eftersom spärrar kunde införas på grund av misstänkt brottslig aktivitet eller avtalsbrott, ansåg IMY att hela listan omfattades av artikel 10 i dataskyddsförordningen. Detta motiverades med att underlaget för spärrarna kunde kopplas till potentiella brott. IMY resonerande enligt följande i beslutet:

”Bolaget har uppgett att Bolagens tilltänkta användning av spärrlistan på grund av avtalsbrott skulle kunna inbegripa bl.a. misstanke om brottslig handling. Även om uppgifter om varför en spärr införts, t.ex. på grund av misstanke om brottslig handling, inte skulle behandlas i själva spärrlistan, behandlar det Bolag som fattat beslut om en sådan spärr likväl beslutsunderlaget till spärren i egenskap av personuppgiftsansvarig.

Datainspektionen anser därför att de personuppgifter som Bolaget kommer att behandla avseende de individer som finns upptagna i spärrlistan baserat på personnummer, måste ses i ett sammanhang och inte separat.

Det sagda innebär att möjligheten att sammankoppla en uppgift (vilket i detta fall skulle vara beslutsunderlag för en spärr på grund av avtalsbrott i form av misstanke om brottslig handling) till en individ (vilket i detta fall skulle vara en spärr, baserad på personnummer) i princip ska vara utesluten i praktiken, för att inte anses utgöra en så kallad brottsuppgift.

Mot bakgrund av det anförda, konstaterar Datainspektionen att behandlingen i spärrlistan innefattar behandling av personuppgifter som rör lagöverträdelser.”

IMY:s rättsliga ställningstagande

IMY har i ett rättsligt ställningstagande (IMYRS 2021:1)[26] ytterligare klargjort begreppet "personuppgifter som rör lagöverträdelser". När det gäller misstankar om brott uttalar IMY följande:

”Uppgifter om att en fysisk person har eller kan ha begått ett visst brott (brottsmisstankar) kan utgöra brottsuppgifter, även om något rättsligt förfarande inte har inletts. För detta krävs normalt att uppgifterna har en viss konkretionsgrad. En tillräcklig konkretionsgrad har nåtts om uppgifterna avser ett visst brott eller en viss brottskategori. En tillräcklig konkretionsgrad kan också nås genom att uppgifter sammanställs på ett sådant sätt att uppgifterna motsvarar de objektiva rekvisiten i en straffbestämmelse. Om syftet med behandlingen helt eller delvis är att behandla brottsuppgifter, talar det för att det är fråga om brottsuppgifter.”

Vad gäller faktiska iakttagelser eller passiv registrering av händelseförlopp, exempelvis vid kamerabevakning, utgör dessa normalt inte behandling av uppgifter enligt artikel 10

[25] Datainspektionens beslut 2020-06-25, dnr DI-2020-3321-3321 m.fl., Beslut om tillstånd att behandla personuppgifter om lagöverträdelser.
[26] Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen.

även om objektiva brottsrekvisit uppfylls. Dock blir det fråga om brottsuppgifter om inspelat material senare avskiljs för dokumentation, uppföljning eller polisanmälan.

4.4. Behandling av personuppgifter om lagöverträdelser

Vad som är en behandling av personuppgifter definieras i artikel 4.2 i dataskyddsförordningen. Med behandling avses i princip allt som kan göras med en uppgift. Det kan till exempel vara att samla in, registrera, lagra, dela, analysera, lämna ut eller radera dem. Begreppet ”behandling” har i likhet med begreppet ”personuppgifter” en vid innebörd. Nästintill all hantering av personuppgifter är att betrakta som en behandling utifrån ett dataskyddsrättsligt perspektiv.

När det gäller behandling av personuppgifter om lagöverträdelser är bestämmelsen i artikel 10 i dataskyddsförordningen restriktiv i sin tillämpning och tillåter endast behandling under vissa särskilda förutsättningar. Behandlingen får endast utföras:

1. under kontroll av en myndighet, eller
2. när det är tillåtet enligt EU-rätten eller medlemsstaternas nationella rätt, förutsatt att lämpliga skyddsåtgärder för de registrerades rättigheter och friheter finns på plats.

Det framgår av 3 kap. 8–9 §§ dataskyddslagen att personuppgifter som avses i artikel 10 i dataskyddsförordningen får behandlas av andra än myndigheter om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. I andra fall får regeringen, eller den myndighet som regeringen bestämmer, meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter. Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter. Ett sådant beslut får förenas med villkor.

Det följer av 5 § förordningen (2018:219) med kompletterande bestämmelser till dataskyddsförordningen (kompletteringsförordningen) att personuppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen får behandlas av andra än myndigheter om behandlingen är nödvändig för att:

1. rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller
2. en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

IMY har med stöd av 3 kap. 9 § dataskyddslagen och 6 § andra stycket kompletteringsförordningen möjlighet att meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter om lagöverträdelser och även i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter.[27]

4.5. IMY:s kommentarer

I detta projekt önskar bankerna att dela information om en individs namn, personnummer och flaggning (alternativ 1), eller en individs namn, personnummer och flaggning tillsammans med uppgifter om den bakomliggande orsaken till flaggningen (alternativ 2). Informationen är kopplad till en potentiell, befintlig eller avvisad/avslutad kund. Punkterna 1–3 rör rapportering till Polismyndigheten eller Åklagarmyndigheten, det vill säga uppgifter om att en individ har rapporterats för misstänkt bedrägeri,

[27] Se vidare avsnitt 5 nedan om rättslig grund för behandling av personuppgifter om lagöverträdelser.

penningtvätt eller terroristfinansiering enligt penningtvättslagen. Punkterna 4–6 rör polisanmälningar gjorda av banken eller en extern part, exempelvis uppgifter om att en individ har polisanmälts som möjliggörare eller målvakt vid penningtvätt. Punkten 7 rör nekande eller avslutande av en kundrelation till följd av bankens interna riskbedömning baserad på bestämmelserna i penningtvättslagen.

IMY bedömer att bankernas planerade informationsdelning, enligt både alternativ 1 och alternativ 2, utgör en behandling av personuppgifter enligt dataskyddsförordningen. I båda alternativen ska uppgifter som kan knytas till en enskild individ, såsom namn och personnummer, delas med en annan verksamhet. I alternativ 2 ska även information om den bakomliggande orsaken till att individen har flaggats delas med den pingande banken. Eftersom uppgifterna ska delas mellan bankerna rör det sig om en behandling av personuppgifter i dataskyddsförordningens mening.

De uppgifter som avses i punkterna 1–6 utgör uppgifter om anmälan eller rapport till polisen om misstänkta brott. Dessa uppgifter omfattas med utgångspunkt i IMY:s praxis av artikel 10 i dataskyddsförordningen. När det gäller uppgifter som avses i punkten 7 kan konstateras att en riskbedömning *i sig* normalt inte utgör en uppgift om lagöverträdelser.

Detta medför att en flaggning kommer innebära att den berörda personen med stor sannolikhet varit föremål för rapport eller anmälan om misstanke om brott. Det kommer sannolikt inte gå att utesluta möjligheten att sammankoppla flaggningen med en uppgift om lagöverträdelser. IMY:s praxis (särskilt BankID-beslutet) innebär att uppgifterna i sådana fall utgör uppgifter som omfattas av artikel 10.

Det sagda innebär att behandlingen gällande både alternativ 1 (att dela uppgifter om en individs namn och personnummer tillsammans med information om individen är flaggad i systemet) och alternativ 2 (att dela uppgifter om en individs namn och personnummer samt information om att individen är flaggad i systemet tillsammans med den bakomliggande orsaken) utgör en personuppgiftsbehandling som omfattas av artikel 10 i dataskyddsförordningen.

5. Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för att dela uppgifter enligt alternativ 1 eller alternativ 2 inom ramen för en annan banks kundkännedomsprocess och riskbedömning?

Enligt artikel 5.1 a i dataskyddsförordningen ska personuppgifter behandlas på ett lagligt sätt. För att behandlingen ska anses vara laglig krävs att åtminstone ett av villkoren i artikel 6.1 är uppfyllt.

Enligt principen om ansvarsskyldighet i artikel 5.2 i dataskyddsförordningen ska den personuppgiftsansvarige ansvara för och kunna visa att behandlingen är förenlig med principerna i artikel 5.1.

Med beaktande av den tilltänkta personuppgiftsbehandlingens art och syfte, kommer IMY i detta avsnitt inte närmare att utreda de rättsliga grunderna samtycke enligt artikel 6.1 a i dataskyddsförordningen eller avtal enligt artikel 6.1 b. Det gäller främst på grund av att ett krav på samtycke från den registrerade i princip hade omöjliggjort bankernas syfte att förhindra penningtvätt, terroristfinansiering och bedrägeri. Den aktuella personuppgiftsbehandlingen skulle också sannolikt anses gå utöver vad som objektivt sett är nödvändigt för att kunna fullgöra ett avtal om banktjänster med en registrerad, eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.[28]

Såsom har framförts i avsnitt 4 ovan, följer det av artikel 10 i dataskyddsförordningen att behandling av personuppgifter som rör lagöverträdelser som huvudregel endast får utföras under kontroll av en myndighet, eller då behandlingen är tillåten enligt EU-rätten eller medlemsstaternas nationella rätt. Då bankerna inte omfattas av huvudregeln som gäller för myndigheter, innebär det att det behövs rättsligt stöd i EU-rätten eller i svensk rätt för att den tilltänkta personuppgiftsbehandlingen ska anses vara tillåten enligt artikel 10.

Sådant rättsligt stöd finns i 3 kap. 9 § dataskyddslagen och 6 § kompletteringsförordningen där det framgår att andra än myndigheter får behandla personuppgifter om lagöverträdelser med stöd av meddelade föreskrifter av IMY eller med stöd av meddelat tillstånd av IMY i enskilda fall. Som tidigare nämnts har IMY inte utfärdat några föreskrifter som kan tillämpas i det aktuella fallet. Vidare följer det av 5 § kompletteringsförordningen att personuppgifter om lagöverträdelser får behandlas av andra än myndigheter om det är nödvändigt för att fastställa, göra gällande eller försvara rättsliga anspråk, eller för att fullgöra en rättslig förpliktelse enligt lag eller förordning.

[28] Jfr EDPB:s uttalande om detta i ”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 subject”, version 1.0, 8 oktober 2019, s. 14.

5.1. Rättslig förpliktelse enligt artikel 6.1 c i dataskyddsförordningen

Det följer av artikel 6.1 c i dataskyddsförordningen att en personuppgiftsbehandling kan vara laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

Enligt artikel 6.3 i dataskyddsförordningen ska den grund för behandlingen som avses i artikel 6.1 c fastställas i enlighet med EU-rätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, vilket är svensk rätt i detta fall. Av bestämmelsen framgår vidare att syftet med behandlingen ska fastställas i den rättsliga grunden. Det innebär att denna rättsliga grund behöver kompletterande regler utöver vad som framgår av dataskyddsförordningen.

Av skäl 41 i dataskyddsförordningen framgår att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsebar för de som omfattas av den, i enlighet med rättspraxis vid EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen). Kravet på förutsebarhet ska ses från den registrerades – och inte den personuppgiftsansvariges – perspektiv. EU-domstolen har i sin praxis ställt höga krav på utformningen av de rättsliga grunder som ska ligga till grund för personuppgiftsbehandling.[29]

Avseende vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en personuppgiftsbehandling ska anses vara nödvändig, har regeringen i förarbetena till dataskyddslagen uttalat att detta måste bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär.[30] Regeringen framförde vidare att ett mer kännbart intrång kräver en mer preciserad rättslig grund, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund.

Det följer av skäl 45 i dataskyddsförordningen att behandling som grundar sig på bland annat en rättslig förpliktelse som åvilar den personuppgiftsansvarige, bör ha en grund i EU-rätten eller i en medlemsstats nationella rätt. Vidare framgår det av aktuellt skäl att dataskyddsförordningen inte medför något krav på en särskild lag för varje enskild behandling, utan det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Behandlingens syfte bör också fastställas i EU-rätten eller i medlemsstaternas nationella rätt.

Relevanta bestämmelser i penningtvättslagen

Mot bakgrund av kraven i artiklarna 6.1 c och 6.3 i dataskyddsförordningen blir det nödvändigt att redogöra för relevant nationell lagstiftning i förhållande till

---

[29] EU-domstolens dom den 24 februari 2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 83, där EU-domstolen uttalar följande: ”I detta sammanhang ska det dock erinras om att för att uppfylla det proportionalitetskrav som föreskrivs i artikel 5.1 c i förordning 2016/679 (se för ett liknande resonemang, dom av den 22 juni 2021, Latvijas Republikas Saeima (Prickning), C-439/19, EU:C:2021:504, punkt 98 och där angiven rättspraxis), måste de föreskrifter som ligger till grund för behandlingen innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter lämnas ut ges tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Dessa föreskrifter måste även vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd för behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt (dom av den 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punkt 68 och där angiven rättspraxis)”.

[30] Prop. 2017/18:105, s. 51.

personuppgiftsbehandlingen i fråga. I sammanhanget är penningtvättslagen mest aktuell med beaktande av de bakomliggande orsaker som bankerna har uppgett att de avser att förhålla sig till.

Av 5 kap. 2 § penningtvättslagen följer att en verksamhetsutövare får behandla personuppgifter i syfte att kunna fullgöra sina skyldigheter enligt penningtvättslagen.

Enligt 5 kap. 6 § penningtvättslagen får personuppgifter om lagöverträdelser behandlas endast om det är nödvändigt för vissa däri uppräknade ändamål. IMY konstaterar att ändamålet som är relevant inom ramen för detta projekt är det som framgår av punkten 1 och som avser att bedöma den risk som kan förknippas med kundrelationen, det vill säga kundkännedomsskyldigheten som har beskrivits i avsnitt 3 ovan.

Verksamhetsutövares, såsom bankers, delning av personuppgifter om lagöverträdelser med varandra i syfte att fullgöra kundkännedomsskyldigheten är inte uttryckligen reglerat i penningtvättslagen, eller i övrigt i gällande svensk rätt. Däremot finns det vissa bestämmelser i penningtvättslagen som berör delning av personuppgifter bland vissa verksamhetsutövare under vissa omständigheter, samt mellan verksamhetsutövare och myndigheter under vissa förutsättningar. Dessa redogörs för i korthet nedan.

Som utgångspunkt gäller enligt 5 kap. 11 § första stycket penningtvättslagen att den som är verksam hos en verksamhetsutövare inte obehörigen får röja bland annat att personuppgifter om lagöverträdelser behandlas enligt 6 § och att sådana uppgifter bevaras.

Trots detta får exempelvis verksamhetsutövare enligt 3 kap. 21 § penningtvättslagen, inom ramen för vissa åtgärder som ska vidtas för grundläggande kundkännedom (i form av identifiering av kunden, utredning av om kunden har en verklig huvudman samt inhämtande av information om affärsförbindelsens syfte och art), förlita sig på åtgärder som har utförts av en utomstående[31], om verksamhetsutövaren utan dröjsmål:

1. får del av de uppgifter som den utomstående har inhämtat, och
2. på begäran kan få del av den dokumentation som ligger till grund för uppgifterna.

Det följer av 4 kap. 1 § penningtvättslagen att en verksamhetsutövare ska övervaka pågående affärsförbindelser och bedöma enstaka transaktioner. Av 4 kap. 2 § första stycket framgår att om avvikelser eller misstänkta aktiviteter eller transaktioner uppmärksammas enligt 1 § eller på annat sätt, ska en verksamhetsutövare genom skärpta åtgärder för kundkännedom och andra nödvändiga åtgärder bedöma om det finns skälig grund att misstänka att det är fråga om penningtvätt eller finansiering av terrorism, eller att egendom annars härrör från brottslig handling.

Enligt 4 kap. 9 § första stycket penningtvättslagen får en verksamhetsutövare, eller den som är verksam hos verksamhetsutövaren, inte för en kund eller någon utomstående obehörigen röja att en bedömning enligt 2 § utförs, har utförts eller kommer att utföras. Undantag från denna tystnadsplikt finns i andra stycket. Där anges

[31] I 3 kap. 22 § penningtvättslagen anges att med utomstående enligt 21 § avses bland annat fysiska eller juridiska personer som är etablerade inom EES med verksamhet som anges i 1 kap. 2 § första stycket 1, vilket omfattar exempelvis banker.

bland annat i punkten 4 att om uppgifter rör samma kund och samma transaktion, och omfattar fler än en verksamhetsutövare, får uppgifterna lämnas mellan sådana juridiska och fysiska personer som bland annat anges i 1 kap. 2 § första stycket 1 (exempelvis banker), förutsatt att de tillhör samma verksamhets- eller yrkeskategori och omfattas av skyldigheter i fråga om tystnadsplikt och skydd för personuppgifter i penningtvättslagen. Ett annat undantag är om uppgifterna lämnas i samverkan enligt 4 a kap.

Viss samverkan enligt 4 a kap. penningtvättslagen får ske för att förebygga, förhindra eller upptäcka penningtvätt och finansiering av terrorism. I samverkan får brottsbekämpande myndigheter[32], Finansinspektionen och verksamhetsutövare som avses i 1 kap. 2 § första stycket 1 (såsom exempelvis banker), eller brottsbekämpande myndigheter och tillsynsmyndigheter[33], delta. Av 4 a kap. 3 § framgår att den som deltar i samverkan, trots sekretess eller tystnadsplikt och under vissa förutsättningar, ska lämna en uppgift till en annan deltagare om det behövs för mottagarens deltagande i samverkan. Det följer av 4 a kap. 4 § att beslut om samverkan ska fattas av den myndighet eller de myndigheter som deltar i samverkan.

Enligt 5 kap. 8 § penningtvättslagen får en verksamhetsutövares register med uppgifter om misstänkt penningtvätt eller finansiering av terrorism inte samköras med motsvarande register hos någon annan. Undantag finns dock i 9 § för bland annat fall då samkörning av register sker mellan verksamhetsutövare som avses i exempelvis 1 kap. 2 § första stycket 1 (såsom banker), och som ingår i samma koncern, om verksamhetsutövarna har hemvist i Sverige eller inom EES.

Relevanta bestämmelser i betaltjänstlagen

Mot bakgrund av att några av de bakomliggande orsakerna för flaggning som bankerna har kommit överens om enligt vad som framgår av avsnitt 3.5 ovan avser misstanke om bedrägeri, är även betaltjänstlagen relevant då den innehåller bestämmelser om bekämpning av bedrägeri.

I 6 kap. betaltjänstlagen finns det bestämmelser om behandling av personuppgifter i vissa fall. I avsnitt 3.1 ovan har det redogjorts för att en betaltjänstleverantör, såsom en bank, får behandla personuppgifter samt föra register, enligt vad som närmare anges i 6 kap. 2–9 §§ betaltjänstlagen, vid granskning av betalningstransaktioner i syfte att kunna upptäcka sådana transaktioner som kan misstänkas utgöra ett led i bedrägeri. Det följer av förarbeten till betaltjänstlagen att uppräkningen i betaltjänstlagen av de uppgifter som får registreras är uttömmande.[34]

På motsvarande sätt som i penningtvättslagen finns det i betaltjänstlagen bestämmelser om tystnadsplikt. Av exempelvis 3 kap. 12 § första stycket framgår det att den som är eller har varit knuten till ett betalningsinstitut eller betaltjänstleverantör som anställd eller uppdragstagare inte obehörigen får röja eller utnyttja det denne i anställningen eller under uppdraget i verksamheten med betaltjänster har fått veta om enskildas förhållanden till institutet eller leverantören. Det följer vidare av 6 kap. 9 § att den som är verksam hos en betaltjänstleverantör, eller hos den som har ansvar för ett betalningssystem, inte obehörigen får röja uppgifter i ett register som avses i 1 § eller uppgifter som lämnats ut med stöd av 5 § andra stycket betaltjänstlagen.

---

[32] Dessa definieras som Ekobrottsmyndigheten, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket och Åklagarmyndigheten.
[33] Dessa definieras som myndigheter som utövar tillsyn enligt penningtvättslagen.
[34] Prop. 2009/10:220, s. 267.

Det följer av 6 kap. 5 § andra stycket betaltjänstlagen att uppgifter i ett register enligt 1 § får lämnas ut till betaltjänstleverantörer och de som har ansvar för ett betalningssystem när uppgifterna har lämnats till Polismyndigheten eller Åklagarmyndigheten. Det följer vidare av bestämmelsens tredje stycke att ett sådant utlämnande av uppgifter får ske trots tystnadsplikten som gäller bland annat enligt 3 kap. 12 § betaltjänstlagen och den så kallade banksekretessen enligt 1 kap. 10 § banklagen.

5.2. IMY:s kommentarer

IMY konstaterar inledningsvis att bestämmelserna i 5 kap. 2 § och 6 § 1 penningtvättslagen inte föreskriver en skyldighet att dela personuppgifter om lagöverträdelser med andra banker för att dessa ska kunna uppfylla kundkännedomsskyldigheten eller skyldigheterna i penningtvättslagen i övrigt.

Som framgår av redogörelsen i avsnitt 5.1 finns, trots bestämmelserna om tystnadsplikt i penningtvättslagen, vissa bestämmelser som berör delning av personuppgifter bland vissa verksamhetsutövare under särskilda omständigheter, samt mellan verksamhetsutövare och myndigheter under vissa förutsättningar. Enligt IMY:s mening är dock ingen av dessa bestämmelser tillämplig på bankernas tilltänkta delning av personuppgifter om lagöverträdelser inom ramen för detta projekt.

Den tilltänkta delningen gäller inte återanvändning av åtgärder för grundläggande kundkännedom - såsom identifiering av kunden, utredning om verklig huvudman eller inhämtning av information om affärsförbindelsens syfte och art - som exempelvis en annan bank har utfört i enlighet med bestämmelserna i 3 kap. 21–22 §§ penningtvättslagen.

Inte heller undantaget i 4 kap. 9 § andra stycket 4 penningtvättslagen är tillämpligt, då bankernas tilltänkta delning av personuppgifter om lagöverträdelser avser att gå utöver delning av uppgifter som endast rör samma kund, samma transaktion och som omfattar fler än en av bankerna.

Vidare vill bankerna, inom ramen för detta projekt, dela personuppgifter om lagöverträdelser sinsemellan utan att involvera brottsbekämpande myndigheter eller tillsynsmyndigheter i samarbetet. Därför är bestämmelserna om samverkan i 4 a kap. penningtvättslagen inte heller tillämpliga.

Slutligen gäller bankernas planerade delning av personuppgifter om lagöverträdelser inte delning inom en och samma koncern. Undantaget om samkörning av register som följer av 5 kap. 9 § penningtvättslagen är därför inte tillämpligt.

Mot denna bakgrund anser IMY att de aktuella bestämmelserna om delning av personuppgifter i penningtvättslagen inte kan utgöra en rättslig grund enligt artikel 6.1 c i dataskyddförordningen för den delning som bankerna önskar genomföra inom ramen för detta projekt.

Som framgår av redogörelsen i avsnitt 5.1, följer det vidare av 6 kap. 5 § andra stycket betaltjänstlagen att uppgifter i ett register som avses i 1 § får lämnas ut till exempelvis betaltjänstleverantörer, såsom banker, och de som har ansvar för ett betalningssystem när uppgifterna har lämnats till Polismyndigheten eller Åklagarmyndigheten. Av bestämmelsens tredje stycke följer att ett sådant utlämnande av uppgifter får ske trots

tystnadsplikten som gäller bland annat enligt 3 kap. 12 § betaltjänstlagen och den så kallade banksekretessen enligt 1 kap. 10 § banklagen.

IMY konstaterar dock att denna bestämmelse inte föreskriver en skyldighet att dela personuppgifter om lagöverträdelser med andra banker för att dessa ska kunna uppfylla skyldigheter i betaltjänstlagen. Detta stöds även av att bestämmelsen i 6 kap. 1 § betaltjänstlagen inte innebär en skyldighet för en betaltjänstleverantör att behandla personuppgifter samt föra register i syfte att kunna upptäcka sådana transaktioner som kan misstänkas utgöra ett led i bedrägeri. Bestämmelsen ger endast betaltjänstleverantörer en möjlighet att utföra sådan behandling för det nämnda syftet. Det finns inte heller någon skyldighet för betaltjänstleverantörer att rapportera misstankar om bedrägeri till exempelvis finanspolisen, utan betaltjänstleverantörer har enligt 6 kap. 5 § första stycket en möjlighet att lämna sådana uppgifter till Polismyndigheten eller Åklagarmyndigheten om misstanke om bedrägeri kvarstår efter närmare analys.

IMY:s bedömning är därför att bestämmelserna i 6 kap. 1 § och 5 § betaltjänstlagen inte innebär en sådan rättslig förpliktelse som enligt artikel 6.1 c i dataskyddförordningen kan ligga till grund för bankernas tilltänkta delning av personuppgifter inom ramen för projektet.

Med beaktande av vad som anförts ovan är IMY:s samlade bedömning att den tilltänkta delningen av personuppgifter om lagöverträdelser inte kan anses vara nödvändig för att uppfylla en rättslig förpliktelse som följer av lag eller förordning, vare sig enligt penningtvättslagen, betaltjänstlagen eller någon annan författning i svensk rätt.

5.3. Uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen

Bankerna har under projektets gång lyft frågan om den tilltänkta personuppgiftsbehandlingen skulle kunna stödjas på den rättsliga grunden uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen. Frågan ställdes bland annat mot bakgrund av artikel 43 i det så kallade fjärde penningtvättsdirektivet[35] som har införlivats i svensk rätt genom penningtvättslagen. Av denna artikel framgår att behandling av personuppgifter på grundval av direktivet för att förebygga penningtvätt och finansiering av terrorism ska betraktas som något som är i det allmännas intresse enligt det så kallade dataskyddsdirektivet[36]. Detta direktiv införlivades i svensk rätt genom den numera upphävda personuppgiftslagen.

IMY noterar att det inte finns något uttryckligt konstaterande om att behandling av personuppgifter för att förebygga penningtvätt och finansiering av terrorism ska betraktas som något som är i det allmännas intresse, varken i penningtvättslagen eller i dataskyddsförordningen som har ersatt personuppgiftslagen.

Det följer av artikel 6.1 e i dataskyddsförordningen att en personuppgiftsbehandling kan vara laglig om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse, eller som ett led i den personuppgiftsansvariges myndighetsutövning.

[35] Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG.
[36] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Bankernas tilltänkta behandling aktualiserar inte myndighetsutövning och därmed blir frågan istället om bankernas tilltänkta personuppgiftsbehandling av lagöverträdelser skulle kunna anses som nödvändig för att utföra en uppgift av allmänt intresse.

Liksom för rättslig förpliktelse gäller för allmänt intresse, enligt artikel 6.3 i dataskyddsförordningen, att den grund för behandlingen som avses i artikel 6.1 e ska fastställas i enlighet med EU-rätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, vilket i detta fall är svensk rätt. Vidare följer det av bestämmelsen att syftet med behandlingen ska vara nödvändigt för att utföra en uppgift av allmänt intresse. Det framgår även att EU-rätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Det sagda innebär att denna rättsliga grund behöver kompletterande regler utöver vad som framgår av dataskyddsförordningen.

De relevanta bestämmelserna i svensk rätt återfinns i betaltjänstlagen och penningtvättslagen och finns beskrivna i avsnitt 5.1 ovan.

Skäl 41 i dataskyddsförordningen blir tillämplig även i relation till den rättsliga grunden uppgift av allmänt intresse. Såsom har beskrivits under avsnitt 5.1 ovan, framgår det av detta skäl att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsebar för de som omfattas av den.

I förarbetena till dataskyddslagen framförde IMY att det förelåg en risk för att behandling av personuppgifter av vikt för samhällets funktioner inte kunde utföras, om det inte säkerställdes att särskild nationell lagstiftning infördes där det fanns ett behov.[37] Vidare konstaterade IMY att personuppgiftsansvariga måste göra en bedömning av om den författning som kan utgöra rättslig grund för behandlingen uppfyller kraven på bland annat tydlighet, precisering och förutsägbarhet i enlighet med skäl 41 i dataskyddsförordningen.

Regeringen framhöll att kravet i dataskyddsförordningen om att den grund för behandling som avses i bland annat artikel 6.1 e ska vara fastställd i enlighet med EU-rätten eller den nationella rätten inte innebär ett krav på att själva behandlingen av personuppgifter måste regleras, utan det är uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen.[38]

Regeringen konstaterade vidare att detta krav i dataskyddsförordningen innebar en väsentlig förändring för privata aktörer, då det inte längre var självklart att en personuppgiftsansvarig inom den sektorn som utför en uppgift av allmänt intresse kunde utföra nödvändig behandling av personuppgifter på den grunden.[39] Genom kravet på att grunden för behandlingen ska fastställas i enlighet med EU-rätten eller den nationella rätten, begränsas tillämpningsområdet för artikel 6.1 e. Det räcker inte att en behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse utan uppgiften måste också vara fastställd i enlighet med gällande rätt.

Regeringen framförde att när det är tveksamt om den verksamhet som en privat aktör bedriver är av allmänt intresse i EU-rättslig mening, är det istället ofta möjligt att grunda nödvändig behandling på exempelvis ett berättigat intresse i enlighet med

[37] Prop. 2017/18:105, s. 48-49.
[38] Ibid., s. 48.
[39] Ibid., s. 56.

artikel 6.1 f i dataskyddsförordningen.[40] Samma sak gäller om verksamheten visserligen är av allmänt intresse, men uppgiften inte är fastställd i enlighet med vare sig EU-rätten eller den nationella rätten.

Relevanta förarbetsuttalanden

IMY konstaterar att regeringen i en proposition avseende författningsändringar på finansmarknadsområdet med anledning av dataskyddsförordningen ansåg att sådan behandling av personuppgifter som var nödvändig till följd av lagarna på finansmarknadsområdet kunde ske med stöd av dataskyddsförordningen.[41]

IMY framförde i samband med remissbehandlingen att det inte var tillräckligt att endast konstatera att grunden för behandlingen var fastställd i nationell rätt utan att närmare redovisa vilken rättslig grund som avsågs eller beskriva hur den var fastställd.[42] IMY efterfrågade även en redogörelse för vilka överväganden som hade gjorts i fråga om det nationella rättsliga stödet för behandlingen av personuppgifter och som uppfyllde ett mål av allmänt intresse.

Regeringen konstaterade att det på finansmarknadsområdet fanns ett antal lagar enligt vilka såväl myndigheter som privata aktörer åläggs uppgifter och förpliktelser som kräver behandling av personuppgifter, exempelvis skyldigheten för sådana verksamhetsutövare som avses i penningtvättslagen att behandla personuppgifter i syfte att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism.[43] Vidare konstaterade regeringen att de uppgifter som myndigheter och privata aktörer har enligt lagarna på finansmarknadsområdet, eller enligt beslut som har meddelats med stöd av sådana lagar, regelmässigt är uppgifter av allmänt intresse, och att de i vart fall utgör rättsliga förpliktelser. Regeringen ansåg att uppgifterna och förpliktelserna var fastställda i den nationella rätten.

IMY efterfrågade i detta sammanhang ett tydligt utpekande av de rättsliga grunderna för behandlingen av personuppgifter och hur de var fastställda i den nationella rätten.[44] Regeringen ansåg sammanfattningsvis att nödvändig behandling av personuppgifter enligt bestämmelserna på finansmarknadsområdet var tillåten enligt dataskyddsförordningen och att dataskyddsförordningen inte medförde några behov av författningsändringar i detta avseende.[45] Regeringen framhöll dock att det var en annan sak att personuppgiftsansvariga är skyldiga att försäkra sig om att den konkreta behandlingen i det enskilda fallet sker lagligt, det vill säga att det rör sig om nödvändig behandling med rättsligt stöd, och att övriga krav på behandlingen av personuppgifter är uppfyllda.

5.4. IMY:s kommentarer

IMY anser att uppgifterna att bekämpa penningtvätt och finansiering av terrorism enligt penningtvättslagen, och att bekämpa bedrägeri enligt betaltjänstlagen, kan betraktas som uppgifter av allmänt intresse.

---

[40] Ibid., s. 59.
[41] Prop. 2017/18:142, s. 23–24.
[42] Ibid., s. 24.
[43] Ibid., s. 27.
[44] Ibid., s. 27.
[45] Ibid., s. 28.

Dessa uppgifter av allmänt intresse kan ligga till grund för viss personuppgiftsbehandling som får ske med stöd av särskilda bestämmelser i penningtvättslagen och betaltjänstlagen.

Som framgår av redogörelsen i avsnitt 5.1 och IMY:s kommentarer i avsnitt 5.2 ovan, finns det i penningtvättslagen vissa bestämmelser som berör delning av personuppgifter bland vissa verksamhetsutövare under särskilda omständigheter, samt mellan verksamhetsutövare och myndigheter under vissa förutsättningar. IMY:s bedömning är dock att ingen av dessa bestämmelser är tillämplig på bankernas tilltänkta delning av personuppgifter om lagöverträdelser inom ramen för detta projekt.

Som angetts i avsnitt 5.1 ovan följer det av 6 kap. 1 § betaltjänstlagen att betaltjänstleverantörer, såsom banker, har en möjlighet att behandla personuppgifter samt föra register vid granskning av betalningstransaktioner i syfte att kunna upptäcka sådana transaktioner som kan misstänkas utgöra ett led i bedrägeri. Av 6 kap. 2 § framgår det att om det är nödvändigt för granskning av betalningstransaktioner enligt 1 §, får personuppgifter i form av uppgifter om identitet i betaltjänstanvändares pass eller annan identitetshandling och unika beteckningar som identifierar en viss person som betaltjänstanvändare behandlas. Det följer av 6 kap. 3 § att ett register får föras av en betaltjänstleverantör eller den som har ansvar för ett betalningssystem om det är nödvändigt för granskning av betalningstransaktioner enligt 1 §. Av 6 kap. 4 § framgår det att ett register som avses i 1 § endast får innehålla namn och person-, samordnings- eller organisationsnummer, betalkontonummer eller motsvarande, unika beteckningar som identifierar en viss person som en betaltjänstanvändare, och övriga uppgifter som framkommit vid granskningen av betalningstransaktioner. Det framgår vidare av 6 kap. 5 § andra stycket att uppgifter i ett register som avses i 1 § får lämnas ut till exempelvis betaltjänstleverantörer och de som har ansvar för ett betalningssystem när uppgifterna har lämnats till Polismyndigheten eller Åklagarmyndigheten.

Bestämmelsen i 6 kap. 5 § andra stycket ger alltså betaltjänstleverantörer en möjlighet att lämna uppgifter i ett register som avses i 1 §, som förs i syfte att granska betalningstransaktioner för att kunna upptäcka transaktioner som betaltjänstleverantören misstänker utgör ett led i bedrägeri, till andra betaltjänstleverantörer om uppgifterna har lämnats till Polismyndigheten eller Åklagarmyndigheten. Enligt IMY:s mening bör den typ av uppgifter i ett register som omfattas av 6 kap 5 § andra stycket rimligtvis kunna omfatta vissa uppgifter om lagöverträdelser kopplat till bedrägerier. Syftet med regleringen är att möjliggöra informationsdelning som till viss del kan innehålla den typen av uppgifter.

IMY konstaterar dock att bankernas tilltänkta delning av personuppgifter som är föremål för detta projekt har ett mer långtgående och till stor del annat syfte än det som avses i 6 kap. 1 § betaltjänstlagen som tar sikte på granskning av betalningstransaktioner för att kunna upptäcka bedrägerier. Såsom har beskrivits i avsnitt 3 ovan, är bankernas avsikt att informera andra banker om kunder som har bedömts ha en förhöjd riskprofil genom att dela en flagga avseende sådana kunder med övriga banker, vilket gör det möjligt för en pingande bank att vidta utökade åtgärder för kundkännedom mot flaggade kunder. Därtill avser bankernas behandling av personuppgifter att gå utöver de uppgifter som är tillåtna i ett sådant register som 6 kap. 4 § betaltjänstlagen tar sikte på.

Mot bakgrund av det sagda och med hänvisning till beskrivningen samt analysen av de relevanta bestämmelserna i penningtvättslagen och betaltjänstlagen i övrigt enligt

avsnitt 5.1 och 5.2 ovan, är IMY:s bedömning att det inte finns stöd för den delning som bankerna önskar genomföra inom ramen för detta projekt som har beskrivits i avsnitt 3.

IMY:s samlade bedömning är därför att mycket talar emot att den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen kan användas som stöd för bankernas tilltänkta delning av personuppgifter om lagöverträdelser.

5.5. Berättigat intresse enligt artikel 6.1 f i dataskyddsförordningen

Det följer av artikel 6.1 f i dataskyddsförordningen att en behandling kan vara laglig om den är nödvändig för ändamål som rör den personuppgiftsansvariges, eller en tredje parts, berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre. Vid bedömningen ska, enligt skäl 47 i dataskyddsförordningen, de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige beaktas. Ett berättigat intresse kan till exempel finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige. Till exempel kan det gälla i situationer när den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Vidare framgår det av skälet att ett berättigat intresse kräver ”en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske”. Det nämns även uttryckligen att exempelvis sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör ett berättigat intresse.

EDPB har i en vägledning[46] om berättigat intresse utvecklat vad som krävs för att denna rättsliga grund ska kunna användas. EDPB framför bland annat att begreppet ”förhindra bedrägerier” i skäl 47 i dataskyddsförordningen omfattar alla åtgärder för att förhindra bedrägerier, samt att upptäcka bedrägerier också kan anses omfattas av detta begrepp på en principiell nivå.[47] Vidare anför EDPB att bedömningen av huruvida en personuppgiftsbehandling är absolut nödvändig för att förhindra bedrägerier ska bedömas tillsammans med principen om uppgiftsminimering enligt artikel 5.1 c i dataskyddsförordningen, samt att ett sådant förhindrande av bedrägerier behöver vara av ”väsentlig betydelse” för att den registrerades intressen inte ska anses väga tyngre vid själva intresseavvägningen.[48]

Vägledningen går även igenom den bedömning i tre steg som behöver göras för att avgöra om en personuppgiftsbehandling kan grundas på ett berättigat intresse. Dessa tre steg är följande:

1. Personuppgiftsbehandlingen ska avse ett berättigat intresse för den personuppgiftsansvarige, eller en tredje part,
2. personuppgiftsbehandlingen måste vara nödvändig för de ändamål som rör det berättigade intresset, samt

[46] EDPB:s ”Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR”, version 1.0, 8 oktober 2024.
[47] Ibid., s. 28.
[48] Ibid., s. 29.

3. själva intresseavvägningen behöver visa att berörda registrerades intressen inte väger tyngre än den personuppgiftsansvariges, eller en tredje parts, berättigade intresse.[49]

Vidare framgår det av vägledningen att den rättsliga grunden berättigat intresse inte bör ses som ett sista alternativ när någon annan rättslig grund inte är tillämplig eller som en ”öppning” för att legitimera personuppgiftsbehandlingar som inte faller in under någon annan rättslig grund. Istället bör den tolkas restriktivt precis som övriga rättsliga grunder i artikel 6.1 i dataskyddsförordningen.

En grundläggande förutsättning, i relation till det första steget i bedömningen av om en personuppgiftsbehandling kan grundas på ett berättigat intresse, är att det intresse som en personuppgiftsansvarig, eller en tredje part, vill uppfylla är legitimt. Detta kräver enligt EDPB att följande tre kumulativa kriterier är uppfyllda:

1. Intresset är lagligt, det vill säga det strider inte mot EU-rätten eller medlemsstaternas nationella rätt,
2. intresset är tydligt och precist artikulerat och identifierat, samt
3. intresset är riktigt och aktuellt, inte spekulativt eller hypotetiskt.[50]

Det följer också av vägledningen att i de fall ett berättigat intresse avser en tredje parts intressen ska den legitima karaktären av ett berättigat intresse bedömas enligt samma tre kumulativa kriterier som för den personuppgiftsansvariges egna intressen.

Mot bakgrund av vad som har redogjorts för ovan gällande den rättsliga grunden berättigat intresse, skulle det inledningsvis krävas att bankernas intresse av att motverka penningtvätt, terroristfinansiering och bedrägeri, genom att dela vissa kunduppgifter sinsemellan, kan anses vara legitimt. En del av denna bedömning består, enligt de tre kumulativa kriterierna som EDPB har uppställt, i att intresset ska vara lagligt. Det innebär att det inte får strida mot EU-rätten eller medlemsstaternas nationella rätt, vilket är svensk rätt i detta fall.

Banksekretessen i svensk rätt

Det följer av 4 kap. 2 § första stycket penningtvättslagen att en verksamhetsutövare ska vidta skärpta åtgärder för kundkännedom och andra nödvändiga åtgärder vid avvikande eller misstänkta aktiviteter och transaktioner. Det är för att bedöma om det finns skälig grund att misstänka penningtvätt eller finansiering av terrorism, eller att egendom annars härrör från brottslig handling. Det framgår av 4 kap. 9 § första stycket penningtvättslagen att en verksamhetsutövare, eller den som är verksam hos verksamhetsutövaren, inte för en kund eller någon utomstående obehörigen får röja att en bedömning enligt 2 § utförs, har utförts eller kommer att utföras. Vidare följer det av 5 kap. 11 § första stycket penningtvättslagen att den som är verksam hos en verksamhetsutövare inte obehörigen får röja bland annat att personuppgifter om lagöverträdelser behandlas enligt 6 § och att sådana uppgifter bevaras.

På liknande sätt finns det bestämmelser om tystnadsplikt i betaltjänstlagen. Av 3 kap. 12 § första stycket framgår bland annat att den som är eller har varit knuten till ett betalningsinstitut eller betaltjänstleverantör, som anställd eller uppdragstagare, inte obehörigen får röja eller utnyttja det denne i anställningen eller under uppdraget i verksamheten med betaltjänster har fått veta om enskildas förhållanden till institutet

[49] Ibid., s. 6–19.
[50] Ibid., s. 8–9.

eller leverantören. Det följer vidare av 6 kap. 9 § att den som är verksam hos en betaltjänstleverantör, eller hos den som har ansvar för ett betalningssystem, inte obehörigen får röja uppgifter i ett register som avses i 1 §, eller uppgifter som lämnats ut med stöd av 5 § andra stycket i betaltjänstlagen.

Det följer också av den så kallade banksekretessen, enligt 1 kap. 10 § första stycket banklagen, att enskildas förhållanden till kreditinstitut, såsom banker, inte obehörigen får röjas.

Banksekretessen enligt förarbeten

Enligt förarbetena omfattar 1 kap. 10 § första stycket banklagen såväl handlingssekretess som tystnadsplikt, samt alla uppgifter som rör en bankkunds mellanhavanden med banken, oavsett om de är dokumenterade eller inte.[51] Det framgår vidare att som bankkund i sammanhanget avses en fysisk eller juridisk person som anses som kund i förhållande till banken. Begreppet omfattar dock inte endast den som har en löpande kundrelation till banken, utan även den som förhandlar, eller utan framgång har förhandlat, med banken om att inleda en kundrelation, samt även den som tidigare har varit kund till banken.

Det konstateras vidare att banksekretessen inte är absolut, utan kan brytas för att tillgodose exempelvis viktiga informations- och kontrollbehov för samhället. Den kan till exempel inskränkas i viss utsträckning genom uttryckliga lagbestämmelser som innebär en skyldighet för exempelvis en bank att lämna vissa uppgifter till en myndighet.[52] Det är enbart ett obehörigt röjande av kunduppgifter som är förbjudet. I förarbetena ges några exempel på situationer då det kan anses behörigt av en bank att lämna ut information om sina kunder. Så är fallet exempelvis när en bank enligt lag är skyldig att lämna information om en bankkund.[53]

Exempel på när en bank enligt lag är skyldig att lämna information om en kund finns i bland annat penningtvättslagen, såsom rapporteringsskyldigheten till Polismyndigheten enligt 4 kap. 3 §. En liknande bestämmelse finns i 6 kap. 5 § första stycket betaltjänstlagen som föreskriver att om misstanke om bedrägeri kvarstår efter närmare analys får uppgifter om alla omständigheter som kan tyda på bedrägeri i samband med tillhandahållande eller användning av betaltjänster lämnas till Polismyndigheten eller Åklagarmyndigheten.

Banksekretessen enligt litteratur på området

I litteratur på området, som huvudsakligen baseras på Per-Ola Janssons verk ”Banksekretess och annan finansiell sekretess”[54], har det anförts fyra huvudsakliga situationer då ett röjande av banksekretessen inte skulle anses som obehörigt.[55] En sådan situation är när uppgifterna gäller bankkunden själv. En annan situation är när bankkunden har medgett att ett röjande till en tredje part kan ske, det vill säga då det finns ett samtycke från kunden. En tredje situation är om en bank är skyldig att lämna uppgifter om en viss bankkund, eller om sina bankkunder generellt, med anledning av exempelvis lagkrav. En fjärde situation är då det inte finns någon sådan rättslig skyldighet för banken, men då det ändå inte skulle anses som obehörigt för banken att

[51] Prop. 2002/03:139, Del 1, s. 477 samt däri gjorda hänvisningar.
[52] Ibid., s. 477–478.
[53] Ibid., s. 478–479.
[54] Jansson, Per-Ola, *Banksekretess och annan finansiell sekretess*, Svenska Bankföreningen, 2010.
[55] Ibid., s. 64.

lämna uppgifter om en bankkund. Det är dessa situationer som det mycket allmänt hållna uttrycket ”inte obehörigen” kan anses omfatta enligt Jansson. Vidare framgår det att obehörighetsrekvisitet ska tolkas restriktivt. Utan en sådan tolkning skulle sekretessen snabbt kunna förlora i betydelse.[56]

Jansson har utvecklat exempel på när banksekretessen skulle kunna röjas på ett icke-obehörigt sätt. Inom ramen för aktuellt projekt är det främst exempel i relation till den tredje och fjärde situationen som skulle kunna vara relevanta för bankernas tilltänkta delning. Ett sådant exempel är när sekretessen måste brytas för att uppgifter kan ha betydelse för utredning av brott. I sådana situationer framträder ett allmänt intresse av att kunna genomföra tillförlitliga förundersökningar. Jansson betonar att det behöver göras en avvägning för och emot ett utlämnande för brottsutredningssyften i ljuset av obehörighetsrekvisitet, särskilt när det avser helt obestyrkta misstankar om brott, så att sekretesskyddet inte efterges i onödan.[57]

Ytterligare exempel som Jansson framför är att det kan tänkas förekomma situationer som är så allvarliga att ett finansiellt institut, såsom en bank, kan lämna upplysningar om en kund till en annan bank eller flera andra banker.[58] Det skulle exempelvis kunna handla om synnerligen allvarlig brottslighet som kan befaras vara riktad mot den finansiella verksamheten i stort, såsom systematiska kreditbedrägerier eller systematiska försök att ta sig in i bankens datasystem. Om en bank skulle ha uppmärksammat något sådant bör den, i vart fall när det är brådskande och en brottsutredning inte kan avvaktas, kunna varna andra banker genom att uppge relevant personidentitet. Enligt Jansson måste det också uppmärksammas att en brottsanmälan kan behöva göras, liksom att det finns förbud som kan vara tillämpliga för att röja vissa åtgärder i samband med brott. Det följer vidare att om situationen inte är så brådskande bör det i första hand vara de brottsbekämpande myndigheternas eller Finansinspektionens uppgift att varna andra banker.

Enligt Jansson bör varje uppgift som exempelvis en bank har om en bankkund prövas för sig i relation till banksekretessen.[59] Det betyder att banken inte skulle kunna röja samtliga uppgifter som banken har om kunden, även om det skulle kunna anses icke-obehörigt. Om det är tveksamt om ett röjande kan ske behörigen, bör rekvisitet ”obehörigen” enligt Jansson tolkas snävt. Det innebär att banksekretessen gäller tills det finns en omständighet som medger att sekretessen kan brytas.

Jansson noterar vidare att banksekretessen till viss del har urholkats under de senaste årtiondena, bland annat till följd av den intensifierade kampen mot penningtvätt och finansiering av terrorism.[60] Jansson utvecklar att det föreligger en gråzon inom vilka banker får lämna vissa uppgifter utöver de som är föreskrivna i lag. För att sekretessen inte ska urholkas måste dock denna zon ges en restriktiv utsträckning och tolkas så att sekretess ska gälla så snart det råder eventuell tvekan om en kunds sekretesskydd.[61] Följderna skulle annars kunna bli att sekretessen tappar i betydelse och blir meningslös, vilket inte kan anses vara lagstiftarens avsikt.[62] Vidare anför Jansson att när det kommer till lagbestämmelser om uppgiftsskyldighet för en bank, bör banker kunna utgå ifrån att lagstiftaren har satt gränsen för uppgiftsskyldigheten och att detta

[56] Ibid., s. 63.
[57] Ibid., s. 148.
[58] Ibid., s. 188.
[59] Ibid., s. 50.
[60] Ibid., s. 27.
[61] Ibid., s. 103.
[62] Ibid., s. 63.

normalt sett kan uppfattas såsom en uttömmande precisering av skyldigheten inom ett berört område.[63]

5.6. IMY:s kommentarer

Inledningsvis anser IMY att bekämpning av penningtvätt och finansiering av terrorism enligt penningtvättslagen, samt bekämpning av bedrägeri enligt betaltjänstlagen, kan utgöra berättigade intressen.

Mot bakgrund av vad som har framförts i avsnitt 5.5 ovan, är en grundläggande förutsättning för att kunna basera en personuppgiftsbehandling på ett berättigat intresse att intresset som en personuppgiftsansvarig, eller en tredje part, vill uppfylla kan anses vara legitimt. Detta i sin tur förutsätter först och främst att intresset är lagligt. Det innebär att det inte får strida mot EU-rätten eller nationell rätt, vilket är svensk rätt i detta fall. Tillämpligheten av denna rättsliga grund kräver därmed att bankernas intresse av att bekämpa penningtvätt, terroristfinansiering och bedrägeri, genom den tilltänkta delningen av personuppgifter om lagöverträdelser, kan anses vara legitimt.

IMY anser att frågan om huruvida relevanta sekretessbestämmelser i penningtvättslagen, betaltjänstlagen och banklagen uppställer hinder för bankernas tilltänkta delning av personuppgifter om lagöverträdelser inom ramen för detta projekt som har beskrivits i avsnitt 3 blir avgörande för tillämpligheten av berättigat intresse som rättslig grund.

Såsom IMY har redogjort för i avsnitt 5.1 ovan, finns det vissa bestämmelser i penningtvättslagen och betaltjänstlagen som utgör exempel på situationer då lagstiftaren har funnit att delning av uppgifter kan ske trots tystnadsplikten som gäller bland annat enligt 3 kap. 12 § betaltjänstlagen, 5 kap. 11 § penningtvättslagen och banksekretessen enligt 1 kap. 10 § banklagen.

IMY konstaterar dock att det inte finns någon specifik sekretessbrytande bestämmelse som är tillämplig för bankernas tilltänkta delning av personuppgifter inom ramen för detta projekt.

Såsom har konstaterats i förarbeten är banksekretessen inte absolut, utan det är endast obehörigt röjande som är förbjudet.[64] I litteratur på området anförs dock att obehörighetsrekvisitet ska tolkas restriktivt.[65] Enligt IMY:s mening bör detta förstås som att utgångspunkten är att banksekretess gäller och att bedömningen av huruvida ett potentiellt röjande kan ske icke-obehörigen ska göras restriktivt.

I förarbeten har det angetts exempel på ett antal situationer då det kan anses behörigt av en bank att lämna information om sina kunder. Till exempel gäller det när en bank enligt lag är skyldig att lämna information om en bankkund.[66] Mot bakgrund av det som tidigare har anförts om den tilltänkta delningens art och syfte, är IMY:s tolkning att inget av de exempel som anges i förarbetena är tillämpligt inom ramen för det aktuella projektet.

I litteratur på området lyfts fram exempel på situationer då det inte finns någon skyldighet för banker att lämna ut uppgifter om en bankkund, men då det ändå inte

[63] Ibid., s. 64 f.
[64] Prop. 2002/03:139, Del 1, s. 477–478.
[65] Jansson, Per-Ola, *Banksekretess och annan finansiell sekretess,* s. 63.
[66] Prop. 2002/03:139, Del 1, s. 478–479.

skulle anses som obehörigt för banker att göra ett sådant utlämnande. Detta har bland annat ansetts vara fallet när det finns en misstanke om brott och uppgifter som omfattas av banksekretessen kan ha betydelse för utredningen av brottet. Denna situation, förefaller enligt IMY:s mening, omfatta utlämnanden till brottsbekämpande myndigheter genom en brottsanmälan för brott i bredare bemärkelse än den i lag föreskrivna rapporteringsskyldigheten för skälig misstanke om brott kopplat till penningtvätt, terroristfinansiering och/eller bedrägerier. Situationen förefaller därmed inte omfatta utlämnanden mellan exempelvis banker.

Enligt litteratur på området kan det dock finnas situationer av så allvarlig eller nära förestående brottslighet att ett finansinstitut, såsom en bank, kan lämna uppgifter om kund till en annan bank eller andra banker, till exempel om en bank utsätts för systematiska kreditbedrägerier eller systematiska försök av obehöriga att ta sig in i bankens datasystem. I situationer där en sådan upplysning till andra banker inte är lika brådskande, föreslås däremot detta röjande överlåtas på de brottsbekämpande myndigheterna eller Finansinspektionen. I nuvarande projekt vill bankerna kunna flagga individer i form av potentiella, befintliga eller avvisade/avslutade kunder som anses vara förknippade med förhöjd risk för penningtvätt, terroristfinansiering och/eller bedrägerier och dela denna information med varandra. Syftet är att andra banker ska kunna vidta utökade kundkännedomsåtgärder om de vid pingning av en individ noterar att en potentiell eller befintlig kund hos dem är flaggad i systemet. IMY anser att mycket talar för att bankernas tilltänkta delning inte ryms inom det nämnda exemplet gällande en så allvarlig och nära förestående brottslighet, eftersom den är avsedd att vara mer systematisk och förebyggande till sin karaktär.

IMY konstaterar även att det i litteratur på området har anförts att utgångspunkten är att banksekretessen gäller och att det kan antas att lagstiftaren har satt gränserna för uppgiftsskyldigheten inom det berörda området. Inom ramen för detta projekt avser detta de relevanta lagbestämmelser om icke-obehöriga röjanden i penningtvättslagen och betaltjänstlagen som har beskrivits i avsnitt 5.1 ovan. Detta talar alltså, enligt IMY:s mening, för att lagstiftaren på ett uttömmande sätt har reglerat de situationer då bland annat delning av personuppgifter mellan exempelvis banker är tillåtna inom det nu aktuella området.

Sammanfattningsvis anser IMY att mycket talar för att den av bankerna tilltänkta delningen av personuppgifter om lagöverträdelser genom flaggning inte kan ske i förenlighet med banksekretessen enligt 1 kap. 10 § banklagen. IMY:s tolkning är att detta gäller bankernas tilltänkta delning enligt både alternativ 1 (delning av namn, personnummer och förekomst av flaggning) och alternativ 2 (delning av namn, personnummer och förekomst av flaggning samt den bakomliggande orsaken till flaggningen).

Mot den bakgrunden är IMY:s samlade bedömning att det framstår som svårt för bankerna att grunda den tilltänkta delningen av personuppgifter om lagöverträdelser på den rättsliga grunden berättigat intresse enligt artikel 6.1 f i dataskyddsförordningen.

6. Avslutande kommentar

IMY bedömer sammanfattningsvis att det sannolikt behövs lagändringar för att möjliggöra den delning av personuppgifter om lagöverträdelser som bankerna önskar genomföra inom ramen för det aktuella projektet. IMY konstaterar att ändamålen med delningen, det vill säga att motverka penningtvätt, finansiering av terrorism och bedrägerier, är allmänna intressen. Dessa intressen kan motivera lagstiftning som skapar en rättslig grund för delningen av personuppgifter, även uppgifter om lagöverträdelser. En sådan reglering behöver innehålla särskilda skyddsåtgärder och uppfylla de grundläggande kraven på nödvändighet och proportionalitet.