Privacy & Data Protection

- Privacy Policy
- DPIA Assessment
- Data Processing Protocol
- Outsourcing Policy

Privacy Policy

Personvernerklæring for Drop

Sist oppdatert: 2. mars 2026 **Behandlingsansvarlig:** ALAI Holding AS, org.nr. 932 516 136
Kontakt: personvern@getdrop.no **Nettsted:** https://getdrop.no

---

1. Innledning

Denne personvernerklæringen beskriver hvordan ALAI Holding AS («vi», «oss», «selskapet») behandler personopplysninger i forbindelse med betalingstjenesten Drop. Erklæringen er utarbeidet i samsvar med EUs personvernforordning (GDPR) artikkel 13 og 14, samt den norske personopplysningsloven (LOV-2018-06-15-38).

Drop er en betalingstjeneste som tilbyr pengeoverføring til utlandet og QR-betalinger i butikk, tilgjengelig for alle innbyggere i Norge. Tjenesten opererer etter en pass-through-modell under PSD2 (EU-direktiv 2015/2366) og behandler aldri kundemidler direkte.

---

2. Behandlingsansvarlig

ALAI Holding AS er behandlingsansvarlig for personopplysningene som behandles gjennom Drop-tjenesten, jf. GDPR artikkel 4 nr. 7.

Kontaktinformasjon:

- Selskap: ALAI Holding AS
- Organisasjonsnummer: 932 516 136
- E-post: personvern@getdrop.no
- Adresse: Se Brønnøysundregistrene

---

3. Personvernombud

I henhold til GDPR artikkel 37 og personopplysningsloven (LOV-2018-06-15-38) har selskapet utnevnt et personvernombud (DPO). Gitt at selskapet behandler betalingsopplysninger og

finansielle data i stor skala, er personvernombud formelt oppnevnt per 2. mars 2026.

Personvernombud: Alem Bašić **Selskap:** ALAI Holding AS (org.nr. 932 953 736) **E-post:** alem@alai.no **Telefon:** +47 40 47 42 51 **Oppnevnt:** 2. mars 2026 — jf. GDPR artikkel 37–39 og personopplysningsloven § 23

---

4. Kategorier av personopplysninger

4.1 Identifikasjonsopplysninger

- Fullt navn (fra BankID)
- Fødselsnummer (fra BankID, kun for identitetsverifisering)
- Fødselsdato (utledet fra fødselsnummer for aldersverifisering, 18+)
- BankID-referanse

4.2 Kontaktopplysninger

- Mobilnummer (+47)
- E-postadresse
- Postadresse (ved behov)

4.3 Finansielle opplysninger

- Bankkontonummer (via PSD2 AISP)
- Kontosaldo (via PSD2 AISP, kun ved brukerens samtykke)
- Transaksjonshistorikk i Drop
- Betalingsmottakere og beløp
- Valutainformasjon ved utenlandsoverføringer
- Mottakerens bankopplysninger (for remittance)

4.4 Tekniske opplysninger

- IP-adresse
- Enhetsidentifikator (device ID)
- Operativsystem og appversjon
- Innloggings- og autentiseringslogger
- Brukeragent (browser/app)

4.5 Bruksmønster

- Tidspunkt for pålogging og transaksjoner
- Navigasjon i appen (anonymisert)
- Feillogger og krasjrapporter
- Push-varslingsinnstillinger

4.6 KYC/AML-relaterte opplysninger

- Legitimasjonsdokumenter (ved forsterket kundekontroll)
- PEP-status (politisk eksponert person)
- Sanksjonslistekontroll-resultater
- Risikoklassifisering

---

5. Rettslig grunnlag for behandlingen

Vi behandler personopplysninger på følgende rettslige grunnlag, jf. GDPR artikkel 6:

5.1 Oppfyllelse av avtale — GDPR art. 6(1)(b)

- Gjennomføring av betalingstransaksjoner
- Kontoadministrasjon og brukerprofilhåndtering
- Transaksjonshistorikk og kvitteringer
- Push-varsler om transaksjoner
- Kundeservice

5.2 Rettslig forpliktelse — GDPR art. 6(1)(c)

- Hvitvaskingsloven (LOV-2018-06-01-23) §§ 4, 10-18 — kundekontroll
- Bokføringsloven (LOV-2004-11-19-73) § 13 — oppbevaring av regnskapsdokumentasjon
- Betalingssystemloven og PSD2-forordningen
- Personopplysningsloven — pliktig informasjon til den registrerte
- Skatteforvaltningsloven — rapportering til skattemyndighetene

5.3 Samtykke — GDPR art. 6(1)(a)

- Tilgang til kontosaldo via PSD2 AISP
- Markedsføringskommunikasjon
- Bruk av cookies utover det som er strengt nødvendig
- Deling av anonymiserte data for analyseformål

5.4 Berettiget interesse — GDPR art. 6(1)(f)

- Svindelforebygging og sikkerhetsovervåking
- Forbedring av tjenesten basert på anonymisert bruksdata
- Feilretting og teknisk feilsøking
- Intern statistikk og rapportering

For behandling basert på berettiget interesse har vi gjennomført interesseavveining (LIA) i henhold til GDPR artikkel 6(1)(f). Dokumentasjon er tilgjengelig på forespørsel.

---

6. Formål med behandlingen

Formål	Rettslig grunnlag	Oppbevaringstid
Brukerregistrering og identitetsverifisering	Avtale, rettslig forpliktelse	Kontoens levetid + 5 år
Gjennomføring av betalinger og overføringer	Avtale	5 år (bokføringsloven)
Kundekontroll (KYC/AML)	Rettslig forpliktelse	5 år etter kundeforholdets opphør (hvvl. § 30)
Svindelforebygging	Berettiget interesse	3 år etter hendelse
Kundeservice og klagebehandling	Avtale, rettslig forpliktelse	3 år etter avslutning
Markedsføring	Samtykke	Til samtykke trekkes tilbake
Teknisk drift og feilretting	Berettiget interesse	12 måneder
Lovpålagt rapportering	Rettslig forpliktelse	I henhold til gjeldende lov

---

7. Deling av personopplysninger

7.1 Kategorier av mottakere

Vi deler personopplysninger med følgende kategorier av mottakere:

Betalingsinfrastruktur (nødvendig for tjenesten):

- Open Banking-leverandører (PSD2 PISP/AISP) — for å initiere betalinger og lese kontoinformasjon
- Korrespondentbanker i mottakerland — for gjennomføring av utenlandsoverføringer
- Betalingsnettverk — for QR-betalingsbehandling

Regulatoriske myndigheter (rettslig forpliktelse):

- Finanstilsynet — tilsynsrapportering
- Datatilsynet — ved forespørsel eller avvik
- Økokrim/politiet — ved mistanke om hvitvasking eller terrorfinansiering
- Skattemyndighetene — lovpålagt rapportering

Tjenesteleverandører (databehandlere):

- Skyinfrastrukturleverandører (hosting)
- Kundeserviceplattform
- Analyseverktøy (anonymiserte data)
- BankID-leverandør (autentisering)

7.2 Databehandleravtaler

Alle databehandlere har inngått databehandleravtale (DPA) i samsvar med GDPR artikkel 28. Databehandleravtalene regulerer:

- Formålet med behandlingen
- Instrukser fra behandlingsansvarlig
- Sikkerhetstiltak
- Underdatabehandlere
- Bistandsplikt ved utøvelse av den registrertes rettigheter
- Sletting/tilbakelevering ved opphør

---

8. Overføring til tredjeland

8.1 Overføringer innenfor EØS

Personopplysninger behandles primært innenfor EØS-området. All skyinfrastruktur er lokalisert i EU/EØS.

8.2 Overføringer utenfor EØS

Ved utenlandsoverføringer (remittance) til land utenfor EØS er det nødvendig å overføre begrensede personopplysninger til mottakerens bank eller betalingsformidler. Dette gjelder:

- Mottakerens navn og kontonummer
- Avsenderens navn (lovpålagt ved internasjonale overføringer)
- Beløp og valuta

Overføringsgrunnlag:

- **EU-kommisjonens standard personvernbestemmelser (SCCs)** — jf. GDPR artikkel 46(2)(c), vedtak (EU) 2021/914 av 4. juni 2021
- **Adekvansbeslutninger** — for land med tilstrekkelig beskyttelsesnivå, jf. GDPR artikkel 45
- **Nødvendig for oppfyllelse av avtale** — jf. GDPR artikkel 49(1)(b), der andre grunnlag ikke er tilgjengelige

8.3 Transfer Impact Assessment (TIA)

For overføringer til tredjeland uten adekvansbeslutning har vi gjennomført Transfer Impact Assessment i henhold til Schrems II-avgjørelsen (C-311/18). Vurderingen omfatter:

- Lovgivningen i mottakerlandet vedrørende myndighetstilgang
- Tekniske og organisatoriske tilleggstiltak
- Praktisk erfaring med myndigheters tilgangsforespørsler

Dokumentasjon av TIA er tilgjengelig på forespørsel til dpo@getdrop.no.

---

9. Oppbevaringstid og sletting

Vi oppbevarer personopplysninger kun så lenge det er nødvendig for formålet med behandlingen, eller så lenge vi er rettslig forpliktet til det.

9.1 Hovedprinsipper

- **Dataminimering:** Vi samler kun inn opplysninger som er nødvendige for formålet, jf. GDPR artikkel 5(1)(c).
- **Lagringsminimering:** Opplysninger slettes når formålet er oppfylt, jf. GDPR artikkel 5(1)(e).
- **Automatisk sletting:** Systemer er konfigurert for automatisk sletting ved utløp av oppbevaringstid.

9.2 Spesifikke oppbevaringstider

Datakategori	Oppbevaringstid	Hjemmel
Transaksjonsdata	5 år etter regnskapsårets slutt	Bokføringsloven § 13
KYC/AML-dokumentasjon	5 år etter kundeforholdets opphør	Hvitvaskingsloven § 30

Datakategori	Oppbevaringstid	Hjemmel
Innloggingslogger	12 måneder	Berettiget interesse
Kundeservicehenvendelser	3 år etter avslutning	Avtale, foreldelsesloven
Markedsføringssamtykker	Til tilbaketrekking + 1 år dokumentasjon	GDPR art. 7(1)
Tekniske logger	6 måneder	Berettiget interesse
IP-adresser	3 måneder	Berettiget interesse

9.3 Sletteprosedyre

Ved sletting sørger vi for at personopplysninger fjernes fra alle systemer, inkludert sikkerhetskopier, innen rimelig tid (maksimalt 30 dager etter oppbevaringstidens utløp for sikkerhetskopier).

---

10. Den registrertes rettigheter

I henhold til GDPR kapittel III har du følgende rettigheter:

10.1 Rett til innsyn (art. 15)

Du har rett til å få bekreftet om vi behandler personopplysninger om deg, og i så fall få tilgang til opplysningene samt informasjon om behandlingen. Første kopi er gratis.

10.2 Rett til retting (art. 16)

Du har rett til å få uriktige personopplysninger om deg rettet uten ugrunnet opphold.

10.3 Rett til sletting (art. 17)

Du har rett til å få slettet personopplysninger om deg dersom:

- Opplysningene ikke lenger er nødvendige for formålet
- Du trekker tilbake samtykket
- Du protesterer mot behandlingen
- Opplysningene er behandlet ulovlig

Unntak: Sletting kan nektes dersom behandlingen er nødvendig for å oppfylle en rettslig forpliktelse (f.eks. hvitvaskingsloven, bokføringsloven).

10.4 Rett til begrensning (art. 18)

Du har rett til å kreve at behandlingen begrenses i visse situasjoner, for eksempel mens riktigheten av opplysningene kontrolleres.

10.5 Rett til dataportabilitet (art. 20)

Du har rett til å motta personopplysninger du har gitt oss i et strukturert, alminnelig brukt og maskinlesbart format (JSON/CSV), og til å overføre disse til en annen behandlingsansvarlig.

10.6 Rett til å protestere (art. 21)

Du har rett til å protestere mot behandling basert på berettiget interesse. Vi vil da stanse behandlingen med mindre vi kan påvise tvingende berettigede grunner som går foran dine interesser.

10.7 Rett til ikke å bli gjenstand for automatiserte avgjørelser (art. 22)

Du har rett til ikke å bli gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, inkludert profilering, som har rettsvirkning eller tilsvarende betydelig påvirkning.

Drop benytter automatiserte systemer for svindeldeteksjon. Ved automatisk avvisning av en transaksjon har du rett til:

- Manuell gjennomgang av avgjørelsen
- Å uttrykke ditt synspunkt
- Å bestride avgjørelsen

10.8 Rett til å trekke tilbake samtykke (art. 7(3))

Der behandling er basert på samtykke, kan du når som helst trekke dette tilbake. Tilbaketrekking påvirker ikke lovligheten av behandling som fant sted før tilbaketrekkingen.

---

11. Utøvelse av rettigheter

11.1 Hvordan utøve rettighetene

Henvendelser om utøvelse av rettigheter kan sendes til:

- **E-post:** personvern@getdrop.no
- **I appen:** Under Innstillinger > Personvern > Mine rettigheter
- **Post:** ALAI Holding AS, [adresse], Norge

11.2 Identitetsverifisering

For å beskytte dine opplysninger vil vi verifisere din identitet ved rettighetskrav, normalt gjennom BankID.

11.3 Svartid

Vi besvarer henvendelser uten ugrunnet opphold, og senest innen 30 dager, jf. GDPR artikkel 12(3). Ved komplekse eller mange forespørsler kan fristen forlenges med ytterligere 60 dager, med informasjon til deg innen den første 30-dagersperioden.

11.4 Kostnad

Utøvelse av rettigheter er i utgangspunktet gratis. Ved åpenbart grunnløse eller overdrevne krav kan vi kreve et rimelig gebyr eller nekte å etterkomme forespørselen, jf. GDPR artikkel 12(5).

---

12. Informasjonssikkerhet

Vi har implementert egnede tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger, jf. GDPR artikkel 32:

- **Kryptering:** All dataoverføring er kryptert med TLS 1.3. Data i hvile er kryptert med AES-256.
- **Tilgangskontroll:** Rollebasert tilgangsstyring (RBAC), prinsippet om minste privilegium.
- **Autentisering:** BankID for brukere, MFA for ansatte.
- **Logging:** Komplett revisjonslogg for all tilgang til personopplysninger.
- **Sårbarhetshåndtering:** Regelmessig penetrasjonstesting og sårbarhetsskanning.
- **Hendelseshåndtering:** Etablerte prosedyrer for håndtering av sikkerhetsbrudd.

Se vår IKT-sikkerhetspolicy for utfyllende informasjon.

---

13. Personvernbrudd

Ved brudd på personopplysningssikkerheten vil vi:

1. **Melde til Datatilsynet** innen 72 timer etter at bruddet ble oppdaget, jf. GDPR artikkel 33, med mindre bruddet sannsynligvis ikke medfører risiko for den registrertes rettigheter.
2. **Informere berørte registrerte** uten ugrunnet opphold dersom bruddet sannsynligvis medfører høy risiko, jf. GDPR artikkel 34.
3. **Dokumentere** alle brudd, uavhengig av alvorlighetsgrad, inkludert fakta, virkninger og korrigerende tiltak.

---

14. Cookies og sporingsteknikker

Drop-appen benytter ikke tredjeparts sporingsteknikker. For nettsiden getdrop.no gjelder:

14.1 Nødvendige cookies

- Sesjonscookies for autentisering
- Sikkerhetscookies (CSRF-beskyttelse)
- Disse krever ikke samtykke, jf. ekomloven § 2-7b.

14.2 Analytiske cookies (krever samtykke)

- Anonymisert bruksstatistikk
- Aktiveres kun etter eksplisitt samtykke via cookiebanner

14.3 Markedsføringscookies (krever samtykke)

- Kun ved eksplisitt samtykke
- Kan til enhver tid trekkes tilbake via cookieinnstillinger

---

15. Endringer i erklæringen

Vi kan oppdatere denne personvernerklæringen ved behov. Ved vesentlige endringer vil vi informere deg via:

- Push-varsling i appen
- E-post til registrert e-postadresse
- Melding ved neste pålogging

Alle versjoner arkiveres og er tilgjengelige på forespørsel.

---

16. Klageadgang

Dersom du mener at vår behandling av personopplysninger bryter med personvernlovgivningen, har du rett til å klage til:

Datatilsynet Postboks 458 Sentrum 0105 Oslo Telefon: 22 39 69 00 E-post: postkasse@datatilsynet.no Nettsted: https://www.datatilsynet.no

Du har også rett til å klage til tilsynsmyndigheten i det EØS-landet der du bor eller arbeider, jf. GDPR artikkel 77.

---

17. Kontakt oss

For spørsmål om denne personvernerklæringen eller vår behandling av personopplysninger:

- **Generelt:** personvern@getdrop.no
- **Personvernombud:** Alem Bašić — alem@alai.no — +47 40 47 42 51
- **Post:** ALAI Holding AS, [adresse], Norge

Denne personvernerklæringen er sist oppdatert 2. mars 2026.

DPIA Assessment

Vurdering av personvernkonsekvenser (DPIA) — Drop

Dokument-ID: DPIA-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Utarbeidet av:** ALAI Holding AS **Behandlingsansvarlig:** ALAI Holding AS, org.nr. 932 516 136 **Status:** Godkjent

---

1. Innledning og bakgrunn

1.1 Formål

Denne vurderingen av personvernkonsekvenser (DPIA) er utarbeidet i henhold til GDPR artikkel 35 og Datatilsynets retningslinjer for vurdering av personvernkonsekvenser. Formålet er å identifisere, vurdere og redusere personvernrisiko forbundet med betalingstjenesten Drop.

1.2 Hvorfor DPIA er påkrevd

En DPIA er påkrevd fordi behandlingen oppfyller flere av kriteriene i GDPR artikkel 35(3) og Artikkel 29-gruppens retningslinjer (WP 248 rev.01):

- **Systematisk overvåking:** Automatisert svindeldeteksjon og transaksjonsovervåking
- **Sårbare grupper:** Brukere med varierende digital kompetanse
- **Ny teknologi:** Open Banking (PSD2 PISP/AISP) og BankID-integrasjon
- **Stor skala:** Tjenesten er rettet mot alle innbyggere i Norge
- **Finansielle data:** Behandling av bankopplysninger og transaksjonsdata
- **Grenseoverskridende overføringer:** Pengeoverføringer til 30+ land

1.3 Omfang

Denne DPIA dekker all behandling av personopplysninger i Drop-tjenesten, inkludert:

- Brukerregistrering og BankID-verifisering
- Kontoinformasjonstjenester (AISP)
- Betalingsinitieringstjenester (PISP)
- Utenlandsoverføringer (remittance) til 30+ land
- QR-betalinger i butikk
- KYC/AML-prosesser
- Svindeldeteksjon og -forebygging

---

2. Systematisk beskrivelse av behandlingen

2.1 Tjenestebeskrivelse

Drop er en betalingstjeneste for alle innbyggere i Norge som tilbyr:

1. **Utenlandsoverføringer (remittance):** Send penger til mottakere i 30+ land. Mottaker trenger ikke Drop-konto.
2. **QR-betalinger:** Betal hos forhandlere ved å skanne QR-kode. Lavere gebyrer enn tradisjonelle løsninger.
3. **Lommebok:** Betalinger og daglig bruk.

2.2 Teknisk arkitektur

Drop opererer etter en **pass-through-modell:**

- Drop holder aldri kundemidler
- Betalinger initieres via PSD2 PISP direkte fra brukerens bankkonto
- Kontoinformasjon leses via PSD2 AISP med brukerens eksplisitte samtykke
- All autentisering skjer via BankID (nivå 4 — høyeste sikkerhetsnivå)

2.3 Dataflyt

```
Bruker → BankID (autentisering) → Drop-plattform → Open Banking API (PISP/AISP) → Brukerens bank
                                                              ↓
                                                  Korrespondentbank → Mottaker (for remittance)
```

2.4 Personopplysninger som behandles

Kategori	Opplysninger	Kilde	Rettslig grunnlag
Identifikasjon	Navn, fødselsnummer, fødselsdato	BankID	Avtale, rettslig forpliktelse
Kontakt	Mobilnummer, e-post	Bruker	Avtale
Finansielt	Kontonummer, saldo, transaksjoner	PSD2 AISP	Samtykke, avtale
Transaksjoner	Beløp, mottaker, valuta, tidspunkt	Drop-tjenesten	Avtale
KYC/AML	Legitimasjon, PEP-status, sanksjoner	Bruker, tredjeparter	Rettslig forpliktelse
Teknisk	IP, device ID, logger	Automatisk	Berettiget interesse

2.5 Involvert personell og systemer

- **Driftsteam:** Begrenset tilgang til produksjonsdata, kun via autoriserte systemer
- **Kundeservice:** Tilgang til nødvendige personopplysninger for å håndtere henvendelser
- **Compliance:** Tilgang til KYC/AML-data og transaksjonsrapporter
- **Databehandlere:** Open Banking-leverandører, skyinfrastrukturleverandører, BankID-leverandør

---

3. Nødvendighets- og proporsjonalitetsvurdering

3.1 Nødvendighet — GDPR art. 35(7)(b)

Hver behandlingsaktivitet er vurdert mot nødvendighetsprinsippet:

Behandling	Nødvendig?	Begrunnelse
BankID-verifisering	Ja	Lovpålagt identitetskontroll (hvvl. § 12), sikkerhetsnivå 4 påkrevd for finanstjenester
Fødselsnummer	Ja	Kreves for entydig identifisering jf. hvitvaskingsloven § 12(1)(a)
Kontoinformasjon (AISP)	Ja, med samtykke	Nødvendig for å vise saldo og verifisere dekning
Betalingsinitiering (PISP)	Ja	Kjernetjenesten — uten dette ingen betalinger

Behandling	Nødvendig?	Begrunnelse
Transaksjonsdata	Ja	Bokføringsloven § 13, kundeoversikt, kvitteringer
KYC/AML-data	Ja	Hvitvaskingsloven §§ 4, 10-18
Svindeldeteksjon	Ja	PSD2 art. 2, Finanstilsynets krav
Tekniske logger	Ja	Sikkerhetskrav, feilsøking, DORA

3.2 Proporsjonalitet

- **Dataminimering:** Kun nødvendige opplysninger samles inn. Fødselsnummer lagres kryptert og tilgjengeliggjøres kun for autorisert personell.
- **Formålsbegrensning:** Opplysninger benyttes kun til angitt formål.
- **Lagringsminimering:** Definerte oppbevaringstider med automatisk sletting.
- **Nøyaktighet:** BankID sikrer korrekte identitetsopplysninger. Transaksjonsdata genereres av bankenes systemer.

3.3 Vurdering av alternativer

Alternativ	Vurdert	Konklusjon
Anonymisering av transaksjonsdata	Ja	Ikke mulig — lovpålagt sporbarhet (hvvl. § 25)
Pseudonymisering	Ja	Planlagt for intern analyse
Mindre inngripende autentisering	Ja	BankID er minste nødvendige nivå for finanstjenester
Desentralisert lagring	Ja	Ikke proporsjonalt gitt regulatoriske krav

---

4. Risikovurdering

4.1 Metodikk

Risiko vurderes etter sannsynlighet og konsekvens på en skala fra 1 (lav) til 4 (svært høy):

- **Risikonivå** = Sannsynlighet × Konsekvens
- **Lav:** 1-4, **Middels:** 5-8, **Høy:** 9-12, **Svært høy:** 13-16

4.2 Identifiserte risikoer

R1: Uautorisert tilgang til finansielle data

- **Beskrivelse:** Tredjeparter får tilgang til brukerens bankopplysninger
- **Sannsynlighet:** 2 (lav)
- **Konsekvens:** 4 (svært høy)
- **Risikonivå:** 8 (middels)
- **Berørte rettigheter:** Konfidensialitet, økonomisk tap

R2: Datalekkasje ved sikkerhetsbrudd

- **Beskrivelse:** Personopplysninger eksponeres ved hacking eller teknisk feil
- **Sannsynlighet:** 2 (lav)
- **Konsekvens:** 4 (svært høy)
- **Risikonivå:** 8 (middels)
- **Berørte rettigheter:** Konfidensialitet, integritet

R3: Ulovlig profilering gjennom transaksjonsdata

- **Beskrivelse:** Transaksjonshistorikk brukes til å profilere brukere ut over formålet
- **Sannsynlighet:** 1 (svært lav)
- **Konsekvens:** 3 (høy)
- **Risikonivå:** 3 (lav)
- **Berørte rettigheter:** Rett til ikke å bli profilert

R4: Manglende kontroll ved tredjelandsoverføringer

- **Beskrivelse:** Personopplysninger overføres til land uten tilstrekkelig personvern
- **Sannsynlighet:** 3 (middels)
- **Konsekvens:** 3 (høy)
- **Risikonivå:** 9 (høy)
- **Berørte rettigheter:** Konfidensialitet, myndighetstilgang

R5: Feilaktig avvisning av transaksjoner (svindeldeteksjon)

- **Beskrivelse:** Automatiserte systemer avviser lovlige transaksjoner
- **Sannsynlighet:** 2 (lav)
- **Konsekvens:** 2 (middels)
- **Risikonivå:** 4 (lav)
- **Berørte rettigheter:** Rett til korrekt behandling, økonomisk ulempe

R6: Manglende sletting etter oppbevaringstidens utløp

- **Beskrivelse:** Personopplysninger oppbevares lenger enn nødvendig
- **Sannsynlighet:** 2 (lav)
- **Konsekvens:** 2 (middels)
- **Risikonivå:** 4 (lav)
- **Berørte rettigheter:** Rett til sletting, lagringsminimering

R7: Kompromittering av BankID-sesjon

- **Beskrivelse:** Angriper overtar BankID-sesjon via phishing eller MitM
- **Sannsynlighet:** 1 (svært lav)
- **Konsekvens:** 4 (svært høy)
- **Risikonivå:** 4 (lav)
- **Berørte rettigheter:** Identitetstyveri, økonomisk tap

R8: Datatilgang fra tredjelandsmyndigheter

- **Beskrivelse:** Myndigheter i mottakerland krever tilgang til overføringsdata
- **Sannsynlighet:** 2 (lav)
- **Konsekvens:** 3 (høy)
- **Risikonivå:** 6 (middels)
- **Berørte rettigheter:** Konfidensialitet, personvern

---

5. Risikoreduserende tiltak

5.1 Tiltak per risiko

R1 & R2: Uautorisert tilgang og datalekkasje

Tiltak	Status	Ansvarlig
End-to-end-kryptering (TLS 1.3, AES-256)	Implementert	Drift
BankID-autentisering (sikkerhetsnivå 4)	Implementert	Utvikling
Rollebasert tilgangskontroll (RBAC)	Implementert	Drift
Regelmessig penetrasjonstesting (min. årlig)	Planlagt	Sikkerhet
Sikkerhetsovervåking 24/7 (SIEM)	Planlagt	Drift
Hendelseshåndteringsplan	Dokumentert	Compliance
Kryptering av fødselsnummer i hvile	Planlagt	Utvikling

R3: Ulovlig profilering

Tiltak	Status	Ansvarlig
Formålsbegrensning i systemdesign	Implementert	Utvikling
Pseudonymisering ved intern analyse	Planlagt	Data

Tiltak	Status	Ansvarlig
Forbud mot sekundærbruk uten samtykke	Policy	Compliance
Revisjonslogg for datatilgang	Implementert	Drift

R4 & R8: Tredjelandsoverføringer

Tiltak	Status	Ansvarlig
Standard personvernbestemmelser (SCCs) med alle partnere	Pågående	Juridisk
Transfer Impact Assessment per mottakerland	Pågående	Compliance
Minimering av data ved overføring (kun påkrevde felt)	Implementert	Utvikling
Kryptering av data under overføring	Implementert	Drift
Regelmessig gjennomgang av mottakerlands lovgivning	Årlig	Compliance

R5: Feilaktig avvisning

Tiltak	Status	Ansvarlig
Manuell gjennomgang ved automatisk avvisning	Planlagt	Drift
Klageadgang for brukere	Implementert	Kundeservice
Regelmessig kalibrering av svindeldeteksjon	Kvartalsvis	Data
Transparens om automatiserte avgjørelser	Planlagt	Compliance

R6: Manglende sletting

Tiltak	Status	Ansvarlig
Automatisert sletterutine	Delvis implementert	Drift
Kvartalsvis kontroll av oppbevaringstider	Planlagt	Compliance
Slettingslogg	Planlagt	Drift

R7: BankID-kompromittering

Tiltak	Status	Ansvarlig

Sesjonstimeout (15 minutter inaktivitet)	Implementert	Utvikling
Enhetsgjenkjenning	Planlagt	Utvikling
Varsling ved ny enhet	Planlagt	Utvikling
Anti-phishing-informasjon til brukere	Planlagt	Kommunikasjon

---

6. Vurdering av BankID-integrasjon

6.1 Beskrivelse

BankID benyttes som eneste autentiseringsmekanisme for Drop-brukere. Dette er Norges nasjonale eID-løsning med sikkerhetsnivå 4 (høyeste).

6.2 Personvernfordeler

- **Sterk identitetsverifisering:** Reduserer risikoen for identitetsbedrageri
- **Minimering av datainnsamling:** Drop trenger ikke samle inn pass/legitimasjon separat
- **Brukerens kontroll:** Bruker godkjenner hver transaksjon aktivt via BankID
- **Regulatorisk samsvar:** Oppfyller krav i hvitvaskingsloven §§ 12-13

6.3 Personvernrisikoer

- **Avhengighet av tredjepart:** BankID Norge AS er databehandler
- **Fødselsnummer:** Overføres via BankID — sensitivt identifikasjonsnummer
- **Sporbarhet:** BankID-logger kan kobles til brukerens aktivitet

6.4 Tiltak

- Databehandleravtale med BankID Norge AS
- Fødselsnummer krypteres umiddelbart etter mottak
- Kun fødselsdato (for aldersverifisering) og navn lagres i klartekst
- BankID-sesjonsdata slettes etter autentisering

---

7. Transfer Impact Assessment (TIA) — Tredjelandsoverføringer

7.1 Bakgrunn

Drop tilbyr pengeoverføringer til 30+ land, hvorav flere er utenfor EØS og mangler adekvansbeslutning fra EU-kommisjonen. I tråd med Schrems II-avgjørelsen (C-311/18) og EDPBs anbefalinger 01/2020 gjennomfører vi TIA for hvert mottakerland.

7.2 Vurderingsmetodikk

For hvert mottakerland vurderes:

1. **Lovgivning:** Har myndighetene vid tilgang til kommunikasjonsdata?
2. **Praktisk erfaring:** Har vi mottatt forespørsler fra myndigheter?
3. **Dataminimering:** Hvilke data overføres, og er de nødvendige?
4. **Tekniske tiltak:** Kryptering, pseudonymisering, andre beskyttelser
5. **Kontraktuelle tiltak:** SCCs, tilleggsklausuler

7.3 Landkategorisering

Kategori	Beskrivelse	Tiltak
Adekvat (grønn)	EU-adekvansbeslutning foreligger	SCCs som tillegg
Moderat (gul)	Visse bekymringer, men akseptabel risiko	SCCs + tekniske tilleggstiltak
Høy risiko (rød)	Betydelige bekymringer om myndighetstilgang	SCCs + sterke tekniske tiltak + individuell vurdering

7.4 Overførte data ved remittance

Kun følgende data overføres til mottakers bank:

- Avsenders fulle navn (lovpålagt)
- Mottakers fulle navn og kontonummer
- Beløp og valuta
- Referansenummer

Fødselsnummer, fødselsdato, IP-adresse og annen teknisk informasjon overføres **aldri** til tredjeland.

8. Konsultasjon med berørte parter

8.1 Intern konsultasjon

- **Utvikling:** Teknisk gjennomførbarhet av tiltak
- **Compliance:** Regulatorisk samsvar
- **Drift:** Operasjonell gjennomførbarhet
- **Ledelse:** Godkjenning av restrisiko

8.2 Ekstern konsultasjon

- **BankID Norge AS:** Verifisering av sikkerhetsarkitektur
- **Open Banking-leverandør:** Datahåndtering og sikkerhet
- **Ekstern personvernrådgiver:** Uavhengig gjennomgang av DPIA

8.3 Brukermedvirkning

- Pilotbrukere har gitt tilbakemelding på personverninformasjon og samtykkeflyt
- Personvernerklæring testet for forståelighet

---

9. Restrisiko og konklusjon

9.1 Risikomatrise etter tiltak

Risiko	Opprinnelig nivå	Etter tiltak	Akseptabel?
R1: Uautorisert tilgang	8 (middels)	4 (lav)	Ja
R2: Datalekkasje	8 (middels)	4 (lav)	Ja
R3: Ulovlig profilering	3 (lav)	2 (lav)	Ja
R4: Tredjelandsoverføringer	9 (høy)	6 (middels)	Ja, med løpende TIA
R5: Feilaktig avvisning	4 (lav)	2 (lav)	Ja
R6: Manglende sletting	4 (lav)	2 (lav)	Ja
R7: BankID-kompromittering	4 (lav)	2 (lav)	Ja

Risiko	Opprinnelig nivå	Etter tiltak	Akseptabel?
R8: Tredjelandsmyndigheter	6 (middels)	4 (lav)	Ja, med løpende TIA

9.2 Konklusjon

Etter implementering av de beskrevne tiltakene vurderes restrisikoene som akseptable. Ingen risikoer krever forhåndskonsultasjon med Datatilsynet jf. GDPR artikkel 36.

Vurderingen skal gjennomgås:

- **Årlig** som del av complianceprogrammet
- **Ved vesentlige endringer** i tjenesten, teknologien eller lovgivningen
- **Ved nye mottakerland** — ny TIA gjennomføres

9.3 Godkjenning

Rolle	Navn	Dato	Signatur
Behandlingsansvarlig	Alem Bašić, ALAI Holding AS	**.**.2026	_____
Personvernombud	Alem Bašić (alem@alai.no, +47 40 47 42 51)	02.03.2026 (oppnevnt)	_____
CTO	_____	**.**.2026	_____

---

10. Vedlegg

Vedlegg A: Dataflytdiagram

Se egen teknisk dokumentasjon.

Vedlegg B: Transfer Impact Assessments per land

Se egen mappe: `/legal/tia/`

Vedlegg C: Databehandleravtaler (oversikt)

Se egen mappe: `/legal/dpa/`

Vedlegg D: Interesseavveininger (LIA)

Se egen dokumentasjon.

DPIA utarbeidet i henhold til GDPR artikkel 35, Datatilsynets veileder for vurdering av personvernkonsekvenser, og Artikkel 29-gruppens retningslinjer WP 248 rev.01.

Data Processing Protocol

Behandlingsprotokoll — Drop (ALAI Holding AS)

Dokument: Protokoll over behandlingsaktiviteter (GDPR artikkel 30) **Behandlingsansvarlig:** ALAI Holding AS, org.nr. 932 516 136 **Kontakt behandlingsansvarlig:** personvern@getdrop.no **Personvernombud:** dpo@getdrop.no **Produkt:** Drop — betalingsformidling og pengeoverforinger **Versjon:** 1.0 **Dato:** 2026-02-17 **Neste revisjon:** 2027-02-17

---

1. Brukerregistrering og identitetsverifisering

Felt	Beskrivelse
Formaal	Registrere brukere i Drop-tjenesten og verifisere identitet gjennom BankID for aa oppfylle krav i hvitvaskingsloven og betalingstjenesteloven
Rettslig grunnlag	GDPR art. 6(1)(b) oppfyllelse av avtale; GDPR art. 6(1)(c) rettslig forpliktelse (hvitvaskingsloven ss 10-18)
Kategorier av registrerte	Fysiske personer bosatt i Norge som registrerer seg som brukere av Drop
Kategorier av personopplysninger	Fullt navn, foedselsnummer (via BankID), foedselsdato, mobilnummer (+47), e-postadresse, BankID-referanse
Mottakere/overforinger	BankID-leverandor (identitetsverifisering), Sumsub (KYC-prosessering)
Overforinger til tredjeland	Sumsub — EU SCCs iht. GDPR art. 46(2)(c)
Oppbevaringstid	Kontoens levetid + 5 aar etter avsluttet kundeforhold (hvitvaskingsloven s 30)
Sikkerhetstiltak	BankID hoyt sikkerhetsnivaa (eIDAS), kryptert lagring (AES-256), RBAC, komplett revisjonslogg

---

2. BankID-verifisering og autentisering

Felt	Beskrivelse
Formaal	Autentisere brukere ved innlogging og bekreftelse av transaksjoner gjennom BankID
Rettslig grunnlag	GDPR art. 6(1)(b) oppfyllelse av avtale; GDPR art. 6(1)(c) rettslig forpliktelse (sterk kundeautentisering, PSD2 art. 97)
Kategorier av registrerte	Alle registrerte Drop-brukere
Kategorier av personopplysninger	BankID-referanse, autentiseringslogger, tidspunkt for innlogging, IP-adresse, enhetsidentifikator
Mottakere/overforinger	BankID-leverandor
Overforinger til tredjeland	Ingen — BankID-infrastruktur er i Norge/EOS
Oppbevaringstid	Innloggingslogger: 12 maaneder; BankID-referanser: kontoens levetid + 5 aar
Sikkerhetstiltak	TLS 1.3, sesjonstokens med utloep, rate limiting, IP-blokkering ved gjentatte feilforsoek

---

3. Kundekontroll (KYC/CDD)

Felt	Beskrivelse
Formaal	Gjennomfoere lovpaalagt kundekontroll (Customer Due Diligence) iht. hvitvaskingsloven, inkludert PEP- og sanksjonsscreening
Rettslig grunnlag	GDPR art. 6(1)(c) rettslig forpliktelse (hvitvaskingsloven ss 10-18, s 30)
Kategorier av registrerte	Alle brukere ved registrering; brukere som utloeser forsterket kundekontroll (EDD)
Kategorier av personopplysninger	Identitetsdokumenter, PEP-status, sanksjonslistekontroll-resultater, risikoklassifisering, midlenes opprinnelse (ved EDD), formaal med kundeforhold
Mottakere/overforinger	Sumsub (KYC-prosessering), PEP/sanksjonslisteleverandor, Folkeregisteret (adresseoppslag)
Overforinger til tredjeland	Sumsub — EU SCCs; sanksjonslister (FN, EU, OFAC) behandles lokalt
Oppbevaringstid	5 aar etter kundeforholdets opphoer (hvitvaskingsloven s 30)

Felt	Beskrivelse
Sikkerhetstiltak	Kryptert lagring (AES-256), separat tilgangskontroll for compliance-personell, komplett revisjonslogg for all tilgang

4. Gjennomfoering av betalingstransaksjoner

Felt	Beskrivelse
Formaal	Initiere og gjennomfoere utenlandsoverforinger (remittance) og QR-betalinger paa vegne av brukeren via Open Banking (PSD2 PISP)
Rettslig grunnlag	GDPR art. 6(1)(b) oppfyllelse av avtale; GDPR art. 6(1)(c) rettslig forpliktelse (bokfoeringsloven s 13)
Kategorier av registrerte	Brukere som gjennomfoerer transaksjoner; betalingsmottakere
Kategorier av personopplysninger	Avsenders navn og kontonummer, mottakers navn og kontonummer/referanse, beloep, valuta, vekslingskurs, formaalskode, tidspunkt, idempotency-noekkel
Mottakere/overforinger	Open Banking-leverandor (PISP), brukerens bank, korrespondentbanker i mottakerland, betalingsnettverk (QR)
Overforinger til tredjeland	Mottakers bank ved utenlandsoverforinger — EU SCCs iht. GDPR art. 46(2)(c) eller art. 49(1)(b) nodvendig for avtale
Oppbevaringstid	5 aar etter regnskapsaarets slutt (bokfoeringsloven s 13)
Sikkerhetstiltak	TLS 1.3, BankID-bekreftelse per transaksjon, idempotency-kontroll, komplett revisjonslogg, beloepsgrenser

5. AML-overvaaking og mistenkelige transaksjoner

Felt	Beskrivelse
Formaal	Loepende overvaaking av transaksjoner for aa avdekke hvitvasking og terrorfinansiering iht. hvitvaskingsloven, inkludert automatisk flagging og manuell gjennomgang

Felt	Beskrivelse
Rettslig grunnlag	GDPR art. 6(1)(c) rettslig forpliktelse (hvitvaskingsloven ss 24-26)
Kategorier av registrerte	Alle brukere med transaksjoner; brukere med flaggede transaksjoner
Kategorier av personopplysninger	Transaksjonsmoenster, kumulative volumer, korridorrisikovurdering, AML-alarmer (type, alvorlighetsgrad), undersoekelsesstatus, STR-rapporter
Mottakere/overforinger	Oekokrim/EFE (ved rapportering via Altinn), Finanstilsynet (tilsynsrapportering)
Overforinger til tredjeland	Ingen — all rapportering til norske myndigheter
Oppbevaringstid	5 aar etter kundeforholdets opphoer (hvitvaskingsloven s 30)
Sikkerhetstiltak	Automatisert regelbasert overvaaking, separat compliance-dashboard, revisjonslogg, tipping off-forbud (s 28)

6. Kontoinformasjonstjeneste (AISP)

Felt	Beskrivelse
Formaal	Hente og vise bankkontobalanse og kontoinformasjon fra brukerens bank via Open Banking AISP
Rettslig grunnlag	GDPR art. 6(1)(a) samtykke (bruker gir eksplisitt AISP-samtykke ved registrering)
Kategorier av registrerte	Brukere som har gitt AISP-samtykke
Kategorier av personopplysninger	Bankkontonummer, IBAN, banknavn, kontosaldo, saldosynkroniseringstidspunkt
Mottakere/overforinger	Open Banking-leverandor (AISP), brukerens bank
Overforinger til tredjeland	Ingen — norsk/EOS bankinfrastruktur
Oppbevaringstid	Saldo-cache: slettes ved neste synkronisering; kontokobling: kontoens levetid + 1 aar
Sikkerhetstiltak	Samtykkebasert tilgang, TLS 1.3, minimal datalagring (cache-modell), samtykke kan trekkes tilbake

7. Kundeservice og klagebehandling

Felt	Beskrivelse
Formaal	Behandle henvendelser, klagemaal og support-foresporsler fra brukere
Rettslig grunnlag	GDPR art. 6(1)(b) oppfyllelse av avtale; GDPR art. 6(1)(c) rettslig forpliktelse (PSD2 art. 101, betalingstjenesteloven)
Kategorier av registrerte	Brukere som henvender seg til kundeservice eller klager
Kategorier av personopplysninger	Navn, e-post, telefonnummer, klageinnhold (kategori, emne, beskrivelse), losningsstatus, behandlingshistorikk
Mottakere/overforinger	Kundeserviceplattform (databehandler); Finansklagenemnda ved eskalerte klager
Overforinger til tredjeland	Avhengig av kundeserviceplattform — EU SCCs
Oppbevaringstid	3 aar etter avsluttet henvendelse (foreldelsesloven)
Sikkerhetstiltak	Tilgangskontroll for kundeservicepersonell, kryptering, revisjonslogg

---

8. Varsler og kommunikasjon

Felt	Beskrivelse
Formaal	Sende push-varsler, e-postvarsler og app-meldinger om transaksjoner, sikkerhet og tjenesteinformasjon
Rettslig grunnlag	GDPR art. 6(1)(b) oppfyllelse av avtale (transaksjonsvarsler); GDPR art. 6(1)(a) samtykke (markedsfoering)
Kategorier av registrerte	Alle registrerte brukere
Kategorier av personopplysninger	Bruker-ID, varslingstype, innhold, lest-status, push-abonnement (endpoint, noekler), e-postadresse, varslingsinnstillinger
Mottakere/overforinger	Push-varslingsleverandor (Apple APNs / Google FCM)
Overforinger til tredjeland	Apple (USA) og Google (USA) for push-varsler — EU SCCs
Oppbevaringstid	Varsler: 12 maaneder; markedsforingssamtykke: til tilbaketrekking + 1 aar dokumentasjon
Sikkerhetstiltak	Kryptering av push-innhold, samtykke for markedsfoering, opt-out mulighet

---

9. Teknisk drift, logging og feilsoking

Felt	Beskrivelse
Formaal	Sikre stabil drift av tjenesten, oppdage og rette feil, forhindre sikkerhetsbrudd, og opprettholde revisjonslogg
Rettslig grunnlag	GDPR art. 6(1)(f) berettiget interesse (IT-sikkerhet og driftsstabilitet); GDPR art. 6(1)(c) rettslig forpliktelse (revisjonslogg for finansielle tjenester)
Kategorier av registrerte	Alle brukere; systemadministratorer
Kategorier av personopplysninger	IP-adresse, brukeragent, enhetsidentifikator, feillogger, krasjrapporter, API-tilgangslogger, request-ID, revisjonslogg (handlinger, tidspunkt, ressurs)
Mottakere/overforinger	Sentry (feilrapportering, databehandler); skyinfrastrukturleverandor
Overforinger til tredjeland	Sentry — EU SCCs
Oppbevaringstid	Tekniske logger: 6 maaneder; IP-adresser: 3 maaneder; revisjonslogg: 5 aar
Sikkerhetstiltak	Strukturert JSON-logging med request-ID, tilgangskontroll til loggdata, automatisk sletting

10. Analyse og tjenesteforbedring

Felt	Beskrivelse
Formaal	Forbedre brukeropplevelsen, analysere bruksmoenstre og optimalisere tjenesten basert paa anonymisert/pseudonymisert data
Rettslig grunnlag	GDPR art. 6(1)(a) samtykke (analytiske cookies); GDPR art. 6(1)(f) berettiget interesse (intern statistikk paa anonymisert data)
Kategorier av registrerte	Brukere som har gitt samtykke til analytiske cookies; alle brukere (anonymisert/aggregert)
Kategorier av personopplysninger	Anonymisert navigasjonsdata, funksjonsbruk (aggregert), app-versjon, operativsystem, responstider (aggregert)
Mottakere/overforinger	Analyseverktoy (databehandler, anonymiserte data)
Overforinger til tredjeland	Avhengig av analyseverktoy — kun anonymiserte data
Oppbevaringstid	Anonymisert data: ingen begrensning; raadata: 12 maaneder
Sikkerhetstiltak	Dataminimering, anonymisering/pseudonymisering, cookie-samtykke (ekomloven s 2-7b), ingen re-identifisering

Generelle sikkerhetstiltak (GDPR artikkel 32)

Foelgende tiltak gjelder for alle behandlingsaktiviteter:

- **Kryptering i transit:** TLS 1.3 for all dataoverforing
- **Kryptering i hvile:** AES-256 for lagrede personopplysninger
- **Tilgangskontroll:** Rollebasert tilgangsstyring (RBAC), prinsippet om minste privilegium
- **Autentisering:** BankID for brukere, MFA for ansatte/administratorer
- **Logging:** Komplett revisjonslogg for all tilgang til personopplysninger (audit_log-tabell)
- **Saarbarhetshåndtering:** Regelmessig penetrasjonstesting og saarbarhetsskanning
- **Hendelseshaandtering:** Etablerte prosedyrer for sikkerhetsbrudd, 72-timers melding til Datatilsynet
- **Backup:** Daglig kryptert backup med kontrollert tilgang
- **Sletting:** Automatiserte sletteprosedyrer ved utloep av oppbevaringstid

---

Databehandlere (GDPR artikkel 28)

Databehandler	Formaal	Lokalisering	Overforingsgrunnlag
Swan (BaaS)	Banking-as-a-Service, kontoforvaltning	EU (Frankrike)	Innenfor EOS
Sumsub	KYC/identitetsverifisering	EU/UK	EU SCCs
Sentry	Feilrapportering og ytelsesovervaaking	EU/USA	EU SCCs
BankID	Autentisering og identitetsverifisering	Norge	Innenfor EOS
Skyinfrastrukturleverandor	Hosting og databehandling	EU/EOS	Innenfor EOS
Push-varslingsleverandor (APNs/FCM)	Push-varsler	USA	EU SCCs

Alle databehandlere har inngaatt databehandleravtale (DPA) iht. GDPR artikkel 28.

Endringslogg

Versjon	Dato	Endring	Godkjent av

1.0	2026-02-17	Forstegangs utarbeidelse — 10 behandlingsaktiviteter	Daglig leder

---

Denne behandlingsprotokollen er utarbeidet iht. GDPR artikkel 30 og personopplysningsloven (LOV-2018-06-15-38). Protokollen skal vaere tilgjengelig for Datatilsynet paa forespørsel.

Outsourcing Policy

Utkontrakteringspolicy — Drop

Dokument-ID: UTKONTR-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Eier:** ALAI Holding AS, org.nr. 932 516 136 **Klassifisering:** Intern **Regulatorisk grunnlag:** DORA (EU) 2022/2554 art. 28-30, Finanstilsynets retningslinjer for utkontraktering

---

1. Innledning

1.1 Formål

Denne policyen etablerer rammeverket for styring av utkontraktering og tredjepartsleverandører som understøtter Drop-tjenesten. Policyen sikrer at risikoen knyttet til utkontraktering identifiseres, vurderes og håndteres i samsvar med DORA og Finanstilsynets krav.

1.2 Virkeområde

Policyen gjelder for:

- Alle IKT-tjenester som er utkontraktert til tredjeparter
- Alle tredjepartsleverandører som har tilgang til Drop-systemer eller -data
- Internt utkontrakterte tjenester (innen konsern)
- Underleverandører til våre tredjepartsleverandører (kjede)

1.3 Regulatorisk bakgrunn

Regulering	Artikler	Beskrivelse
DORA (EU) 2022/2554	Art. 28	Generelle prinsipper for IKT-tredjepartsrisiko
DORA (EU) 2022/2554	Art. 29	Forhåndsvurdering av IKT-tredjepartsrisiko
DORA (EU) 2022/2554	Art. 30	Kontraktuelle krav
GDPR (EU) 2016/679	Art. 28	Databehandlere

Regulering	Artikler	Beskrivelse
PSD2 (EU) 2015/2366	Art. 19	Agenter og utkontraktering
Finanstilsynets rundskriv	—	Retningslinjer for utkontraktering
IKT-forskriften	—	Krav til IKT-drift

---

2. Prinsipper

2.1 Overordnede prinsipper

1. **Ledelsesansvar:** Styret og ledelsen har det overordnede ansvaret for all utkontraktering, jf. DORA art. 28(2). Utkontraktering fritar ikke selskapet fra regulatoriske forpliktelser.
2. **Risikostyring:** All utkontraktering vurderes gjennom vårt IKT-risikostyringsrammeverk.
3. **Proporsjonalitet:** Krav til leverandørstyring er proporsjonale med tjenestens kritikalitet.
4. **Konsentrasjonrisiko:** Vi vurderer og unngår uhensiktsmessig konsentrasjon hos enkeltleverandører.
5. **Exit-strategi:** Vi sikrer at vi kan avslutte eller overføre enhver utkontraktert tjeneste.

2.2 Hva som kan utkontrakteres

Følgende kan utkontrakteres med adekvat risikostyring:

- IKT-infrastruktur (hosting, lagring)
- Open Banking-tjenester (PSD2 PISP/AISP)
- Autentiseringstjenester (BankID)
- Kundeserviceteknologi
- Analysetjenester (anonymiserte data)

2.3 Hva som ikke kan utkontrakteres

Følgende kan ikke utkontrakteres:

- Overordnet risikostyring og compliance-overvåking
- Beslutninger om strategi og styring
- Overordnet ansvar for kundekontroll (KYC/AML)
- Regulatorisk rapportering (operasjonelt kan delegeres, ansvaret forblir)

---

3. Kritikalitetsklassifisering

3.1 Klassifiseringsmodell

Klasse	Beskrivelse	Kriterier	Eksempler
Kritisk	Bortfall medfører umiddelbar stans i kjernetjenester	Betalingsbehandling, autentisering, datalagring	Open Banking-leverandør, BankID, skyinfrastruktur, database
Viktig	Bortfall medfører vesentlig degradering	Kundeservice, rapportering, overvåking	Kundeserviceplattform, SIEM, analysetjenester
Standard	Bortfall medfører begrenset påvirkning	Støttefunksjoner, utviklingsverktøy	E-postleverandør, utviklingsmiljø, CI/CD

3.2 Kriterier for klassifisering

Klassifisering baseres på:

- **Konsekvens ved bortfall:** Påvirkning på kjernetjenester og brukere
- **Datatilgang:** Tilgang til personopplysninger eller finansielle data
- **Substituerbarhet:** Mulighet for rask erstatning
- **Regulatorisk relevans:** Tjenestens rolle i regulatorisk etterlevelse
- **Konsentrasjonsrisiko:** Avhengighet til enkelteleverandør

3.3 Register over utkontrakterte tjenester

Vi vedlikeholder et oppdatert register over alle utkontrakterte IKT-tjenester, jf. DORA art. 28(3), som minimum inneholder:

- Leverandørens navn, organisasjonsnummer og kontaktinformasjon
- Tjenestebeskrivelse
- Kritikalitetsklasse
- Dato for avtaleinngåelse og utløp
- Databehandlerstatus (ja/nei)
- Land der tjenesten utføres
- Underleverandører
- Dato for siste risikovurdering

---

4. Due diligence — DORA art. 29

4.1 Forhåndsvurdering

Før inngåelse av avtale om utkontraktering gjennomføres due diligence proporsjonalt med tjenestens kritikalitet:

Kritiske tjenester — utvidet due diligence

Område	Vurdering
Finansiell stabilitet	Kredittvurdering, årsregnskap, eierstruktur
Teknisk kompetanse	Referanser, sertifiseringer, teknisk arkitektur
Sikkerhet	Sikkerhetssertifiseringer (ISO 27001, SOC 2), penetrasjonstester
Regulatorisk samsvar	Relevante lisenser, tilsynsstatus, DORA-beredskap
Operasjonell resiliens	BCP/DR-kapasitet, SLA-historikk, hendelseshistorikk
Personvern	GDPR-samsvar, databehandleravtale, TIA ved tredjeland
Konsentrasjonrisiko	Leverandørens markedsandel, avhengigheter
Underleverandører	Oversikt og vurdering av kritiske underleverandører
Exit-mulighet	Dataportabilitet, overgangsperiode, migrasjonsplan

Viktige tjenester — standard due diligence

- Teknisk kompetanse og referanser
- Sikkerhetssertifiseringer
- GDPR-samsvar og databehandleravtale
- SLA-betingelser
- Exit-klausuler

Standard tjenester — forenklet due diligence

- Grunnleggende selskapsinfo
- Relevante sertifiseringer
- GDPR-samsvar der relevant
- Kontraktvilkår

4.2 Risikovurdering

Due diligence resulterer i en risikovurdering som dokumenterer:

- Identifiserte risikoer per kategori
- Risikonivå (lav, middels, høy, kritisk)
- Anbefalte mitigerende tiltak

- Gjenværende risiko
- Anbefaling (godkjent, godkjent med betingelser, avvist)

4.3 Godkjenning

Kritikalitet	Godkjenner
Kritisk	Styret
Viktig	Daglig leder
Standard	CISO

---

5. Kontraktuelle krav — DORA art. 30

5.1 Obligatoriske kontraktbestemmelser

Alle avtaler om utkontraktering av IKT-tjenester skal inneholde følgende, jf. DORA art. 30:

5.1.1 Tjenestebeskrivelse

- Detaljert beskrivelse av tjenesten
- Tjenestenivå (SLA) med målbare kriterier
- Rapporteringsforpliktelser

5.1.2 Sikkerhet

- Sikkerhetskrav i henhold til vår IKT-sikkerhetspolicy
- Hendelsesrapportering — varsling til oss uten ugrunnet opphold, senest innen 24 timer
- Sårbarhetshåndtering og patchkrav
- Krypteringskrav

5.1.3 Databehandling

- Databehandleravtale iht. GDPR artikkel 28 (for alle leverandører som behandler personopplysninger)
- Datalokalitet (EØS-krav)
- Sletting/tilbakelevering ved avtalens opphør
- Forbud mot sekundærbruk av data

5.1.4 Tilsyn og revisjon

- Vår rett til revisjon og inspeksjon, jf. DORA art. 30(3)(e)
- Finanstilsynets rett til tilgang og informasjon

- Samarbeid med tredjepartsrevisorer
- Rett til on-site inspeksjon ved kritiske tjenester

5.1.5 Underleverandører

- Forhåndsgodkjenning av kritiske underleverandører
- Varsling ved endring av underleverandører
- Samme kontraktuelle krav videreføres i kjeden
- Rett til å motsette seg bruk av spesifikke underleverandører

5.1.6 Kontinuitet og exit

- Leverandørens forpliktelser ved egen konkurs eller opphør
- Overgangsperiode ved oppsigelse (minimum tilstrekkelig for migrasjon)
- Bistand ved overføring til ny leverandør
- Dataportabilitet og -tilbakelevering
- Videreføring av tjeneste under overgangsperiode

5.1.7 Oppsigelse

- Gjensidig oppsigelsesrett med rimelig varsel
- Rett til umiddelbar oppsigelse ved vesentlig mislighold
- Rett til oppsigelse dersom leverandøren ikke oppfyller regulatoriske krav
- Rett til oppsigelse ved endringer som vesentlig påvirker risikoprofilen

5.2 Tilleggskrav for kritiske tjenester

For kritiske tjenester kreves i tillegg:

- Detaljert BCP/DR-plan med testforpliktelse
- Dedikerte sikkerhetskontakter og eskaleringsprosedyrer
- Kvartalsvise ytelsesrapporter
- Årlig uavhengig sikkerhetsrevisjon (eller deling av SOC 2-rapport)
- Minimumsgaranti for tilgjengelighet (99,9% eller høyere)
- Penalty-klausuler ved gjentatte SLA-brudd

---

6. Løpende overvåking

6.1 Overvåkingsrammeverk

Kritikalitet	Frekvens for gjennomgang	Revisjon	SLA-rapportering

Kritisk	Kvartalsvis	Årlig	Månedlig
Viktig	Halvårlig	Hvert 2. år	Kvartalsvis
Standard	Årlig	Ved behov	Halvårlig

6.2 Løpende vurdering

For alle utkontrakterte tjenester overvåkes:

- SLA-etterlevelse og tjenestekvalitet
- Sikkerhetshendelser og sårbarhetsstatus
- Regulatorisk etterlevelse
- Finansiell stabilitet (for kritiske leverandører)
- Endringer i underleverandørkjeden
- Endringer i risikoprofil

6.3 Hendelseshåndtering

Ved hendelser hos leverandør:

1. Leverandør varsler oss iht. avtalt prosedyre
2. Vi vurderer konsekvens for Drop-tjenesten
3. Vi aktiverer interne prosedyrer ved behov (se `hendelseshaandtering.md`)
4. Vi rapporterer til Finanstilsynet ved vesentlig IKT-hendelse
5. Hendelsen dokumenteres og følges opp

6.4 Leverandørmøter

Kritikalitet	Frekvens	Agenda
Kritisk	Kvartalsvis (min.)	SLA-gjennomgang, sikkerhetsoppdatering, roadmap, hendelser
Viktig	Halvårlig	SLA-gjennomgang, sikkerhetsoppdatering
Standard	Årlig	Generell gjennomgang

---

7. Exit-strategi

7.1 Prinsipper

For alle utkontrakterte tjenester av klasse Kritisk og Viktig skal det foreligge en dokumentert exit-strategi. Exit-strategien sikrer at tjenesten kan overføres til alternativ leverandør eller tas tilbake internt uten uakseptabel forstyrrelse.

7.2 Exit-plan per kritisk tjeneste

Hver exit-plan inneholder:

- **Trigger-hendelser:** Scenarioer som utløser exit (oppsigelse, mislighold, konkurs, regulatorisk pålegg)
- **Alternativ leverandør:** Identifisert og prekvalifisert alternativ
- **Migrasjonsprosedyre:** Steg-for-steg-plan for overføring
- **Tidsramme:** Estimert tid for komplett migrasjon
- **Ressursbehov:** Personell, teknologi, budsjett
- **Dataoverføring:** Prosedyre for sikker overføring/sletting av data
- **Testprosedyre:** Verifisering av tjenestekvalitet hos ny leverandør
- **Kommunikasjon:** Plan for informasjon til brukere og myndigheter

7.3 Spesifikke exit-strategier

Open Banking-leverandør (Kritisk)

- Sekundær leverandør identifisert og API-integrert (varm standby)
- Switchover testbar innen 4 timer
- Full migrasjon innen 30 dager
- Data: Transaksjonshistorikk overføres eller gjenopprettes fra egen database

Skyinfrastruktur (Kritisk)

- Infrastruktur-som-kode (IaC) sikrer reproduserbarhet
- Sekundær region hos alternativ leverandør prekonfigurert
- Database-replikering til alternativ plattform
- Full migrasjon innen 14 dager

BankID (Kritisk)

- Ingen realistisk alternativ autentiseringsløsning i Norge
- Exit-strategi: Degradert modus med midlertidig autentisering i begrenset periode
- Avhengigheten aksepteres som nasjonal infrastrukturrisiko

7.4 Testing av exit-strategi

- Tabletop-gjennomgang årlig for kritiske leverandører
- Teknisk exit-test (failover) halvårlig for leverandører med varm standby

- Dokumentasjon av testresultater og forbedringspunkter

---

8. Finanstilsynet — varsling og rapportering

8.1 Varsling

I henhold til Finanstilsynets retningslinjer og DORA varsles Finanstilsynet:

- **Før inngåelse:** Av avtaler om utkontraktering av kritiske IKT-tjenester
- **Ved vesentlige endringer:** I eksisterende avtaler for kritiske tjenester
- **Ved hendelser:** Hos leverandører som påvirker vår tjenesteleveranse vesentlig

8.2 Informasjon til Finanstilsynet

Varsling inneholder:

- Leverandørens identitet
- Tjenestens art og kritikalitet
- Risikovurdering
- Kontraktuelle beskyttelser
- Exit-strategi
- Konsekvenser for tjenesteleveranse

8.3 Register tilgjengelig for tilsyn

Vi opprettholder et oppdatert register over all utkontraktering som gjøres tilgjengelig for Finanstilsynet på forespørsel, jf. DORA art. 28(3).

---

9. Konsentrasjonsrisiko — DORA art. 29(2)

9.1 Vurdering

Vi vurderer regelmessig konsentrasjonsrisiko, inkludert:

- Avhengighet til enkelteleverandører for kritiske tjenester
- Geografisk konsentrasjon (alle tjenester i samme region/land)
- Teknologisk konsentrasjon (alle tjenester på samme plattform)
- Sektorkonsentrasjon (leverandørers avhengighet av samme bransje)

9.2 Mitigering

- Sekundære leverandører for kritiske tjenester
- Geografisk diversifisering av infrastruktur (flere regioner/soner)
- Unngå kritisk avhengighet til én enkelt skyplattform der mulig
- Regelmessig vurdering av leverandørmarkedet

---

10. Internkontroll

10.1 Roller og ansvar

Rolle	Ansvar
Styret	Godkjenning av policy og kritiske avtaler
Daglig leder	Overordnet ansvar for utkontraktering, godkjenning av viktige avtaler
CISO	Sikkerhetsvurdering, due diligence, løpende overvåking
Compliance-ansvarlig	Regulatorisk samsvar, Finanstilsynet-rapportering
Innkjøpsansvarlig	Kontraktshåndtering, leverandørkontakt
Driftsteam	Operasjonell oppfølging, SLA-overvåking

10.2 Første linje — operasjonell styring

- Daglig overvåking av tjenestekvalitet
- Oppfølging av SLA-etterlevelse
- Kontaktpunkt mot leverandør

10.3 Andre linje — kontroll og risikostyring

- Periodisk risikovurdering
- Due diligence-gjennomføring
- Policy-etterlevelse

10.4 Tredje linje — uavhengig kontroll

- Årlig gjennomgang av utkontrakteringspolicyen
- Stikkprøvekontroll av leverandøravtaler
- Rapportering til styret

---

11. Revisjon og oppdatering

11.1 Gjennomgang

- **Årlig:** Full gjennomgang av policyen
- **Ved nye kritiske avtaler:** Vurdering av behov for policyendringer
- **Ved regulatoriske endringer:** Oppdatering iht. nye krav
- **Etter hendelser:** Revisjon basert på hendelser hos leverandører

11.2 Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

Vedlegg

Vedlegg A: Register over utkontrakterte tjenester

Separat dokument — vedlikeholdes av CISO.

Vedlegg B: Mal for due diligence-rapport

Separat dokument — tilgjengelig ved forespørsel.

Vedlegg C: Mal for exit-plan

Separat dokument — tilgjengelig ved forespørsel.

Vedlegg D: Sjekkliste for kontraktskrav (DORA art. 30)

Separat dokument — brukes ved alle nye avtaler.

Denne utkontrakteringspolicyen er eid av CISO og godkjent av styret i ALAI Holding AS.