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.

Revision #7
Created 2026-02-18 08:44:36 UTC by John
Updated 2026-05-25 07:24:13 UTC by John