AML Procedures

Hvitvaskingsrutiner — Drop (ALAI Holding AS)

Dokument: Internrutiner for tiltak mot hvitvasking og terrorfinansiering **Hjemmel:** Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven, LOV-2018-06-01-23) **Virksomhet:** ALAI Holding AS, org.nr 932 516 136 **Produkt:** Drop — betalingsformidling og pengeoverføringer **Versjon:** 1.0 **Dato:** 2026-02-12 **Godkjent av:** Daglig leder / Styre **Neste revisjon:** 2027-02-12

---

1. Formål og virkeområde

1.1 Formål

Disse rutinene skal sikre at ALAI Holding AS («Selskapet») gjennom produktet Drop etterlever kravene i hvitvaskingsloven med forskrifter, og bidrar til å forebygge og avdekke hvitvasking og terrorfinansiering.

1.2 Virkeområde

Rutinene gjelder for all virksomhet knyttet til Drop, herunder:

- Pengeoverføringer til utlandet (remittance) til 30+ land
- QR-baserte betalinger i butikk
- Kunderegistrering og -oppfølging
- Alle ansatte, styremedlemmer og tredjeparter som utfører oppgaver på vegne av Selskapet

1.3 Forretningsmodell — pass-through

Drop opererer en pass-through-modell under PSD2 (PISP/AISP). Drop holder aldri kundemidler. Alle transaksjoner initieres via Open Banking-grensesnitt mot kundens egen bankkonto. Denne modellen reduserer enkelte risikoer, men endrer ikke de grunnleggende pliktene etter

hvitvaskingsloven.

1.4 Regulatorisk klassifisering

Selskapet søker konsesjon som betalingsforetak etter finansforetaksloven, jf. også hvitvaskingsloven §4 første ledd bokstav c (betalingsforetak).

---

2. Lovgrunnlag og sentrale bestemmelser

Bestemmelse	Innhold
Hvvl. §4	Rapporteringspliktige — betalingsforetak er omfattet
Hvvl. §6	Virksomhetsinnrettet risikovurdering
Hvvl. §§7-8	Rutiner og internkontroll
Hvvl. §§9-18	Kundetiltak (CDD)
Hvvl. §§17-18	Forsterkede kundetiltak (EDD)
Hvvl. §§24-25	Løpende oppfølging
Hvvl. §26	Undersøkelsesplikt
Hvvl. §26 tredje ledd	Rapporteringsplikt til Økokrim/EFE
Hvvl. §30	Oppbevaringsplikt (5 år)
Hvvl. §§36-38	Internkontroll og opplæring
Sanksjonslovgivningen	FN, EU, norske sanksjonslister
PEP-forskriften	Politisk eksponerte personer

---

3. Virksomhetsinnrettet risikovurdering (§6)

3.1 Krav

Selskapet skal gjennomføre og dokumentere en helhetlig risikovurdering av virksomheten, som identifiserer og vurderer risikoen for hvitvasking og terrorfinansiering. Risikovurderingen

oppdateres minst årlig og ved vesentlige endringer.

3.2 Risikokategorier

Risikovurderingen dekker følgende kategorier:

- **Kundebasert risiko** — risikobasert tilnærming basert på kundens adferd, transaksjonsvolum og korridorer
- **Geografisk risiko** — land og korridorer med høyere HV/TF-risiko
- **Produkt- og tjenestebasert risiko** — grensekryssende overføringer, QR-betalinger
- **Kanal- og leveringsrisiko** — digital onboarding, mobilapp

Se eget dokument: `risikovurdering-hvitvasking.md`

3.3 Risikonivåer

Nivå	Beskrivelse	Tiltak
Lav	Norsk bosatt, norsk BankID, lavrisiko-korridor	Standard kundetiltak (CDD)
Middels	Høyere transaksjonsvolum, middels risiko-korridor	Utvidet overvåking, mulig EDD
Høy	Høyrisiko-korridor, PEP, uvanlig transaksjonsmønster	Forsterkede kundetiltak (EDD)
Uakseptabel	Sanksjonert person/land, bekreftet mistanke	Avvisning eller avvikling av kundeforhold

---

4. Kundetiltak (KYC/CDD) — §§9-16

4.1 Når kundetiltak skal gjennomføres

Kundetiltak skal gjennomføres ved:

- Etablering av kundeforhold (registrering i Drop), jf. §10
- Enkeltstående transaksjoner over NOK 10 000 utenfor etablert kundeforhold, jf. §10
- Mistanke om hvitvasking eller terrorfinansiering, uavhengig av beløp, jf. §10
- Tvil om tidligere innhentede opplysninger, jf. §24

4.2 Standard kundetiltak (CDD)

4.2.1 Fysiske personer (alle kunder)

Følgende opplysninger skal innhentes og verifiseres, jf. §12:

Opplysning	Kilde	Verifisering
Fullt navn	BankID	Automatisk via BankID-integrasjon
Fødselsnummer (11 siffer)	BankID	Automatisk — brukes til alderskontroll (18+) og identifisering
Adresse	Kunde oppgir, sjekkes mot Folkeregisteret	Folkeregisteroppslag
Statsborgerskap	Kunde oppgir	Krysssjekk mot BankID-data
Formål med kundeforholdet	Kunde velger ved registrering	Dokumenteres i kundeprofil

4.2.2 Juridiske personer (merchants)

For merchanter som registrerer seg for QR-betalinger:

Opplysning	Kilde	Verifisering
Foretaksnavn og org.nr	Kunde oppgir	Brønnøysundregistrene
Forretningsadresse	Kunde oppgir	Brønnøysundregistrene
Reelle rettighetshavere	Kunde oppgir	Aksjonærregisteret, egenoppgave
Daglig leder/kontaktperson	Kunde oppgir	BankID-verifisering av kontaktperson
Formål med kundeforholdet	Kunde velger	Dokumenteres

4.2.3 Identitetsbekreftelse

- **Primær metode:** Norsk BankID (nivå «høyt» etter eIDAS)
- BankID gir verifisert navn, fødselsnummer og sikrer at kunden er den de utgir seg for
- Kunder uten gyldig norsk BankID kan ikke registrere seg i Drop
- Minstealder 18 år kontrolleres automatisk basert på fødselsnummer

4.3 Forsterkede kundetiltak (EDD) — §§17-18

Forsterkede tiltak skal gjennomføres når risikoen er vurdert som høy, herunder:

4.3.1 Situasjoner som utløser EDD

- Kunder som sender penger til høyrisikoland (jf. EUs liste over høyrisikoland og FATFs gråliste/svarteliste)
- Politisk eksponerte personer (PEP), jf. §18
- Uvanlige eller mistenkelige transaksjonsmønstre
- Kunder med vesentlig høyere transaksjonsvolum enn oppgitt formål tilsier

- Kundeforhold der det er vanskelig å verifisere reelle rettighetshavere

4.3.2 EDD-tiltak

- Innhenting av tilleggsinformasjon om midlenes opprinnelse
- Innhenting av dokumentasjon for formålet med transaksjonen
- Hyppigere oppdatering av kundeinformasjon
- Økt transaksjonsovervåking (lavere terskelverdier)
- Godkjenning av kundeforholdet av hvitvaskingsansvarlig
- Risikovurdering dokumenteres i kundeprofilen

4.4 PEP-screening — §18

4.4.1 Hvem er PEP

Politisk eksponerte personer inkluderer:

- Statsoverhoder, regjeringsmedlemmer, parlamentsmedlemmer
- Høyesterettsdommere, riksrevisorer, sentralbankstyremedlemmer
- Ambassadører, militære offiserer av høy rang
- Ledere av statsforetak
- Nære familiemedlemmer og kjente medarbeidere til ovennevnte

4.4.2 PEP-prosedyre

1. **Screening ved onboarding:** Automatisk PEP-sjekk mot anerkjent database (f.eks. Refinitiv World-Check, Dow Jones)
2. **Løpende screening:** Automatisk re-screening ved endringer i PEP-lister
3. **Positive treff:** Manuell vurdering av hvitvaskingsansvarlig
4. **EDD ved bekreftet PEP:** Tilleggsdokumentasjon, godkjenning av daglig leder, hyppigere overvåking

4.5 Sanksjonsscreening

4.5.1 Lister som sjekkes

- FNs konsoliderte sanksjonsliste
- EUs konsoliderte sanksjonsliste
- Norske forskrifter om sanksjoner (UD)
- OFAC SDN-listen (for USD-transaksjoner)

4.5.2 Prosedyre

1. **Ved onboarding:** Automatisk screening av kundens navn og fødselsdato mot alle sanksjonslister

2. **Ved hver transaksjon:** Automatisk screening av mottaker mot sanksjonslister
3. **Positive treff:** Transaksjon fryses automatisk. Hvitvaskingsansvarlig varsles.
4. **Bekreftet treff:** Transaksjon avvises. Rapportering til Utenriksdepartementet og EFE.
5. **Falske positive:** Dokumenteres og godkjennes av hvitvaskingsansvarlig.

---

5. Løpende oppfølging — §§24-25

5.1 Transaksjonsinformasjon

Alle transaksjoner skal inneholde følgende informasjon, jf. betalingssystemloven og EU-forordning 2015/847:

- Avsenders fulle navn, adresse, kontonummer
- Mottakers fulle navn, kontonummer/referanse
- Beløp og valuta
- Tidspunkt
- Formål (for beløp over NOK 10 000)

5.2 Transaksjonovervåking

5.2.1 Automatisk overvåking

Selskapet implementerer et automatisert transaksjonsovervåkingssystem som flagger:

Regel	Terskel	Handling
Enkelt-transaksjon over terskel	> NOK 50 000	Manuell gjennomgang
Kumulativt daglig volum	> NOK 100 000	Manuell gjennomgang
Kumulativt månedlig volum	> NOK 500 000	EDD-vurdering
Hyppige transaksjoner til høyrisikoland	> 5/uke til samme korridor	Manuell gjennomgang
Splitting av transaksjoner	Flere transaksjoner like under terskel	Automatisk flagging
Avvik fra kundeprofil	> 200% av oppgitt bruksformål	Manuell gjennomgang
Round-trip-transaksjoner	Penger sendt og mottatt fra samme korridor	Automatisk flagging
Uvanlig adferd	Hurtig endring av mottakerland	Manuell gjennomgang

5.2.2 Manuell gjennomgang

- Flaggede transaksjoner gjennomgås av compliance-teamet innen 24 timer
- Vurderingen dokumenteres med konklusjon og eventuell oppfølgingshandling
- Ved fortsatt mistanke: undersøkelsesplikt, jf. §26

5.3 Oppdatering av kundeinformasjon

- **Lav risiko:** Kundeinformasjon oppdateres hvert 3. år
- **Middels risiko:** Kundeinformasjon oppdateres årlig
- **Høy risiko:** Kundeinformasjon oppdateres hvert halvår
- **Ved enhver transaksjon:** Kontroll av at kundeinformasjon er oppdatert

---

6. Undersøkelsesplikt og rapportering — §26

6.1 Undersøkelsesplikt

Når det foreligger forhold som gir grunnlag for mistanke om at en transaksjon har tilknytning til hvitvasking eller terrorfinansiering, skal Selskapet:

1. **Gjennomføre nærmere undersøkelser** — innhente tilleggsinformasjon om kundens identitet, midlenes opprinnelse, transaksjonens formål
2. **Dokumentere undersøkelsen** — alle funn, vurderinger og konklusjoner nedtegnes
3. **Konkludere** — enten avkreftes mistanken (dokumenteres) eller bekreftes (rapportering)

6.2 Rapportering til Økokrim/EFE

Dersom undersøkelsen ikke avkrefter mistanken:

1. **Rapport sendes til EFE (Enheten for finansiell etterretning)** via Altinn-portalen
2. **Rapporten skal inneholde:**
   - Identifikasjon av kunden (navn, fødselsnummer, adresse)
   - Beskrivelse av transaksjonen(e)
   - Grunnlag for mistanken
   - Resultater av undersøkelsen
   - Relevant dokumentasjon
3. **Tidsfrist:** Uten ugrunnet opphold etter at undersøkelsen er fullført
4. **Konfidensialitet:** Kunden skal ikke underrettes om at rapport er sendt (tipping off-forbud, §28)

5. **Transaksjoner kan holdes tilbake** i inntil 2 virkedager etter rapportering, jf. betalingssystemloven

6.3 Statistikk og oppfølging

- Antall flaggede transaksjoner per måned
- Antall undersøkelser gjennomført
- Antall rapporter sendt til EFE
- Rapporteres kvartalsvis til styret

---

7. Oppbevaringsplikt — §30

7.1 Lagringstid

Alle opplysninger innhentet i forbindelse med kundetiltak og transaksjonsovervåking skal oppbevares i **minst 5 år** etter at kundeforholdet er avsluttet eller transaksjonen er gjennomført.

7.2 Hva oppbevares

Datatype	Lagringstid	Format
Kundidentifikasjon (KYC-data)	5 år etter avsluttet kundeforhold	Kryptert database
Kopi av legitimasjon/BankID-bekreftelse	5 år etter avsluttet kundeforhold	Kryptert lagring
Transaksjonsdata	5 år etter transaksjonsdato	Database med revisjonsspor
Korrespondanse med kunden	5 år etter avsluttet kundeforhold	Kryptert lagring
Risikovurderinger og EDD-dokumentasjon	5 år etter avsluttet kundeforhold	Kryptert lagring
Undersøkelser og rapporter til EFE	5 år etter avsluttet kundeforhold	Kryptert lagring
Opplæringslogg	5 år etter gjennomføring	Intern database

7.3 Datasikkerhet

- All KYC- og transaksjonsdata krypteres ved lagring (AES-256)
- Tilgang logges og begrenses til autorisert personell
- GDPR/personopplysningsloven overholdes — personopplysninger slettes etter utløp av lovpålagt oppbevaringstid

---

8. Korridorbasert risikovurdering

8.1 Tilnærming

Drop tilbyr pengeoverføringer til 30+ land. Risikoen varierer etter mottakerland/korridor. Selskapet benytter en risikobasert tilnærming der **alle kunder** vurderes etter samme rammeverk, uavhengig av etnisk bakgrunn eller statsborgerskap. Risikofaktoren er knyttet til **transaksjonskorridoren** (mottakerlandet), ikke kundens opprinnelse.

8.2 Korridorklassifisering

Risikonivå	Land/korridorer	Grunnlag
Lav	EU/EØS-land (PLN, EUR), Storbritannia	FATF-compliant, EU-regulerte
Middels	Serbia (RSD), Bosnia-Hercegovina (BAM), Tyrkia (TRY)	Ikke EU, men MONEYVAL/FATF-prosesser pågår
Høy	Pakistan (PKR)	FATF gråliste-historikk, høy korrupsjonsrisiko
Svært høy / sperret	Land på EUs høyrisikoliste eller FNs/EUs sanksjonslister	EU-forordning, FN-resolusjon

8.3 Tiltak per korridorrisiko

Korridorrisiko	CDD	Transaksjonsovervåking	Tilleggstiltak
Lav	Standard	Standard terskler	Ingen
Middels	Standard + ekstra spørsmål om formål	Lavere terskler (50% av standard)	Kvartalsvis profil-oppdatering
Høy	EDD obligatorisk	Halverte terskler, manuell review >NOK 25 000	Dokumentasjon av midlers opprinnelse, månedlig oppdatering
Svært høy / sperret	Avvises	N/A	Korridor blokkert i systemet

---

9. Roller og ansvar

9.1 Hvitvaskingsansvarlig

Selskapet utpeker en hvitvaskingsansvarlig (AML Compliance Officer), jf. §8 fjerde ledd.

Ansvar:

- Daglig oppfølging av hvitvaskingsrutinene
- Behandling av flaggede transaksjoner og EDD-saker
- Rapportering til EFE
- Årlig revisjon av risikovurdering og rutiner
- Opplæring av ansatte
- Rapportering til styret

9.2 Daglig leder

- Overordnet ansvar for etterlevelse av hvitvaskingsloven
- Godkjenner høyrisiko-kundeforhold
- Sikrer tilstrekkelige ressurser til compliance

9.3 Styret

- Godkjenner hvitvaskingsrutiner og risikovurdering
- Mottar kvartalsvis rapport fra hvitvaskingsansvarlig
- Beslutter risikoappetitt

9.4 Alle ansatte

- Plikter å følge disse rutinene
- Plikter å rapportere mistenkelige forhold til hvitvaskingsansvarlig
- Plikter å gjennomføre obligatorisk opplæring

---

10. Opplæring — §36

10.1 Obligatorisk opplæring

Alle ansatte med kundetilgangs- eller transaksjonsrelaterte oppgaver skal gjennomføre opplæring i:

- Hvitvaskingsloven og forskrifter — grunnleggende forståelse
- Selskapets hvitvaskingsrutiner
- Gjenkjennelse av mistenkelige transaksjoner
- Rapporteringsprosedyrer
- PEP- og sanksjonsregler
- Roller og ansvar

10.2 Frekvens

- **Ved ansettelse:** Grunnkurs (innen 30 dager)
- **Årlig:** Oppdateringskurs med gjennomgang av endringer i lovverk og rutiner
- **Ved vesentlige endringer:** Ekstra opplæring ved nye produkter, korridorer eller regelverk

10.3 Dokumentasjon

- Opplæring registreres med dato, deltaker, innhold og beståttresultat
- Opplæringslogg oppbevares i 5 år

---

11. Internkontroll og revisjon — §37

11.1 Internkontroll

- Hvitvaskingsansvarlig utfører stikkprøvekontroller månedlig
- Minimum 10% av flaggede transaksjoner re-vurderes
- Kvaliteten på KYC-dokumentasjon kontrolleres kvartalsvis

11.2 Uavhengig gjennomgang

- Årlig uavhengig gjennomgang av hvitvaskingsrutinene
- Utføres av ekstern revisor eller compliance-rådgiver
- Funn rapporteres til styret med handlingsplan

11.3 Avviksbehandling

- Avvik fra rutinene dokumenteres umiddelbart
- Korrigerende tiltak iverksettes innen 30 dager
- Alvorlige avvik rapporteres til styret og eventuelt Finanstilsynet

---

12. Behandling av avviste eller avsluttede kundeforhold

12.1 Avvisning

Dersom kundetiltak ikke kan gjennomføres tilfredsstillende, jf. §21:

- Kundeforholdet **skal ikke etableres**
- Eksisterende kundeforhold **skal avsluttes**
- Vurdering av om forholdet skal rapporteres til EFE

12.2 Avslutning av kundeforhold

- Kunden informeres om at kundeforholdet avsluttes (uten å oppgi HV/TF som grunn dersom rapport sendes)
- Eventuelle midler tilbakeføres til kundens opprinnelige bankkonto
- KYC-dokumentasjon oppbevares i 5 år etter avslutning

---

13. Tekniske tiltak

13.1 Automatiserte kontroller i Drop-appen

- BankID-verifisering ved registrering (alderskontroll, identifikasjon)
- Automatisk PEP- og sanksjonsscreening ved onboarding og ved transaksjoner
- Regelbasert transaksjonsovervåking med konfigurbare terskler
- Automatisk blokkering av transaksjoner til sanksjonerte land/personer
- Logging av alle transaksjoner med fullstendig revisjonsspor

13.2 Manuelt dashboard

- Compliance-dashboard for hvitvaskingsansvarlig
- Oversikt over flaggede transaksjoner, ventende EDD-saker, rapporterte saker
- Søkefunksjon i transaksjonshistorikk

---

14. Forholdet til personopplysningsloven (GDPR)

14.1 Behandlingsgrunnlag

- KYC-data behandles med hjemmel i **rettslig forpliktelse** (GDPR art. 6(1)(c)), jf. hvitvaskingsloven
- Oppbevaringstiden på 5 år har hjemmel i hvitvaskingsloven §30
- Etter utløp av oppbevaringstiden slettes personopplysningene

14.2 Personvernserklæring

- Kundene informeres om behandling av personopplysninger i forbindelse med hvitvaskingslovens krav
- Informasjon gis i personvernerklæring og ved registrering

---

15. Endringslogg

Versjon	Dato	Endring	Godkjent av
1.0	2026-02-12	Førstegangs utarbeidelse	Daglig leder

---

16. Vedlegg

- **Vedlegg A:** Risikovurdering — `risikovurdering-hvitvasking.md`
- **Vedlegg B:** Internkontrollrutiner — `internkontroll.md`
- **Vedlegg C:** EFE-rapporteringsskjema (Altinn-mal)
- **Vedlegg D:** Sjekkliste for kundetiltak
- **Vedlegg E:** Opplæringsplan

Dokumentet er utarbeidet i henhold til hvitvaskingsloven (LOV-2018-06-01-23) med tilhørende forskrift, Finanstilsynets veiledning om tiltak mot hvitvasking og terrorfinansiering, og FATFs anbefalinger.

Revision #5
Created 2026-02-18 08:44:37 UTC by John
Updated 2026-05-25 07:24:18 UTC by John