SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Grundläggande vägledning om behandling av personuppgifter

Beslutad av Simpts styrgrupp i november 2019

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 intagen 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 praktiskt inriktade delarna av vägledningen. Rubriknumreringen i de delarna motsvarar numreringen i denna grundläggande vägledning.

Företrädare för medlemsföretagen har deltagit i arbetet med att ta fram denna del av vägledningen.

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.

1 Behandling av personuppgifter

1.1 Vad är en personuppgift?

Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person (artikel 4 i EU:s dataskyddsförordning).

Personuppgifter är all slags information som kan knytas till en levande person. Det kan röra sig om namn, adress och personnummer. Även foton på personer kan klassas som personuppgifter. Se vidare https://www.datainspektionen.se/om-integritet/vad-ar-en-personuppgift/.

Denna vägledning omfattar endast den personuppgiftsbehandling som avser kunduppgifter.

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).

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. Behandling av personuppgifter är tillåten enligt penningtvättslagen i syfte att kunna fullgöra de skyldigheter som följer av den lagen. En behandling för andra syften kan alltså inte grundas på penningtvättslagen.

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).

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 dataskyddsförordning. 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.

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 verksamhetsutövaren 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 penningtvättslagen 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?

De handlingar och uppgifter som ska bevaras är 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).

Verksamhetsutövaren bör ställa sig frågan om en viss handling eller uppgift har inhämtats för att uppfylla kraven på att vidta åtgärder för kundkännedom eller för något annat syfte. En viss 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 §), finns det inte något krav enligt penningtvättslagen på att den ska bevaras. Krav på att bevara uppgiften kan dock finnas enligt andra regelverk.

Det är också fråga om åtgärder för kundkännedom som vidtagits vid bedömning av avvikande eller annars misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §.

Verksamhetsutövaren ska också bevara handlingar och uppgifter om de transaktioner som genomförts inom ramen för affärsförbindelser eller enstaka transaktioner (se prop. 2016/17:173 s. 544).

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 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).

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). 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 avseende de uppgifter som har inhämtats.

Om verksamhetsutövaren avstår från att ingå en affärsförbindelse eller om verksamhetsutövaren nekar en enstaka transaktion på grund av misstankar om penningtvätt eller finansiering av terrorism, ska dock uppgifterna sparas eftersom de ingår i rapporteringsunderlaget till Finanspolisen.

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 EU:s dataskyddsförordning, får behandlas i vissa fall.

3.2 Vad är känsliga personuppgifter?

Med känsliga personuppgifter eller särskilda kategorier av personuppgifter (som är det begrepp som används i EU:s dataskyddsförordning) 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 Datainspektionens hemsida https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/detta-ar-kansliga-personuppgifter/

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 6 §§.
- Bevara handlingar och uppgifter enligt 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 i EU:s dataskyddsförordning, 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 EU:s dataskyddsförordning 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 i EU:s dataskyddsförordning 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 §§.

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

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

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.

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.

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 1–12 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 1–12 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.

Den som är verksam hos en verksamhetsutövare får inte heller obehörigen röja att sådana person-uppgifter 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.