SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Vägledning om behandling av personuppgifter

Tredje upplagan

Beslutad av Simpts styrgrupp i november 2025

Innehållsförteckning

Simpts vägledning har tagits fram av sju organisationer i finansbranschen och deras medlemmar. Den utgår från medlemmarnas behov av vägledning och är inte avsedd att vara heltäckande.

Vägledningen beskriver hur branschen tolkar och tillämpar penningtvättsregelverket i aktuella delar.

Vägledningen ersätter inte lagar, föreskrifter och andra rättskällor. Dessa måste alltid beaktas och tillämpas i förekommande fall.

Det finns inte någon skyldighet att använda vägledningen. Den som använder vägledningen måste alltid göra bedömningen om vägledningen är tillämplig i det enskilda fallet.

Denna del av vägledningen är branschgemensam. Den är relevant för alla verksamhetsutövare, om inte annat anges. Vägledningen ska läsas tillsammans med och kompletterar den grundläggande vägledningen om behandling av personuppgifter.

Denna del av vägledningen utgår framför allt från lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). Alla laghänvisningar avser penningtvättslagen, om inte annat anges. Hänvisningar görs också till Europeiska bankmyndighetens (Eba) riktlinjer EBA/2021/02 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) enligt direktiv (EU) 2015/849 (Eba:s riktlinjer för riskfaktorer).

I denna tredje upplaga finns ett nytt avsnitt om IMY:s föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1). Vägledningen har uppdaterats med anledning av ändringar som har gjorts av Eba:s riktlinjer för riskfaktorer, EBA/GL/2021/02. Ändringarna är gjorda genom EBA/GL/2024/01. Uppdateringar har också gjorts med anledning av ändringar i penningtvättslagen (prop. 2024/25:134). Det har även gjorts vissa justeringar och redaktionella ändringar.

Penningtvättslagen (rättslig förpliktelse) som rättslig grund[1]

Behandling av personuppgifter avseende den som är kund och den som inte är kund

Enligt 5 kap. 2 § penningtvättslagen får verksamhetsutövare behandla personuppgifter i syfte att kunna fullgöra sina skyldigheter enligt penningtvättslagen. Den rättsliga grunden för den personuppgiftsbehandling som sker enligt penningtvättslagen är därmed de rättsliga förpliktelser som följer av penningtvättslagen.

Personuppgifter kan behöva behandlas både avseende den som är kund och den som inte är kund enligt penningtvättslagen, men där efterlevnaden av penningtvättsregelverket ändå förutsätter att uppgifter behandlas, t.ex. genom att information eller dokumentation inhämtas. Med ”den som inte är kund” avses här andra fysiska personer än den som är kund, verklig huvudman eller företrädare för kunden.

[1] Se också avsnitt 1 i den grundläggande vägledningen om behandling av personuppgifter.

Uppgift beträffande den som inte är kund kan avse den som är person i politiskt utsatt ställning (PEP), när kunden är en familjemedlem eller nära medarbetare till denne. Av 3 kap. 10 § penningtvättslagen följer en skyldighet att utreda om kunden eller kundens verkliga huvudman är en PEP eller *en familjemedlem eller känd medarbetare till en sådan person.* Den rättsliga grunden för att behandla uppgifter om den som är PEP men som inte själv är kund är därmed den rättsliga förpliktelse som följer av penningtvättslagen. Motsvarande uttryckliga förpliktelser finns inte beträffande andra personer som inte är kund. Uppgifter om den som inte är kund kan ändå – när det är motiverat – behöva behandlas i syfte att fullgöra de skyldigheter som följer av penningtvättslagen.

Uppgifter om den som inte är kund kan framför allt behöva behandlas i syfte att verksamhetsutövaren ska kunna fullgöra skyldigheten i 2 kap. 3 § penningtvättslagen att riskbedöma kunden och därmed den risk som kan förknippas med kundrelationen. När kundens riskprofil ska bestämmas kan det vara motiverat att behandla uppgifter om personer som på olika sätt har kopplingar till kunden och som kan påverka risken med denne, t.ex. borgensmän (se Simpts vägledning om borgensmän och tredjemanspantsättare) eller personer som har fått sina tillgångar spärrade till följd av misstankar om finansiering av terrorism, jfr Eba:s riktlinjer för riskfaktorer, riktlinje 2.5. Så länge som uppgifter om den som inte är kund behandlas i syfte att fullgöra skyldigheter som följer av penningtvättslagen, bedöms behandlingen vara tillåten med stöd de rättsliga förpliktelser som följer av penningtvättslagen som rättslig grund.

Den behandling av personuppgifter som inte grundar sig på en uttrycklig skyldighet att vidta åtgärder enligt penningtvättslagen (t.ex. 3 kap. 10 §), bör ha stöd i verksamhetsutövarens allmänna riskbedömning. Det kan t.ex. vara uppgifter i media (s.k. negativ media eller adverse media). Det bör noteras att det gäller både beträffande den som är respektive inte är kund. Som för all personuppgiftsbehandling gäller att personuppgifter bara får samlas in för specifika, särskilt angivna och berättigade ändamål samt att fler personuppgifter än vad som behövs för ändamålen inte får behandlas.

Särskilt om person i politiskt utsatt ställning[2]

Av 3 kap. 10 § penningtvättslagen följer en skyldighet att utreda om kunden är en familjemedlem eller känd medarbetare till en PEP. Det innebär att också uppgifter om den som är PEP men utan att själv vara kund, behandlas med stöd av de rättsliga förpliktelser som följer av penningtvättslagen som rättslig grund.

Verksamhetsutövaren förutsätts göra relativt omfattande kontroller kring om kunden har nära förbindelser med den som är PEP, se Eba:s riktlinjer för riskfaktorer, riktlinje 2.4,. I sammanhanget kan också den vägledning som har tagits fram av JMLSG noteras, se del 1, annex 4-II, 1 A. Så länge som uppgifterna behandlas i syfte att fullgöra skyldigheterna som följer av penningtvättslagen, bedöms behandlingen vara tillåten. Som för all personuppgiftsbehandling gäller att personuppgifter bara får samlas in för specifika, särskilt angivna och berättigade ändamål samt att fler personuppgifter än vad som behövs för ändamålen inte får behandlas.

Uppgifter som behandlas om den som är PEP kan i vissa fall kan vara känsliga personuppgifter. I 5 kap. 5 § penningtvättslagen ges en rätt att behandla sådana uppgifter, om det är nödvändigt för att bedöma om kunden är PEP eller familjemedlem eller känd medarbetare till en sådan person. Uppgifterna kan vara tydligt offentliggjorda av personen själv, t.ex. beträffande personer som företräder

[2] Se också avsnitt 3 i den grundläggande vägledningen om behandling av personuppgifter.

politiska partier. När personen själv tydligt offentliggjort uppgifterna får även andra behandla uppgifterna, se Integritetsskyddsmyndigheten När får ni behandla känsliga personuppgifter? | IMY.

Behandling av personuppgifter i samband med lånelöfte

Lånelöfte

Ett lånelöfte är ett preliminärt förhandsbesked som visar hur mycket en person får låna utifrån sina förutsättningar. Lånelöftet gäller vanligtvis för viss tid, ofta för 3–6 månader, under förutsättning att personens ekonomi inte har förändrats och att uppgifterna som har lämnats i ansökan fortfarande stämmer.

En ansökan om lånelöfte är inte samma sak som en låneansökan och lånelöftet innebär inte att ett avtal om kredit har ingåtts. Ett lånelöfte behöver inte heller innebära att den som fått lånelöftet står i begrepp att träda i avtalsförbindelse med kreditgivaren.

Penningtvättslagen (rättslig förpliktelse) som rättslig grund

En person kan ansöka om lånelöfte hos flera kreditgivare innan denne bestämmer sig för om och i så fall med vilken kreditgivare som denne önskar ingå ett kreditavtal.

För att penningtvättslagens bestämmelser ska bli tillämpliga är det avgörande att parterna *står i begrepp att träda i avtalsförbindelse med varandra*. Det är tidigast vid den tidpunkten som någon anses vara kund i penningtvättslagens mening. Verksamhetsutövaren behöver därför göra en bedömning av huruvida personen i fråga står i begrepp att ingå avtal med verksamhetsutövaren. Det är först då som personuppgifter behandlas med stöd av penningtvättslagen som rättslig grund, under förutsättning att det sker i syfte att uppfylla de krav som ställs i penningtvättslagen.

Behandling av personuppgifter på försäkringsområdet

Inledning

Försäkringstagaren och den som är berättigad till försäkringsersättning behöver inte vara samma person. Frågor kan uppstå om behandling av personuppgifter när uppgifter om den ena personen kan inverka på de bedömningar och åtgärder som vidtas enligt penningtvättslagen avseende den andra personen.

Försäkringstagaren är försäkringsföretagets kund enligt penningtvättslagen och försäkringsföretaget ska vidta åtgärder för kundkännedom avseende försäkringstagaren. Mellan försäkringsföretaget och förmånstagaren finns det inte något avtalsförhållande, vilket innebär att förmånstagaren inte är kund till försäkringsföretaget. Försäkringsföretaget ska emellertid, senast när försäkringsersättningen betalas ut, vidta åtgärder beträffande förmånstagaren, se 3 kap. 26 § punkten 1 penningtvättslagen (se också prop. 2016/17:173 s. 535). Av 3 kap. 28 § penningtvättslagen framgår att kontrollerna och åtgärderna enligt 26 och 27 §§ ska vidtas i den omfattning det behövs med hänsyn till den risk som kan förknippas med kundrelationen enligt 2 kap. 3 § penningtvättslagen, dvs. risken med försäkringstagaren. Om det behövs för att bedöma risken ska omständigheter hänförliga till förmånstagaren också beaktas.

Det finns ofta starka kopplingar mellan försäkringstagaren och förmånstagaren till en försäkring (det gäller dock inte alltid, ibland kan förmånstagaren vara t.ex. en ideell förening). Av penningtvättslagen framgår att riskbedömningen av försäkringstagaren ska vara utgångspunkten för de åtgärder som vidtas beträffande förmånstagaren. Uppgifter om förmånstagaren kan också vara relevanta att behandla inom ramen för affärsförbindelsen med försäkringstagaren.

Det bör noteras att såväl försäkringstagaren som förmånstagaren kan vara en juridisk person. Det är endast i den mån uppgifterna går att knyta till en fysisk person som det är aktuellt med personuppgifter.

Behandling av personuppgifter hänförliga till försäkringstagaren

Förmånstagaren ska inte riskbedömas, men åtgärderna som vidtas avseende förmånstagaren ska vara riskbaserade (3 kap. 28 § penningtvättslagen). Det är riskbedömningen avseende försäkringstagaren som ska ligga till grund för omfattningen på de åtgärder som ska vidtas avseende förmånstagaren. Det innebär att personuppgifter avseende försäkringstagaren kan behöva behandlas när det behövs för att kunna bestämma omfattningen på de åtgärder som ska vidtas avseende förmånstagaren, dvs. i syfte att uppfylla kraven i penningtvättslagen (se 5 kap. 2 § penningtvättslagen). Den rättsliga grunden för behandlingen är därmed de rättsliga förpliktelser som följer av penningtvättslagen.

Behandling av personuppgifter hänförliga till förmånstagaren

Affärsförbindelsen med försäkringstagaren upphör många gånger i samband med att försäkringsersättning betalas ut till förmånstagaren. Det är t.ex. fallet när försäkringsersättning betalas ut på grund av försäkringstagarens dödsfall. I andra fall fortsätter affärsförbindelsen mellan försäkringsföretaget och försäkringstagaren att löpa. Det är framför allt fallet vid pensionsutbetalningar.

Förmånstagaren ska inte riskbedömas, men åtgärder ska vidtas avseende denne senast vid utbetalning av försäkringsersättningen (3 kap. 26 § penningtvättslagen). Om de uppgifter som då framkommer om förmånstagaren bedöms kunna inverka på riskbedömningen av försäkringstagaren och därmed den risk som kan förknippas med kundrelationen enligt 2 kap. 3 § penningtvättslagen, bedöms dessa kunna behandlas också inom ramen för affärsförbindelsen med försäkringstagaren. I syfte att kunna fullgöra skyldigheten att göra en riskbedömning av försäkringstagaren kan det alltså vara ändamålsenligt att behandla personuppgifter avseende förmånstagaren (se 5 kap. 2 § penningtvättslagen). Den rättsliga grunden för behandlingen är därmed de rättsliga förpliktelser som följer av penningtvättslagen.

Polismyndighetens återkoppling

Enligt 4 kap. 3 b § punkten 1 penningtvättslagen ska Polismyndigheten, i de fall det är möjligt, ge lämplig återkoppling till verksamhetsutövarna om effektiviteten och uppföljningen av rapporter enligt 4 kap. 3 § penningtvättslagen. I den mån återkopplingen skulle omfatta uppgifter om lagöverträdelser, får dessa behandlas om det bedöms vara nödvändigt för att uppfylla de skyldigheter som framgår av 5 kap. 6 § penningtvättslagen, t.ex. för riskbedömningen av kunden. Det bedöms alltså inte vara någon skillnad om verksamhetsutövaren får del av uppgifter om lagöverträdelser via Polismyndigheten, s.k. adverse media/negativ media eller på annat sätt.

Polismyndighetens och Säkerhetspolisens frågerätt

Polismyndigheten och Säkerhetspolisen har enligt 4 kap. 6 § penningtvättslagen rätt att begära att verksamhetsutövaren lämnar alla uppgifter som behövs för en utredning om penningtvätt eller finansiering av terrorism, de behöver inte ange varför uppgiften begärs.

Det innebär att verksamhetsutövaren måste lämna alla uppgifter som efterfrågas, även uppgifter som inte har inhämtats för att uppfylla kraven i penningtvättsregelverket utan på annan grund. Så länge uppgiften finns hos verksamhetsutövaren måste den alltså lämnas ut.

Att en uppgift har lämnats till Polismyndigheten eller Säkerhetspolisen enligt 4 kap. 6 § penningtvättslagen bedöms inte innebära att uppgiften behöver hanteras annorlunda än före begäran. Att uppgiften har lämnats ut innebär alltså inte i sig att den t.ex. behöver bevaras enligt bestämmelserna i penningtvättsregelverket. Det kan t.ex. vara uppgifter som har hämtats in vid ett rådgivningssamtal eller på annat sätt för att uppfylla krav som följer av IDD- eller MiFID-regelverket och uppgifter som har hämtats in enligt krav som ställs i skattelagstiftningen. Verksamhetsutövaren kan dock, mot bakgrund av begäran, göra bedömningen att uppgiften som har lämnats ut också behövs för riskbedömningen av kunden, dvs. för att kunna fullgöra skyldigheterna enligt penningtvättslagen.

I sammanhanget kan noteras att när en uppgift har lämnats till Polismyndigheten eller Säkerhetspolisen enligt 4 kap. 6 § penningtvättslagen aktualiseras tystnadsplikten enligt 4 kap. 9 § penningtvättslagen. Det innebär att verksamhetsutövaren inte får röja att uppgiften har lämnats ut.

Bevarande av handlingar och uppgifter[3]

Kan uppgifter från en avslutad affärsförbindelse användas i en ny affärsförbindelse?

En tidigare kund kan bli kund på nytt inom den femårsfrist som följer av 5 kap. 3 § penningtvättslagen. Verksamhetsutövaren kan inhämta uppgifter om kunden på olika sätt. De personuppgifter som hämtades in om kunden inom ramen för den tidigare affärsförbindelsen och som har bevarats enligt 5 kap. 3 § penningtvättslagen kan därför behandlas också såvitt avser den nya affärsförbindelsen, under förutsättning att det sker i syfte att kunna fullgöra de skyldigheter som följer av penningtvättslagen. Uppgifterna kan emellertid behöva uppdateras.

Kan inaktuella uppgifter gallras?

I 5 kap. 3 § penningtvättslagen finns en skyldighet att bevara handlingar och uppgifter under viss tid, därefter ska uppgifterna gallras. Bestämmelsen innebär bland annat att uppgifter som avser åtgärder som har vidtagits för kundkännedom ska bevaras i fem år efter att affärsförbindelsen avslutades. Det finns inte något uttryckligt undantag i regelverket från denna bestämmelse. Syftet med bestämmelsen är att myndigheter ska kunna förebygga, upptäcka och utreda möjlig penningtvätt eller finansiering av terrorism (jfr artikel 40.1 första stycket fjärde penningtvättsdirektivet och prop. 2016/17:173 s. 315).

Många affärsförbindelser pågår under en lång tid. Det innebär att en hel del uppgifter som verksamhetsutövaren har om kunden blir inaktuella, t.ex. uppgifter om den adress som kunden hade som barn och som har ändrats när kunden blivit vuxen. Frågan är om uppgifter som blivit inaktuella måste bevaras enligt 5 kap. 3 § penningtvättslagen eller om de i vissa fall kan gallras tidigare.

[3] Se också avsnitt 2 i den grundläggande vägledningen om behandling av personuppgifter.

Trots att det inte finns några uttryckliga undantag från bevaranderegeln i 5 kap. 3 § penningtvättslagen är bedömningen att gallring i vissa fall kan vara möjlig när det gäller inaktuella uppgifter. All gallring bör dock föregås av noggranna överväganden kring om uppgifterna fortsatt behövs för att myndigheter ska kunna förebygga, upptäcka och utreda möjlig penningtvätt eller finansiering av terrorism. Verksamhetsutövaren har ansvar för den gallring som görs. De överväganden som ligger till grund för beslutet att gallra uppgifter bör alltid dokumenteras. Verksamhetsutövaren bör också ha rutiner och interna styrdokument för när gallring av inaktuella uppgifter kan ske. Verksamhetsutövaren bör även kunna visa att det, genom t.ex. rutiner eller systemstöd, vid var tid har funnits aktuella uppgifter om kunden.

Vissa uppgifter om kunden inhämtas enligt uttryckliga krav i penningtvättslagen, såsom uppgift om syfte och art med affärsförbindelsen, kundens ägar- och kontrollstruktur samt uppgift om kunden är en person i politiskt utsatt ställning. Därutöver inhämtas ett antal andra uppgifter i syfte att kunna uppfylla kravet på att bestämma kundens riskprofil och för att uppnå tillräcklig kundkännedom för att kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen och övervaka och bedöma kundens aktiviteter och transaktioner. Olika verksamhetsutövare kan för dessa syften inhämta olika typer av uppgifter om kunden. Av betydelse för vilka uppgifter som inhämtas är exempelvis de produkter och tjänster som verksamhetsutövaren erbjuder och de kundtyper som verksamhetsutövaren vänder sig till samt kundens beteende under pågående affärsförbindelse.

Följande utgångspunkter bör gälla för frågan om gallring:

- Uppgifter som ligger till grund för en bedömning av att kunden bedöms utgöra en ökad risk för penningtvätt och finansiering av terrorism bör aldrig gallras tidigare än vad som följer av 5 kap. 3 § penningtvättslagen.
- Uppgifter om kunden som har inhämtats på grund av ett uttryckligt krav i penningtvättsregelverket och som inte går att få fram från externa källor, t.ex. uppgifter i en utredning om kundens ägar- och kontrollstruktur som inte går att hämta från Bolagsverket bör aldrig gallras tidigare än vad som följer av 5 kap. 3 § penningtvättslagen.
- Uppgifter som kan tas fram från externa källor, t.ex. från Skatteverket eller Bolagsverket, bör kunna gallras när de har blivit inaktuella och om verksamhetsutövaren kan göra en välgrundad bedömning av att de inaktuella uppgifterna inte längre behövs för att myndigheter ska kunna förebygga, upptäcka och utreda möjlig penningtvätt eller finansiering av terrorism. Verksamhetsutövaren bör i dessa fall kunna visa att det vid var tid har funnits aktuella uppgifter om kunden. Det bör dock noteras att även i dessa fall gäller att uppgifterna inte bör gallras om de t.ex. har legat till grund för en bedömning av att kunden bedöms utgöra en ökad risk för penningtvätt och finansiering av terrorism. Detta skulle kunna vara fallet om kunden har flyttat ovanligt ofta och verksamhetsutövaren i sin riskbedömning har bedömt att detta medför en förhöjd risk.
- Andra uppgifter än de som har inhämtats på grund av uttryckliga krav i penningtvättsregelverket bör kunna gallras när de blivit inaktuella och om verksamhetsutövaren kan göra en välgrundad bedömning av att de inaktuella uppgifterna inte längre behövs för att myndigheter ska kunna förebygga, upptäcka och utreda möjlig penningtvätt eller finansiering av terrorism.

Personuppgifter om lagöverträdelser[4]

Inledning

Uppgifter som rör lagöverträdelser har ett starkt skydd i artikel 10 GDPR. Personuppgifter som avses i artikel 10 GDPR får behandlas av andra än myndigheter om behandlingen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras eller för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras. Integritetsskyddsmyndigheten (IMY) får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avses i artikel 10 GDPR. IMY får även i enskilda fall besluta att andra än myndigheter får behandla sådana personuppgifter (3 kap. 9 § lagen [2018:218] med kompletterande bestämmelser till EU:s dataskyddsförordning samt 5 och 6 §§ förordningen [2018:219] med kompletterande bestämmelser till EU:s dataskyddsförordning, se också prop. 2017/18:105 s. 100 och 101).

För att få behandla personuppgifter om lagöverträdelser krävs alltså författningsstöd. I penningtvättslagen ges visst stöd för sådan behandling. Det finns också stöd i vissa EU-förordningar. EU-förordningar är direkt tillämpliga i svensk nationell rätt. Behandling av personuppgifter om lagöverträdelser får också ske om det finns stöd i föreskrifter, se nedan om Integritetsskyddsmyndighetens föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1). Om det inte finns författningsstöd för behandlingen kan IMY, som också framgår ovan, meddela beslut om tillstånd att behandla personuppgifter om lagöverträdelser.

IMY har publicerat ett rättsligt ställningstagande om innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen (IMYRS 2021:1).

Behandling av uppgifter om lagöverträdelser enligt penningtvättslagen

Behandling av personuppgifter om lagöverträdelser är tillåten under de förutsättningar som anges i 5 kap. 6 § penningtvättslagen. Behandlingen får ske om den är nödvändig för att bedöma den risk som kan förknippas med kundrelationen, uppfylla övervakningsskyldigheten, bedöma misstänkta transaktioner och aktiviteter och för att lämna uppgifter till Polismyndigheten och Säkerhetspolisen.

Det är endast uppgifter som påverkar risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism som kan anses vara *nödvändiga*. Det innebär att många typer av lagöverträdelser faller utanför vad som kan anses vara nödvändigt för att bedöma risken med kunden i detta hänseende. Bedömningen av vad som är nödvändigt bör vara riskbaserad. För högriskkunder kan fler uppgifter bedömas vara nödvändiga jämfört med kunder som inte bedöms utgöra hög risk.

Det bör ankomma på verksamhetsutövaren att i varje enskilt fall bedöma om behandlingen är *nödvändig*. Det är, som alltid, viktigt att kunna motivera varför en viss uppgift har hämtats in och att uppgifter inte hämtas in slentrianmässigt. Personuppgifter får bara samlas in för specifika, särskilt angivna och berättigade ändamål. Fler personuppgifter än vad som behövs för ändamålen får inte behandlas. En alltför snäv tolkning av vad som kan anses vara nödvändigt, medför dock en risk för att uppgifter som är relevanta för riskbedömningen av kunden missas.

[4] Se också avsnitt 4 i den grundläggande vägledningen om behandling av personuppgifter.

Vad gäller i fråga om sanktionsregelverket?

Kopplingen mellan sanktionsregelverket och penningtvättsregelverket

Sverige är bundet av internationella sanktionsregimer. EU kan besluta om internationella sanktioner inom ramen för den gemensamma utrikes- och säkerhetspolitiken. Det kan antingen vara beslut om att gemensamt genomföra FN:s sanktioner eller självständiga beslut om sanktioner. De åtgärder som faller inom EU:s behörighet (t.ex. handelsrestriktioner eller frysning av tillgångar för vissa individer eller företag) genomförs sedan i en EU-förordning som blir direkt tillämplig i svensk nationell rätt. Sanktionslistor kan innehålla uppgifter om lagöverträdelser. En EU-förordning innebär att det finns författningsstöd och en rättslig förpliktelse att behandla personuppgifter. För andra sanktionslistor kan behandlingen av personuppgifterna vara tillåten enligt IMY:s föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1), se nedan.

De kontroller som krävs enligt sanktionsregelverket görs inte enligt penningtvättslagen, men regelverken har starka beröringspunkter, särskilt vad avser terrorismfinansiering. Det kan inom ramen för sanktionsutredningen beträffande kunden framkomma sådant som att kunden i olika sammanhang har använt sig av olika namn, vilket kan inverka på den riskbedömning som görs av kunden enligt penningtvättslagen. Det kan också framkomma att kunden, dess företrädare eller ägare har kopplingar till personer som är föremål för sanktioner, till länder som är föremål för sanktioner eller till länder där många personer är upptagna på sanktionslistor. Dessa uppgifter kan vara nödvändiga att behandla för riskbedömningen av kunden enligt penningtvättslagen.

I Eba:s riktlinjer för riskfaktorer[5], riktlinje 2.5, anges att följande faktorer kan vara relevanta vid bedömningen av den risk som sammanhänger med en kunds eller verklig huvudmans anseende (kundriskfaktorer): Har kunden, den verkliga huvudmannen eller någon person som enligt vad som är allmänt känt har nära kopplingar till dem fått sina tillgångar spärrade till följd av administrativa eller straffrättsliga förfaranden eller anklagelser om terrorism eller finansiering av terrorism? Har företaget rimliga skäl att misstänka att kunden eller den verkliga huvudmannen eller någon person som enligt vad som är allmänt känt har nära kopplingar till dem vid någon tidigare tidpunkt har fått sina tillgångar spärrade av dessa skäl?

För att utreda om kunden har kopplingar till personer som är föremål för sanktioner och länder kan verksamhetsutövaren beakta bland annat uppgifter i media (s.k. negativ media/adverse media). Uppgifter som framkommer i detta sammanhang bör dock behandlas med försiktighet i fråga om tillförlitligheten.

Utredningen om kundens kopplingar till personer som är föremål för sanktioner och länder kan komma att omfatta uppgifter om lagöverträdelser. I penningtvättslagen ges stöd för viss behandling av uppgifter om lagöverträdelser (5 kap. 6 § penningtvättslagen). Uppgifter får bland annat behandlas om det är nödvändigt för att bestämma kundens riskprofil.

I förarbetena till penningtvättslagen konstateras att Esa:s riktlinjer om riskfaktorer innebär att verksamhetsutövarna vid sin riskklassificering av kunder ska beakta bl.a. uppgifter i media (s.k. adverse

[5] Eba:s riktlinjer gäller som allmänna råd. Se om allmänna råd i avsnitt 1.1 i den grundläggande vägledningen om kundkännedom.

media) om att kunden är misstänkt för brott eller förekommer i brottsliga sammanhang. Verksamhetsutövare förutsätts också beakta att kunden är föremål för ett beslut om frysning av tillgångar till följd av exempelvis misstänkt finansiering av terrorism samt om verksamhetsutövaren tidigare har rapporterat kunden för misstänkt penningtvätt eller finansiering av terrorism. Regeringen konstaterar vidare att en korrekt tillämpning av direktivet förutsätter att verksamhetsutövare i viss utsträckning kan behandla personuppgifter om lagöverträdelser vid riskklassificeringen av kunder (prop. 2016/17:173 s. 310). De riktlinjer som det hänvisas till har ersatts av Eba:s riktlinjer för riskfaktorer.

I den mån sanktionsrisker beaktas inom ramen för kundkännedomsprocessen, bör verksamhetsutövaren i sin allmänna riskbedömning beskriva hur potentiella sanktionsrisker är kopplade till penningtvätts- eller terrorismfinansieringsrisker och varför det därmed kan vara motiverat att utföra en sådan utredning som en del av de åtgärder för kundkännedom som vidtas enligt penningtvättslagen. Som för all personuppgiftsbehandling gäller att personuppgifter bara får samlas in för specifika, särskilt angivna och berättigade ändamål samt att fler personuppgifter än vad som behövs för ändamålen inte får behandlas.

Integritetsskyddsmyndighetens föreskrifter om behandling av personuppgifter som rör lagöverträdelser

Enligt 6 § i Integritetsskyddsmyndighetens (IMY) föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1) får företag under Finansinspektionens tillsyn behandla personuppgifter som avses i artikel 10 GDPR för kontroller mot sanktionslistor, om

1. 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,

2. sanktionslistorna är fastställda i demokratisk ordning och allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser, och

3. företaget har vidtagit relevanta skyddsåtgärder för att kunna skilja på äkta och falska träffar.

Personuppgiftsbehandlingen får endast avse

1. företagets styrelsemedlemmar, fullmaktshavare, ställföreträdare, firmatecknare, ägare, verkliga huvudmän, arbetstagare, arbetssökande, tredjemanspantsättare, borgensmän och motparter i en transaktion,

2. företagets befintliga och presumtiva kunder, leverantörer, samarbetspartners, förmedlare och uppdragstagare,

3. styrelsemedlemmar, fullmaktshavare, ställföreträdare, firmatecknare, ägare, verkliga huvudmän, tredjemanspantsättare, borgensmän och motparter i en transaktion för juridiska personer som avses i punkten 2, och

4. kategorier av personer som är jämförliga med de i punkterna 1–3.

Enligt föreskrifterna krävs det alltså att behandlingen är nödvändig för att efterleva penningtvättslagen, andra föreskrifter eller regelverk på finansmarknadsområdet utfärdade av utländska myndigheter, EU-organ eller mellanstatliga organisationer. I IMY:s vägledning om föreskrifterna[6] ges följande exempel på sådana föreskrifter och regelverk:

- Lagen (2004:297) om bank- och finansieringsrörelse
- Lagen (2007:528) om värdepappersmarknaden
- Regelverk utfärdade av U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC)
- Rekommendationer från Financial Action Task Force (FATF)
- Riktlinjer från de europeiska tillsynsmyndigheterna European Banking Authority (EBA), European Securities and Markets Authority (ESMA)

Av IMY:s vägledning framgår också att kravet på att behandlingen ska vara *nödvändig* ska tolkas på samma sätt som nödvändighetskravet i artikel 6.1 i GDPR. Det krävs inte att föreskrifterna och regelverken ställer krav på kontroller mot sanktionslistor för att behandlingen ska anses vara nödvändig.

Enligt föreskrifterna krävs det också att sanktionslistorna är fastställda i demokratisk ordning och allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser. Av IMY:s vägledning framgår att detta innebär att exempelvis interna listor som upprättas av enskilda företag eller koncerner inte omfattas av bestämmelserna.

Nedan finns exempel på sanktionslistor som IMY har bedömt vara fastställda i demokratisk ordning och som är allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser (se IMY:s vägledning om föreskrifterna).

UTFÄRDARE	**LISTOR**			
FN	United Nations Security Council Consolidated List			
AMERIKANSKA MYNDIGHETER				
U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC)	Specially Designated Nationals List (“SDN-listan”)	Consolidated Sanctions List		
U.S. Department of State	List of Administratively Debarred Parties	List of Statutorily Debarred Parties	CAATSA Section 231(e) – Defence and Intelligence Sectors of the Government of the Russian Federation	Terrorist Exclusion List

[6] Dnr IMY-2024-7587

U.S. Department of Commerce - Bureau of Industry and Security (BIS)	Denied Persons List	Entity List	Unverified List	
BRITTISKA MYNDIGHETER				
Home Office	Proscribed Terrorist Organisations			
HM Treasury – Office of Financial Sanctions Imple-mentation	Consolidated List of Financial Sanctions Targets in the UK			

Enligt föreskrifterna krävs det att företaget har vidtagit relevanta skyddsåtgärder för att kunna skilja på äkta och falska träffar. Av IMY:s vägledning framgår en sådan åtgärd kan vara att ha rutiner som säkerställer att den person som finns upptagen på en sanktionslista och som ett företag får träff på vid kontroll mot sanktionslistan utgör samma person som den person företaget avsett att kontrollera, exempelvis en person som företaget avser att ingå en affärsförbindelse med.