



Premium Årsrapport



Innholdsfortegnelse

01	Innledning årsrapport	4	09	Svindel	52
02	Regulatorisk nytt	8		Investerings- og kjærlighetssvindel tilbake i fokus	53
	Utviklingen innen antihvitvasking og -terrorfinansiering i 2025	9		Statistikk fra FinKN i 2025:	54
	Endringer i Norge	9		Oppsummering	55
	Endringer fra EU	11	10	Bedre datadeling i finanssektoren	56
	Oppsummering	13		Sandkasseprosjekter om informasjonsdeling	57
03	Oppsummering av tekniske standarder på høring	14		EU forenkler datadeling i finanssektoren	58
	Kundetiltak RTS (AMLR artikkel 28(1))	15		Hva innebærer forordningen?	58
	Risikovurdering av rapporteringspliktige (AMLD artikkel 40(2))	17		Forventet effekt på AML området	59
	Kundeforhold, tilknyttede transaksjoner og beløpsgrenser (AMLR artikkel 19(9))	18		Oppsummering	60
	Oppsummering	20	11	Krypto – den store nye trusselen?	62
04	Tilsynsaktiviteter i 2025	22		Markedsutvikling og bruk	63
	Antall tilsynsrapporter/overtredelsesgebyr per virksomhetsområde	24		Regulatorisk tilnærming	63
05	Geografisk risiko	28		Kriminalitet og tilsynsutfordringer	64
	EUs høyrisikoland for hvitvasking og terrorfinansiering	29		Oppsummering	64
	Status: Sanksjoner mot Russland	33	12	2025 og veien videre	66
	Oppsummering	34	13	Kilder	70
06	Politiets trusselvurdering for 2025	36		Generelle kilder	71
07	PSTs Nasjonal Trusselvurdering 2025	40		Kontakt	72
08	AI som støtte i arbeidet mot økonomisk kriminalitet	44			
	Transaksjonsovervåkning - utfordringen med falske positive treff	45			
	Hvordan vil AI kunne påvirke transaksjonsovervåkingen?	46			
	Suksessfaktorene og risiko knyttet til AI	47			
	Oppsummering	50			

01 Innledning årsrapport

Verden går inn i 2026 med høy puls! Året 2025 bærer preg av ny politisk kurs fra Washington og spørsmålene er mange: Hvor går geopolitiske grenser i Arktis? Hva skjer med Venezuela etter maktskiftet? Kan spenninger mellom USA og Iran eskalere til fullskala krig i Midtøsten? Men kanskje viktigere, hvilke internasjonale organisasjoner og avtaler vil myndighet ha fremover og hvordan vil dette påvirke transaksjoner og globale markeder? Hvordan vil den teknologiske utviklingen påvirke oss fremover? Alle disse forholdene vil påvirke arbeidet mot økonomisk kriminalitet, våre risikovurderinger og arbeidsprosesser.

Vi vet at det geopolitiske trykket påvirker kriminaliteten. Høye renter, gjeldsgrad og tøffere tider øker fristelsen for vinningskriminalitet, særlig når risikoen for å bli oppdaget, dømt og straffet oppleves som lav. Artificial Intelligence (AI), digitale plattformer og globale betalingsløsninger gir helt nye muligheter for skalering, desinformasjon og rekruttering av kriminelle, samtidig som sporene blir mer krevende å følge. For rapporteringspliktige betyr dette ikke bare økt uforutsigbarhet, men også et temposkifte. Verden endres fra dag til dag.

Økonomisk kriminalitet må behandles som en direkte trussel mot vårt samfunn: arbeidsplasser, konkurransekraft og fellesfinansiert velferd. Målet kan ikke være å ha krysset av riktig i sjekklisten, men å gjøre kriminalitet vanskeligere, mindre lønnsomt og avdekke kriminelle nettverk. Arbeidet mot hvitvasking og terrorfinansiering har høy prioritet i EU. Den nye antihvitvaskingspakken er nå på høring i Norge og det er forventet at implementering blir samtidig som EU.

Hvitvaskingspakken og etableringen av Anti-Money Laundering Authority (AMLA) er et strukturelt skifte: sterkere tilsyn, like regler, og bedre informasjonsdeling. De nye kravene kommer også med korte frister. For virksomheter vil det bety omfattende tilpasninger i prosesser, systemer, datainnhenting og kompetanse. Alle detaljene er ikke fastsatt ennå, men 2026 blir året man raskt må analysere og tolke endelig regelverk, ta stilling til hvordan endringene treffer egen organisasjonen og ikke minst gjennomføre de nødvendige tilpasningene.

Alt dette, og mer, har vi skrevet om i årets rapport. I tillegg oppsummerer vi årets oppdateringer tilknyttet geografisk risiko, tilsynspraksis fra det norske Finanstilsynet, observasjoner fra PSTs og Politiets trusselvurderinger, samt fagartikler som dekker andre nærliggende temaer, inkludert utviklingen på svindelområdet.

2026 er totalforsvarets år, og innsatsen fra både det offentlige og private Norge vil samle krefter blant annet i kampen mot at kriminelle utnytter eksisterende infrastruktur. Vi håper at rapporten kan inspirere til å løfte blikket, se helheten og flytte fokuset fra etterlevelse, til reell risikostyring, slik at vi sammen beskytter felles verdier.

Kjersti Aksnes Gjesdahl
Partner



02 Regulatorisk nytt

Utviklingen innen antihvitvasking og -terrorfinansiering i 2025

2025 har markert et tydelig taktskifte i arbeidet mot hvitvasking og terrorfinansiering, både i Norge og EU.¹ Regelverksutviklingen preges av tre hoveddrivere:

- Et mer komplekst kriminalitets- og trusselbilde, påvirket av geopolitikk og sanksjoner.
- Teknologiske endringer, særlig digitalisering og bruk av kryptovaluta.
- Et sterkere internasjonalt press for harmonisering og transparens.¹

Felles for årets regulatoriske tiltak er økte krav til datadrevne risikovurderinger, med vekt på datakvalitet i eierskapsinformasjonen og mer sammenlignbare tilsynsstandarder på tvers av landegrenser basert på en felles metodikk.²

Endringer i Norge

Register over reelle rettighetshavere

Etableringen av registeret over reelle rettighetshavere har vært det mest gjennomgripende tiltaket i 2025. Rapporteringspliktige har lenge etterspurt bedre eierskapsdata og nyheten om et register for reelle rettighetshavere ble i utgangspunktet godt mottatt. Ved lansering viste det seg imidlertid at registeret benyttet en annen definisjon av reell rettighetshaver enn hvitvaskingsloven,³ noe som har skapt betydelig usikkerhet om hvilke regler som gjelder og verdien av å speile egne eierskapsdata mot et register med avvikende begrepsbruk og beregningsmetodikk.⁴ Dette har særlig hemmet muligheten til å automatisere kjerneprosesser i AML, der høy datakvalitet er kritisk, og den praktiske bruken av registeret har vært uklar. I forslaget til ny anti-hvitvaskingslov adresseres dette nå med forslag om harmonisering av

1 Den europeiske kommisjon, Anti-money laundering and countering the financing of terrorism legislative package, 2021, link: [Anti-money laundering and countering the financing of terrorism legislative package - Finance](#)

2 Den europeiske kommisjon, Better data sharing, 2025, link: https://finance.ec.europa.eu/news/better-data-sharing-2025-02-24_en

3 Brønnøysundregistrene, Register over reelle rettighetshavere, 2025, link: https://www.brreg.no/wp-content/uploads/Veileder_reelle_rettighetshavere_bokmaal.pdf

4 Brønnøysundregistrene, Register over reelle rettighetshavere – offisiell beskrivelse, 2025, link: <https://www.brreg.no/om-oss/registrene-vare/om-register-over-reelle-rettighetshavere/>

definisjonene.⁵ Grepet er nødvendig for å gjøre registeret operativt nyttig og styrke presisjonen og effektiviteten ved utførelsen av kundetiltak.

Fokus har ligget på:

- Innfasing av rapporteringskrav
- Kvaliteten på innrapporterte data
- Tydeligere forventning om verifikasjon.

Virksomheter har brukt betydelige ressurser på å identifisere og dokumentere eierskap, og Finanstilsynet har varslet reaksjoner ved feil eller mangler. Registeret vil bli et sentralt verktøy i tilsyn, etterretning og kundetiltak fremover.

Kryptosektoren

Fra og med 1. juli 2025 er to europeiske forordninger som omhandler kryptovaluta implementert i norsk rett. Forordningen Markets in Crypto-assets Regulation (MiCA) er inntatt i ny lov om kryptoeiendeler (Kryptoeiendelsloven), og Transfer of Funds Regulation II (TRF II) er inntatt i hvitvaskingsloven.⁶

Kryptoeiendelslovens formål er å sikre finansiell stabilitet samtidig som den legger til rette for innovasjon.⁷ Regelverket omfatter krav knyttet til utstedelse og handel med kryptovaluta, investorbeskyttelse og forbud mot markedsmanipulasjon. TRF II stiller krav til hvilke opplysninger som skal følge overføringer i kryptovaluta (og penger for øvrig),⁸ og fører til at aktører som tilbyr kryptooverføringer blir underlagt rapporteringsreglene i hvitvaskingsloven. I hovedtrekk betyr dette at sektoren får:

- Strengere forventninger til kundetiltak
- Behov for mer sofistikerte overvåkingssystemer
- Flere signaler om skjerpet tilsyn.

5 Finansdepartementet, Høringsnotat – forslag til ny antihvitvaskingslov, 2025, link: <https://www.regjeringen.no/no/aktuelt/horing-om-nytt-antihvitvaskingsregelverk-og-lavere-grenser-for-kontantbetaling/id3147190/>

6 Regjeringen.no, Europeisk rammeverk for markeder for kryptoeiendeler (MiCA), 2025, link: <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2025/juli/europeisk-rammeverk-for-markeder-for-kryptoverdier-mica-utfyllende-bestemmelser-om-registre-over-alle-ordre-og-transaksjoner-med-kryptoaktiva/id3114570/>

7 Den europeiske kommisjon, Markets in Crypto-Assets Regulation – objectives, 2024, link: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

8 Den europeiske kommisjon, Transfer of Funds Regulation, 2024, link: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113>

Endringer fra EU

Anti-Money Laundering Authority (AMLA)

AMLA er EUs nye tilsynsmyndighet for hvitvasking og terrorfinansiering som ble etablert i 2025.⁹ Den introduserer en ny europeisk tilsynsmodell ved å føre direkte tilsyn med et utvalg høyrisikovirksomheter (40 virksomheter skal snart velges ut), utvikle felles regler, metoder og tilsynsstandarder, og koordinere nasjonale tilsyn på tvers av EU/EØS. Flere av disse oppgavene lå tidligere under EBAs ansvarsområde, men har nå blitt flyttet til AMLA fra nyttår 2025.

Hva betyr dette i praksis:

- Mer harmoniserte krav på tvers av land: like forventninger til styring, risikovurdering, kundetiltak og transaksjonsovervåking.
- Strengere og mer datadrevet tilsyn: høyere krav til dokumentasjon, nøkkeltall og rask oppfølging av avvik.

Selv om de fleste norske foretak ikke blir underlagt direkte AMLA-tilsyn, vil AMLA indirekte påvirke norsk tilsynspraksis gjennom at Finanstilsynet vil ta i bruk AMLAs metodikk, verktøy og veiledninger. Noe som vil gi mer ensartet håndheving og høyere forventninger til etterlevelse av det nye regelverket også i Norge.

”Money laundering corrodes public trust, fuels organized crime, corruption, and tax evasion, and distorts fair competition. Our response must be strong and unified.”¹⁰

Bruna Szego

Chair of the European Anti-Money Laundering Authority (AMLA)

9 Den europeiske kommisjon, Anti-Money Laundering Authority (AMLA), 2025, link: https://www.amla.europa.eu/about-amla_en

10 Den europeiske kommisjon, Anti-Money Laundering Authority (AMLA) - Bruna Szego addresses the public for AMLA in Dublin, 2025, link: https://www.amla.europa.eu/news-media/news-articles/bruna-szego-addresses-public-amla-dublin_en

Harmonisering av regelverket (AMLR og AMLD6)

For å bistå AMLA med det regulatoriske harmoniseringsarbeidet innfører EU nå et felles og mer detaljert regelverk for antihvitvasking. Kjernen er Anti-Money Laundering Regulation (AMLR), en forordning som blir direkte gjeldende i EU og som i Norge skal utarbeides via ny antihvitvaskingslov. Denne loven vil erstatte gjeldende hvitvaskingslov fra 2018, som i stor grad er bygget på AMLD4/5 (fjerde og femte hvitvaskingsdirektiv).

Samtidig kommer AMLD6 (det sjette hvitvaskingsdirektiv), som setter de institusjonelle rammene for tilsyn, sanksjoner og samarbeid. Summen er mindre rom for nasjonale særregler enn tidligere og mer lik håndheving på tvers av land.

Forslaget til ny antihvitvaskingslov er nå ute på høring i Norge og innebærer blant annet:

- Flere omfattes som blant annet forhandlere av verdifulle og kultur-gjenstander, samt fotballklubber og agenter.
- Skjerpet risikovurdering og tydeligere krav ved nye produkter, kunde-segmenter og utvidelse til nye markeder.
- Ny beregningsmetodikk for eierskap og ny metode for å beregne indirekte eierskap i eierkjeder (multiplikasjon).
- Utvidet PEP-definisjon hvor enkelte lokalpolitikere omfattes av definisjonen.
- Mer lovlig informasjonsdeling, særlig internt i konsern.
- Bedre tilgang til registre og eiendoms- og bankkontodata struktureres og åpnes mer.
- Lavere kontantgrenser med forslag om å sette ned beløpsgrensen til 10 000 kroner, også for tjenester.
- Skadeforsikring tas ut og skadeforsikringsforetak omfattes ikke lenger av AML regelverket direkte.

Oppsummering

Regelverksutviklingen i 2025 markerer et tydelig skifte mot mer harmoniserte og skjerpede krav i arbeidet mot hvitvasking og terrorfinansiering i Norge og EU. Et mer komplekst trusselbilde og økt bruk av teknologi stiller høyere krav til risikoforståelse og etterlevelse.

Utviklingen kjennetegnes særlig av:

- Økt harmonisering og standardisering gjennom AMLR, AMLD6 og etableringen av AMLA
- Sterkere fokus på eierskapstransparens
- Skjerpede forventninger til kryptosektoren
- Mer risikobasert og datadrevet etterlevelse

For norske virksomheter betyr dette at kravene til dokumentasjon, risikovurderinger og kontroll vil bli mer detaljerte. For å kunne etterleve regelverket innenfor et forsvarlig kostnadsnivå vil rapporteringspliktige i større grad måtte investere i teknologiske løsninger, automatisering og arbeide mot å heve datakvalitet på tvers av organisasjonen. De som forbereder seg tidlig og bruker endringene strategisk, vil kunne ta ut både effektivitets- og konkurransegevinster.

Våre 3 råd for rapporteringspliktige i 2026

- 1. Følg regelendringer tett og juster kursen løpende:** Overvåk nivå 2-regelverk og veiledninger fra EU, og oppdater planer raskt når tolkninger avklares.
- 2. Se regelverket som en mulighet:** Bruk endringene til å standardisere og forenkle kjerneprosesser. Fjern unødvendig kompleksitet, innfør felles arbeidsmåter og omgjør der effekten er størst.
- 3. Identifiser teknologimuligheter:** Kartlegg hvor teknologi gir størst gevinst i deres prosesser og prioriter tiltak med rask og målbar effekt.

03 Oppsummering av tekniske standarder på høring

AMLA, EUs nye anti-hvitvaskingsmyndighet, er nå i gang med å utarbeide nivå 2-regelverk i form av tekniske standarder som skal utfylle EUs anti-hvitvaskingspakk. Flere av disse forslagene er for tiden ute på høring i EU, og det er grunn til å tro at reglene vil bli tatt inn i EØS-avtalen og gjennomført i norsk rett. Nedenfor oppsummerer vi de viktigste forslagene som nå er på høring, og hva de kan bety for norsk praksis.

Kundetiltak RTS (AMLR artikkel 28(1))

AMLA har sendt utkast til tekniske standarder (RTS) under artikkel 28(1) i den nye EU-hvitvaskingsforordningen på høring.¹¹ Forslaget harmoniserer i detalj hvordan kundetiltak skal gjennomføres og adresserer forenklete tiltak, standard kundekontroll og forsterkede tiltak ved høy risiko.

Identifikasjon og verifisering – Europa samles om norsk standard

Kravene til hvilken informasjon som skal innhentes (navn, fødselsdato, fødested, nasjonalitet, adresse for fysiske personer; foretaksnavn, organisasjonsform, adresse og registreringsnummer for juridiske personer) er i stor grad sammenfallende med det som allerede praktiseres i Norge.¹² Det nye er at resten av EU nå beveger seg mot samme standard.

Relevant for norske aktører er imidlertid de nye reglene for fjern onboarding uten BankID/eID. I tilfeller der elektronisk ID på nivå «substantial» eller «high» (som BankID) ikke er tilgjengelig, kan fjernløsninger likevel brukes, men med strenge vilkår. Løsningen må ha kontroller som sikrer at personen som presenterer dokumentet er personen på bildet, kommunikasjonens integritet og konfidensialitet må være sikret, bilder og video må lagres i lesbart format, og prosessen skal avbrytes ved tekniske feil eller tvil om identiteten.

¹¹ Regulation (EU) 2024/1624 (AMLR), Article 28(1) – draft Regulatory Technical Standards on Customer Due Diligence, 2025, link: <https://amlr.eu/article-28-regulatory-technical-standards-on-the-information-necessary-for-the-performance-of-customer-due-diligence/>

¹² AMLA, Regulatory Instruments – status for tekniske standarder (RTS/ITS) og deres mandat, 2025, link: https://www.amla.europa.eu/policy/regulatory-instruments_en

I Norge i dag er slike alternative digitale løsninger tillatt som «ytterligere tiltak» ved kundeetablering uten personlig fremmøte, men det er opp til den rapporteringspliktige å risikovurdere løsningen som brukes.

Reelle rettighetshavere og komplekse selskapsstrukturer

I forslaget kreves det at det gjøres oppslag i sentrale registre, men at dette alene ikke er tilstrekkelig for å verifisere reelle rettighetshavere, det må suppleres med minst ytterligere en kilde. Denne tilleggsilden kan imidlertid være informasjon innhentet fra kunden selv (f.eks. en kundeerklæring), offentlige registre utover sentralregisteret, kredittbyråer, eller bekreftelser fra andre finansinstitusjoner. I praksis betyr dette at den vanlige norske tilnærmingen, kundeerklæring sjekket opp mot register, fortsatt vil være tilstrekkelig, så lenge de to kildene brukes til henholdsvis identifikasjon og verifisering.

Noe som er nytt, er at forslaget innfører en konkret definisjon av «kompleks selskapsstruktur». En eierstruktur skal behandles som kompleks der det er tre eller flere lag mellom kunden og reell rettighetshaver, i tillegg må flere enn ett av følgende vilkårene være oppfylt:

- Det finnes en trust, stiftelse eller lignende juridisk arrangement i strukturen.
- Kunden eller mellomliggende enheter er registrert utenfor EU.
- Det er forvalterregistrering (nominee shareholders/directors) involvert.
- Strukturen tilslører eierskap uten legitimt økonomisk formål.

Ved komplekse strukturer skal det innhentes tilleggsinformasjon, som organisasjonskart, og den rapporteringspliktige må forsikre seg om at informasjonen er troverdig, at det finnes en økonomisk eller juridisk begrunnelse for strukturen, og at de forstår hvordan strukturen påvirker hvitvaskingsrisikoen. Dersom reell rettighetshaver ikke kan identifiseres, kan «senior managing officials» (SMO) identifiseres i stedet, men forslaget presiserer at dette kun er tillatt der alle mulige identifiseringsmidler er uttømt. At strukturen er vanskelig å gjennomskue er ikke det samme som «tvil», kompleksitet alene gir altså ikke grunnlag for å gi opp identifisering.

I dag i Norge skal identiteten til reelle rettighetshavere bekreftes ved «egnede tiltak» basert på risikovurdering. AMLAs forslag gir langt mer presise minstekrav, og den konkrete definisjonen av en kompleks struktur er ny sammenlignet med norsk praksis i dag.

Forenklede og forsterkede kundetiltak – nye minimumskrav

Ved lav risiko (forenklede tiltak) setter forslaget klare minimumskrav. For fysiske personer skal det minimum innhentes navn, fødselsdato, fødested og nasjonalitet. For juridiske personer: organisasjonsform, registrert navn, adresse og eventuelt registreringsnummer. For reelle rettighets-

havere ved lav risiko er det tilstrekkelig å konsultere én kilde (sentralregister, kundeinformasjon eller åpen kilde) for identifikasjon, og en annen kilde for verifisering.

AMLA understreker at forenklede tiltak ikke er et fritak fra kundetiltak, men en redusert kontrollprosess som fortsatt skal dekke alle komponentene i standardprosedyren. Forordningen gir allerede mulighet til f.eks. å utsette verifisering med inntil 60 dager eller redusere mengden informasjon om kundeforholdets formål.

Ved høy risiko (forsterkede tiltak) kreves det tilleggsinformasjon av tilstrekkelig kvalitet fra uavhengige og pålitelige kilder. Konkret spesifiserer forslaget hva som skal innhentes for å dokumentere midlenes og formuens opprinnelse: skattemeldinger, lønsslipper, reviderte regnskaper, investeringsdokumentasjon, låneavtaler, kjøpskontrakter, skjøter, arveavtaler og informasjon fra pålitelige registre eller medier. Den rapporteringspliktige skal også vurdere om transaksjonene er konsistente med kundens virksomhet og risikoprofil, samt innhente informasjon om formålet med transaksjoner der det er identifisert forhøyet risiko.

I Norge er prinsippene i hovedsak de samme i dag – forenklede tiltak ved lav risiko, forsterkede ved høy – men veilederen gir i stor grad rom for skjønn. AMLAs forslag fjerner mye av dette skjønnrommet ved å liste opp konkrete minimumskrav og akseptable dokumentasjonstyper for begge kategorier.

Risikovurdering av rapporteringspliktige (AMLD artikkel 40(2))

I dag varierer tilsynsmyndighetenes tilnærming til risikovurdering betydelig mellom EU-land, noe som gir usammenlignbare resultater og ulike prosesser og kostnader for foretak som opererer på tvers av landegrenser. AMLA har derfor vedtatt et utkast til tekniske standarder (RTS) under artikkel 40(2) som innfører én felles metodikk for hvordan alle tilsynsmyndigheter, inkludert Finanstilsynet, skal vurdere og klassifisere hvitvaskingsrisikoen til den enkelte rapporteringspliktige.¹³

Metodikken følger en tre-trinns modell:

- Først vurderes foretakets iboende risiko (kundetype, produkter, geografi og distribusjonskanaler)
- Deretter kvaliteten på foretakets AML-kontroller

¹³ AMLA, AMLA risk methodology and classification, 2025, link: https://www.amla.europa.eu/document/download/b78bee2f-16b9-4742-a3a1-23e7aad394ab_en?filename=AMLA_Work_Programme_July%202025_0.pdf

- Til slutt kombineres dette til en samlet restrisikoscore – klassifisert som lav, middels, vesentlig eller høy.

En viktig del av metodikken er et felles sett med datapunkter som de rapporteringspliktige skal rapportere inn. Eksempler er:

- Antall kunder fordelt per land
- Antall PEP-kunder
- Antall kunder med komplekse eierstrukturer
- Volum og verdi av grensekryssende transaksjoner, kontant-transaksjoner og kryptotransaksjoner

De fleste foretak vil måtte levere mellom 100 og 150 datapunkter.

Vurderingen skal som hovedregel gjøres årlig, men hvert tredje år for små foretak eller foretak med lav-risiko aktiviteter. Forslaget gjelder foreløpig kun finanssektoren, tilsvarende regler for ikke-finansiell sektor kommer senere.

Kundeforhold, tilknyttede transaksjoner og beløpsgrenser (AMLR artikkel 19(9))

I dag er skillet mellom et løpende kundeforhold og en enkelttransaksjon avgjørende for hvilke kundetiltak (identitetskontroll, oppfølging osv.) som skal gjennomføres. AMLA mener at dette skillet tolkes ulikt mellom EU-land, og at dette skaper smutthull for kriminelle. Derfor er det sendt ut på høring utkast til tekniske standarder (RTS) under den nye EU-hvitvaskingsforordningen som skal klargjøre dette området.

Når er noen «fast kunde»?

- Nettjenester: Registrering for tilgang til en nettbasert tjeneste (nettbank, krypto, gambling) peker i seg selv mot et kundeforhold.
- Advokater, regnskapsførere m.fl.: Tjenester ved flere anledninger eller ulike tjenester til samme person peker mot kundeforhold.
- Vekslingskontor/pengeoverføring: Tre eller flere transaksjoner i en rullerende 12-månedersperiode peker mot kundeforhold.
- Spilltilbydere og fotballklubber: Egne kriterier knyttet til medlemskap og spilleroverganger.

I Norge gir dagens veileder til hvitvaskingsloven lite detaljert veiledning om akkurat når et forhold går fra enkelttransaksjon til kundeforhold¹². AMLAs forslag er vesentlig mer presist.

Når henger transaksjoner sammen?

AMLA foreslår også detaljerte kriterier for «tilknyttede transaksjoner», bl.a. når samme person, familiemedlemmer, forretningspartnere, felles digital infrastruktur, eller at transaksjonene gjelder samme kjøp. For veksling/pengeoverføring settes perioden til bare én måned.

I dag i Norge skal transaksjoner som «ser ut til å ha sammenheng» ses samlet over en tolv månedersperiode, men kriteriene er langt mindre spesifikke.

Lavere terskelverdier?

AMLA hadde mandat til å foreslå lavere beløpsgrenser i høyrisikosektorer, men velger ikke å gjøre det nå da de mangler underlag for at eksisterende grenser er utilstrekkelige. Hovedgrensen forblir derfor 10 000 euro, med allerede vedtatte lavere terskler for krypto (1 000 €), kontanter (3 000 €) og spill (2 000 €).

I Norge er hovedgrensen i dag på 100 000 kroner og 8 000 kroner for virtuell valuta så dette vil i praksis gi lite endringer.

“In cooperation with the national anti-money laundering authorities and the financial investigation authorities, the AMLA forms a robust supervisory system that strengthens the effectiveness and efficiency of anti-money laundering efforts in Europe.”

Oliver Eis

Partner, Compliance Service AFC/IA at PwC Germany

Oppsummering

AML er i full fart med å utforme detaljene i det nye europeiske AML-regelverket gjennom en rekke tekniske standarder. Forslagene harmoniserer alt fra hvordan kundetiltak skal gjennomføres til når et kundeforhold anses etablert, og hvordan tilsynsmyndigheter skal risikovurdere finansforetak. For norske rapporteringspliktige betyr dette at mye av dagens skjønnsbaserte tilnærming erstattes av mer detaljerte felleseuropeiske minstekrav, og at det blir viktig å posisjonere seg tidlig. Norske aktører bør snarlig starte med å analysere og vurdere hvordan dagens prosesser, systemer og kompetanse må endres for å møte de nye europeiske kravene.

Våre 3 råd for rapporteringspliktige i 2026:

- 1. Kartlegg gapet mellom dagens praksis og de nye kravene:** Forslagene innfører konkrete definisjoner og minstekrav som ikke finnes i norsk rett i dag, blant annet for komplekse selskapsstrukturer, fjern onboarding uten eID, og kriterier for når et kundeforhold er etablert. Gjør en systematisk gjennomgang av egne rutiner opp mot de nye standardene for å identifisere hvor tilpasninger trengs.
- 2. Prioriter datakvalitet og rapporteringsevne:** Den nye tilsynsmetodikken bygger på standardiserte datapunkter som foretakene skal levere, fra antall PEP-kunder til volum av grensekryssende transaksjoner. Sørg for at interne systemer kan produsere disse dataene pålitelig og effektivt, da de vil danne grunnlaget for tilsynets risiko-klassifisering av foretaket.
- 3. Bruk regelverksendringen som anledning til å modernisere:** Overgangen til et mer standardisert regime er et godt tidspunkt for å investere i automatisering av kundetiltaksprosesser, styrke AML-kompetansen i organisasjonen, og etablere løpende rutiner for regelverksovervåking, slik at dere er rigget, ikke bare for det som kommer nå, men også for fremtidige oppdateringer fra AMLA.



04 Tilsyns-aktiviteter i 2025

I 2025 fortsatte Finanstilsynet å prioritere tilsyn med etterlevelse av hvitvaskingsregelverket. Tilsynet gjennomførte stedlige inspeksjoner, skriftlige undersøkelser og dialogmøter, og har publisert flere rapporter som identifiserer og eksemplifiserer typiske mangler i etterlevelse.

På lik linje med rapporteringspliktige virksomheter arbeider Finanstilsynet risikobasert. Sektorer med identifisert høyere risiko for hvitvasking og terrorfinansiering prioriteres i tilsynsarbeidet, mens mindre aktører følges opp mer sporadisk gjennom mindre omfattende tilsyn.¹⁴

Ettersom det i praksis ofte går flere år mellom hver gang en rapporteringspliktig virksomhet får tilsyn på AML-området, vil de årlige gjennomgangene av tilsynspraksis til en viss grad reflektere hvilke virksomheter som er blitt kontrollert det aktuelle året. Det er likevel verdifullt å merke seg tilsynets kommentarer og vurderinger for å danne et helhetlig bilde av status og utvikling. I år har tilsynsaktiviteten særlig omfattet mindre eiendoms- meglingsforetak, regnskapsfører- og revisjonsfirmaer, i tillegg til enkelte banker. Tilsynet har påpekt mangler innenfor flere områder. Under finner du de viktigste punktene som blir trukket frem og hva som er identifiserte forbedringsområder. I tillegg har Advokattilsynet som driver tilsyn med advokaters etterlevelse av hvitvaskingsregelverket satt fornyet fokus på temaet gjennom å starte 2026 med et betydelig opplæringsprogram.¹⁵

Risikovurdering

Kravene til å gjennomføre en virksomhetsinnrettet risikovurdering i henhold til hvitvaskingsloven § 7 står sentralt også i tilsynsrapportene fra 2025. Tilsynsrapportene peker på at flere risikovurderinger fremstår generelle og bransjeoverordnede, med svake koblinger mellom iboende risiko, faktisk eksponering og restrisiko. Det etterlyses tydeligere speiling av egen virksomhet, der risikoer beskrives og vurderes med utgangspunkt i egne produkter og tjenester, kundegrupper, geografi og faktiske eksponeringer. Risikovurderingen skal være styrende for valg av tiltak og oppfølging. Ofte blir det følgefeil når denne ikke er godt gjennomarbeidet. Terrorfinansieringsrisiko er ifølge Finanstilsynet gjennomgående for lite konkret vurdert.

Observasjoner fra tilsyn:

- Mange risikovurderinger er fortsatt for generelle og ligner bransjemaler.

¹⁴ Finanstilsynet, Tilsynsrapporter – arkiv, 2025, link: <https://www.finanstilsynet.no/nyhetsarkiv/tilsynsrapporter/?query=&t=104&years=2025&page=1&language=no>

¹⁵ Advokattilsynet, Informasjon om tilsyn og opplæring i hvitvasking, 2025, link: 240906 Veiledning til etterlevelse av hvitvaskingsregelverket med vedlegg.pdf

30

Tilsynsrapporter
som dekker AML (13 der AML er hoved- eller deltema)

4

Overtredelsesgebyr
Der AML er et viktig tema

12

Tilbakekall av autorisasjon/konsesjon/godkjenning
12 (2 saker der AML er viktig tema)

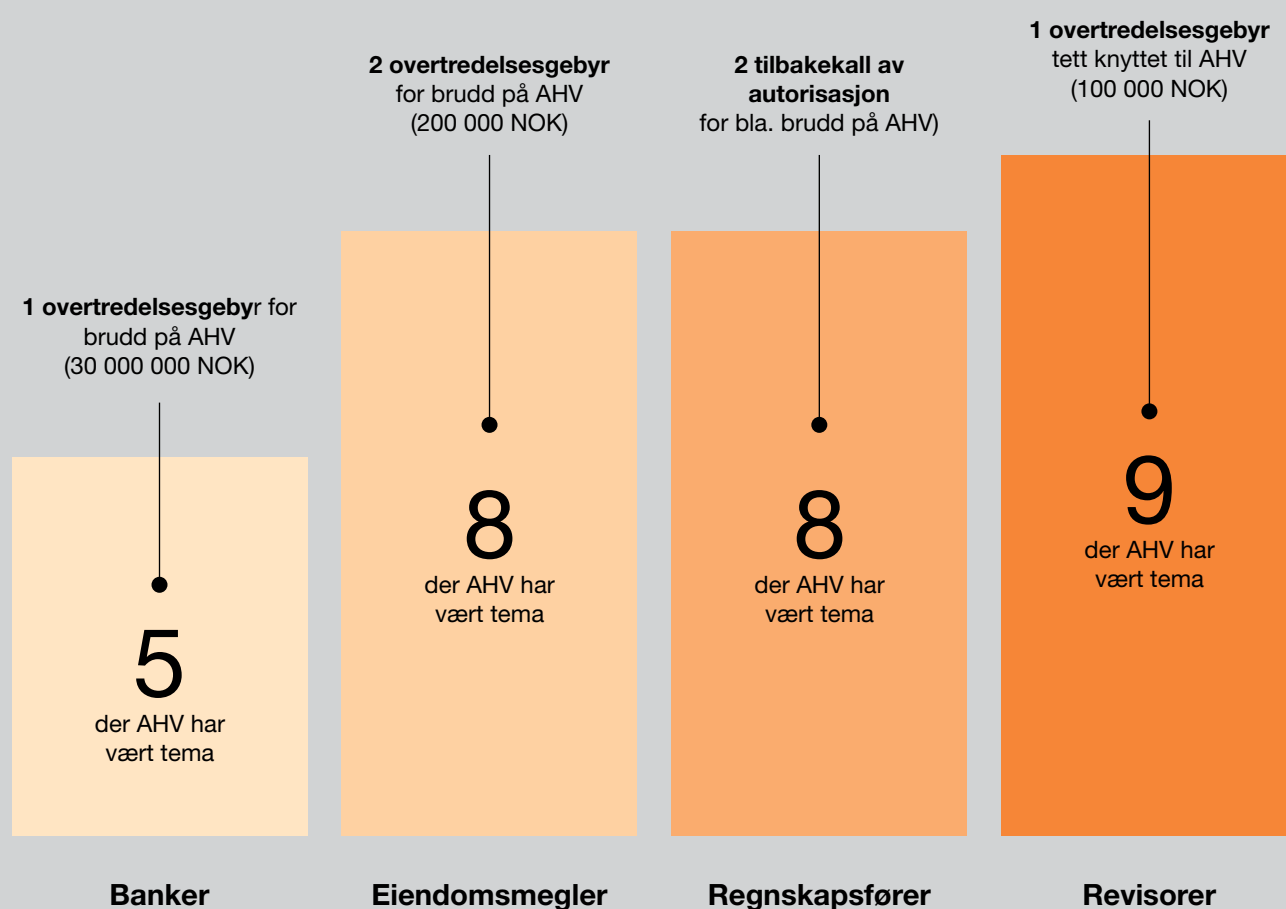
2

Pålegg om retting

30,3 mill NOK

Total sum overtredelsesgebyr ifm. hvvl.

Antall tilsynsrapporter/overtredelsesgebyr per virksomhetsområde



- Foretakene beskriver ikke egne produkter, kunder, geografi eller eksponeringer godt nok.

*Ingen betalingsforetak, forsikringsselskap, tilbydere av spilltjeneste, verdipapirforetak/AIF-forvalter (initiert etter tematisyn) eller virtuelle valutatenester har hatt tilsyn på AML området i perioden. Terrorfinansiering vurderes i for liten grad eller omtales ikke i det hele tatt.

Identifiserte forbedringsområder:

- Risikovurderinger bør i større grad benyttes som reelle levende dokumenter, vedlikeholdes og aktivt benyttes til opplæring av ansatte og forbedring av tiltak og rutiner.

Rutiner

Plikten til å ha oppdaterte og virksomhetsinnrettede rutiner etter hvitvaskingsloven § 8 er fortsatt et område med forbedringsbehov. Tilsynet peker på at operasjonaliseringen av risikovurderingen i rutinene ikke alltid er tilstrekkelig, herunder manglende veiledning om skjønnsutøvelse i sentrale prosesser. Kriterier for risikoklassifisering, bruk av forsterkede kundetiltak og håndtering av nærmere undersøkelser bør beskrives klart i rutinene. Enkelte foretak mangler også lovpålagte rutiner. I flere rapporter påpekes manglende kobling mellom identifiserte risikoer og rutiner. Finanstilsynet fremhever også at god systemstøtte og arbeidsflyt kan støtte etterlevelsen, men dette erstatter ikke kravet til skriftlig, tilgjengelig rutineverk. For eiendomsmeglere pekes det særlig på at skillet mellom forsterkede kundetiltak og nærmere undersøkelser må tydeliggjøres i rutineverket for å sikre riktig behandling av mistenkelige forhold.

Observasjoner fra tilsyn:

- Rutiner er ofte ikke koblet til den faktiske risikovurderingen.
- Mangelfulle beskrivelser av risikoklassifisering, forsterkede tiltak og nærmere undersøkelser.
- Systemer kan støtte, men erstatter ikke skriftlige rutiner.

Identifiserte forbedringsområder:

- Rutiner må være konkrete, oppdaterte og forklare hvordan ansatte faktisk skal jobbe. De bør til enhver tid adressere eventuelle endringer som gjøres i den virksomhetsinnrettede risikovurderingen.

Kundetiltak og løpende oppfølging

Plikten til å gjennomføre og dokumentere kundetiltak følger av hvitvaskingsloven § 9, og de skal gjennomføres i henhold til §§ 10–20 samt § 24 for løpende kundetiltak. Tilsynsrapportene viser at generiske kundeerklæringer gir et svakt grunnlag for risikoklassifisering og overvåking, og at tilpasning av tiltak til den konkrete risikoen ved kunden ofte kan bli for overfladisk. Særlig fremheves mangelfull informasjonsinnhenting om kundeforholdets formål og tilsiktede art, midlenes opprinnelse, rollen og identiteten til reelle rettighetshavere, samt personer som handler på vegne av kunden. Tilsynet peker på at gruppe- eller konsernklassifiseringer ikke kan erstatte individuelle vurderinger for den

enkelte juridiske enhet. Forsterkede tiltak må være risikoriktige og rettet mot forhold som faktisk er knyttet til høy risiko, herunder PEP-relasjoner, høyrisikogeografi og tidligere mistenkelige forhold.

Når det gjelder løpende oppfølging, kritiseres ensidig vekt på periodisk innhenting av skjemaer og automatisk modellscoring uten tilstrekkelige manuelle, risikobaserte kontroller ved endringer, avvik og alarmer. I bank er det avdekket svakheter i risikoklassifiseringsmodeller som fører til feilklassifisering og manglende utløsning av forsterkede tiltak, samt utilstrekkelig kalibrering og dokumentasjon av terskelverdier i transaksjons-overvåkingen. Tilsynet understreker at foretak må kunne påvise at treffsikkerhet og dekningsgrad i overvåkingen samsvarer med identifiserte risikoer, herunder kombinasjonsrisiko. I vurderingen av nærmere undersøkelser etter § 25 vektlegges behovet for klar terskel- og prosessforståelse, simultan håndtering av kundetiltak og undersøkelser, samt dokumenterte og begrunnede konklusjoner, herunder rettidig rapportering og etterlevelse av avsløringsforbudet. Overordnet presiseres det at høyrisikokunder krever hyppigere og mer dyptgående oppfølging, og at alarmer ikke kan lukkes på grunnlag av en oppdatert kundeerklæring alene.

Observasjoner fra tilsyn:

- Kundeopplysninger er ofte for generelle og gir dårlig grunnlag for risikoklassifisering med særlige mangler på:
 - formål og tilsiktet art
 - midlenes opprinnelse
 - reelle rettighetshavere
- Innhenting av dokumentasjon og legitimasjon er mangelfull eller gjøres i etterkant av et utført oppdrag eller en transaksjon.
- Gruppe/konsernvurderinger brukes i stedet for for individuelle vurderinger for enkelte juridiske enheter.
- Transaksjonsovervåkingen er ofte for mekanisk, med dårlig kalibrerte modeller og svake manuelle kontroller.
- Alarmer lukkes uten reell vurdering av om underliggende aktivitet for alarmen gir mening.

Identifiserte forbedringsområder:

- Kunde kjennskap må være konkret, risikobasert og dokumentert – spesielt for høyrisikokunder. Det må gjøres en reell og konkret vurdering av risiko. Gjengivelse av fakta og informasjon om kunden er ikke tilstrekkelig.

Kompetanse og opplæring

Opplæringsplikten i hvitvaskingsloven § 36 adresseres i tilsynsrapportene gjennom å sette krav til planlagt, rolletilpasset og virksomhetsnær opplæring. Tilsynet etterlyser dokumentasjon av innhold, målgruppe, frekvens og gjennomføring, samt sporbar kobling til foretakets risikovur-

dering, gjeldende trusselbilde og sanksjonsregelverket. Det fremheves at opplæringen må tilpasses ulike roller, inkludert styret, og sikre forståelse av skillet mellom forsterkede kundetiltak og nærmere undersøkelser (særlig for eiendomsmeglerforetak). I enkelte revisjons- og regnskapsforetak fremheves manglende grunnopplæring i hvitvasking og terrorfinansiering, foretaksspesifikke sårbarheter og bransjerisiko, samt revisors og regnskapsførers særlige plikter og kontroller. Flere rapporter identifiserer mangelfull eller udokumentert opplæring som medvirkende årsak til etterlevelseseffekt.

Observasjoner fra tilsyn:

- Opplæring er ofte udokumentert eller for generell.
- Mangler tilpasning til roller og virksomhet.
- Svak forståelse av forskjellen mellom forsterkede tiltak og nærmere undersøkelser.

Identifiserte forbedringsområder:

- Opplæring må være planlagt, dokumentert og risikospesifikk. Opplæringen bør ta hensyn til utvikling og trender innenfor hvitvaskingsområdet for å ruste de ansatte til å kunne fange opp mistenkelige forhold i sitt daglige arbeid.

Internkontroll:

Finanstilsynet legger stor vekt på internkontrollen etter hvitvaskingsloven § 35. Funnene i 2025 inkluderer lav frekvens og dekning av kontroller i førstelinje sett opp mot risiko og virksomhetens art og omfang, samt behov for mer planmessige og metodiske kontroller som vurderer innhold og skjønnsutøvelse, ikke bare dokumentinnhenting. Det etterlyses tydelige krav til kontrollplaner som over tid dekker alle sentrale plikter, kompetansekrav for de som kontrollerer, sporbare stikkprøver med klare kriterier, og systematisk oppfølging med ansvar, frister og effektmåling. Rapportering til styret må gi et reelt bilde av etterlevelsen i forretningsområdene, herunder avvik, tiltaksstatus og vurdering av tiltakseffekt. Tilsynet fremhever også betydningen av tydelige roller og ansvar, inkludert utpeking av hvitvaskingsansvarlig og avgrensning mot etterlevelseseffekt- og risikofunksjoner, samt uavhengig rapportering til styret per forretningsområde.

Observasjoner fra tilsyn:

- Kontrollene er for få, for overfladiske og lite risikobaserte.
- Manglende kontrollplaner og sporbarhet.
- Styre og ledelsen får ofte ikke dekkende og god rapportering, og i den forbindelse utilstrekkelige beslutningsgrunnlag.

Identifiserte forbedringsområder:

- Internkontrollen må være systematisk, dokumentert og gi styret et realistisk bilde av risiko på området.

05 Geografisk risiko

Geografisk risiko er en sentral faktor i vurderingen av hvitvaskingsrisiko og terrorfinansieringsrisiko, og utgjør et av de risikoelementene med store endringering som rapporteringspliktige må forholde seg til. EU oppdaterer jevnlig sine lister over høyrisikoland basert på landenes evne til å etterleve internasjonale standarder for antihvitvasking og terrorfinansiering, slik de fastsettes av Financial Action Task Force (FATF). Endringer i disse vurderingene påvirker direkte hvilke kundeforhold og transaksjoner som krever forsterkede tiltak, og danner dermed et viktig grunnlag for organisasjonens risikostyring.

Med dette som bakteppe følger nedenfor en samlet og oppdatert oversikt over EUs høyrisikoliste,¹⁶ listen over ikke-samarbeidende jurisdiksjoner, FATFs grå- og svartelister¹⁷ samt sentrale endringer i sanksjonsregimet mot Russland, alle faktorer som er relevante for virksomhetens risikovurderinger i 2026.

EUs høyrisikoland for hvitvasking og terrorfinansiering

Banker og andre rapporteringspliktige virksomheter har et særlig ansvar for å vurdere geografisk risiko. Når et kundeforhold eller en transaksjon involverer et høyrisikoland, skal virksomheten:

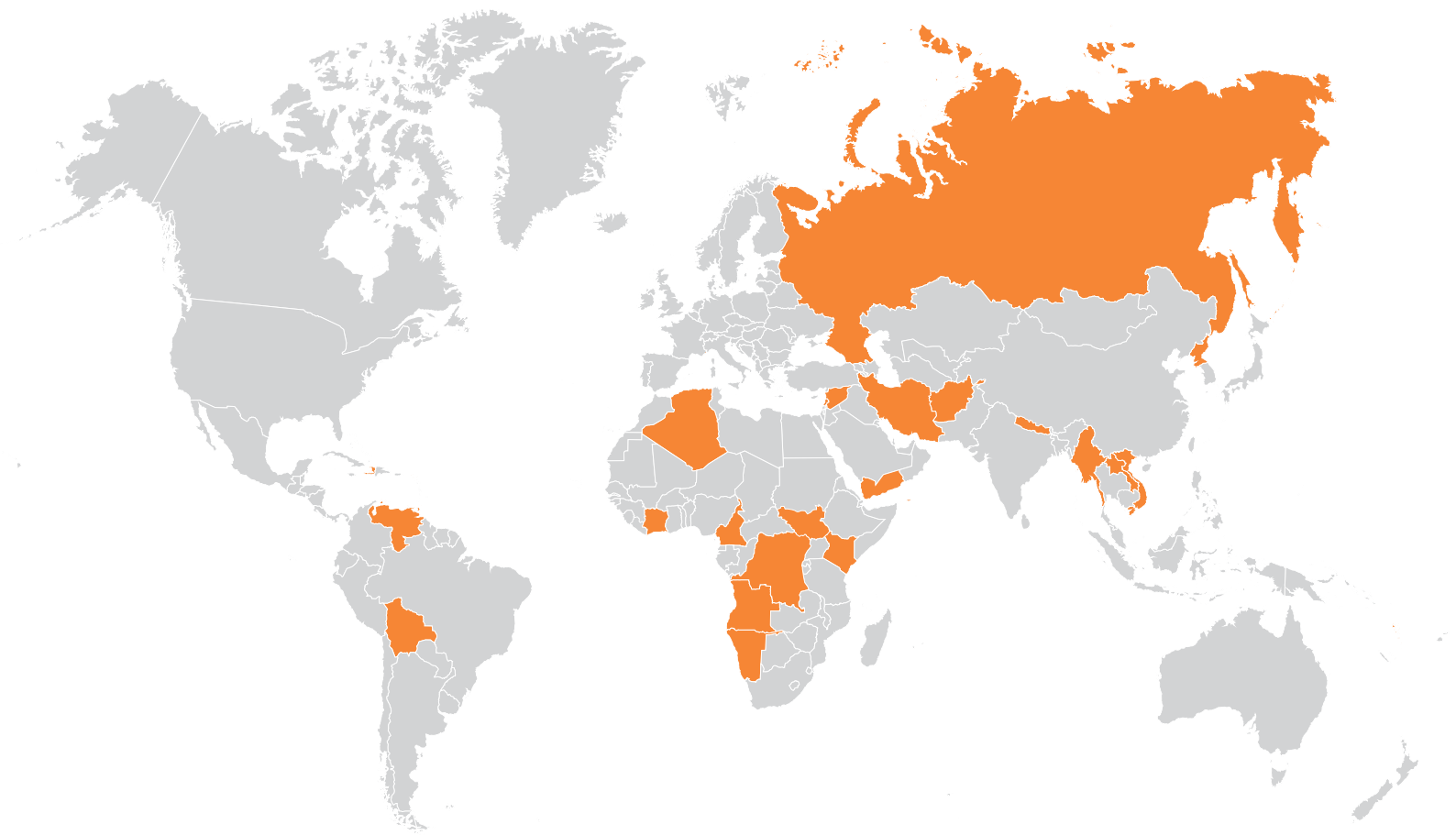
- gjennomføre forsterkede kundetiltak
- følge opp transaksjoner tettere
- dokumentere vurderinger og tiltak tydelig.

¹⁶Den europeiske kommisjon, High-risk third countries for AML/CFT, 29 januar 2026, link: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-counteracting-financing-terrorism-international-level_en

¹⁷Financial Action Task Force (FATF), Jurisdictions under increased monitoring, 24th of October 2025, link: <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>

EUs høyrisikoland

Dette er land utenfor EU som har store mangler i sine systemer for å bekjempe hvitvasking av penger og finansiering av terrorisme, og som derav utgjør en betydelig trussel mot EUs finansielle system. Ved utgangen av januar 2026 var følgende land på listen:



Land	Ikrafttredelsesdato
Afghanistan	23.sep.16
Algerie	05.aug.25
Angola	05.aug.25
Bolivia	05.des.25
De britiske jomfruøyene (BVI)	05.des.25
Kamerun	18.okt.23
Den demokratiske republikken Kongo	16.mar.23
Haiti	13.mar.22
Iran	23.sep.16
Elfenbenskysten (Côte d’Ivoire)	05.aug.25
Kenya	05.aug.25

Laos	05.aug.25
Libanon	05.aug.25
Monaco	05.aug.25
Myanmar	01.okt.20
Namibia	05.aug.25
Nepal	05.aug.25
Nord-Korea	23.sep.16
Russland	20.jan.26
Sør-Sudan	13.mar.22
Syria	23.sep.16
Trinidad og Tobago	06.mar.18
Vanuatu	23.sep.16
Venezuela	05.aug.25
Vietnam	18.okt.23
Jemen	23.sep.16

EUs liste over ikke-samarbeidende jurisdiksjoner

Denne listen vurderer land ut fra skatteåpenhet og samarbeidsvilje. Land på listen anses å ikke oppfylle internasjonale krav til åpenhet, rettferdig beskatning og tiltak mot skatteomgåelse.¹⁸

1. American Samoa
2. Anguilla
3. Fiji
4. Guam
5. Palau
6. Panama
7. Russland
8. Samoa
9. Trinidad og Tobago
10. De Amerikanske jomfruøyene
11. Vanuatu

Financial Action Task Force (FATF)

FATF er den internasjonale standardsetteren på området og den viktigste globale institusjonen som overvåker landrisiko for hvitvasking og terrorfinansiering. På plenumsmøtet i oktober 2025 ble det gjort følgende oppdateringer:

- Flere land ble fjernet fra grålisten etter fremgang
- Fire nye land ble satt på grålisten
- Svartelisten ble videreført uten endringer

¹⁸Council of the European Union, EU list of non-cooperative jurisdictions for tax purposes, 2025, link: <https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/>

4 ↑

Fire nye land ble lagt
til i Grålisten

3 ↓

Tre land ble fjernet
fra Grålisten

- Det kom en ny veiledning for tilbakeføring av midler
- Risikoen ved bruk av ny teknologi, som AI og deep fakes, ble trukket frem.

Følgende nye land har i løpet av 2025 blitt grålistet:

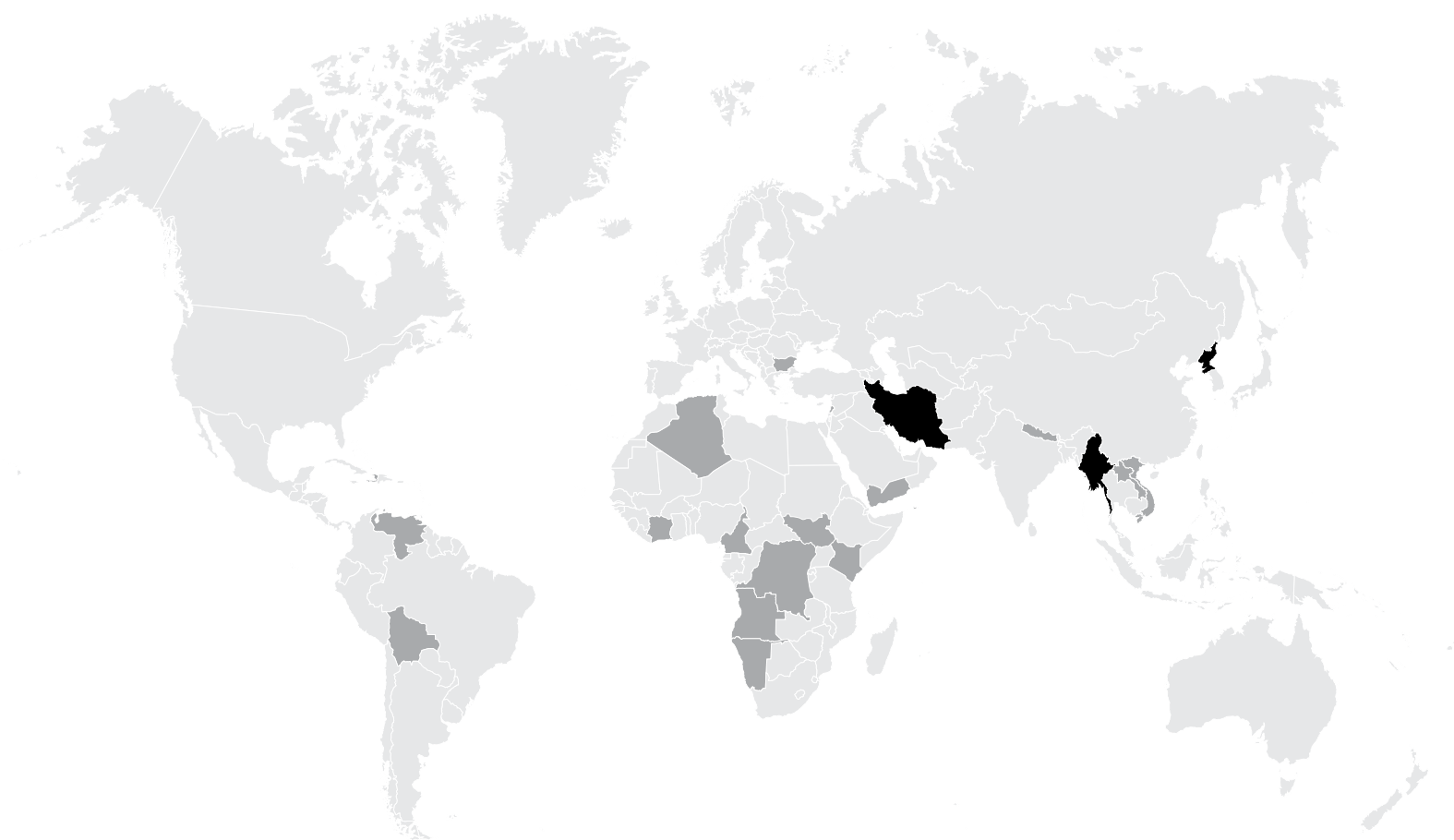
1. Bolivia
2. Haiti
3. Syria
4. De britiske jomfruøyene (BVI)

Følgende land er ikke underlagt økt overvåkning av FATF lenger (fjernet fra grålisten):

1. Burkina Faso
2. Mosambik
3. Nigeria

Status per siste FATF plenum 24. oktober 2025 er nå:

Gråliste:



1. Algeria
2. Angola
3. Bolivia
4. Bulgaria
5. Kamerun
6. Elfenbenskysten (Côte d'Ivoire)
7. Den demokratiske republikken Kongo
8. Haiti
9. Kenya
10. Laos
11. Libanon
12. Monaco
13. Namibia
14. Nepal
15. Sør-Sudan
16. Syria
17. Venezuela
18. Vietnam
19. De britiske jomfruøyene (BVI)
20. Yemen

Svartelisten (uendret):

1. Den demokratiske folkerepublikken Korea (Nord-Korea)
2. Iran
3. Myanmar

Status: Sanksjoner mot Russland

I september 2025 la EU fram sin 19. sanksjonspakke mot Russland¹⁹ og for første gang ble digitale valutaer rammet.²⁰ EU strammet inn på transaksjoner i krypto og mot kryptoplattformer spesifikt for å hindre at sanksjoner omgås gjennom disse virkemidlene. Videre stanset EU import av russisk flytende naturgass (LNG), senket pristaket på russisk råolje til 47,6 dollar per fat, og svartelistet 118 nye skip i Russlands «skyggeflåte» (som nå er på over 560 fartøy totalt).

Store energiselskaper som Rosneft og Gazpromneft fikk også totalforbud mot transaksjoner i EU, og flere banker i Russland og tredjeland nektes nå å gjøre oppgjør. Målet er å «skru av kranen» for russiske inntekter, etter en periode med store drone- og missilangrep mot Ukraina

¹⁹VG - Historisk sanksjonspakke fra EU: – På tide å skru av kranen

²⁰Council of the European Union, EU restrictive measures against Russia – sanctions packages, 2025–2026, link: <https://www.consilium.europa.eu/en/policies/sanctions-against-russia/>

og krenkelser av EU-luftrom i Polen og Romania. Russlands oljeinntekter i Europa har falt med 90 prosent de siste tre årene, og sanksjonene justeres fortløpende for å holde tritt med forsøk på omgåelse og presse Russland til reelle forhandlinger om en varig fred.

For Norges del innførte regjeringen i oktober 2025 nye sanksjoner som speiler EUs 18. sanksjonspakke. Norge har også sluttet opp om EUs 19. sanksjonspakke,²¹ og arbeidet med å gjennomføre disse reglene i norsk rett pågår. I praksis betyr dette at Norge forbereder tilsvarende innstramminger i krypto, energi og finans som EU har vedtatt, slik at norske og europeiske tiltak henger sammen og får størst mulig effekt. Status nå er altså at EUs 19. pakke gjelder i EU, mens Norge er i ferd med å innføre de samme reglene nasjonalt. I praksis er det ikke uvanlig med noe tidsforskyvning mellom EU-vedtak og norsk ikrafttredelse, men norske sanksjoner følger i hovedsak EU.

I 2026 er den 20. sanksjonspakken også på vei fra EU og det forventes fullt forbud mot å yte maritime tjenester til skip som frakter russisk olje. Siden om lag en tredel av Russlands oljeeksport bruker vestlige shipping-tjenester, ofte fra Hellas, Kypros og Malta, er målet at forbudet skal kutte denne kanalen.

Oppsummering

Sanksjonene mot Russland ble ytterligere skjerpet i 2025 og forventes strammet inn ytterligere i 2026, med særlig fokus på krypto, energi og maritime tjenester. Målet er å tette smutthull i hele verdikjeden og hindre omgåelse via tredjeland. Ettersom den geopolitiske situasjonen i verden endrer seg raskt, blir dette et viktig område å følge med på for rapporteringspliktige i 2026.

Våre 3 råd for rapporteringspliktige i 2026:

- Hold dere løpende oppdatert på EU-vedtak og på hvor Norge ligger i prosessen med sin gjennomføring av sanksjonspakkene. Oppdater raskt sanksjonslister, rutiner og kontrakter ved vesentlige endringer. Direktoratet for eksportkontroll og sanksjoner (DEKSA) er en god kilde.
- Vurder kontinuerlig risiko i kundeporteføljen og verdikjedene til deres kunder (motparter, eierskap, og tjenester), særlig shipping/forsikring/finans i Hellas, Kypros og Malta er ansett som utsatt.
- Vær oppmerksom på forsøk på omgåelser via naboland/tredjeland (re-eksport, frontelskaper, alternative betalingsløp).

²¹ Regjeringen.no, Norge slutter opp om EUs sanksjoner mot Russland, 2025, link: <https://www.regjeringen.no/no/aktuelt/norge-slutter-opp-om/id3114560/>



06

Politiets trusselvurdering for 2025

Hvorfor trusselvurderingen betyr noe?

Politiets årlige trusselvurdering tegner et samlet og oppdatert bilde av kriminaliteten i Norge, hva som driver den, hvordan den har utviklet seg, og hvilke trusler som kan ramme oss i året som kommer.²² Den gir et felles kunnskapsgrunnlag for myndigheter, næringsliv og innbyggere, slik at forebygging og beredskap kan målrettes der sårbarheten er størst. Vi håper at oppsummeringen gir rapporteringspliktige et innblikk i et oppdatert trusselbilde som styrker grunnlaget for å gjøre nødvendige justeringer i risikovurderinger, kundetiltak og transaksjonsovervåking for å fange opp reelle risikoer.

Drivkreftene bak kriminaliteten

Krigene og konfliktene i verden merkes også her hjemme. Migrasjon skaper sårbarhet som kriminelle utnytter, mens sanksjoner åpner rom for aktører som tilbyr ulovlige tjenester tilknyttet omgørelser. Polariseringen i samfunnet tiltar, og risikoen for utenlandsk påvirkning og statlig støttede angrep mot norsk infrastruktur vurderes som mer reell enn tidligere.

Samtidig gir digitaliseringen kriminelle et større handlingsrom. AI visker ut skillet mellom ekte og fabrikkert innhold og brukes til å produsere alt fra syntetisk overgrepsmateriale til falsk dokumentasjon som benyttes i sofistikerte bedragerier.

Økonomisk press med høy inflasjon og renter driver pengemotivert kriminalitet og gjør enkelte barn og unge mer utsatt for rekruttering og vold²⁵. Klimaendringer endrer fiskebestander og kvoter og kan utløse mer fiskerikriminalitet og handel med truede arter i tiden som kommer²⁵.

Kriminalitetsbildet i 2024

For første gang på flere år økte narkotikakriminaliteten, med tegn til normalisering av kokain i enkelte urbane miljøer og risiko for overgang til potente syntetiske opioider. Særlig innførsel via post er tiltagende.

Voldslovbrudd steg, drapstallene var over tiårssnittet, og politiet ser med bekymring spesielt på vold begått av mindreårige.

Økonomisk kriminalitet hadde den sterkeste veksten, særlig drevet av digitale bedragerier, mens vinningskriminalitet fortsatt er mest anmeldt. Når det gjelder miljøkriminalitet var det færre anmeldelser, delvis fordi administrative sanksjoner brukes mer, men turisme-relaterte lovbrudd fortsatte å øke. Cyberkriminalitet er vanligere, tross store mørketall, mens seksuallovbrudd gikk ned.

²² Politiet, Politiets trusselvurdering 2025, link: <https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2025.pdf>

Samfunnstruende trusler fremover

De mest fremtredende truslene er ifølge rapporten transnasjonale nettverk som utnytter anonymisering og digital infrastruktur til narkotika, vold, menneskesmugling og dataangrep. Videre er innsideproblematikk i næringsliv og offentlig forvaltning, som undergraver tillit og verdier, samt bruk av teknologi i forbindelse med overgrep mot barn, særlig fremtredende. Spesielt bruken av syntetisk overgrepsmateriale til utpressing utmerker seg på området.



POLITIET
OSLO POLITIDISTRIKT

**KAMERAOVERVÅKET
OMRÅDE**



07 PSTs Nasjonal Trusselvurdering 2025

PSTs Nasjonal trusselvurdering 2025 er den årlige analysen av trusler mot Norge innen statlig etterretning, sabotasje, påvirkning, ekstremisme og terror.²³ Den gir virksomheter et oppdatert bilde av hvem som truer, med hvilke metoder og mot hvilke mål, slik at innsikten kan omsettes til konkrete prioriteringer i sikkerhet, etterlevelse og beredskap.

Statlig etterretning og sabotasje

PST vurderer utenlandsk statlig etterretning som en av de mest alvorlige truslene i 2025. Russland og Kina er hovedaktørene, med forventet aktivitet også fra Iran og Nord-Korea. Russlands behov for å omgå sanksjoner driver skjulte anskaffelser av varer, tjenester og teknologi, og risikoen for sabotasje er høyere enn i fjor. Vestlige land registrerte en rekke sabotasjeaksjoner i 2024, og lignende hendelser kan også ramme norske interesser. Spenningen i nordområdene gjør norske næringslivsledere mer utsatt for russisk etterretning og påvirkning. Kina utgjør en betydelig og økende trussel, med vekt på cyberspionasje og forsøk på å rekruttere næringslivsaktører for innsyn i politiske prosesser. Viktige virkemidler er økonomiske, som strategiske investeringer i logistikk som kan gi langsiktig tilstedeværelse, eksempelvis Kirkenes havn.

“Et nært og godt samarbeid med andre samfunnsaktører er avgjørende for at vi lykkes i å motvirke truslene vi står overfor?”

Beate Gangås

Sjef PST

Terror og ekstremisme

PST vurderer terrortrusselnivået i Norge som moderat. Den mest alvorlige terrortrusselen kommer fortsatt fra ekstreme islamister og høyreekstremister. Aktiviteten blant ekstreme islamister økte i 2024, påvirket av internasjonale konflikter, særlig krigen i Gaza, og oppfordringer fra IS og al-Qaida. Norge er ikke et prioritert mål, men angrep kan rettes mot tilfeldige sivile, institusjoner og grupper i fiendebildet eller mot aktører som oppfattes å krenke islam. Slike hendelser kan gi direkte skader og store indirekte konsekvenser for virksomheter, fra omdømme til drift.

²³ Politiets sikkerhetstjeneste (PST), Nasjonal trusselvurdering 2025, link: <https://www.pst.no/wp-content/uploads/2026/01/Nasjonal-trusselvurdering-2025.pdf>

Myndighetspersoner og påvirkning

Voldelige angrep mot myndighetspersoner vurderes som lite sannsynlig men hets og trusler forventes å øke, særlig rundt stortings- og same-tingsvalget. Myndighetspersoner er også attraktive mål for utenlandsk etterretning.

Terrorfinansiering via Norge

PST mener at midler kanaliseres fra Norge til terrorformål i utlandet. I økende grad brukes kanaler og aktører som ikke er rapporteringspliktige i Norge, inkludert kryptovaluta og utenlandske finansinstitusjoner som rekrutterer kunder via internett. PST forventer at denne utviklingen vil fortsette, og at markedet for betalingsformidling og overføringer vil være i kontinuerlig endring.

Våre 2 råd for rapporteringspliktige i 2026:

1. Risikovurdering og operasjonalisering: Bruk den virksomhets-innrettede risikovurderingen aktivt som styrings- og læringsverktøy. Oppdater jevnlig, og sørg for opplæring som gir tydelige priorite-ringer og tiltak i virksomheten.
2. Systematisk kompetanseheving: Integrer løpende innsikt om utvikling og modus i opplæringen, slik at trusselbildet forankres og omsettes til handling i det daglige.



08 AI som støtte i arbeidet mot økonomisk kriminalitet

Banker bruker betydelige ressurser på AML-aktiviteter for innhenting av kundeinformasjon, utførelse av kundetiltak, screening og i den løpende transaksjonsmonitoreringen.²⁴ Det er identifisert at agentisk AI kan endre dagens prosesser og samtidig gi både effektivisering og kvalitetsheving. Agentisk AI representerer en videreutvikling av analytisk AI og tilbyr automatisering og økt produktivitet gjennom hele kundens livssyklus. I motsetning til tradisjonell AI, kan agentiske AI-agenter samarbeide for å utføre komplekse oppgaver autonomt, fra start til slutt. Dette innebærer et paradigmeskifte der banker kan ta i bruk en «arbeidsstyrke» av AI-agenter som kan ta beslutninger og handle selvstendig. AI-agentene kan utføre hele eller deler av prosesser og aktuelle bruksområder vil kunne være

- Automatisering av kundeetablering for både personkunder og bedrifter
- Transaksjonsovervåkning
- Sanksjons- og svindeletterforskning.

Vi har sett nærmere på hvordan AI kan bidra til forbedringer i transaksjonsovervåkingen.

“Our track record shows that for 25% to 75% of all alerts a manual investigation can be limited or even avoided.”

PwC Poland

Transaksjonsovervåkning - utfordringen med falske positive treff

Transaksjonsovervåkning er et krav i hvitvaskingsloven § 8 – krav om løpende oppfølging av kunder og transaksjoner.²⁵ Tradisjonelle, regelbaserte systemer har ofte utfordringer med at de gir et høyt antall falske positive treff. Falske positive er en utfordring da det medfører merarbeid og øker risikoen for at man overser reell risiko. Hvitvaskingsforskriften sier at alarmer ikke kan lukkes automatisk uten manuell vurdering, men i dag er denne oppgaven mer manuell enn den kan forventes å være i fremtiden.

²⁴ McKinsey & Company, How agentic AI can change the way banks fight financial crime, 2024, link: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-agentic-ai-can-change-the-way-banks-fight-financial-crime>

²⁵ Lovdata, Hvitvaskingsloven § 8 og § 24, konsolidert versjon 2024, link: [Lov om tiltak mot hvitvasking og terrorfinansiering \(hvitvaskingsloven\) - Lovdata](#)

Utviklingen går fort og i dag vil de fleste ha løsninger basert på statiske regler og terskler med begrenset konfigurasjon som gir mange unødige alarmer og lav presisjon, særlig når komplekse modus og kombinasjonsrisiko skal identifiseres. Samtidig endres kriminelle modus raskt. Det er ofte krevende å teste og validere nye regler før de tas i bruk og justering tar derfor lang tid.

Prosessene knyttet til transaksjonsmonitorering er ofte tunge og manuelle og det brukes i dag betydelige ressurser. Det er uklart hvor stor andel av de kriminelle pengestrømmene man faktisk fanger opp med dagens modeller alene. Mange arbeidsprosesser krever oppslag i flere systemer og består av skriftlig saksbehandling. Dette øker både risiko for operative feil og muligheter for utnyttelse gjennom interne misligheter.

Hvordan vil AI kunne påvirke transaksjonsovervåkingen?

Transaksjonsovervåking er et område som kan få god effekt av AI. Det er flere analyser som anbefaler å supplere tradisjonelle rammeverk med mer avansert teknologi, herunder AI og forbedret datakvalitet. Områder som bør vil være aktuelle å vurdere for AI-muligheter.

Regeljustering

AI og maskinlæring kan evaluere og justere eksisterende regler og terskler basert på sanntidsdata, historiske data og nye mønstre. Dette forventes å forbedre analysen av normal vs mistenkelig aktivitet og redusere falske positive. Kombinert med tilbakemeldinger fra Økokrim på kvaliteten av meldte saker vil dette gi bedre læringssløyfer og mer presise treff over tid.

Bistand i vurdering av alarmer og rapportering av mistenkelige forhold

AI kan hente og sammenstille informasjon fra interne og eksterne kilder og automatisk utforme strukturerte oppsummeringer og rapporter. Automatisert innhenting og utfylling av nøkkelinformasjon til rapporter og utkast til vurderinger om mistenkelige forhold reduserer manuelt arbeid og feil, og styrker etterlevelsen. Dette gir saksbehandlere raskere oversikt og bedre kontekst. Kvaliteten sikres ved at et menneske gjør kvalitetskontroll og endelig vurdering, såkalt «human in the loop».

AI-drevet kundesegmentering

Segmentering etter atferd og risikoprofiler gjør det mulig å prioritere alarmer på en smartere måte og rette overvåkingen mot områder der tradisjonelle systemer har svak dekning.

Agentisk AI og hentingsforsterket generering (Retrieval-Augmented- Generation (RAG))

Autonome AI-løsninger kan utføre avgrensede oppgaver, planlegge arbeidsflyter, hente og validere data, overvåke prosesser og sammenstille analyser. Hentingsforsterket generering (RAG) har tilgang til bedriftens egne dokumenter eller data og søker i et bedre datagrunnlag. Det gjør at det kan hentes ut bedre og mer presis informasjon som utgangspunkt for svarene som genereres. Dette sikrer presisjon og etterprøvbarehet ved å hente relevant informasjon fra interne og eksterne kilder før analyser eller forslag lages. Dette gir produktivetsgevinster og mer konsistent kvalitet, samtidig som mennesker kan håndtere avvik og sikre styring med prosesser og AI agenter.

AI-støttet faglig sparring

AI kan foreslå relevante momenter og risikoreduserende tiltak basert på regelverk, veiledning og interne rutiner. Dette gir mer konsistente og etterprøvbare vurderinger, samtidig som beslutningsansvaret forblir hos mennesker.

Nye kompetansekrav

Økt bruk av tekniske støtteverktøy med bruk av både agentisk og generativ AI vil også medføre økt kompetanse i virksomhetene. Dette vil omfatte et større behov for dataanalyse- og compliancekompetanse både i operasjonelle og kontrollerende miljøer. Det vil også være viktig å dokumentere hvordan støttesystemene kontrolleres, blant annet gjennom governance-struktur, ansvarsfordeling, prosesser og regelvalidering.

Suksessfaktorene og risiko knyttet til AI

Foretak som lykkes, kombinerer teknologi med tydelige rammer for styring, data og kompetanse. Følgende fem områder bør prioriteres:

- **Mennesker:** AML-fag og risiko-/dataferdigheter, samt kompetanseheving knyttet til bruk av nye verktøy
- **Prosess:** Klarhet i hvordan AI inngår i prosesser og tydelige grenser for automatisering og når menneskelig validering er nødvendig
- **Teknologi:** Skalerbar arkitektur, tilgang til modeller og data via API-er
- **Data:** Datakvalitet og økt bruk av ustrukturerte kilder
- **Endringsledelse:** Roller, opplæring og gradvis implementering med måling av effekt og gevinstrealisering.

Det er risikofaktorer knyttet til implementering av AI og det er viktig å ha en gjennomtenkt tilnærming til bruken. AI bør ikke brukes kun som et parallelt verktøy, men innlemmes i risikovurdering, kundetiltak og oppfølging.

Funn fra PwCs EMEA AML Survey 2024

28 %

av respondentene oppga at ansatte med AML-kompetanse er den mest effektive kontrollen. Til tross for økende fokus på teknologi, er den menneskelige faktoren fortsatt svært viktig.

35 %

mener at mangelen på kompetanse er en av de største hindringene for økt bruk av ny teknologi i deres AML-prosesser.

55 %

av respondentene vil bruke mer enn 10 % av AML-budsjettet sitt på digitale verktøy i løpet av de neste 2 årene.

69 %

av respondentene mener at det å ha samme standard på tvers av land/bransjer vil forbedre deres AML-effektivitet betydelig.

Hva er dine største utfordringer på AML området? (Top 5 Svar)*

Økt regulatorisk press



Datastyring og datakvalitet



Regelverk som kompliserer operasjonelle prosesser



Automatisering av prosesser som er manuelle eller fragmenterte



Oppdatering av KYC-dokumentasjon



EMEA Norden

*PwC EMEA AML Survey 2024



Områder med potensiale for anvendelse av AI i AML-arbeid og forebygging av finansiell kriminalitet



Tydelig strategi, god styring, kontroll og tydelig rollefordeling er essensielt for å unngå:

- Bruk av uautoriserte verktøy («skygge-IT»), med risiko for deling av sensitive data
- Manglende sporbarhet
- Uklare ansvarsforhold og feil bruk av AI
- Feilaktige eller hallusinerende resultater som påvirker beslutningsgrunnlaget

En moden tilnærming kombinerer AI-støtte med krav til etterprøvbarehet, kildebruk og menneskelig kontroll.

Oppsummering

AI gir foretak et reelt mulighetsrom til å redusere støy, øke presisjonen og bruke ressursene mer målrettet, samtidig som kravene til kontroll, dokumentasjon og etterprøvbarehet ivaretas. Etter vår erfaring vil gevinstene realiseres når teknologien kombineres med tydelige rammer for styring, datakvalitet og kompetanse, og når automatisering innføres med klart definert menneskelig ansvar. Slik kan transaksjonsovervåkning utvikles fra en ressurskrevende kontrollfunksjon til en datadrevet, risiko-basert kapabilitet som bedre oppfyller pliktene etter hvitvaskingsloven.

Våre 3 råd for rapporteringspliktige i 2026:

1. Identifiser mulighetsrommet for hvilke prosesser som kan forbedres med AI
2. Etabler en tydelig strategi, styring og kontroll med AI-verktøy og konkrete anvendelsesområder
3. Gjennomfør tiltak som sikrer kompetanseheving knyttet til AI for hele organisasjonen.



09 Svindel

Investerings- og kjærlighetssvindel tilbake i fokus

Bank- og finanssektoren er stadig preget av økt risiko for svindel mot kundene, et komplekst område med stadig omskiftelig risikobilde.²⁶

I 2025 advarer Finans Norge om følgende populære modus:

- **Investeringssvindel:** Svindlere frister med svært lukrative muligheter i kryptovaluta eller aksjer, og kundene lures til å investere penger de aldri får tilbake.
- **Kjærlighetssvindel:** Svindlere bygger tillit og innleder romantiske eller vennskapelige forhold via dating-apper eller sosiale medier, og ofrene lures til å overføre penger.
- **Gavekortsvindel:** Ofre blir bedt om å kjøpe fysiske gavekort i butikk og deretter sende disse til svindlerne. Dette moduset er ofte koblet til kjærlighetssvindel.

Norge har etablert et sterkt forbrukervern på svindelområdet. Likevel er en fellesnevner for de ovennevnte modusene at banken trolig ikke vil være pliktig til å tilbakeføre midler til kundene. Dette fordi bankenes tilbakeføringsplikt kun omfatter "ikke godkjente transaksjoner". Ved investerings-, kjærlighets- og gavekortsvindel vil kunden med viten og vilje godkjenne en transaksjon ut av sin egen konto og over til en motpart.²⁷ Av saker meldt inn til Finansklagenemnda (FinKN) gjenspeiles dette i en økning i andelen saker i favør av finansforetak i 2025.

Bankenes svindeltap:

Finanstilsynet rapporterer om svindelstatistikk fra norske betalings-tjenesteytere på halvårlig basis. Følgende statistikk er hentet fra rapporten for andre halvår 2024:²⁸

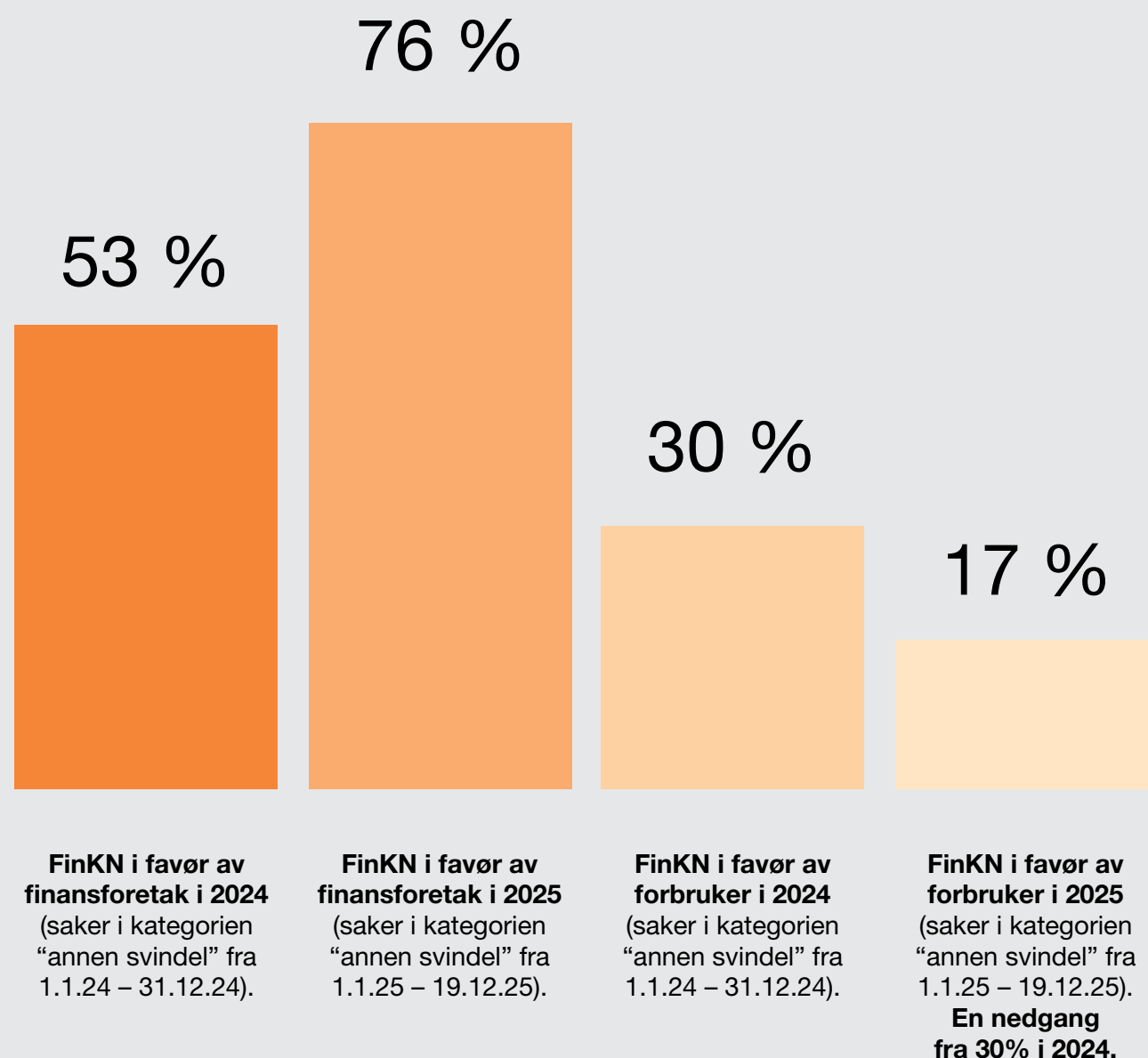
- Totale tap som følge av svindel har økt med 19% siden 2023, og med 157% siden andre halvår av 2021.
- Ca. to tredjedeler av tapene kommer fra kontosvindel, og én tredjedel fra kortsvindel, i likhet med tidligere år. Forhindrede tap knytter seg i størst grad til kortsvindel.
- Svindeltapene fordeler seg relativt likt mellom svindel der offeret manipuleres til å utføre transaksjonen selv (sosial manipulasjon) og svindel der svindleren selv initierer eller modifierer betalingen.

²⁶ Finans Norge, Nye svindeltrender: Dette advarer bankene mot nå, 2025, link: <https://www.finansnorge.no/artikler/2025/09/nye-svindeltrender-dette-advarer-bankene-mot-na/>

²⁷ Finansklagenemnda Bank (FinKN), Nemndsregister – saker om «annen svindel», 2024–2025

²⁸ Finanstilsynet, Svindelstatistikk – andre halvår 2024, link: <https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2024/h2/svindelstatistikk-andre-halvar-2024/>

Statistikk fra FinKN i 2025:



7% av sakene i 2025 er avvist eller ikke avgjort, mot 17% i 2024.

- Svindeltap som andel av den samlede transaksjonsverdien var 0,2%, hvilket er en økning på 25% fra 2023.

Bankene er avhengige av samspill og mulighet for informasjonsdeling seg imellom for å oppnå god sikkerhet på svindelområdet. Finansdepartementet har i september 2025 sendt ut et høringsnotat om finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet.²⁹

Oppsummering

Utviklingen i svindelbildet og de økende tapstallene, sammen med praksis fra Finansklagenemnda, viser at ansvaret i stor grad fortsatt legges på kundene når transaksjoner er godkjent av dem selv, selv i tilfeller der de har vært utsatt for manipulasjon. Dette tydeliggjør behovet for mer målrettet forebygging, videreutvikling av bankenes systemstøtte og tettere informasjonsdeling mellom banker og myndigheter, særlig i møte med stadig mer organiserte og teknologisk avanserte svindelforsøk i tiden fremover.

Våre 3 råd for rapporteringspliktige i 2026:

1. Etabler automatisk sperring av mistenkelige transaksjoner utenfor bankens åpningstider
2. Benytt AI for å detektere avvikende transaksjonsmønster
3. Etabler gode rutiner for logging av svindel og før statistikk. God oversikt over hvilke moduser som treffer banken vil gjøre det lettere å holde kundene informert.

²⁹ Regjeringen.no, Høring – finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet, 2025, link: <https://www.regjeringen.no/no/dokumenter/horing-finansforetaks-informasjonsdeling-for-a-bekjempe-okonomisk-kriminalitet/id3118997/>

10 Bedre datadeling i finanssektoren

Sandkasseprosjekter om informasjonsdeling

I 2025 har Finanstilsynet og Datatilsynet gjennomført fire sandkasseprosjekter som undersøkte handlingsrommet for informasjonsdeling mellom finansforetak for å bekjempe økonomisk kriminalitet. Resultatene ble presentert i februar 2026 og hovedkonklusjonen ble at Finansnæringen har større muligheter for datadeling enn tidligere antatt. Tilsvarende at GDPR i mindre grad er et hinder enn mange har trodd.

De fire prosjektene

Det første prosjektet, gjennomført av Eika Gruppen og KPMG, undersøkte mulighetene for informasjonsdeling mellom banker i anti-hvitvaskingsarbeidet. Prosjektet så på en sentralisert løsning for samarbeid på tvers av alliansen, og vurderte juridiske rammer for deling i tre faser: deteksjon av mistanke, utredning av mistenkelige forhold og kundevurdering. Konklusjonen var at det finnes gode muligheter for deling i utredningsfasen, men at dagens regelverk ikke åpner for felles datainnsamling for deteksjonsformål.

Finans Norge Forsikringsdrift undersøkte muligheten for å etablere en tipskanal for forsikringssvindel. Løsningen innebærer at publikum kan melde fra om mistanke via et nettbasert skjema, der overskuddsinformasjon og sjikanøse tips fjernes før videreformidling til riktig forsikringsselskap. Prosjektet konkluderte med at det er rettslig grunnlag for en slik løsning, med planlagt lansering i første halvdel av 2027.

Stø AS utforsket handlingsrommet for utvidet datainnsamling og -deling i antisvindelløsninger knyttet til elektronisk ID. Bakgrunnen er at BankID gir tilgang til offentlige tjenester, økonomiske midler og sensitiv informasjon, noe som gjør beskyttelse mot svindel kritisk. Prosjektet konkluderte med at Stø har rettslig grunnlag for å samle inn nye datapunkter, men pekte på behovet for klarere hjemler for sektorovergripende deling.

Det fjerde prosjektet samlet DNB, Nordea, SpareBank 1, Eika Gruppen og Norsk Regnesentral for å undersøke informasjonsdeling i bekjempelsen av betalingsbedrageri. Et sentralt funn var at banker opererer i siloer mens kriminelle ikke gjør det, og at finansforetaksloven gir større rom for deling enn bankene har trodd. Prosjektet resulterte i en datadelingsliste som beskriver scenarioer og datafelter for deling, samt planer om et pilotprosjekt med Nordic Financial CERT som sentralisert hub.

Sentrale funn

Prosjektene avdekket at det finnes et betydelig handlingsrom i gjeldende regelverk som finansnæringen ikke har utnyttet fullt ut. En gjennomgående erfaring var at mye av tilbakeholdenheten med å dele informasjon skyldes konservative tolkninger og usikkerhet, snarere enn faktiske juridiske hindre. Deltakerne identifiserte både reelle rettslige begrensninger og opplevde barrierer, der sistnevnte ofte har ført til at aktørene har sagt nei til datadeling uten at dette var nødvendig.

Prosjektene viste også at personvern fungerer som en viktig sikkerhetsmekanisme i datadelingen, men at GDPR ikke er det største hinderet for samarbeid. Det ble påpekt at den praktiske gjennomføringen av regelverket ofte er mer utfordrende enn selve jussen. Videre vil foreslåtte endringer i finansforetaksloven og EUs 6. AML-pakke åpne ytterligere muligheter for informasjonsdeling, særlig i deteksjonsfasen.

Erfaringene er brukt som innspill til Finansdepartementets høring om endringer i finansforetaksloven, med proposisjon forventet våren 2026. Vi er spente på hva som kan komme ut av dette arbeidet fremover.

EU forenkler datadeling i finanssektoren

I 2023 la Europakommisjonen frem et forslag om å revidere EU-regelverket for rapportering i finansielle tjenester og investeringsstøtte. Målet var å effektivisere datainnsamlingen, unngå dobbelt rapportering og redusere byrden for både myndigheter og finansinstitusjoner.³⁰ I oktober 2025 ble EU enige om en ny rapporteringsforordning som forenkler reglene for datadeling mellom de europeiske tilsynsmyndighetene, EBA, ESMA og EIOPA (ESAs), samt andre finansmyndigheter, samtidig som nye rapporteringskrav begrenses.³¹ Det er forventet at dette også vil forenkle rapporteringen og datadelingen for underliggende finansinstitusjoner. Forordningen gjelder ikke for Norge per i dag, men forventes å bli innlemmet i EØS-avtalen og få virkning for norske rapporteringspliktige på sikt.

30 European Commission, Better data sharing, 24 February 2025, link: <https://finreg.aoshearman.com/better-data-sharing-regulation-to-streamline-eu-f>

31 Council of the EU, Better data sharing: Council and Parliament strike deal, 17 December 2024, link: <https://www.consilium.europa.eu/en/press/press-releases/2024/12/17/better-data-sharing-council-and-parliament-strike-deal-on-financial-reporting-requirements/>

Hva innebærer forordningen?

Forordningen skisserer en integrert løsning med mulighet for et felles rapporteringssystem på tvers av sektorer, og innfører prinsippet om «Report Once». Dette betyr at tilsynsmyndigheter, med unntak av tidskritiske forespørsler, først skal sjekke om informasjon allerede finnes hos andre myndigheter før de ber om den på nytt. Målet er å redusere den administrative byrden for finanssektoren og tilsynsmyndigheter.

Forventet effekt på AML området

AMLA omfattes av forordningen: AMLA er eksplisitt nevnt blant tilsynsmyndighetene som pålegges å gjennomgå og foreslå fjerning av overflødig eller utdaterte rapporteringskrav. Dette betyr at AML-rapportering vil være en del av det overordnede forenklingsprogrammet.

”Report once”-prinsippet: Prinsippet om at myndigheter skal sjekke om informasjon allerede finnes før de etterspør den på nytt, vil også kunne gjelde for AML-relatert rapportering. Dette kan redusere dobbelt-rapportering der foretak i dag må levere overlappende informasjon til både Finanstilsynet og AML-myndigheter.

Datadeling mellom myndigheter: Forordningen legger til rette for trygg deling og gjenbruk av tilsynsdata mellom myndigheter. Dette kan styrke samarbeidet mellom AML-myndigheter og andre finanstilsyn, noe som er i tråd med ambisjonene i EUs 6. AML-pakke om bedre informasjonsutveksling.

Forordningen bør ses i sammenheng med EUs 6. AML-pakke, som innfører omfattende nye krav til rapportering og informasjonsdeling. Mens AML-pakken utvider rapporteringsforpliktelsene, skal denne forordningen sikre at det samlede rapporteringsregimet ikke blir unødvendig stort gjennom:

- Koordinering mellom ulike myndigheters krav
- Fjerning av duplikate rapporteringspunkter
- Felles standarder for dataformat og -kvalitet

For finansforetak som er underlagt hvitvaskingsregelverket kan forordningen på sikt bety:

- Færre tilfeller der samme kundeinformasjon må rapporteres til flere myndigheter
- Bedre koordinerte rapporteringskrav mellom Finanstilsynet, Økokrim (FIU) og eventuelle andre mottakere

- Mulighet for å melde inn opplevde duplikat- eller overflødige AML-rapporteringskrav til et permanent kontaktpunkt

Det gjenstår å se hvordan forordningen konkret vil implementeres på AML-området, og hvordan den vil samspille med de spesifikke rapporteringskravene i AML-pakken. Veikart for et felles, sektorkryssende integrert rapporteringssystem skal etter planen utredes innen 2030.

Oppsummering

Regelverksutviklingen for datadeling i finanssektoren viser en klar ambisjon om å effektivisere rapporteringsprosessene og styrke samarbeidet mellom europeiske tilsynsmyndigheter. Samtidig betyr dette også et mer konsistent og pålitelig datagrunnlag, noe som er særlig viktig for arbeidet innenfor antihvitvasking. Innføringen av «Report once» og mer felles dataløsninger reduserer unødvendig dobbeltarbeid og vil bidra til bedre kvalitet i informasjonen som brukes i risikovurdering og tilsyn. Med tydelige rammer for informasjonsdeling, kombinert med strenge krav til personvern og taushetsplikt, legger forordningen til rette for et mer målrettet og effektivt tilsynsarbeid – både nasjonalt og på tvers av Europa. Erfaringer fra sandkasseprosjektene viser i tillegg at et betydelig potensial ligger i selve praktiseringen av regelverket, og at klarere hjemler og felles tekniske løsninger vil være avgjørende for å realisere disse ambisjonene fremover.³²

Våre 3 råd for rapporteringspliktige i 2026:

1. Ha kontroll på data og datakvalitet.
2. Tydelig eierskap til data og rapportering i organisasjonen.
3. Oversikt over rapporteringskrav og prosesser for utføring og kvalitetssikring av rapportering.

³² Datatilsynet og Finanstilsynet, Sandkasseprosjekter om datadeling, 2026.



11

Krypto – den store nye trusselen?

Markedsutvikling og bruk

Markedet for kryptovaluta og digitale eiendeler har fortsatt sterk vekst og har i 2025 passert et globalt volum på over 4 billioner dollar.³³ Også i Norge rapporteres det om økt eierskap.³⁴

2025 omtales som et gjennombruddsår for institusjonell adopsjon av kryptovaluta, og flere store finans- og betalingsaktører har lansert eller annonsert kryptorelaterte produkter. En stor drivkraft er den økende bruken av Stablecoins, som nå har blitt den raskeste og billigste måten å sende en amerikansk dollar.

Stablecoins er imidlertid også identifisert som et sentralt risiko-element knyttet til økonomisk kriminalitet, og er ifølge analyseselskapet Chainalysis den foretrukne kryptovalutaen for sanksjonsomgørelser.³⁵

Bruken av krypto varierer geografisk:

- I industrialiserte økonomier dominerer investering og spekulasjon
- I enkelte utviklings- og høyrisikomarkeder brukes krypto som alternativ betalings- og verdilagringsmekanisme
- Teknologien benyttes særlig der nasjonal valuta er ustabil, og finansielle tjenester er begrenset.

Regulatorisk tilnærming

Økt bruk av krypto har forsterket behovet for regulering, men tilnærmingen er fortsatt fragmentert globalt. Dette skaper regulatorisk arbitrage og utfordrer effektiv risikohåndtering.³⁶

EU innførte MiCA-forordningen fra desember 2024. Regelverket skal styrke forbrukerbeskyttelse og redusere omgåelse gjennom lav-regulerte jurisdiksjoner. Det fremkommer imidlertid spørsmål om forholdsmessighet (særlig for mindre aktører) og hvordan grensekryssende kontroll av stablecoins skal håndteres. Den europeiske sentralbanken (ECB) jobber



Stablecoins er en type kryptovaluta der verdien er bundet til en annen mer stabil eiendel, for eksempel amerikanske dollar, norske kroner eller gull. Formålet er å skape en mindre volatil kryptovaluta som kombinerer sikkerheten og hastigheten til krypto med stabiliteten til tradisjonelle verdier

³³ Andreessen Horowitz (a16z Crypto), State of Crypto Report 2025, link: <https://a16zcrypto.com/posts/article/state-of-crypto-report-2025/>

³⁴ Skatteetaten, Over 54 000 oppgir at de eier kryptovaluta – dette er kommunene med flest kryptoeiere, 2025, link: <https://www.skatteetaten.no/presse/nyhetsrommet/over-54000-oppgir-at-de-eier-kryptovaluta--dette-er-kommunene-med-flest-kryptoeiere/>

³⁵ Chainalysis, The 2025 Crypto Crime Report, 2025, link: <https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf>

³⁶ International Consortium of Investigative Journalists (ICIJ), Cryptocurrency regulations: A global explainer, 2025, link: <https://www.icij.org/investigations/coin-laundry/cryptocurrency-regulations-global-explainer/>

med etablering av digitale sentralbankpenger (DSP) i euro.³⁷ Dersom Parlamentet vedtar nødvendig lovgivning, kan den digitale euroen lanseres i 2029.

Digitale sentralbankpenger (DSP) er elektroniske penger utstedt av sentralbanken i landets offisielle pengeenhet. En oversikt fra Atlantic Council viser at 137 land (inkludert valutaunioner) utforsker mulighetene til å opprette DSP. Lovgivere uttrykker likevel en viss skepsis, blant annet har Kina benyttet DSP for å omgå vestlige sanksjoner.³⁸

USA har valgt en annen strategi enn EU, med større vekt på private stablecoins og skepsis til DSP. Ulike strategier mellom store økonomier bidrar til et komplekst og uensartet regelverksbilde.

Kriminalitet og tilsynsutfordringer

Kryptovaluta benyttes, på linje med andre betalingsmidler, til økonomisk kriminalitet. Manglende harmonisering av regelverk og varierende modenhet hos markedsaktører forsterker risikoen.

Kryptobørser og tjenestetilbydere utgjør sentrale kontrollpunkter, men erfaringer fra 2025 viser betydelige svakheter, som

- Ujevn etterlevelse av antihvitvaskings- og terrorfinansieringskrav
- Mangelfull styring og internkontroll, også hos store aktører
- Høyprofilerte tilsynssaker som illustrerer systemiske svakheter, blant annet en bot på 21,5 millioner euro til kryptobørsen Coinbase, for brudd på hvitvaskingsregler.

Dette understreker behovet for robuste kontrollrammer, tydelig ansvars plassering og effektivt tilsyn i takt med økende integrasjon mellom krypto og det tradisjonelle finansielle systemet.

³⁷ The Sumsub, Luke Owaint Boulton, European Central Bank Moves to Accelerate Digital Euro Rollout with 2029 Target, 3rd of November 2025, link: <https://sumsub.com/media/news/european-central-bank-moves-to-accelerate-digital-euro/>

³⁸ Fondation Robert Schuman, Patrice Cardot, The digital euro at the dawn of a new monetary world, 4th of November 2025, link: <https://www.robert-schuman.eu/en/european-issues/809-the-digital-euro-at-the-dawn-of-a-new-monetary-world>

Oppsummering

Utviklingen innen kryptomarkedet i 2025 viser økende institusjonell adopsjon, sterk vekst i bruk av stablecoins og tettere kobling mot det tradisjonelle finansielle systemet. Samtidig forsterkes risiko knyttet til hvitvasking, sanksjonsomgåelse og svindel, særlig som følge av fragmentert regulering og varierende etterlevelse hos markedsaktører. MiCA representerer et viktig skritt mot harmonisering i EU, men effektiv risikohåndtering forutsetter robuste kontrollrammer, tydelig ansvar og tett tilsyn i takt med markedets videre utvikling.

Våre 3 råd for rapporteringspliktige i 2026:

1. Vurdering av egen risiko knyttet til krypto.
2. Hvordan kundetiltak skal utføres kundeforhold eller transaksjoner som involverer krypto, herunder dokumentasjonskrav.
3. Hvordan fange opp transaksjoner med krypto-involvering.



12 2025 og veien videre

2025 har gitt oss et mer sammensatt og dynamisk risikobilde enn noen gang.³⁹ I oppbygningen til det mange mener er en ny multipolar verdensordre utnytter kriminelle digitale verktøy, grensekryssende betalinger og komplekse nettverk samtidig for å berike seg. For å håndtere problemet forventes det nå mer av de rapporteringspliktige. Det som for mange har blitt ansett å være rent compliancepreget arbeid, skal fremover forankres i tiltak som reduserer risiko. Teknologi og data som gir bedre treffsikkerhet og krever god styring, riktig kompetanse og sporbarhet kommer i 2026 til å bli et veiskille: tempoet i regulering og gjennomføring øker, og forskjellen mellom minimumsetterlevelse og moderne, risikodrevet AML arbeid vil bare tydeligere.

Hva vi ser:

- **Risikobildet:** Flere kriminalitetsformer virker sammen og forsterker hverandre. Evnen til å se helheten på tvers av geografi, produkter og kanaler er avgjørende.
- **Regulering og tilsyn:** Forventningene er tydeligere og mer konsekvente. Generiske risikovurderinger og hyllevare-prosedyrer uten reell håndtering av risiko holder ikke lenger.
- **Teknologi:** AI, automatiserte prosesser og avansert analyse kan styrke etterlevelsen, men bare når de understøttes av god datakvalitet, klare roller og kompetanse.⁴⁰

Hvordan blir 2026?

I Europa peker ny regelverksutvikling og etableringen av felles strukturer mot et mer samordnet rammeverk, selv om det også finnes krefter som ønsker forenkling og mindre detaljstyring. I USA er signalene mer blandede, særlig rundt krypto og myndighetenes regulering og tilsyn av bransjen. Globalt ventes standardene å utvikle seg videre innen krypto, sanksjoner og åpenhet om eierskap, og land som ikke henger med vil fort oppleve svekket tilgang til internasjonale markeder.

I Norge ligger 2026 an til å bli et gjennomføringsår. Etter utredning i 2025, forventes lov- og forskriftsendringer som styrker registre, datakvalitet og informasjonsflyt, og som tydeliggjør ansvar og virkemidler for tilsynsmyndigheter å komme på plass. For rapporteringspliktige betyr dette høyere forventninger til virksomhetsspesifikke risikovurderinger, bedre dokumentasjon og mer presis rapportering. Overgangen fra mistenkelige transaksjoner til mistenkelige forhold markerer også et reelt skifte mot mer datadrevet, integrert og tidsnær rapportering.

³⁹ Nasjonal sikkerhetsmyndighet (NSM), Risiko 2025, link: <https://nsm.no/getfile.php/1314212-1738741587/NSM/Files/Dokumenter/Rapporter/Risiko%202025.pdf>

⁴⁰ ComplyAdvantage, State of Financial Crime 2025, link: <https://get.complyadvantage.com/insights/the-state-of-financial-crime-2025-download>

Den operasjonelle hverdagen

Mange virksomheter har hatt en kraftig kostnadsvekst i sitt AML-arbeid uten at kvaliteten nødvendigvis har økt. Særlig tre forhold går igjen:

- For mye manuelt og fragmentert arbeid
- Lag på lag med teknologi uten reell prosessforenkling
- Svakt samspill mellom risiko, compliance, IT og forretning.

Konsekvensen er at innsats ikke alltid treffer der risikoen er størst. 2026 bør derfor brukes til å gjøre arbeidet mer målrettet og effektivt. Vi anbefaler fokus på:

- Standardisering av prosesser
- Bedre dataintegrasjon på tvers av produkter og enheter
- Automatisering av manuelle prosesser
- Målrettet bruk av analyse og AI som et støtteverktøy
- Kompetanseheving, da nye verktøy gir liten verdi uten forståelse for både risikobildet og regelverket.

Start med å standardisere kjerneprosessene og rydde i grensesnittene mellom enheter. Sørg for at data flyter bedre på tvers av produkter og systemer, slik at det som oppdages ett sted raskt kan gi verdi et annet sted⁴³. Automatiser repetitive og regelstyrte oppgaver, og bruk analyse og AI der de faktisk forbedrer beslutninger, ikke som pynt. Til slutt: bygg kompetanse. Verktøy og data har liten verdi uten ansatte som forstår risikoene, kjenner mønstrene og kan omsette funn til riktig handling i det daglige.

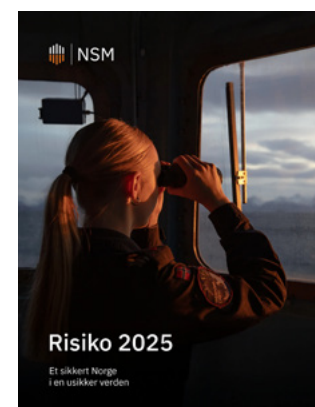
Hva vil skille vinnerne fra taperne?

De kommende årene vil skille dem som bruker risikostyring og regulering som motor for modernisering, fra dem som bare sikter mot minimum. Vinnerne vil få bedre etterlevelse med lavere kostnader og høyere kvalitet over tid og vil kjennetegnes av fire ting:

- Helhetlig risikostyring
- Videreføring av kompetanse- og kulturbygging
- Gjennomføringsevne.
- Bruk av teknologi og data - støttet av riktig kompetanse og tydelig ansvarsfordeling.



13 Kilder



Nasjonal sikkerhetsmyndighet (NSM) (2025).



Politiet (2025). Politiets trusselvurdering 2025.



Politiets sikkerhetstjeneste (PST) (2025). Nasjonal trusselvurdering 2025.

De store trendene i AML og CTF

- ComplyAdvantage (2025). State of Financial Crime 2025.
- KPMG (2025). Innsiderisiko: Dybdeundersøkelse om økonomisk kriminalitet og innsidetrusselen.
- Nasjonal sikkerhetsmyndighet (NSM) (2025).

Svindel

- Finans Norge (2025). Nye svindeltrender: Dette advarer bankene mot nå.
- Finanstilsynet (2024). Svindelstatistikk – andre halvår 2024.
- Finansklagenemnda Bank. Nemndsregister.

Geografisk risiko

- Den europeiske kommisjon (2025). Commission updates list of high-risk countries.
- Financial Action Task Force (FATF) (2025). Jurisdictions under increased monitoring.

Politiets trusselvurdering

- Politiet (2025). Politiets trusselvurdering 2025.

PST – Nasjonal trusselvurdering

- Politiets sikkerhetstjeneste (PST) (2025). Nasjonal trusselvurdering 2025.

Tilsynsaktiviteter

- Finanstilsynet (2025). Tilsynsrapporter – arkiv.

Regulatorisk nytt

- Regjeringen.no (2025). EUs 18. sanksjonspakke innført i norsk rett.
- The Associated Press (2025). UBS fined over Credit Suisse's Mozambique "tuna bonds" money-laundering scandal.

EU og AMLA

- Det europeiske banktilsyn (EBA) (2025). EBA response to EC Call for Advice on six AMLA mandates.
- Det europeiske banktilsyn (EBA) (2025). Letter to Mr. Berrigan on the EBA response to the Call for Advice of 12.03.2024 (AMLA RTS and GLs).

Bedre datadeling i finanssektoren

- Den europeiske kommisjon (2025). Better data sharing.

Krypto

- Andreessen Horowitz (a16z) (2025). State of Crypto Report 2025.
- Chainalysis (2025). The 2025 Crypto Crime Report.
- International Consortium of Investigative Journalists (ICIJ) (2025). Cryptocurrency regulations: A global explainer.
- Atlantic Council (2025). CBDC Tracker.
- Atlantic Council (2025). Central bank digital currencies versus stablecoins: Divergent EU and US perspectives.
- Skatteetaten (2025). Over 54 000 oppgir at de eier kryptovaluta – dette er kommunene med flest kryptoeiere.

Hva kommer i 2026

- European Banking Authority (EBA) (2025). EBA response to EC Call for Advice on six AMLA mandates.
- European Commission. EU Anti-Money Laundering Package (AMLR, AMLD6, AMLA).

Generelle kilder

- Finans Norge (2025). Nye svindeltrender: Dette advarer bankene mot nå.
- Finanstilsynet (2024). Svindelstatistikk – andre halvår 2024.
- Regjeringen.no (2025). Høring – finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet.

Kontakt



Kjersti Aksnes Gjesdahl
Partner

kjersti.gjesdahl@pwc.com
+47 415 58 225



Fredrik B. Grimstad
Direktør

fredrik.grimstad@pwc.com
+47 984 59 372

