SENSOR FONDER - INSTRUKTION OM ÅTGÄRDER MOT PENNINGTVÄTT OCH FINANSIERING AV TERRORISM SAMT ANNAN BROTTSLIGHET

1. Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism
2. Finansinspektionens föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism (FFFS 2017:11)
3. Lag om straff för penningtvättsbrott
4. Lag om straff för finansiering av särskild allvarlig brottslighet i vissa fall.

Syftet med denna instruktion är att förhindra att Bolaget utnyttjas för penningtvätt, finansiering av terrorism eller annan allvarlig brottslighet samt att upptäcka och rapportera företeelser, händelser, personer och kunder, affärer eller transaktioner som kan ha beröring med sådan verksamhet.

A. TILLÄMPNINGSOMRÅDE OCH DEFINITIONER

Tillämpningsområde och definitioner specificeras i SFS 2017:630, 1 kap.

B. RISKBEDÖMNING OCH RUTINER

1. Allmän riskbedömning - Produkter och tjänster m. m.
Bolaget ska dokumentera en *allmän riskbedömning* som visar hur stora riskerna är för att något av nedanstående kan utnyttjas för penningtvätt och finansiering av terrorism:

- produkter,
- tjänster,
- distributionskanaler och
- geografiska riskfaktorer.

Den allmänna riskbedömningen ska dokumenteras på Bilaga 1 och uppdateras när det behövs eller minst en gång per år.
Riskbedömningen ska även uppdateras innan vi erbjuder eller marknadsför väsentligt förändrade nya produkter eller tjänster, vänder oss till nya marknader eller använder nya distributionskanaler, eller om verksamheten i övrigt förändras på något annat avgörande sätt.

2. Riskbedömning av kunder (kunders riskprofil)
Bolaget ska bedöma den risk för penningtvätt, finansiering av terrorism och/eller annan brottslighet som kan förknippas med kundrelationen (kundens riskprofil).
Innan en affärsförbindelse inleds ska nya kunder kontrolleras mot sanktionslistor.
Dessa kontroller bör omedelbart upprepas om anledning till misstanke uppkommer och minst göras rutinmässigt en gång per år.

Om gränsöverskridande transaktioner förekommer ska dessa kontrolleras mot sanktionslistorna.

Kundens riskprofil ska bestämmas med utgångspunkt i den allmänna riskbedömningen och vår kännedom om kunden.

Exempel på omständigheter som kan tyda på att kundens riskprofil är hög (SFS 2017:630):

• kundens ägarstruktur är ovanlig eller onödigt komplicerad,
• kunden bedriver kontantintensiv verksamhet,
• kunden har hemvist i stat med betydande korruption, brottslighet, brist på system mot ekonomisk brottslighet, är föremål för sanktioner, embargon e. dyl., en stat där terrorister är verksamma,
• kundens affärstransaktioner sker på distans utan att identiteter kan fastställas.

Bedömning av kundens riskprofil ska göras av Bolaget innan affärsförbindelse ingås med vårt Kundavtalet som underlag. Minst en gång per år ska kundens riskprofil utvärderas så länge affärsförbindelsen består genom att de initiala kundavtalen på nytt granskas och bedöms och jämförs med erhållna erfarenheter av kunden. Kontrollen ska dokumenteras på respektive avtal genom notering av datum för granskningen samt ansvarig tjänstemans signatur. Om kundens riskprofil anses försämrad, ska detta noteras på avtalet och rapporteras till VD.
Information om kunder får delas inom Bolaget, såsom t.ex. kundkännedom, konto- och transaktionsinformation, för att förhindra penningtvätt eller finansiering av terrorism.

3. Utbildning av egna anställda och bedömning av uppdragstagare
Bolaget ska säkerställa att anställda och uppdragstagare är lämpliga för verksamheten och har tillräcklig kompetens för att förhindra att Bolaget utnyttjas för penningtvätt eller finansiering av terrorism.

Compliance Officer ska löpande informera anställda och uppdragstagare om nya trender, mönster, metoder samt annan information som kan vara relevant för att förhindra penningtvätt eller finansiering av terrorism.

Anställda ska årligen delta i intern utbildning initierad av Compliance Officer. Utbildningens innehåll ska dokumenteras, varav minst följande ska framgå: utbildningens innehåll, namn på deltagare samt datum för utbildningen. Dessutom ska alla anställda inneha aktiv licens utfärdad av SwedSec AB samt genomgå årlig kunskapsuppdatering och kunskapstest Uppdragstagare ska minst två gånger om året bedömas efter att de besvarat ett Frågeformulär.

Om Bolagets allmänna riskbedömning uppdateras eller på annat sätt ändras, ska utbildning för anställda och kontrollen av uppdragstagare ändras och anpassas.

4. Fysisk skydd och förbud mot repressalier för Bolagets anställda
Bolaget ska ha beredskap och vidta nödvändiga åtgärder för att skydda anställda och uppdragstagare från hot eller andra fientliga åtgärder till följd av att de fullgör skyldigheter enligt denna lag.

Bolaget ska identifiera vilka hot eller fientliga åtgärder som kan uppkomma mot anställda, uppdragstagare eller andra som deltar i vår verksamhet. Eventuella incidenter ska utredas och kunskapen användas för att uppdatera rutinerna.

Bolaget, ägare, styrelse eller dess ledning, får inte utsätta anställd eller uppdragstagare för repressalier på grund av att denne har informerat om misstänkt penningtvätt eller finansiering av terrorism, internt eller externt till Polismyndighet eller Finansinspektionen.

C. KUNDKÄNNEDOM

1 Förbud mot affärsförbindelser och transaktioner

Otillräcklig kundkännedom
Bolaget får inte etablera eller upprätthålla en affärsförbindelse eller utföra en transaktion om Bolaget inte har tillräcklig kännedom om kunden för att kunna
• hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen,
• övervaka och bedöma kundens aktiviteter och transaktioner.

Misstanke om penningtvätt eller finansiering av terrorism
• Affärsförbindelse får inte etableras om det finns misstanke om att Bolagets produkter eller tjänster kommer att användas för penningtvätt eller finansiering av terrorism.
• Bolaget får inte utföra en transaktion om det på skälig grund kan misstänkas att den utgör ett led i penningtvätt eller finansiering av terrorism. Om en rapport har lämnats till Polismyndighet ska Bolaget beakta information som Polismyndigheten kan lämna om ärendet.
• Om det inte är möjligt att låta bli att utföra en misstänkt transaktion, eller om ett avstående att genomföra transaktionen skulle försvåra den vidare utredningen, får transaktionen genomföras.

2. Situationer som kräver kundkännedom

Bolaget måste vidta åtgärder för kundkännedom vid etableringen av en affärsförbindelse. Om Bolaget inte har en affärsförbindelse med kunden, ska åtgärder för kundkännedom vidtas:

• vid enstaka transaktioner som uppgår till ett belopp motsvarande 15 000 euro eller mer,
• vid transaktioner som understiger 15 000 euro där Bolaget borde inse att samband finns med en eller flera andra transaktioner som tillsammans uppgår till minst detta belopp.

3. Åtgärder som ska vidtas för kundkännedom

Identifiering och kontroll av kunden
Kunden ska identifieras genom identitetshandlingar. Om kunden företräds av person som uppger sig handla på kundens vägnar, ska den personens identitet och behörighet att företräda kunden kontrolleras. Om kunden är en juridisk person, ska ägarstruktur och verklig huvudman utredas. Det ska utredas om kunden är en person i politisk utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person. Se SFS

2017:630, 3 kap. 7-11 §§. Kopia av identitetshandlingen ska infogas på vårt kundavtal eller bifogas och arkiveras med kundavtalet i högst tio år.

Fysisk person
Identiteten ska kontrolleras hos en fysisk person genom svenskt körkort, svenskt pass eller identitetskort utfärdat av en svensk myndighet eller ett svensk certifierat identitetskort. Om fysisk person saknar svensk identitetshandling, ska vi kontrollera identiteten mot pass eller annan identitetshandling som innehåller fotografi av personen, uppgift om medborgarskap och är utfärdat av en myndighet eller annan behörig utfärdare. Om fysisk person helt saknar identitetshandling ska vi kontrollera identiteten genom andra tillförlitliga dokument enligt SFS 2017:630 2 kap. 8 §.

Företrädare för fysisk person
Om fysisk person företräds av person som inte är förvaltare eller god man, ska vi kontrollera företrädarens identitet på samma sätt som för fysisk person, se ovan.
Vi ska dessutom kontrollera att denna har behörighet att företräda den fysiska personen genom att kontrollera skriftlig fullmakt, personbevis eller motsvarande.
Om en fysisk person har en förvaltare eller en god man, ska vi kontrollera förvaltarens eller den gode mannens identitet och kontrollera förordnandet eller motsvarande handling som ligger till grund för uppdraget som förvaltare eller god man.

Fysisk person på distans
Identiteten hos fysisk person kan kontrolleras på distans genom att använda elektronisk legitimation enlig lagen (2016:561) eller
• inhämta personuppgifter på annat sätt,
• kontrollera uppgifterna mot externa register eller annan dokumentation,
• uppmana personen att översända vidimerad kopia av identitetshandling.
Se vidare FFFS 2017:11, 3 kap. 5 §.

Juridisk person
Identiteten hos juridiska personer ska företrädesvis kontrolleras genom registreringsbevis som inte är äldre än sex månader. Den juridiska personens företrädare ska kontrolleras på samma sätt som fysiska personer (ovan). Behörigheten att företräda den juridiska personen ska företrädesvis kontrolleras mot registreringsbevis.
Se vidare FFFS 2017:11, 3 kap. 6 §.

Juridisk person på distans
Identiteten hos juridiska personer på distans ska företrädesvis kontrolleras genom registreringsbevis som inte är äldre än sex månader. Den juridiska personens företrädare ska kontrolleras på samma sätt som fysiska personer på distans (ovan).
Behörigheten att företräda den juridiska personen ska företrädesvis kontrolleras mot registreringsbevis.
Se vidare FFFS 2017:11, 3 kap. 7 §.

Kontroll av verklig huvudmans identitet
Vi ska vid kontroll av identiteten av en kunds verkliga huvudman enligt 3 kap. 8 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, skaffa oss tillförlitliga uppgifter om kundens verkliga huvudman genom att kontrollera uppgifterna mot externa register, relevanta uppgifter från kunden eller

andra tillförlitliga uppgifter. Om kunden är en juridisk person, ska kundens ägarförhållanden utredas. Register över verkliga huvudmän kommer att upprättas och administreras av Bolagsverket. Från 2017-09-01 kan företag anmäla verklig huvudman. Registret kan bli fullständigt och användbart under 2018. Detta register kan vi nå på ***www.bolagsverket.se*** Om den verkliga huvudmannen inte går att fastställa, ska vi avstå från transaktioner och affärsrelationer.

Information om och uppföljning av affärsförbindelser
Vi ska inhämta information om affärsförbindelsens syfta och art. Informationen ska ligga till grund för en bedömning av
• vilka aktiviteter och transaktioner som kunden kan förväntas vidta inom ramen för affärsförbindelsen,
• kundens riskprofil (enligt B.2 ovan).
Vi ska löpande och vid behov följa upp pågående affärsförbindelser i syfte att säkerställa att kännedom om kunden är aktuell och tillräcklig för att hantera den bedömda risken för penningtvätt eller finansiering av terrorism.
4. Åtgärder som krävs för kundkännedom i det enskilda fallet

Utgångspunkter
Åtgärder för kontroll, bedömning och utredning ska utföras i den omfattning det behövs med hänsyn till kundens riskprofil och övriga omständigheter.

Förenklade åtgärder vid låg risk
Om risken för penningtvätt eller finansiering av terrorism är låg, kan förenklade åtgärder tillämpas för kundkännedom. Dessa kan vara av mer begränsad omfattning och vidtas på annat sätt, jämfört med hög risk. Kundens identitet ska dock alltid fastställas liksom även för företrädare för kund eller huvudman i en juridisk person.

Skärpta åtgärder vid hög risk
Om risken för penningtvätt eller finansiering av terrorism bedöms som hög för en viss kund, ska särskilt omfattande kontroller, bedömningar och utredningar göras. Åtgärderna ska kompletteras med ytterligare åtgärder för att motverka den höga risken. Sådana åtgärder kan avse inhämtande av ytterligare information om kundens affärsverksamhet eller ekonomiska situation och uppgifter varifrån kundens ekonomiska medel kommer. Skärpta åtgärder ska vidtas vid affärsförbindelser eller enstaka transaktioner när kunden är etablerad i ett land utanför EES som av Europeiska kommissionen har identifierats som högrisktredjeland. Vissa undantag finns (SFS 2017:630, 3 kap. 17 §).

Vid korrespondentförbindelser med ett kreditinstitut eller finansiellt institut med hemvist utanför EES ska vi, utöver punkt C. 3. ovan, alltid vidta följande:
• inhämta information om motparten så att v kan förstå verksamheten och bedöma motpartens anseende och tillsynens kvalitet,
• bedöma motpartens kontroller för att förhindra penningtvätt och finansiering av terrorism,
• dokumentera respektive instituts ansvar att vidta kontrollåtgärder,
• inhämta godkännande från behörig beslutsfattare innan en ny korrespondentförbindelse ingås,

• förvissa oss om att motparten har kontrollerat identiteten på kunder som har direkt tillgång till konton hos kreditinstitutet eller det finansiella institutet och fortlöpande följer upp dessa kunder samt på begäran kan lämna relevanta kunduppgifter.

Personer i politiskt utsatt ställning
Om kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning, ska vi utöver åtgärder enligt punkt 3. ovan:
• vidta lämpliga åtgärder för att ta reda på varifrån de tillgångar som hanteras inom affärsförbindelsen eller den enstaka transaktionen kommer,
• tillämpa skärpt fortlöpande uppföljning av affärsförbindelsen och övervaka aktiviteter och transaktioner i förhöjd omfattning, inhämta godkännande från behörig beslutsfattare inför beslut om att ingå eller avbryta en affärsförbindelse.
Ovanstående tillämpas också om kunder är en familjemedlem eller känd medarbetare till en person i politiskt utsatt ställning.

5. Åtgärder för kundkännedom som har utförts av utomstående
Vid identifiering och kontroll av kunden får vi under vissa omständigheter förlita oss på åtgärder som vidtagits av utomstående (SFS 2017:630, 3 kap. 21-24 §§)

6. Kundkontroll i särskilda fall
Regelverk och krav gällande
• *Konton med medel som tillhör någon annan*
• *Livförsäkringar och andra investeringsrelaterade försäkringar*
• *Truster och liknande juridiska konstruktioner utan utpekade förmånstagare*
• *Elektroniska pengar*
framgår av SFS 2017:630, 3 kap. 25-31 §§.

7. Kundavtal Sensor Sverige Select
Till hjälp för kontroll och styrning av kunder i Sensor Sverige Select finns två kundavtal:
• Kundavtal – Privatkund
• Kundavtal – Juridisk person
Kundavtalen ska arkiveras i 10 år. Avtalen ska granskas minst en gång per år, så länge kundförhållandet består, så att förnyad bedömning kan göras om förändringar i risknivå kan ha inträffat med hänsyn till erfarenheter av kunden (se vidare också vid punkt B.2 ovan).

8. Kontroll mot offentliga register
Offentliga register, som nämnts ovan flera gånger, är till vår hjälp vid riskkontroll av kunderna, nya som befintliga. Dessa register hålls aktuella och uppdateras kontinuerligt av ansvariga myndigheter. För att uppnå tillfredsställande kundkännedom innan en affärsförbindelse inleds, ska nya kunder kontrolleras mot sanktionslistorna och verklig huvudman mot registret hos
• www.bolagsverket.se
Dessa kontroller ska omedelbart upprepas om anledning till misstanke uppkommer och minst göras rutinmässigt en gång per år av befintliga kunder. Om gränsöverskridande transaktioner förekommer ska dessa kontrolleras mot sanktionslistorna.

D. ÖVERVAKNING OCH RAPPORTERING

1. Övervakning och rapporteringsskyldighet

Övervakning
Vi ska övervaka pågående affärsförbindelser och bedöma enstaka transaktioner i syfte att upptäcka aktiviteter och transaktioner som
• avviker från vad vi anser som naturligt utifrån vår kännedom om kunden,
• de uppgifter som denne lämnat,
• våra produkter och tjänster och
• sådant som kan vara ett led i penningtvätt eller finansiering av terrorism.
Inriktningen och omfattningen av övervakningen ska bestämmas med hänsyn till risker som identifierats.

Rapporteringsskyldighet
Om vi har skälig grund att misstänka penningtvätt eller finansiering av terrorism eller att egendom härrör från brottslig handling, ska uppgifter om alla omständigheter som kan tyda på detta utan dröjsmål rapporteras till Polismyndigheten.
En sådan rapport ska göras även om transaktioner inte genomförs liksom om det före ingåendet av en affärsförbindelse uppkommer misstanke om att kunden avser att använda våra produkter eller tjänster för penningtvätt eller finansiering av terrorism. Se vidare SFS 2017:630, 4 kap. 3-5 §§.

På begäran av Polismyndighet ska vi utan dröjsmål lämna alla uppgifter som behövs för en utredning om penningtvätt eller finansiering av terrorism.

System för rapportering
Våra system och rutiner ska vara organiserade så att vi snabbt och fullständigt kan lämna uppgifter om våra affärsförbindelser under de senaste fem åren inklusive affärsförbindelsens art. Vi ska säkerställa att våra rutiner medger att uppgifterna kan lämnas genom säkra kanaler på ett säkert sätt och att uppgifterna kan behandlas konfidentiellt.

2. Tystnadplikt
Det är förbjudet att för utomstående röja att en utredning om misstänkt brottslighet eller en anmälan om misstanke har gjorts. Förbudet gäller styrelse, ledning, anställda och uppdragstagare. (SFS 2017:630, 4 kap. 9-10 §§)

3. Dispositionsförbud
Om det finns skäl att misstänka att egendom i form av pengar, fordran eller någon annan rättighet är föremål för penningtvätt eller avsedd för finansiering av terrorism och egendomen finns hos oss, får Polismyndigheten eller Säkerhetspolisen besluta att egendomen eller motsvarande värde inte får flyttas eller disponeras på annat sätt (dispositionsförbud). (SFS 2017:630, 4 kap. 11-13 §§)

E. BEHANDLING AV PERSONUPPGIFTER

1. Tillåtna ändamål för behandling av personuppgifter
Vi får behandla personuppgifter i syfte att kunna fullgöra våra skyldigheter enligt

denna lag, SFS 2017:630.

2. Bevarande av handlingar och uppgifter
Handlingar och uppgifter ska bevaras i fem år om de avser
• åtgärder som vidtagits för kundkännedom,
• transaktioner som genomförts inom ramen för affärsförbindelsen och eller vid enstaka transaktioner som omfattas av kraven på åtgärder för kundkännedom.
Om det är nödvändigt för att förebygga, upptäcka eller utreda penningtvätt eller finansiering av terrorism får handlingar bevaras längre tid än fem år, den sammanlagda tiden får dock inte överstiga tio år.

Om handlingar eller uppgifter tyder på penningtvätt, finansiering av terrorism eller annan brottslig handling, ska vi förvara handlingarna i tio år. Det samma gäller om handlingarna utgjort underlag för rapportering till polismyndighet eller om vi erhåller en uppmaning från myndighet.

Våra rutiner ska vara utformade så att handlingar och uppgifter är enkla att ta fram och identifiera.

3. Tystnadplikt
Det får inte röjas för utomstående att personuppgifter behandlas enlig denna lag.
Se vidare om behandling av personuppgifter SFS 2017:630, 5 kap. 1-11 §§

F. INTERN KONTROLL, ANMÄLNINGAR OM MISSTÄNKTA ÖVERTRÄDELSER

Vår verksamhet ska ha aktuella rutiner och riktlinjer som omfattar intern kontroll, riskbedömning och riskklassificering.

Organisation
1. VD är Centralt funktionsansvarig
Styrelsen har utsett Verkställande Direktören att vara centralt funktionsansvarig. Denne ska utgöra ett centralt stöd i frågor som rör åtgärder mot penningtvätt, finansiering av terrorism och allvarlig brottslighet. VD har därutöver ett övergripande ansvar för kontrollsystem, arbetsrutiner, besluts- och rapporteringsrutiner samt de utbildningsprogram som tillämpas i organisationen. VD ska rapportera alla väsentliga händelser och bedömningar gällande penningtvätt, finansiering av terrorism och annan brottslighet till styrelsen. I förekommande fall är det VD som beslutar om uppgifter ska lämnas till polismyndighet (SFS 2017:630, 4 kap. 3 §)

2. Instruktioner och regelverk
Bolagets Compliance Officer är ansvarig för att initiera uppdateringar, kompletteringar, anpassningar och ändringar i Bolagets instruktioner så att dessa är aktuella och anpassade till lagstiftning, föreskrifter och allmänna råd. Styrelsen beslutar om och fastställer de instruktioner som ska gälla för verksamheten. Compliance Officer ska löpande granska och bedöma regelefterlevnaden.

3. Personalutbildning
Compliance Officer ansvarar för att alla anställda får information om nya lagar

och regler som rör penningtvätt, finansiering av terrorism och allvarlig brottslighet. Compliance Officer ska också kontrollera att alla anställda årligen genomgår kunskapsuppdatering och kunskapstest samt innehar aktiv licens från SwedSec. Compliance är ansvarig för att initiera intern utbildning minst en gång per år. (Se vidare ovan, punkt B. 3.)

4. Intern revisor (oberoende granskningsfunktion)
Bolagets interna revisor ska granska och regelbundet utvärdera att intern kontroll, riktlinjer, kontroller, förfaranden, Ramverk och rutiner, som syftar till att uppfylla kraven i SFS 2017:630, efterlevs effektivt och fullständigt.

5. Identitetskontroll
Identitetskontroll ska utföras vid den tidpunkt en kund inleder en affärsförbindelse med bolaget. Alla anställda med uppgifter som inkluderar kundkontakter är ansvariga för att identitetskontroller genomförs innan affärsförbindelse inleds.

6. Kontroll av kundärenden och transaktioner
Alla anställda med relevanta arbetsuppgifter är ansvariga för att fortlöpande kontrollera och analysera affärsförbindelser och transaktioner med syfte att upptäcka penningtvätt, finansiering av terrorism och annan brottslighet eller företeelser som kan utgöra ett led i sådan verksamhet.

7. Rapportering, anmälningar om misstänkta överträdelser
Alla anställda har ansvar för att utan dröjsmål rapportera misstänka ärenden eller transaktioner till VD som är centralt funktionsansvarige och som därefter har att fatta beslut om uppgifter ska lämnas till polismyndighet.

Rutiner för modellriskhantering
Våra rutiner för modellriskhantering, bakomliggande teori och antaganden som har lett fram till bedömningen av riskerna för penningtvätt, finansiering av terrorism eller annan brottslighet (FFFS 2017:11 6 kap, 14-28 §§) ska dokumenteras på bilagor till denna instruktion.

Dessa kan dokumenteras som en sårbarhetsanalys och en riskanalys. Sårbarhetsanalysen kan beakta produkternas eller tjänsternas art och möjliga tillvägagångssätt för dessa att utnyttjas för brottslighet medan riskanalysen kan peka på vilka riskerna är att vår verksamhet blir utnyttjad och hur stora dessa bedöms vara (låg, medel eller förhöjd).

Visselblåsningssystemets egenskaper
Vårt rapporteringssystem ska skydda vår information från åtkomst av obehöriga, förhindra information från att förvanskas eller förstöras och säkerställa att informationen är tillgänglig när den behövs. Vi ska tillse att uppgifter kan lämnas anonymt.

G. RAPPORTERING AV UPPGIFTER TILL FINANSINSPEKTIONEN
Finansinspektionen har möjlighet att begära in uppgifter när som helst för att myndigheten ska kunna bedöma den risk som kan förknippas med vår verksamhet och vårt företag vad gäller penningtvätt, finansiering av terrorism och annan allvarlig brottslighet.

Dessutom ska vi rapportera periodiskt med början 2018. Uppgifterna ska lämnas per balansdagen den 31 december. Den första rapporteringen ska lämnas senast den 31 mars 2018. Därefter ska rapporteringen ske årligen under första kvartalet.

H. INGRIPANDE AV FINANSINSPEKTIONEN

Ingripande mot fysisk person kan ske genom beslut om sanktionsavgift om maximalt 5 miljoner euro eller två gånger den vinst som den fysiska personen gjort till följd av regelöverträdelsen eller beslut om att personen i fråga under en viss tid, lägst tre och högst tio år, inte får ingå i verksamhetsutövares styrelse eller vara dess VD, eller ersättare för någon av dem.

Sanktionslistor:
Information om sanktioner finns här: www.regeringen.se/sanktioner
Register över verkliga huvudmän finns här: www.bolagsverket.se
Anmälan om misstänkt penningtvätt m.m. ska ske till fipo@polisen.se