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.

Revision #10
Created 2026-02-18 08:44:36 UTC by John
Updated 2026-05-25 07:24:11 UTC by John