Personvern og arkitektur

Kortversjon for banker, kommuner og partnere · status per 28. september 2026

Filip er brukerens eget hjelpemiddel, ikke bankens system. Filip er en nettleserutvidelse som brukeren selv installerer, på egen enhet. Den peker på riktig knapp og forklarer neste steg – brukeren utfører alle handlinger selv. Filip har ingen integrasjon mot bankens systemer, ingen API-tilgang og ingen innlogging på bankens vegne. **Banken behandler ingen personopplysninger på grunn av Filip.** Som en skjermleser er Filip brukerens eget verktøy – men Filip sender navn på skjermelementer til en språkmodell, og derfor er det strengt avgrenset hva som sendes.

Hva Filip leser – og hva Filip aldri leser

Leser	Leser aldri
Tekst på knapper, felt-etiketter, overskrifter og menyvalg – det som trengs for å finne neste steg. Maks 80 elementer per steg. Neste versjon: bare navn på knapper og felt (kvitelisting).	Passord, PIN, engangskoder og BankID-koder: feltene utelates helt. Beløp, saldo og kontonumre: tall maskeres før noe sendes. Skjermbilder – Filip tar aldri bilde av skjermen. Personnavn og fritekst: filtreres bort fra neste versjon.

Slik er Filip bygd – prinsipp for prinsipp

Prinsipp	Slik er det gjort	Status
Roller (GDPR)	Brukeren samtykker på en egen skjerm ved første start og kan trekke samtykket ved å avinstallere (art. 6 nr. 1 a). Filip er behandlingsansvarlig (Filip AS når selskapet er stiftet). Banken er ikke part i behandlingen.	Neste versjon
Formål	Kun steg-for-steg-veiledning i det brukeren selv har bedt om. Ingen profilering, markedsføring, analyse av innhold eller trening av modeller.	Innført
Dataminimering	I dag: tall maskeres og kodefelt utelates før noe sendes. Neste versjon: kvitelisting – bare navn på knapper og felt kan forlate enheten.	Neste versjon
Lagring og sletting	Filip lagrer ikke skjerminnhold. Hvor i en oppgave brukeren er, holdes lokalt i nettleseren i inntil 10 minutter per fane og slettes automatisk. Ingen brukerdata lagres på Filips servere.	Innført
Server i midten	Nøklene flyttes fra nettleseren til en server (proxy) som også kontrollerer hva som sendes. Den logger bare metadata som tidspunkt og feilkoder – aldri innhold – og sletter loggene etter 90 dager.	Neste versjon
Underleverandører	Språkmodell: Anthropic (Claude) via API under databehandleravtale; data brukes ikke til trening. Talesyntese: OpenAI, bare Filips egne replikker – aldri verdier. Talegjenkjenning: nettleserens egen, i Chrome behandlet av Google. På sikt: lokal språkmodell i nettleseren.	Innført
Handlinger	Filip kan ikke klikke, fylle inn, sende eller godkjenne noe – bare peke og forklare. Kjører i nettleserens sandkasse med minste nødvendige tillatelser.	Innført
Innsyn	«Hva Filip så»: brukeren kan når som helst se ordrett hva som ble sendt for siste steg. Samtykkeskjermen ved første start forklarer hva Filip ser og aldri ser.	Neste versjon
Svindelvern	I dag: Filip ber aldri om koder og leser aldri kodefelt. Neste versjon: ved BankID minner Filip hver gang om at passordet er brukerens eget, og at ingen ekte hjelper spør etter det.	Neste versjon
Gjennomgang	Personvernvurdering (DPIA) gjøres før pilot. Kildekoden og vurderingen kan deles med bankens sikkerhets- og personvernmiljø. Ekstern sikkerhetsgjennomgang av koden før vi skalerer.	Før pilot

Bankens rolle – to steg

1 · Anbefale. Banken tilbyr Filip til kunder som vil bli selvhjulpne i nettbanken, for eksempel kunder som i dag ringer for enkle oppgaver. Ingen integrasjon, ingen databehandleravtale, ingen DPIA hos banken – kunden bruker sitt eget verktøy på egen enhet.

2 · Bygge inn. Når verdien er dokumentert i pilot, bygger banken Filip inn i nettbanken og appen – også på mobil. Da er Filip leverandør med databehandleravtale, og banken velger hvor modellen kjører: i et europeisk datasenter eller hos banken selv.

Markus Bolli Austrheim · Filip · markusaustrheim@gmail.com · 932 56 491 · heifilip.no