SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Grundläggande vägledning om behandling av personuppgifter

Femte upplagan

I denna upplaga har vägledningen uppdaterats med anledning av lagändringar (prop. 2021/22:251). Hänvisningar har också gjorts till EDPB:s och IMY:s riktlinjer och vägledning. Se ändringsmarkeringar.

Öppen konsultation juni 2023

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.

Simpts vägledning avseende företagens behandling av personuppgifter omfattar dels denna grundläggande vägledning, dels praktiskt inriktad vägledning.

Denna grundläggande vägledning är generell och omfattar till stora delar en beskrivning av vad som krävs enligt penningtvättsregelverket, med inslag av praktisk vägledning. De praktiska inslagen finns främst intagna i rutor samt under rubriker med hänvisning till ”i praktiken”. Vägledningen är relevant för alla verksamhetsutövare, om inte annat anges, och används som en referensram för de andra delarna av vägledningen om behandling av personuppgifter. Rubriknumreringen i de delarna motsvarar numreringen i denna grundläggande vägledning.

Denna grundläggande vägledning utgår framför allt från lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna). Alla laghänvisningar avser penningtvättslagen, om inte annat anges. Det hänvisas också till 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 (EU:s dataskyddsförordning eller General Data Protection Regulation, förkortad GDPR).

I denna femte upplaga har uppdateringar med anledning av ändringar i penningtvättslagen och hänvisningar gjorts till EDPB:s och IMY:s riktlinjer och vägledning.

1 Behandling av personuppgifter

1.1 Vad är en personuppgift?

Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person (artikel 4, GDPR).

Personuppgifter är all slags information som kan knytas till en levande person. Det kan röra sig om namn, adress, personnummer samt transaktionsuppgifter, t.ex. betalningsuppgifter som konto- och betalkortsnummer. Även foton på personer kan klassas som personuppgifter. Se vidare Vad är personuppgifter? (imy.se)

Denna vägledning omfattar endast den personuppgiftsbehandling som avser kunduppgifter.

Regelverken som reglerar behandling av personuppgifter avser fysiska personers personuppgifter. Många av verksamhetsutövarnas kunder är juridiska personer. En juridisk person har typiskt sett inte personuppgifter. Det innebär att uppgifter om den juridiska personen i regel inte omfattas av 5 kap. penningtvättslagen.

Att kunden är en juridisk person innebär dock inte att det går att bortse från 5 kap. penningtvättslagen. De uppgifter som går att knyta till en fysisk person omfattas av 5 kap. penningtvättslagen. En juridisk person företräds av en fysisk person. Dessa omfattas av 5 kap. penningtvättslagen. Det gäller även beträffande verkliga huvudmän (i vissa fall sammanfaller företrädaren med verklig huvudman). Uppgifter om den juridiska personen kan också behöva bevaras enligt 5 kap. 3 § penningtvättslagen. I förarbetena till penningtvättslagen (prop. 2016/17:173 s. 316) kommenteras placeringen av bestämmelsen om att bevara uppgifter i det kapitel som rör behandling av personuppgifter. Det sägs att det kan förutsättas att i princip samtliga handlingar och uppgifter som avser åtgärder för kundkännedom direkt eller indirekt kan hänföras till en viss fysisk person. Det gäller även om kunden är en juridisk person, eftersom uppgifter kommer att finnas om den juridiska personens verkliga huvudman eller i förekommande fall styrelseledamöter och andra företrädare. Detsamma gäller transaktionshistorik som ska bevaras.

1.2 Behandling av personuppgifter enligt penningtvättslagen (5 kap. 1 och 2 §§)

I 5 kap. penningtvättslagen regleras den behandling av personuppgifter som sker enligt penningtvättslagen. Bestämmelserna i 2–11 §§ gäller för verksamhetsutövare (se 5 kap. 1 § första stycket punkten 1). Bestämmelserna i 12 och 13 §§ gäller för andra än verksamhetsutövare (se 5 kap. 1 § första stycket punkten 2).

Behandling av personuppgifter är tillåten enligt penningtvättslagen i syfte att kunna fullgöra de skyldigheter som följer av den lagen, t.ex. för att inhämta uppgifter för kundkännedom eller för att övervaka kundens transaktioner. En behandling för andra syften kan alltså inte grundas på penningtvättslagen.

Det förekommer att verksamhetsutövare i samband med inhämtandet av uppgifter för kundkännedom även inhämtar andra uppgifter om kunden eller att verksamhetsutövaren inhämtar kundkännedomsuppgifter även för andra syften än för att uppfylla kraven enligt penningtvättsregelverket. Det är av flera skäl viktigt att vara klar över den rättsliga grunden för den behandling som sker och att kunna hålla isär uppgifterna, även om de hämtas in i ett sammanhang. Det gäller bland annat för att det kan gälla olika gallringsregler beträffande uppgifterna.

Bestämmelserna om behandling av personuppgifter i penningtvättslagen påverkar inte verksamhetsutövarens skyldigheter i fråga om personuppgiftsbehandling, t.ex. bevarande av uppgifter, som kan följa av annan lagstiftning som reglerar verksamhetsutövarens verksamhet (prop. 2016/17:173 s. 309, 543 och 544).

Det finns ett antal grundläggande principer som gäller för all personuppgiftsbehandling och som framgår av GDPR. Principerna innebär bland annat att:

- All personuppgiftsbehandling måste ha stöd i dataskyddsförordningen (dvs. ha en rättslig grund)
- Personuppgifter får bara samlas in för specifika, särskilt angivna och berättigade ändamål
- Fler personuppgifter än vad som behövs för ändamålen får inte behandlas
- Personuppgifter som inte längre behövs ska raderas eller avidentifieras

Det finns sex rättsliga grunder för personuppgiftsbehandling:

Avtal: Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige. Det krävs att personuppgiftsbehandlingen är nödvändig, antingen för att fullgöra avtalet med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan avtalet ingås.

Intresseavvägning/berättigat intresse: Den personuppgiftsansvarige får behandla personuppgifter om personuppgiftsbehandlingen är nödvändig för ett ändamål som rör ett berättigat intresse och den registrerades intresse av skydd för sina personuppgifter inte väger tyngre.

Rättslig förpliktelse: Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet.

Myndighetsutövning och uppgift av allmänt intresse: Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.

Grundläggande intresse: Den personuppgiftsansvarige måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, till exempel om den är medvetslös.

Samtycke: Den registrerade har sagt ja till personuppgiftsbehandlingen. Enligt Integritetsskydds-myndigheten är det i många fall inte lämpligt eller kanske inte ens möjligt att stödja sig på den registrerades samtycke, varför det alltid i första hand bör övervägas om det går att stödja person-uppgiftsbehandlingen på någon av de andra rättsliga grunderna.

Dataskyddsförordningens (GDPRs) grundläggande principer – Integritetsskyddsmyndigheten (imy.se)

Rättslig grund för personuppgiftsbehandling – Integritetsskyddsmyndigheten (imy.se)

Den behandling av personuppgifter som sker enligt penningtvättslagen sker med stöd av den rättsliga grunden rättslig förpliktelse. Det utesluter dock inte att även andra rättsliga grunder för behandling av personuppgifter kan vara aktuella i syfte att bekämpa penningtvätt och finansiering av terrorism, framför allt den rättsliga grunden berättigat intresse.

1.3 EU:s dataskyddsförordning/GDPR

Sedan den 25 maj 2018 tillämpas 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 (EU:s dataskyddsförordning eller General Data Protection Regulation, förkortad GDPR).

Principen om unionsrättens företräde innebär att en bestämmelse i en sektorsspecifik författning får tillämpas endast om den är förenlig med EU:s dataskyddsförordning och avser en fråga som enligt förordningen får särregleras eller specificeras genom nationell rätt (prop. 2017/18:105 s. 27).

Den personuppgiftsbehandling som sker enligt penningtvättslagen är tillåten enligt EU:s dataskydds-förordning. Uppgifterna anses regelmässigt vara av allmänt intresse, åtminstone utgör de rättsliga förpliktelser (se prop. 2017/18:142 s. 27 och 28).

Dataskyddsförordningen kompletteras med bestämmelser i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Det finns vägledning på dataskyddsområdet som tas fram av Europeiska dataskyddsstyrelsen (EDPB). EDPB består av medlemsstaternas tillsynsmyndigheter och Europeiska datatillsynsmannen (EDPS). EDPB | European Data Protection Board (europa.eu)

Se också information om EDPB på Integritetsskyddsmyndighetens (IMY) hemsida Europeiska dataskyddsstyrelsen (EDPB) | IMY

Även IMY har tagit fram vägledning, www.imy.se.

2 Bevarande av handlingar och uppgifter (5 kap. 3 §)

2.1 Inledning

En verksamhetsutövare ska i fem år bevara vissa handlingar och uppgifter. Bevarandet av handlingar och uppgifter syftar till att göra det möjligt för Polismyndigheten och andra myndigheter att förebygga, upptäcka eller utreda penningtvätt och finansiering av terrorism (prop. 2016/17:173 s. 317).

Det bör framhållas att bevarandet av handlingar och uppgifter också syftar till att verksamhets-utövaren ska kunna efterleva de krav som ställs i penningtvättslagen. Oavsett bakomliggande syfte begränsas verksamhetsutövarens möjligheter att bevara handlingar och uppgifter av den ram som ställs upp i 5 kap. 3 § penningtvättslagen.

Bestämmelserna om att bevara handlingar omfattas inte av någon övergångsbestämmelse. Bestämmelserna tillämpas både på handlingar och uppgifter som inhämtades innan penning-tvättslagen trädde i kraft (den 1 augusti 2017) och sådana som inhämtades efter den tidpunkten (prop. 2016/17:173 s. 317 och 318).

2.2 Vilka handlingar och uppgifter ska bevaras?

Det som ska bevaras är handlingar och uppgifter som avser

1. åtgärder som har vidtagits för kundkännedom enligt 3 kap. och 4 kap. 2 §, eller
2. transaktioner som genomförts med kunder inom ramen för affärsförbindelser eller vid enstaka transaktioner som omfattas av krav på åtgärder för kundkännedom enligt 3 kap. 4–6 §§.

De handlingar och uppgifter som ska bevaras är alltså sådana som har använts för att uppfylla kraven på att vidta åtgärder för kännedom enligt 3 kap. penningtvättslagen. Det kan vara kopior av identitetshandlingar, utredningar och bedömningar avseende den verkliga huvudmannen och andra liknande uppgifter (prop. 2016/17:173 s. 544). Det kan också vara fråga om åtgärder för kundkännedom som vidtagits vid bedömning av avvikande eller annars misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §.

Verksamhetsutövaren måste alltid vara klar över huruvida en viss uppgift har inhämtats för att uppfylla kraven på att vidta åtgärder för kundkännedom eller för något annat syfte. En uppgift som inhämtas beträffande en kund kan ha inhämtats för kundkännedomsändamål, medan motsvarande uppgift för en annan kund kan ha inhämtats i ett helt annat syfte. När uppgiften inte har inhämtats för att uppnå kundkännedom (och inte heller enligt 4 kap. 2 § penningtvättslagen), finns det inte något krav enligt penningtvättslagen på att den ska bevaras. Krav på att bevara uppgiften kan dock finnas enligt andra regelverk.

Personuppgifter som hämtas in om kunden för att uppfylla olika regelverk kan finnas i samma systemstöd eller i samma dokument/blankett (i pappersformat). Det kan t.ex. vara fråga om uppgifter om att någon är person i politiskt utsatt ställning, som ska bevaras i fem år efter att affärsförbindelsen upphörde, och uppgifter som har hämtats in enligt försäkringsdistributionsreglerna, som ska bevaras i tio år efter att affärsförbindelsen upphörde. Verksamhetsutövaren måste vara uppmärksam på att olika gallringsregler kan gälla för uppgifter som finns samlade i ett system eller på en blankett.

2.3 Från när börjar fristen löpa?

Uppgifterna och handlingarna ska bevaras i fem år. Tiden räknas från olika tidpunkter beroende på vad som skett:

- Från det att åtgärderna eller transaktionerna utfördes.
- I de fall en affärsförbindelse har etablerats räknas tiden från det att affärsförbindelsen upphörde.
- Om en enstaka transaktion inte har genomförts till följd av misstanke om penningtvätt eller finansiering av terrorism räknas tiden från det att avståendet skedde.

2.4 Förlängd tid för bevarande (5 kap. 4 §)

I vissa fall får verksamhetsutövaren bevara uppgifter längre tid än fem år. Den sammanlagda tiden får dock inte överstiga tio år. Det gäller även i fråga om handlingar och uppgifter som ska bevaras enligt artikel 16 i förordning (EU) 2015/847.

Verksamhetsutövaren ska, enligt 5 kap. 2 § penningtvättsföreskrifterna, bevara handlingar och uppgifter i tio år om:

- Handlingarna eller uppgifterna kan tyda på penningtvätt, finansiering av terrorism eller att egendom annars härrör från brottslig handling,
- omständigheter enligt punkten ovan har rapporterats till Polismyndigheten eller Säkerhetspolisen enligt 4 kap. 3 eller 6 § penningtvättslagen, och
- en myndighet har uppmärksammat företaget om att handlingarna eller uppgifterna behöver bevaras under denna tidsperiod.

Punkterna är kumulativa, dvs. alla tre måste vara uppfyllda för att det ska finnas ett krav på att bevara handlingar och uppgifter i tio år.

Både underlaget och rapporten till Polismyndigheten ska bevaras (se Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 27).

Verksamhetsutövaren ska inte själv genomföra någon individuell prövning av om en uppgift kan ha sådan betydelse efter att en handling bevarats i fem år att den behöver bevaras under ytterligare tid. Det krävs i stället att verksamhetsutövaren uppmärksammas på detta behov från Polismyndigheten eller en rättsvårdande myndighet (prop. 2016/17:173 s. 317 och 545).

2.5 Hur ska handlingarna och uppgifterna bevaras?

Handlingarna och uppgifterna som ska bevaras enligt 5 kap. 3 och 4 §§ penningtvättslagen ska bevaras på ett säkert sätt, elektroniskt eller i pappersform. Verksamhetsutövaren ska se till att handlingarna och uppgifterna är enkla att ta fram och identifiera (5 kap. 1 § penningtvättsföreskrifterna).

Det finns inte något hinder mot att hantera och bevara uppgifter i olika system eller annars på olika sätt, så länge uppgifterna är enkla att ta fram och identifiera.

I Finansinspektionens tillsynsrapport Erfarenheter från penningtvättstillsynen 2016–2017 konstateras följande (s. 7). Det är vanligt att företag använder sig av någon form av elektroniskt system för att hantera och dokumentera den kundkännedomsinformation som samlas in. I vissa fall kompletteras ett övergripande system med ett flertal andra system. Det finns också exempel på att fysiska kundakter används som komplement till ett elektroniskt system där andra delar av kundkännedomen finns sparad. Utöver elektroniska system och kundakter kan information om vissa speciella omständigheter eller detaljer om kunden finnas hos den kundansvarige, kassapersonal eller liknande. FI har noterat att all information om kunden inte alltid är dokumenterad och samlad på ett ställe. Att kundkännedomsuppgifter finns utspridda på flera system, funktioner och befattningar kan leda till att handlingar och uppgifter om kundkännedom inte är enkla att ta fram och identifiera. Det ökar också risken för att viktig information förbises exempelvis vid den fortlöpande uppföljningen av affärsförbindelserna och vid övervakningen av transaktioner.
Erfarenheter från penningtvättstillsynen 2016–2017 (fi.se)

2.6 Bevara handlingar och uppgifter i praktiken

2.6.1 När det inte blir någon affärsförbindelse

En fråga är vad som gäller när det inte uppstår någon avtals- och affärsförbindelse med verksamhetsutövaren. Verksamhetsutövaren kan av olika skäl neka någon att ingå en avtals- och affärsförbindelse. Personen i fråga kan också av olika skäl själv avbryta kontakterna med verksamhetsutövaren.

Enligt definitionen i penningtvättslagen är kund den som har trätt eller står i begrepp att träda i avtalsförbindelse med en verksamhetsutövare (1 kap. 8 § punkten 4 penningtvättslagen). Om förbindelsen förväntas ha viss varaktighet uppstår en affärsförbindelse (se 1 kap. 8 § punkten 1), vilket ställer krav på kundkännedom.

Flera bestämmelser i penningtvättslagen om åtgärder som måste vidtas avseende kunder aktualiseras därmed i regel redan innan en affärsförbindelse etableras eller en enstaka transaktion utförs, t.ex. skyldigheten att identifiera och kontrollera kundens identitet. Avsikten att ingå en affärsförbindelse måste dock ha manifesterats på ett sådant sätt att verksamhetsutövaren har inlett eller enligt reglerna i penningtvättslagen borde ha inlett processen för kundkännedom, eftersom det är från denna tidpunkt som bestämmelserna avseende åtgärder med kunden i penningtvättslagen blir tillämpliga (se prop. 2016/17:173 s. 188). Det måste för verksamhetsutövaren framstå som klart att en avtalsförbindelse är på väg att ingås, förutsatt att tillräcklig kundkännedom kan uppnås (prop. 2016/17:173 s. 508 och 509).

Exempel: En person kontaktar verksamhetsutövaren med frågor om olika produkter och tjänster utan att ge uttryck för att faktiskt vilja ingå en avtals- och affärsförbindelse med verksamhetsutövaren. Verksamhetsutövaren besvarar frågorna, men vidtar inte några särskilda åtgärder. I dessa fall finns i regel inte något stöd för att bevara eventuella handlingar eller uppgifter.

Exempel: En person kontaktar verksamhetsutövaren i syfte att ingå ett avtal och det står klart för verksamhetsutövaren att en avtalsförbindelse är på väg att ingås, förutsatt att tillräcklig kundkännedom kan uppnås. Innan avtalet och affärsförbindelsen ingås nekar dock verksamhetsutövaren av något skäl personen i fråga att ingå avtals- och affärsförbindelsen, alternativt avbryter personen själv av någon anledning kontakterna med verksamhetsutövaren. En bedömning får då göras utifrån omständigheterna i det enskilda fallet om det finns en skyldighet att bevara handlingar och uppgifter som har inhämtats.

Om en enstaka transaktion inte har genomförts till följd av misstanke om penningtvätt eller finansiering av terrorism, ska tiden räknas från det att avståendet skedde. Detta följer av 5 kap. 3 § andra stycket penningtvättslagen. Uppgifterna som bevaras bör motsvara de som omfattas av rapporteringsunderlaget till Finanspolisen. Situationen då verksamhetsutövaren, på samma skäl, avstår från att ingå en affärsförbindelse regleras inte på samma sätt uttryckligen i penningtvättslagen. I den mån uppgifterna inte sparas enligt 5 kap. 3 § första stycket punkten 1 penningtvättslagen, bör det anses finnas ett berättigat intresse av att bevara uppgifter också i dessa fall, på motsvarande sätt som när en enstaka transaktion nekas. Uppgifterna bör bevaras i den utsträckning som de som omfattas av rapporteringsunderlaget till Finanspolisen och i syfte att göra det möjligt för Polismyndigheten och andra myndigheter att förebygga, upptäcka eller utreda penningtvätt och finansiering av terrorism (jfr prop. 2016/17:173 s. 317).

2.6.2 Enstaka transaktioner som blir en affärsförbindelse

En fråga är vad som gäller för en kund som upprepade gånger utför enstaka transaktioner på ett sådant sätt att verksamhetsutövaren sedermera bedömer att en affärsförbindelse har uppstått.

Enligt Finansinspektionen kan en utgångspunkt för bedömningen av om en affärsförbindelse har uppstått vara tolv transaktioner under en tolvmånadersperiod, som utförs av en och samma person (se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–17 nr 1 12 april 2018 s. 8).

Ett närliggande område måste anses vara s.k. sambandstransaktioner. Beträffande sambandstransaktioner ska verksamhetsutövaren vidta åtgärder för kundkännedom om verksamhetsutövaren inser eller borde inse att transaktionen har ett samband med en eller flera andra transaktioner och som tillsammans uppgår till minst 15 000 euro.

Att verksamhetsutövaren ska ha insett eller borde inse sambandet innebär inte att det ställs några krav på särskilda åtgärder för att identifiera samband mellan transaktioner. Det krävs alltså inte att särskilda eller aktiva åtgärder vidtas för att undersöka om transaktioner har samband med varandra. Om de för verksamhetsutövaren iakttagbara omständigheterna i det enskilda fallet tyder på ett samband, ska däremot aktiva åtgärder vidtas för att fastställa sambandet och i tillämpliga fall utföra åtgärder för kundkännedom (prop. 2016/17:173 s. 522).

Detta resonemang bör gälla även för enstaka transaktioner som tillsammans leder till att en affärsförbindelse ska anses ha uppstått. Det bör inte heller i dessa fall ställas några krav på verksamhetsutövaren att vidta särskilda åtgärder för att identifiera att det är fråga om en mer varaktig förbindelse. Det bedöms inte heller finnas någon skyldighet eller stöd för att bevara handlingar eller uppgifter hänförliga till de tillfällen då det inte bedömdes vara fråga om en affärsförbindelse. Kraven på att bevara uppgifter och handlingar anses uppstå först när verksamhetsutövaren bedömer att en affärsförbindelse har ingåtts.

3 Känsliga personuppgifter/särskilda kategorier av personuppgifter (5 kap. 5 §)

3.1 Inledning

Känsliga personuppgifter, eller ”särskilda kategorier av personuppgifter” enligt artikel 9.1 GDPR får behandlas endast i vissa fall.

3.2 Vad är känsliga personuppgifter?

Med känsliga personuppgifter eller särskilda kategorier av personuppgifter (som är det begrepp som används i GDPR) avses följande personuppgifter.

- Ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- genetiska uppgifter,
- biometriska uppgifter för att entydigt identifiera en fysisk person,
- uppgifter om hälsa, eller
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Läs mer på Integritetsskyddsmyndighetens hemsida Känsliga personuppgifter (imy.se)

3.3 När får känsliga personuppgifter behandlas?

Känsliga personuppgifter får behandlas enligt penningtvättslagen endast om det är nödvändigt för att verksamhetsutövaren ska kunna göra följande.

- Bedöma om kunden är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person enligt 1 kap. 8–10 §§.
- Bedöma den risk som kan förknippas med kundrelationen (riskklassificering) enligt 2 kap. 3 §.
- Uppfylla övervakningsskyldigheten enligt 4 kap. 1 §.
- Bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §.
- Lämna uppgifter till Polismyndigheten enligt 4 kap. 3 § och till Polismyndigheten respektive Säkerhetspolisen enligt 4 kap. 6 §.
- Lämna uppgifter i samverkan enligt 4 a kap.
- Bevara handlingar och uppgifter enligt 5 kap. 3 och 4 §§, om det är tillåtet att behandla uppgifterna enligt punkterna ovan.

4 Personuppgifter om lagöverträdelser (5 kap. 6 §)

4.1 Vad är uppgift om lagöverträdelse?

Personuppgifter om lagöverträdelser är personuppgifter som rör fällande domar i brottmål samt överträdelser och därmed sammanhängande säkerhetsåtgärder. Detta följer av artikel 10 GDPR, dit det hänvisas i 5 kap. 6 § penningtvättslagen.

Med överträdelser avses endast lagöverträdelser som innefattar brott.

Begreppet ”därmed sammanhängande säkerhetsåtgärder” har tolkats som likvärdigt med straffprocessuella tvångsåtgärder (prop. 2016/17:173 s. 98).

Artikel 10 omfattar inte personuppgifter om administrativa sanktioner och avgöranden i tvistemål. Sådana uppgifter är alltså inte särskilt reglerade i GDPR och omfattas därmed inte heller av bestämmelsen i penningtvättslagen, om de inte utgör känsliga personuppgifter enligt artikel 9.1 (prop. 2017/18:105 s. 98).

4.2 När får uppgifter om lagöverträdelser behandlas?

Personuppgifter som avses i artikel 10 GDPR får behandlas endast om det är nödvändigt för att göra följande.

- Bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §.
- Uppfylla övervakningsskyldigheten enligt 4 kap. 1 §.
- Bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §.
- Lämna uppgifter enligt 4 kap. 3 och 6 §§.
- Lämna uppgifter i samverkan enligt 4 a kap.

Personuppgifterna får också behandlas vid bevarande av handlingar och uppgifter enligt 5 kap. 3 och 4 §§, om det är tillåtet att behandla uppgifterna enligt ovan.

5 Information till den registrerade (5 kap. 7 §)

Enligt artikel 15 GDPR har den registrerade som huvudregel rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och viss annan information. Denna rätt har begränsats i 5 kap. 7 § penningtvättslagen.

Besked får inte lämnas ut till den registrerade om att personuppgifter behandlas enligt följande bestämmelser.

- 4 kap. 2 §, dvs. vid den analys som ska genomföras för att avgöra om en transaktion ingår som ett led i penningtvätt eller finansiering av terrorism (prop. 2016/17:173 s. 312).
- 4 kap. 3 §, dvs. att rapportering har skett till Polismyndigheten.
- 4 kap. 6 §, dvs. att uppgifter har lämnats på begäran till Polismyndigheten eller Säkerhetspolisen.

Besked får inte heller lämnas ut till den registrerade om att sådana personuppgifter som räknas upp ovan lagras enligt följande bestämmelser.

- 5 kap. 3 §, dvs. bevaras i fem år.
- 5 kap. 4 §, dvs. bevaras i längre tid än fem år.

Det är alltså inte alla uppgifter om kunden som omfattas av detta undantag eller begränsning.

Europeiska dataskyddsstyrelsen (EDPB) har tagit fram vägledning om den registrerades rätt till tillgång till uppgifter, Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu).

6 Samkörning av register (5 kap. 8 och 9 §§)

En verksamhetsutövares register med uppgifter om misstänkt penningtvätt eller finansiering av terrorism får inte samköras med motsvarande register hos någon annan.

I registret förekommer i huvudsak uppgifter om personer som verksamhetsutövaren har granskat eller rapporterat för misstänkt penningtvätt eller finansiering av terrorism.

Det finns vissa undantag från samkörningsförbudet i fråga om koncerner och för den som bedriver gränsöverskridande verksamhet via filial:

- Det är tillåtet för verksamhetsutövare som avses i 1 kap. 2 § första stycket 1–13 penningtvättslagen att samköra register med *filialer* som är *etablerade utanför EES*, förutsatt att kraven enligt 2 kap. 10 och 11 §§ penningtvättslagen är uppfyllda i fråga om filialen. Det innebär att filialen måste tillämpa gemensamma rutiner avseende informationsdelning och skydd för personuppgifter samt tillämpa bestämmelser för att förhindra penningtvätt eller finansiering av terrorism som är likvärdiga med dem som följer av penningtvättslagen.
- Det är tillåtet för verksamhetsutövare som avses i 1 kap. 2 § första stycket 1–13 penningtvättslagen och som ingår i samma *koncern* att samköra register, om de har hemvist i Sverige eller inom EES.
- Samkörning är tillåten med en verksamhetsutövare inom en *koncern* som har *hemvist utanför EES*, under förutsättning att kraven enligt 2 kap. 10 och 11 §§ penningtvättslagen är uppfyllda i fråga om den verksamhetsutövaren. Det innebär att verksamhetsutövaren måste tillämpa

gemensamma rutiner avseende informationsdelning och skydd för personuppgifter samt tillämpa bestämmelser för att förhindra penningtvätt eller finansiering av terrorism som är likvärdiga med dem som följer av penningtvättslagen.

(Se prop. 2016/17:173 s. 313 och 546).

7 Tystnadsplikt (5 kap. 11 §)

Den som är verksam hos en verksamhetsutövare får inte obehörigen röja att uppgifter behandlas enligt följande bestämmelser.

- 5 kap. 5 §, dvs. känsliga personuppgifter
- 5 kap. 6 §, dvs. personuppgifter om lagöverträdelser
- 4 kap. 2 §, dvs. vid den analys som genomföras för att avgöra om en transaktion ingår som ett led i penningtvätt eller finansiering av terrorism.
- 4 kap. 3 §, dvs. att rapportering har skett till Polismyndigheten.
- 4 kap. 6 §, dvs. att uppgifter har lämnats på begäran av Polismyndigheten eller Säkerhetspolisen.

Den som är verksam hos en verksamhetsutövare får inte heller obehörigen röja att sådana personuppgifter som räknas upp ovan bevaras enligt följande bestämmelser.

- 5 kap. 3 §, dvs. bevaras i fem år.
- 5 kap. 4 §, dvs. bevaras i längre tid än fem år.

8 Andra än verksamhetsutövare (5 kap. 12 och 13 §§)

Bestämmelsen i 5 kap. 12 § innebär att en clearingorganisation som bedriver clearing eller avveckling av betalningar och den som tillhandahåller finansiell infrastruktur som avser omedelbara betalningar, inte får lämna besked om att personuppgifter behandlas enligt 4 kap. 6 § till den registrerade (prop. 2021/22:251 s. 128).

Bestämmelsen i 5 kap. 13 § innehåller bestämmelser om tystnadsplikt. Bestämmelsen innebär att en clearingorganisation som bedriver clearing eller avveckling av betalningar eller den som tillhandahåller finansiell infrastruktur som avser omedelbara betalningar inte obehörigen får röja att personuppgifter behandlas enligt 4 kap. 6 §. Det bör inte anses som ett obehörigt röjande när uppgifter lämnas till en verksamhetsutövare som använder de uppgiftsskyldiga aktörernas tjänster, i den mån uppgifterna avser verksamhetsutövarens egen kund. Det gäller t.ex. när en clearingorganisation lämnar uppgifter till ett kreditinstitut om en betalning som görs av en kund i institutet. Tystnadsplikten är inte straffsanktionerad (prop. 2021/22:251 s. 128 och 129).