



Tillsynsärende - auktoriserade revisorn A-son

Beslut: Revisorsinspektionen ger auktoriserade revisorn A-son en varning.

1 Inledning

Revisorsinspektionen har underrättats om att auktoriserade revisorn A-son har underkänts i FAR:s kvalitetskontroll och har därför öppnat detta ärende. I ärendet behandlas frågan om A-son, i sin egenskap av ställföreträdare för – och ensam styrelseledamot i – det revisionsföretag i vilket han bedrev sin verksamhet, har uppfyllt sina skyldigheter enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen).

Revisionsföretaget registrerades som revisionsbolag under utredningens gång, den 1 mars 2025, och står sedan dess under Revisorsinspektionens direkta tillsyn. Detta ärende behandlar emellertid de skyldigheter enligt penningtvättslagen som revisionsföretaget, och A-son som dess ställföreträdare, hade vid tidpunkten för kvalitetskontrollen hösten 2023.

2 Penningtvättsregelverket

Penningtvättslagen gäller för fysiska och juridiska personer som driver vissa i lagen uppräknade verksamheter, däribland sådan verksamhet som en auktoriserad eller godkänd revisor eller ett registrerat revisionsbolag bedriver, se 1 kap. 2 § första stycket 18. Det

innebär att såväl enskilda revisorer som juridiska personer som bedriver revisionsverksamhet är skyldiga att följa lagens bestämmelser och de föreskrifter som har meddelats på området. Om en verksamhetsutövare är anställd hos en juridisk person, är det enligt 2 kap. 16 § penningtvättslagen den juridiska personen som ansvarar för att kraven i penningtvättslagen avseende allmän riskbedömning samt rutiner och riktlinjer uppfylls. I den utsträckning verksamheten bedrivs i en juridisk person har den juridiska personens ställföreträdare som utgångspunkt ett personligt ansvar för att verksamheten är inrättad så att penningtvättsregelverket kan följas.

Allmän riskbedömning

En verksamhetsutövare ska enligt 2 kap. 1 § penningtvättslagen göra en bedömning av hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism och hur stor risken är för att detta sker (allmän riskbedömning). Vid den allmänna riskbedömningen ska det särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns samt vilka geografiska riskfaktorer som föreligger. Enligt 3 § Revisorsinspektionens föreskrifter (RIFS 2021:1) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna) ska den allmänna riskbedömningen innehålla en identifikation av verksamhetens tjänster och produkter, en beskrivning av de hot som är relevanta för tjänsterna och produkterna, en beskrivning av de egenskaper som kan göra revisionsföretagets verksamhet eller tjänster och produkter sårbara för försök till att utnyttjas för penningtvätt eller finansiering av terrorism och en värdering av riskerna som är förenade med de beskrivna hoten och sårbarheterna. Enligt 2 kap. 2 § penningtvättslagen ska riskbedömningen utformas så att den kan ligga till grund för verksamhetsutövarens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism. Den allmänna riskbedömningen ska dokumenteras och hållas uppdaterad. I 4 § penningtvättsföreskrifterna anges att revisionsföretaget, på grundval av en riskbedömning, men minst en gång per år, ska utvärdera och vid behov uppdatera den allmänna riskbedömningen. Datum för utvärderingen och eventuell uppdatering ska dokumenteras.

Rutiner och riktlinjer

En verksamhetsutövare ska vidare, enligt 2 kap. 8 § penningtvättslagen, ha dokumenterade rutiner och riktlinjer avseende sina åtgärder för kundkännedom,

övervakning och rapportering samt för behandling av personuppgifter. Dessa ska fortlöpande anpassas efter nya och förändrade risker för penningtvätt och finansiering av terrorism. I 4 § penningtvättsföreskrifterna anges att revisionsföretaget, på grundval av en riskbedömning, men minst en gång per år, ska utvärdera och vid behov uppdatera sina rutiner och riktlinjer. Datum för utvärderingen och eventuell uppdatering ska dokumenteras.

Kundens riskprofil

En verksamhetsutövare ska enligt 2 kap. 3 § penningtvättslagen bedöma den risk för penningtvätt och finansiering av terrorism som kan förknippas med kundrelationen (kundens riskprofil). Riskprofilen ska bestämmas med utgångspunkt i den allmänna riskbedömningen och verksamhetsutövarens kännedom om kunden. Lagen förutsätter att verksamhetsutövaren vidtar åtgärder för att skaffa sig kundkännedom (se närmare 3 kap. 7–12 §§). Åtgärderna för kundkännedom ska, enligt 3 kap. 14 §, ha den omfattning som behövs med hänsyn till kundens riskprofil och övriga omständigheter.

Uppföljning av affärsförbindelsen

Enligt 3 kap. 13 § penningtvättslagen ska en verksamhetsutövare löpande och vid behov följa upp pågående affärsförbindelser i syfte att säkerställa att kännedomen om kunden enligt 3 kap. 7, 8 och 10–12 §§ penningtvättslagen är aktuell och tillräcklig för att hantera den bedömda risken för penningtvätt eller finansiering av terrorism.

Övervakning

Enligt 4 kap. 1 § penningtvättslagen ska en verksamhetsutövare övervaka pågående affärsförbindelser och bedöma enstaka transaktioner. Inriktningen och omfattningen av övervakningen ska bestämmas med beaktande av de risker som har identifierats i den allmänna riskbedömningen, den risk för penningtvätt och finansiering av terrorism som kan förknippas med kundrelationen och annan tillgänglig information om tillvägagångssätt för penningtvätt eller finansiering av terrorism.

3 Allmän riskbedömning enligt penningtvättslagen

3.1 Innehållet i den allmänna riskbedömningen

Revisionsföretagets allmänna riskbedömning fanns vid tidpunkten för FAR:s kvalitetskontroll i ett dokument; *Allmän riskbedömning, byråns rutiner och riktlinjer avseende Penningtvättslagen 2022-10-01*. I avsnitt 1, *Inledning*, anges att revisionsföretaget startades i februari 2021 och redogörs för dess ägarförhållanden. Här anges också följande.

Bolaget består av två medarbetare och bedriver revisionsverksamhet med ca: 150 kunder på den lokala marknaden i Östergötland samt i Stockholmsregionen. Utbildning kring penningtvättsregelverket sker regelbundet för oss båda.

I avsnitt 2, *Allmän riskbedömning*, anges följande.

Bolaget bedömer risken som normal för att våra tjänster ska kunna utnyttjas för penningtvätt eller finansiering av terrorism.

Vidare anges att företagets tjänsteområde är lagstadgad revision och övriga revisorsyttranden. Det framgår ingenting i övrigt om vad detta tjänsteområde innebär eller vilka eventuella risker som är förknippade med det. Under detta anges följande.

Risken bedöms som låg pga att vi i revisionen granskar transaktioner som redan skett. Revision skulle dock kunna utnyttjas med syftet att ge en ökad trovärdighet i rapportering vilket ökar risknivån.

Härefter anges återigen att revisionsföretaget har cirka 150 kunder, att dessa uteslutande är små aktiebolag baserade i Östergötland och Stockholmsregionen och att kunderna har verksamhet i "olika branscher". Det anges vidare att revisionsföretaget träffar alla kunder regelbundet, att kunderna är välkända och att en bedömning av varje kunds riskprofil sker åtminstone årligen. Det anges dessutom att ett par av kunderna bedriver restaurangverksamhet där det förekommer kontanter, att ingen av kunderna har verksamhet utanför Sverige och att kunderna har enkla ägarstrukturer.

"Sammantaget utgår vi från normal risk i bedömning av kunder."

Avsnitt 3, *Rutiner och riktlinjer enligt penningtvättslagen*, består av följande text.

En kvalitetspolicy (2022:1) har tagits fram innehållandes rutiner och riktlinjer för:

- Acceptans och behållande av kunder
- Meningsskiljaktigheter
- Vidareutbildning

I dokumentets sista avsnitt, 4 *Sammanfattning och slutsats*, anges att bolaget är litet med relativt få kunder, att kunderna är välkända och små med verksamhet på den lokala

svenska marknaden, att A-son är auktoriserad revisor och medlem i FAR, att de båda medarbetarna årligen utbildar sig på området och att kunskapen om penningtvättslagen därför är god. Slutligen anges att den risk som finns för att utnyttja revisionsföretagets tjänster som ett led i eller för att dölja penningtvätt bedöms som normal.

3.2 Revisorns uppgifter

A-son har uppgett följande.

Revisionsföretaget startade sin verksamhet i februari 2021. Initialt var verksamheten liten med cirka 20 kunder och han var ensamt ansvarig för samtliga kundutvärderingar, för kundkännedomsgångar och för övervakning av penningtvättstransaktioner. Han tog skyndsamt, den 19 februari 2021, fram en allmän riskbedömning som därefter har uppdaterats årligen.

I 2 kap. 2 § penningtvättslagen anges att den allmänna riskbedömningen kan anpassas till företagets storlek och komplexitet. Med den utveckling som har skett i praxis sedan år 2022 och tidpunkten för den allmänna riskbedömning som fanns vid FAR:s kvalitetskontroll, förstår han att det framstår som att riskbedömningen inte var särskilt utförlig. Revisorsinspektionens tematillsyn visade också att många revisionsföretag ansåg att revisionstjänsten utgjorde låg risk, men att de bort välja normal risk i stället. Han anser att den allmänna riskbedömningen är viktig men att det som är än mer viktigt är vad han faktiskt har utfört för penningtvättsåtgärder.

Han har bedömt hur produkter och tjänster kan utnyttjas för penningtvätt genom att i riskbedömningen ange att tjänsterna endast är revision och övriga revisorsyttranden samt att risken är låg, eftersom företaget granskar transaktioner som redan skett. Revision skulle kunna utnyttjas med syftet att ge en ökad trovärdighet i rapportering vilket ökar risknivån. Det var denna risk för hur revisionsföretagets tjänster skulle kunna utnyttjas för penningtvätt som han vid tillfället hade identifierat. FAR:s mall saknar exempel på vad dessa hot kan bestå av. Han hänvisar i övrigt till revisionsföretagets ringa omfattning.

I samtliga versioner av revisionsföretagets allmänna riskbedömningar har det angetts att risken för att dess tjänster ska utnyttjas för penningtvätt eller finansiering av terrorism är lägre, eftersom medarbetarna i revisionen granskar transaktioner som redan har skett. I FAR:s mall för allmän riskbedömning anges att risken för tjänsten revision är lägre än normal. I övrigt saknas uppgifter om vilka egenskaper som kan göra verksamheten eller

produkter sårbara för försök till att utnyttjas för penningtvätt. Han kan dock konstatera att även FAR:s mall för allmän riskbedömning saknar exempel på vad dessa egenskaper kan bestå av.

Ett hot som är relevant för att revisionstjänsten ska kunna utnyttjas för penningtvätt är att kunderna har komplexa strukturer eller har verksamhet utomlands. Genom det anges att revisionsföretaget har kunder med enkla ägarstrukturer och med verksamhet i Sverige anser han att det är underförstått att detta bidrar till att den sammanvägda risken i den allmänna riskbedömningen kan anses vara normal.

När det gäller bedömningen av revisionsföretagets kunder måste det beaktas att revisionsföretaget var litet, med enbart 150 kunder, och hade exakt kontroll över sina kunder. Det har därför inte ansetts nödvändigt att ta in statistik över vilka kunderna är, eftersom den ende som vid tidpunkten var huvudansvarig för kundkännedomsåtgärderna, kundprofilering, övervakning och andra penningtvätsrelaterade åtgärder var han själv. Kunder med restaurangverksamhet anser han innebär en högre risk för penningtvätt eftersom det är en bransch med historiskt större förekomst av fusk och penningtvätt. Det är dock endast mindre än tio procent av revisionsföretagets kunder som är verksamma i branscher med högre risk. Dessa har också vid riskprofilering och kundutvärdering bedömts ha högre risk för att omfattas av penningtvättstransaktioner. Bedömningen att det enbart rör sig om svenska företag görs genom att ägandet i respektive kundföretag kontrolleras. I den kundspecifika riskanalysen dokumenteras även kundens etableringsort. Att kunderna är välkända och med verksamhet på den lokala svenska marknaden har han bedömt minskar risken för penningtvätt eller finansiering av terrorism.

Han anser inte att Östergötland och Stockholmsområdet är ett stort geografiskt område utan snarare ett väldigt vanligt upptagningsområde för ett revisionsföretag som hans, med kontor i Östergötland. Vad han bedömer som avgörande är närvaro och kundkännedomen – inte var kunderna har sin postlåda. Med dagens digitala teknik kan han dessutom vara betydligt mer närvarande med sina kunder än tidigare. Revisionsföretaget föredrar fysiska möten, särskilt med nya kunder, men digitala möten är ett bra komplement för att upprätthålla kundkännedom. Han träffar huvuddelen av sina kunder genom fysiska möten, vilket bidrar till en lägre sammanvägd risk i utvärderingarna.

Sammanfattningsvis har revisionsföretaget sedan det startades haft en allmän riskbedömning. Enligt 2 kap. 2 § penningtvättslagen ska omfattningen av den allmänna

riskbedömningen bestämmas med hänsyn till verksamhetsutövarens storlek, art och de risker för penningtvätt eller finansiering av terrorism som kan antas föreligga. Att revisionsföretaget har haft låg omsättning, få anställda, få tjänster och okomplex verksamhet indikerar minskade krav på omfattningen av den allmänna riskbedömningen. I ljuset av utvecklad av praxis och Revisorsinspektionens frågor i ärendet förstår han att den allmänna riskbedömningen kan utvecklas och göras mer omfattande. Detta har han tagit till sig av och har implementerat framåt.

3.3 Revisorsinspektionens bedömning

Revisorsinspektionen gör följande bedömning.

I avsnitt 2 har redogjorts för de krav som ställs på en revisors allmänna riskbedömning. Revisorsinspektionen tar i detta beslut ställning till om den allmänna riskbedömning som A-son upprättade i oktober 2022 uppfyller dessa krav.

Revisorsinspektionen konstaterar inledningsvis att vid den tidpunkten hade inspektionens penningtvättsföreskrifter gällt i nio månader. Verksamheten i det revisionsföretag som A-son drev hade pågått i ett år och åtta månader och företaget hade 150 kunder. Det var alltså inte fråga om någon helt nystartad eller begränsad verksamhet och det fanns inte anledning att ställa lägre krav på verksamheten än på annan revisionsverksamhet.

Revisionsföretagets allmänna riskbedömning innehåller inte någon bedömning av hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism, fränsett ett uttalande om att revisionen skulle kunna utnyttjas med syftet att ge ökad trovärdighet i rapportering. Det sistnämnda uttalandet kan inte anses som en tillräcklig analys av de förhållanden som ska behandlas i en allmän riskbedömning.

Den allmänna riskbedömningen innehåller inte heller någon beskrivning av de omständigheter som kan göra revisionsföretagets verksamhet eller tjänster sårbara för försök till utnyttjande för penningtvätt eller finansiering av terrorism. En sårbarhet är en inre egenskap hos revisionsföretaget som kan göra verksamheten sårbar för hot. Det kan exempelvis ha att göra med egenskaper hos personal, system eller placering. Att tjänsten revision innebär att transaktioner granskas i efterhand – saknar härvid betydelse, eftersom det inte utgör en utvärdering eller bedömning av revisionsföretagets specifika sårbarheter.

Revisorsinspektionen anser också att den allmänna riskbedömningen i detta fall saknar en tillfredsställande värdering av de risker som är förenade med beskrivna hot och sårbarheter. I det aktuella dokumentet finns i och för sig uppgifter om att revisionsföretagets kunder har enkla ägarstrukturer och verksamhet i Sverige, dvs. omständigheter som skulle kunna anses vara risksänkande. Men dessa uppgifter utgör inte en värdering av riskerna.

I den allmänna riskbedömningen har också antecknats att några kunder driver restaurangverksamhet. Det finns också uppgifter om vilka geografiska områden som revisionsföretagets verksamhet avser. Det framgår dock inte hur dessa omständigheter har påverkat riskbedömningen. I övrigt saknas det uppgifter om sådana riskfaktorer som enligt 2 kap. 1 § penningtvättslagen särskilt ska beaktas vid riskbedömningen.

Sammantaget innehåller revisionsföretagets allmänna riskbedömning flera brister. Genom att inte upprätta en godtagbar allmän riskbedömning har A-son brustit i sina skyldigheter enligt penningtvättslagen.

4 Rutiner och riktlinjer enligt penningtvättslagen

4.1 Innehållet i rutiner och riktlinjer

I revisionsföretagets allmänna riskbedömning, avsnitt 3, *Rutiner och riktlinjer enligt penningtvättslagen*, anges följande.

En kvalitetspolicy (2022:1) har tagits fram innehållandes rutiner och riktlinjer för:

- Acceptans och behållande av kunder
- Meningsskiljaktigheter
- Vidareutbildning

A-son har därutöver gett in ett dokument betecknat *Revisionsmanual*. I dokumentet anges i avsnitt 2.1.1 *Grundakt* att bl.a. identitetshandlingar ska hållas uppdaterade och finnas tillgängliga över tid. Vidare anges i avsnitt 5, *Utvärdering av uppdrag, kundkännedomsgåtgärder samt kundutvärdering enligt PTL*, följande.

Revisionsföretaget följer flödet i revisionsverktyget [revisionsprogram] som innebär att varje uppdrag ska utvärderas årligen i samband med att uppdraget uppstartas. Detsamma gäller vid väsentliga förändringar i uppdraget. Utvärderingen ska inkluderas såväl företagets förmåga och tid att utföra uppdragen såväl som kundkännedomsgåtgärder inklusive att upprätta en kundprofil enligt penningtvättslagen som utförs i programvaran [programverktyget].

A-son har här till hänvisat till ett programverktyg och har gett in utdrag ur detta. Programverktyget innehåller dels en systembeskrivning med ett antal kontrollfrågor, dels en checklista med rubriken *Risikanalys juridisk person* med förfyllda frågor och påståenden att besvara. Vidare har han hänvisat till revisionsprogrammet där rutiner enligt penningtvättslagen uppges finnas. Han har också gett in en utskrift från programmet där det under rubriken *Penningtvätt* finns ett antal förfyllda påståenden att ta ställning till. Slutligen har han gett in två checklistor från revisionsprogrammet rubricerade *Utvärdering av nytt uppdrag* samt *Utvärdering av befintligt uppdrag*. Dessa innehåller förfyllda frågor och påståenden där man kan kryssa i rutor under ”ja”, ”nej” eller ”e/t”. Vid ja-svar finns utrymme för kommentarer. Rubrikerna är *Oberoende, Ägare/ledning, Riskfylld bransch, Företag inom kontantbranschen* (i relation till bokföringsskyldigheten), *Fortsatt drift, Betalningsförmåga, Byråns kompetens och tid, Penningtvättslagen* och slutligen *Övrigt*. Under rubriken *Penningtvätt* ställs tre generella frågor; om det finns indikationer på penningtvätt i uppdraget, om verklig huvudman är registrerad hos Bolagsverket och om kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning.

A-son har också gett in dokumentet *Kvalitetspolicy – Revisions- & redovisningsföretagen [revisionsföretaget], [A-företaget] och [B-företaget]*. I avsnitt 6 i detta dokument, *Acceptera och behålla kunder och uppdrag*, finns en hänvisning till penningtvättslagen och FAR:s uttalanden i etikfrågor (EtikU) 11 *Medlemmarnas tillämpning av lagen om åtgärder mot penningtvätt och finansiering av terrorism*. I avsnitt 6.1, *Acceptera en ny kund*, anges att medarbetare ska inhämta grundinformation om kunden i form av exempelvis kreditupplysning, senaste årsredovisning och information från Bolagsverket om eventuell verklig huvudman. Vidare anges att vid acceptans av ny kund ska beaktas kundens bransch, egenskaper, kundkännedomsinformation enligt penningtvättslagen och EtikU 11 samt huruvida risken för penningtvätt bedöms som hög. I näst sista stycket i avsnitt 6.1 anges följande.

I samband med accept av ett nytt uppdrag ska en kundutvärdering dokumenteras i revisionssystemet. I kundutvärderingen ska bland annat oberoende, väsentliga slutsatser och beslut dokumenteras. Dokumentation ska även innehålla information om riskbedömning avseende risk för penningtvätt och finansiering av terrorism samt handlingar och uppgifter som avser åtgärder för att uppnå kundkännedom. Kundutvärderingen ska godkännas av företagsledningen.

Vidare anges i avsnitt 6.1.1, *Åtgärder mot penningtvätt*, följande.

[Revisionsföretaget, A-företaget och B-företaget] får aldrig acceptera eller behålla en kundrelation om det finns misstanke om att [Revisionsföretaget, A-företaget och B-företaget] kan komma att användas för penningtvätt eller finansiering av terrorism. [Revisionsföretaget, A-företaget och B-företaget] har en dokumenterad

allmän riskbedömning av hur företagets tjänster kan utnyttjas för penningtvätt eller finansiering av terrorism, vilken ska beaktas i samband med processen för att acceptera en ny kundrelation eller ett nytt uppdrag, se avsnitt 6.1 ovan. [Revisionsföretaget, A-företaget och B-företaget] accepterar inga uppdrag där risken för penningtvätt eller finansiering av terrorism som kan förknippas med kunden bedöms vara hög.

Alla medarbetare ska vara uppmärksamma under pågående kundrelationer och uppdrag på omständigheter såsom förändrade ägarförhållanden, vissa transaktioner eller liknande som kan indikera att det finns en risk för att [Revisionsföretaget, A-företaget och B-företaget] kan komma att användas för penningtvätt eller finansiering av terrorism.

Alla medarbetare ska, vid skälig grund för misstanke om att [Revisionsföretaget, A-företaget och B-företaget] kan komma att utnyttjas för penningtvätt eller finansiering av terrorism, omgående rapportera detta till respektive kvalitetsansvarig eller företagsledningen. Företagsledningen ska utan onödigt dröjsmål rapportera omständigheterna som ligger till grund för misstanken till Finanspolisen utan att röja att så kommer att ske för kunden (meddelarförbudet).

Revisorsinspektionen har inte kunnat se att revisionsmanualen eller kvalitetspolicyn innehåller några anpassade rutiner om hur kundkännedom ska inhämtas.

I avsnitt 6.1.1 i kvalitetspolicyn (se ovan) anges att medarbetare under pågående kundrelationer och uppdrag ska vara uppmärksamma på förändrade ägarförhållanden, ”vissa transaktioner” och liknande. Dokumenten anger inte hur medarbetare ska agera för att genomföra sin övervakning.

Kvalitetspolicyns avsnitt 5.6, *Tystnadsplikten*, behandlar tystnadsplikt samt anger att kundinformation och eventuella personuppgifter som inhämtas i ett uppdrag ska användas endast för det syfte som de samlats in för och att de ska hanteras enligt GDPR. Alla medarbetare förväntas enligt texten känna till och följa revisionsföretagets riktlinjer rörande tystnadsplikt.

I kvalitetspolicyns avsnitt 7.5, *Åtkomst till och arkivering av uppdragsdokumentation*, anges följande.

Uppdragsdokumentation ska sparas på [revisionsföretaget, A-företaget och B-företagets] programvara [revisionsprogrammet] för revisionsuppdrag, [X-programmet] för bokslutsuppdrag och på servern för övriga uppdrag. När det gäller räkenskapsinformation, är det kunden som ansvarar för att arkivera materialet om inget annat är avtalat. Räkenskapsinformation som behöver sparas hos [revisionsföretaget, A-företaget och B-företaget] ska även uppfylla bokföringslagens (1999:1078) krav på att räkenskapsinformationen ska sparas på ett betryggande sätt.

Uppdragsdokumentationen ska arkiveras i tio år och på ett sådant sätt att åtkomst enligt 7 kap. 1 § bokföringslagen säkerställs.

Alla arbetspapper, rapporter och andra dokument som har upprättats av [revisionsföretaget, A-företaget och B-företaget], inklusive dokumentation upprättad av kunden, är konfidentiella och ska skyddas från obehörig åtkomst.

Uppdragsansvarig eller företagsledningen måste godkänna alla externa förfrågningar att granska arbetspapper och dokumenten får inte lämnas ut förrän detta medgivande har inhämtats.

Arbetspapper ska inte göras tillgängliga för externa parter såvida inte avtalet eller tillämpliga lagar och regler medger det.

[Revisionsföretaget, A-företaget och B-företaget] ska informera kunden innan arbetspapper lämnas ut enligt lagar och regler (till exempel vid konkurs). Ett skriftligt medgivande måste inhämtas från kunden vid övriga frågor som inte är reglerade i lagstiftning (till exempel potentiell köpare, investerare, långgivare). Juridisk expertis ska rådfrågas om kunden inte godkänner nödvändiga utlämnanden av information.

Ett tillgängligt, permanent register med all uppdragsdokumentation lagrad utanför [revisionsföretaget, A-företaget och B-företaget] ska upprätthållas och i arkivet ska det finnas lämplig märkning för att lätt identifiera och ta fram information. Den som ansvarar för kontoadministrationen ska godkänna gallring av dokumentation.

4.2 Revisorns uppgifter

A-son har uppgett följande.

Revisionsföretaget har arbetat enligt penningtvättslagens riktlinjer sedan bolaget startades och det är inte bara kvalitetspolicyn som utgör företagets rutiner och riktlinjer på penningtvättsområdet. I samband med att revisionsföretaget började använda programverktyget införde han i revisionsmanualen en beskrivning av sin rutin för kundkännedomsgåtgärder. Han har använt sig av FAR:s mall sedan år 2023.

Bolagets storlek, antal kunder, geografisk spridning och risk i de tjänster som erbjuds har beskrivits i de årligen uppdaterade allmänna riskbedömningarna. Han har sedan tagit fram hela kvalitetspolicyn samt rutiner och riktlinjer utifrån förutsättningarna i revisionsföretaget. Den största risken som han har identifierat är att revision skulle kunna utnyttjas i syfte att ge en ökad trovärdighet i rapportering. Genom att genomföra en revision i enlighet med kvalitetspolicyn, revisionsmanualen, programverktyget samt penningtvättsåtgärderna i revisionsprogrammet kan riktigheten i rapporterna säkerställas. Enligt

revisionsmanualen ska, vid den minst årliga kundkännedomprocessen, hänsyn tas till verksamhetens storlek, art och riskerna för penningtvätt och finansiering av terrorism.

Den allmänna riskbedömningen hänvisar i fråga om rutiner och riktlinjer till kvalitetspolicyn. Kvalitetspolicyn hänvisar i sin tur till revisionsmanualen som hänvisar till systemen i revisionsprogrammet och programverktyget. Kvalitetspolicyn, som följer FAR:s mall, innehåller till viss del riktlinjer för hantering av penningtvätt.

Rutiner och riktlinjer avseende åtgärder för kundkännedom

I kvalitetspolicyn avsnitt 6.1, som hänvisar till revisionsprogrammets kundkännedomblankett, anges bl.a. följande.

I samband med accept av ett nytt uppdrag ska en kundutvärdering dokumenteras i revisionssystemet.

Den blanketten hänvisar i sin tur till kundkännedomprocessen som finns i programverktyget. Samma rutin gäller för befintliga uppdrag eller vid en väsentlig förändring i uppdraget. Den generella skrivningen att kundkännedom ska utföras i enlighet med programmet dokument måste tillsammans med revisionsprogrammets blankett anses som väldigt anpassade riktlinjer för hur en kundkännedomprocess ska gå till på revisionsföretaget. I revisionshandboken hänvisas vidare till revisionsverktygets process och här anges även att kundkännedomsåtgärder ska utföras, inklusive upprättandet av en kundprofil. Han anser att en riktlinje är tillräcklig genom att den hänvisar till revisionsprogrammets kundkännedomsflöde, se bilagda checklistor från revisionsprogrammet samt kundkännedomprocessen i den särskilt framtagna checklistan (*Risikanalys juridisk person*) i programverktyget.

Riktlinjerna i kvalitetspolicyn stadgar att revisionsföretagets anställda ska utföra kundutvärderingar och kundkännedomsåtgärder och att övervakning ska ske. Dokumentet indikerar även att man ska utföra riskprofiler eller i vart fall en bedömning av risken på kundnivå. Även revisionsmanualen innehåller riktlinjer om att varje uppdrag vid varje uppstart ska utvärderas och att det i den utvärderingen ingår att utföra kundkännedomsåtgärder som inkluderar att upprätta en kundprofil. Revisionsföretaget använder programverktyget för sina kundkännedomsåtgärder och riskprofiler. Programmet screenar även kunderna mot registren för person i politiskt utsatt ställning och verkliga huvudmän, så att han kan kontrollera kunderna mot detta. Företaget får

också automatiska utskick om det sker förändringar avseende person i politiskt utsatt ställning eller verkliga huvudmän på hela kundstocken, så att han kan uppdatera sin kundkännedom direkt.

I kapitel 6.1 i kvalitetspolicyn anges följande.

I samband med accept av ett nytt uppdrag ska en kundutvärdering dokumenteras i revisionssystemet. I kundutvärderingen ska bland annat oberoende, väsentliga slutsatser och beslut dokumenteras. Dokumentationen ska även innehålla information om riskbedömning avseende risk för penningtvätt och finansiering av terrorism samt handlingar och uppgifter som avser åtgärder för att uppnå kundkännedom. Kundutvärderingen ska godkännas av företagsledningen.

Hela kapitlet om kundutvärdering måste läsas för att man ska få en korrekt bild. Vidare finns i avsnitt 5 i revisionsmanualen, *Utvärdering av uppdrag, kundkännedomsåtgärder samt kundutvärdering enligt penningtvättslagen*, en beskrivning av hur kundkännedomsåtgärder ska utföras i samband med utvärdering av såväl nya som befintliga uppdrag.

I kvalitetspolicyns beskrivning av vad byrån ska göra vid en kundutvärdering finns även en uppräkningslista av vilken information som normalt ska inhämtas.

Han anser att revisionsföretagets riktlinjer är tillräckliga i relation till verksamhetens omfattning.

Rutiner och riktlinjer avseende övervakning

Av revisionsmanualen följer att man ska göra en riskbedömning enligt International Standards on Auditing (ISA). Han anser att en god kundkännedom inklusive kännedom om kundernas verksamhet och en riskbedömning utifrån ISA 315 *Identifiera och bedöma riskerna för väsentliga felaktigheter* innebär att företaget i sin ordinarie revisionsprocess beaktar penningtvättsförhållanden. Att övervaka penningtvättstransaktioner är alltså en del av deras ordinarie revisionsmetodik.

Revisionsprogrammet används som granskningsprogram vid de revisioner som revisionsföretaget utför. Det blir då även en naturlig del av revisionsföretagets kundkännedomsprocess, utvärdering av uppdrag, riskbedömning samt övervakning av eventuella penningtvättstransaktioner. Om han har gjort en bra riskbedömning av kunden och har en god kundkännedom om kunden och dess verksamhet, fångas de risker för väsentliga felaktigheter som kan förekomma upp. För vissa kunder är sannolikheten för att det

förekommer penningtvätt större och där behöver mer övervakning utföras för att uppmärksamma transaktioner eller förhållanden som kan förknippas med penningtvätt. Detta är en naturlig del av revisionsföretagets process och därför används revisionsverktyget även för dokumentation av övervakningen. Penningtvättsrutiner vävs in i revisionsprocessen där revisionsprogrammet blir en naturlig del av arbetssättet.

Rutiner och riktlinjer avseende behandling av personuppgifter enligt penningtvättslagen

Kvalitetspolicyn innehåller riktlinjer avseende kundinformation och eventuella personuppgifter. Riktlinjerna hänvisar inte endast till reglerna i 5 kap. penningtvättslagen, eftersom det inte är särskilt praktiskt att i ett revisionsföretag föra olika register med kunder eller ha olika riktlinjer för efterlevnad av reglerna om personuppgifter.

Den enda punkt som han kan notera där kraven är olika i 5 kap. penningtvättslagen mot de ”allmänna regler” som finns återgivna i kvalitetspolicyn, rör penningtvättslagens krav om arkivering av personuppgifter. Hans slutsats är därför att om revisionsföretaget följer de allmänna riktlinjerna i kvalitetspolicyn följer de också reglerna om personuppgifter enligt 5 kap. penningtvättslagen. Detta innebär att det finns riktlinjer som berör behandling av personuppgifter enligt 5 kap. penningtvättslagen. Om de allmänna riktlinjerna som gäller byråns hela verksamhet efterlevs, följer medarbetarna också penningtvättslagen i detta avseende.

Nedan återges de riktlinjer som finns i kvalitetspolicyn.

Avsnitt 5 Relevanta yrkesetiska krav.

Alla medarbetare på [revisionsföretaget, A-företaget och B-företaget] samt externa tjänsteleverantörer som är föremål för relevanta yrkesetiska krav som gäller [revisionsföretaget, A-företaget och B-företaget], är skyldiga att följa fastställda riktlinjer och allmänna relevanta yrkesetiska krav, inklusive oberoende-krav:

[...]

- skydda och iaktta tystnadsplikt avseende [revisionsföretaget, A-företaget och B-företagets] och kunders data, affärs- och kundinformation samt personuppgifter.

[...]

Av betydelse i detta sammanhang är avsnitt 5.6 *Tystnadsplikten*, i kvalitetspolicyn där inhämtande av personuppgifter regleras. I avsnittet anges följande.

Alla medarbetare ska skydda och iaktta tystnadsplikt för all kundinformation som måste vara konfidentiell och skyddad enligt tillämpliga lagar, föreskrifter, myndighetspraxis, FAR:s etiska regler, [revisionsföretaget, A-företaget och B-företagets] riktlinjer samt särskilda kundinstruktioner eller avtal. Kundinformation och eventuella personuppgifter som inhämtas under ett uppdrag ska endast användas för det syfte som de samlades in för och hanteras enligt GDPR. [revisionsföretaget, A-företaget och B-företaget] kräver också att en förbindelse om tystnadsplikt undertecknas av alla medarbetare vid anställning (dokumenteras av personalansvarig) och en gång per år därefter (dokumenteras av kvalitetsansvarig). Alla medarbetare förväntas känna till [revisionsföretaget, A-företaget och B-företagets] riktlinjer rörande tystnadsplikt samt följa dem.

Dokumentation av penningtvättsåtgärder ingår i avsnitt 7.5 i kvalitetspolicyn. Detta beror på att utvärderingen av uppdraget inklusive kundkännedom alltid är inkluderad i revisionsdokumentationen. Eftersom revisionsföretaget använder sig av programverktöget sparas även varje kundutvärdering där. Detta följer av programmets funktion och programbeskrivning. Vidare hänvisar den allmänna riskbedömningen till kvalitetspolicyn avseende behandling av personuppgifter och dokumentation av vidtagna åtgärder. Punkt 7.2 i kvalitetspolicyn, *Dokumentation av revisionsuppdrag*, hänvisar till revisionsmanualen; av den framgår att programverktöget används. Programverktöget är en av marknadens ledande penningtvättsverktyg för revisionsbranschen. Samtliga moment finns sparade i programverktöget.

Det framgår av kvalitetspolicyn att revisionsdokumentationen ska bevaras. Penningtvättsåtgärder är en del av revisionsprocessen och det finns därmed riktlinjer även för penningtvättsåtgärder såsom kundkännedom och övervakning.

4.3 Revisorsinspektionens bedömning

Rutiner och riktlinjer avseende åtgärder för kundkännedom

Den revisionsmanual och den kvalitetspolicy som A-son har gett in saknar dokumentation av rutiner och riktlinjer för hur medarbetare ska uppnå, dokumentera och uppdatera kundkännedom. När det gäller utvärdering av befintliga kunders riskprofiler framgår av dokumenten att detta ska göras men inte hur eller när. Att i revisionsmanualen ange att revisionsföretaget följer flödet i revisionsverktöget utgör inte en rutinbeskrivning av hur kundkännedom, övervakning eller utvärdering av befintliga kunders riskprofiler uppnås. Det som anges i dokumentet om utvärdering, dvs. uppföljning av affärsförbindelsen, är detsamma som följer av lag. Att i interna dokument upprepa gällande lagkrav utgör inte

en sådan beskrivning av rutiner, grundade på verksamhetsspecifika omständigheter, som lagen förutsätter att en verksamhetsutövare utarbetar.

Ett utdrag ur systemverktyget skulle i sig kunna anses utgöra ett slags dokumenterad rutin. Det förutsätter emellertid att det som sägs i utdraget grundar sig på revisionsföretagets allmänna riskbedömning och unika förhållanden. Det utdrag som A-son har hänvisat till kommer emellertid från ett köpt programverktyg och innehåller endast allmänt hållna frågor.

A-son har även hänvisat till avsnitt 6.1 i kvalitetspolicyn där det anges att kundriskprofil och kundkännedomsåtgärder ska dokumenteras i en kundutvärdering i revisionssystemet. I dokumentet sägs emellertid inget om företagsspecifika rutiner för identitetskontroll, kontroll av etablering i högriskredjeland eller bedömning av personer i politiskt utsatt ställning. Det sägs inte heller något om skärpta åtgärder för kundkännedom eller om underlag för verksamhetsspecifik kundriskbedömning. En hänvisning till EtikU 11, revisionsprogrammet och dess checklistor eller ett köpt programverktyg framstår i detta avseende inte som tillfyllest.

Revisorsinspektionen konstaterar sammanfattningsvis att revisionsföretaget saknar tillräckliga rutiner avseende åtgärder för att uppnå kundkännedom och utvärdering av befintliga kunders riskprofiler. Genom att inte inrätta och dokumentera sådana rutiner har A-son, i egenskap av ställföreträdare för revisionsföretaget, brustit i sina skyldigheter enligt penningtvättslagen.

Rutiner och riktlinjer avseende övervakning

I den rutin som finns i den åberopade kvalitetspolicyn anges att medarbetarna ska vara uppmärksamma på olika omständigheter under pågående kundrelationer och kunduppdrag. Det framgår emellertid inte vilka dessa omständigheter är, utöver förändrat ägande. Det framgår inte heller på vilket sätt som A-son och hans medarbetare ska agera för att genomföra sin övervakning.

A-son har hänvisat till ISA 315 och angett att en riskbedömning utifrån denna standard innebär att företaget i sin ordinarie revisionsprocess beaktar penningtvättsförhållanden. Att följa en internationell revisionsstandard om revisorns ansvar för att identifiera och bedöma riskerna för väsentliga felaktigheter i de finansiella rapporterna, kan mycket väl vara ett sätt att övervaka en affärsförbindelse i det enskilda fallet. Att en revisor vid sin granskning vanligen agerar på ett sätt som är ägnat att uppmärksamma honom eller henne

på penningtvättsrisker innebär dock inte att revisorn därmed uppfyller lagens krav på dokumenterade rutiner och riktlinjer.

Enligt A-son är revisionsprogrammet en naturlig del av revisionsföretagets process och användningen av revisionsprogrammet får enligt hans uppfattning till följd att penningtvättsrutiner vävs in i revisionsprocessen. Revisorsinspektionen konstaterar dock att de rutiner som avses i penningtvättslagen måste vara anpassade efter den verksamhet som bedrivs i det aktuella revisionsföretaget. Användningen av externa revisionsprogram, utan sådana anpassningar, kan därför inte kompensera för interna rutiner.

Sammanfattningsvis finner Revisorsinspektionen att revisionsföretagets rutiner avseende övervakning enligt penningtvättslagen är bristfälliga. A-son har härigenom brustit i sina skyldigheter enligt penningtvättslagen.

Rutiner och riktlinjer avseende behandling av personuppgifter enligt penningtvättslagen

Revisorerna omfattas av EU:s dataskyddsförordning¹ (GDPR). Enligt 5 kap. 2 § penningtvättslagen får en verksamhetsutövare behandla personuppgifter i syfte att kunna fullgöra sina skyldigheter enligt lagen. I 5 kap. 5 § penningtvättslagen anges förutsättningarna för att en verksamhetsutövare ska få behandla känsliga personuppgifter med stöd av penningtvättslagen, medan 5 kap. 6 § rör behandling av personuppgifter om lagöverträdelse. I 5 kap. 7 § anges att besked om att personuppgifter behandlas enligt 4 kap. 2, 3 eller 6 § och om att sådana uppgifter lagras enligt 5 kap. 3 eller 4 § inte får lämnas ut till den registrerade.

Det är inte nödvändigt att ett revisionsföretag har separata ”register” för att tillgodose efterlevnaden av 5 kap. penningtvättslagen respektive GDPR. Revisorsinspektionen konstaterar emellertid att innehållet i 5 kap. 2, 5, 6 och 7 §§ penningtvättslagen inte behandlas uttryckligen i de rutiner och riktlinjer som A-son har hänvisat till.

De avsnitt i kvalitetspolicyn (5 och 5.6) som A-son har hänvisat till behandlar tystnadsplikt, dvs. en annan fråga än personuppgiftsbehandling. Behovet av adekvata riktlinjer för personuppgiftsbehandling tillgodoses inte heller, som A-son synes mena, genom avsnitt 7.5 i kvalitetspolicyn; det som sägs i kvalitetspolicyn om att revisionsföretaget ska informera kunden innan arbetspapper lämnas ut enligt lagar och

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

regler (till exempel vid konkurs) stämmer inte överens med penningtvättslagens bestämmelser.

Revisorsinspektionen finner att revisionsföretagets dokumenterade rutiner och riktlinjer avseende behandling av personuppgifter enligt penningtvättslagen är bristfälliga. A-son har härigenom brutit i sina skyldigheter enligt penningtvättslagen.

5 Sammanfattande bedömning och val av disciplinär åtgärd

Det revisionsföretag som A-son ansvarar för hade vid tiden för kvalitetskontrollen en bristfällig allmän riskbedömning. Vidare saknade företaget på flera lagstadgade områden dokumenterade rutiner och riktlinjer enligt penningtvättslagen. På andra områden innehöll rutinerna och riktlinjerna felaktigheter.

Genom att i egenskap av ställföreträdare för revisionsföretaget underlåta att se till *dels* att revisionsföretaget hade en godtagbar allmän riskbedömning, *dels* att revisionsföretaget hade relevanta och uppdaterade rutiner och riktlinjer på penningtvättsområdet har A-son åsidosatt sina skyldigheter enligt penningtvättslagen. Han har härigenom också åsidosatt sina skyldigheter som revisor och ska därför, med stöd av 32 § andra stycket revisorslagen, meddelas en disciplinär åtgärd. Det som ligger honom till last är allvarligt och ska föranleda en varning.

Ärendet har avgjorts av Revisorsinspektionen genom Tillsynsnämnden för revisorer. I beslutet har deltagit f.d. justitierådet Sten Andersson, ordförande, kammarrättslagmannen Christina Eng, vice ordförande, skattedirektören Tomas Algotsson, redovisningsexperten Sofia Bildstein-Hagberg, auktoriserade revisorn Maria Danckler, rådgivaren Sophie Degenne, auktoriserade revisorn Magnus Fredmer, advokaten Emma Norburg och docenten Jessica Östberg. Vid ärendets slutliga handläggning har i övrigt avdelningsdirektören Lotta Westerberg, som har föredragit ärendet, varit närvarande.

Sten Andersson

Lotta Westerberg

Hur man överklagar, se bilaga.