Regulatoriske avklaringer for datadeling i BankID Antisvindel 2.0

Sluttrapport fra Stø AS' deltakelse i regulatoriske sandkasse

2. februar 2026

Besøksadresse
Biskop Gunnerus gate 14A
0185 Oslo

Postadresse
Postboks 9236 Grønland
0134 Oslo

org.nr
NO 927 611 929 MVA

1 Innhold

Sammendrag

Bruk av BankID (elektronisk ID) er svært utbredt i Norge, både for autentisering og signering. Dette har gjort det enkelt å bruke digitale tjenester, men har også skapt alvorlige utfordringer knyttet til ID-misbruk og økonomisk kriminalitet.

Når antall bedragerier og svindel med elektronisk ID øker, særlig misbruk av BankID til betaling og låneopptak, er det behov for ytterligere sikkerhetstiltak. Dette forutsetter mer samarbeid og informasjonsutveksling mellom aktører som tilrettelegger for digitale tjenester.

Sandkasseprosjektet, som Stø AS (heretter «Stø», «utsteder» eller «tilbyder») deltok i fra april til november 2025, hadde som mål å kartlegge muligheter for å avtaleregulere forpliktelser for BankID-brukersteder om innsendelse av flere datapunkter til BankID Antisvindel 2.0-systemet, utrede lovligheten av behandlingen, samt å vurdere behovet for tydeligere lovhjemler for datadeling (informasjonsutveksling) for å forebygge og avdekke bedrageri (herunder svindel).

Stø, sammen med Datatilsynet og Finanstilsynet, besluttet derfor å diskutere fire rettslige vurderingstemaer innenfor rammebetingelsene for finansforetak og personvernprinsippene; taushetsregler, behandlingsansvar, behandlingsgrunnlag og nødvendigheten av nye datapunkter.

Oppsummert, har Stø gjort følgende juridiske vurderinger, med veiledning fra Datatilsynet og Finanstilsynet:

1. **Taushetsplikt** – utsteder kan opptre som avtalebasert tredjepartstilbyder av IKT-tjenester og «oppdragstaker» i taushetsreglenes forstand og vil dermed ikke være en «uvedkommende».

2. **Behandlingsansvar** – BankID Antisvindel 2.0 er et nødvendig tiltak for en utsteder etter lov om elektroniske tillitstjenester iht. krav i eIDAS og i dagens trusselbilde. Stø som utsteder er behandlingsansvarlig for behandling av personopplysninger i tjenesten, herunder innsamling av nye datapunkter.

3. **Behandlingsgrunnlag** – utsteder benytter «rettslig forpliktelse» som behandlingsgrunnlag, med lov om elektroniske tillitstjenester som supplerende rettsgrunnlag, herunder artikkel 9 nr. 2 bokstav g for eventuelle behandlinger av særlige kategorier personopplysninger.

   Et aktuelt behandlingsgrunnlag for brukerstedets utlevering av datapunkter kan være «berettiget interesse».

   I det tilfelle et brukersted behandler (utleverer) personopplysninger som *kan* indikere særlige kategorier personopplysninger ble temaet diskutert særskilt i sandkassen. Datatilsynet veiledet Stø og utelukket ikke en tolkning av unntaksmuligheten i artikkel 9 nr. 2 bokstav g hvor behandlingen er nødvendig av hensyn til viktige allmenne interesser og åpner for en tolkning at lovgrunnlaget ikke

direkte må rette seg mot den behandlingsansvarlige. Dvs. at brukerstedet kan henvise til lov om elektroniske tillitstjenester.

4. **Nye datapunkter** – omfanget av innsamling av datapunkter i BankID Antisvindel 2.0 ble vurdert i forhold til dataminimeringsprinsippet, nødvendighetsvilkåret og forholdsmessighetsprinsippet. Stø vurderte det slik at databruken er nødvendig, formålsbegrenset og forholdsmessig for å forhindre identitetsmisbruk, selv om den innebærer et begrenset personverninngrep.

I sluttrapporten fremhever Stø behovet for tydeligere regulering av svindelforebyggende tiltak, spesielt gjennom nye forskriftsregler om informasjonsutveksling i alle relevante sektorer hvor elektronisk ID blir benyttet, som for eksempel overfor finansforetak, offentlige myndigheter og telekom, men også tydeligere delingsadgang for andre typer brukersteder som benytter elektronisk ID.

Stø deltok i sandkassen med produkteier for BankID Antisvindel 2.0 og ressurser fra juridisk avdeling og personvernombud. Finanstilsynet og Datatilsynet hadde roller som veiledere i sandkassen.

Om sandkasseprosjektet

Datatilsynet og Finanstilsynet inviterte i november 2024 virksomheter til å søke om å delta med prosjekter i etatenes regulatoriske sandkasse. Prosjektene skulle utforske muligheter for bedre datadeling for å bekjempe økonomisk kriminalitet.

Invitasjon fra Finanstilsynet lød som følger:

> *«Økonomisk kriminalitet er et alvorlig samfunnsproblem. Forebygging og bekjempelse legger beslag på vesentlige ressurser, som bør brukes mer effektivt enn i dag. Det krever bedre systemer for informasjonsutveksling og vilje til deling og samarbeid mellom private og offentlige aktører»*[1]

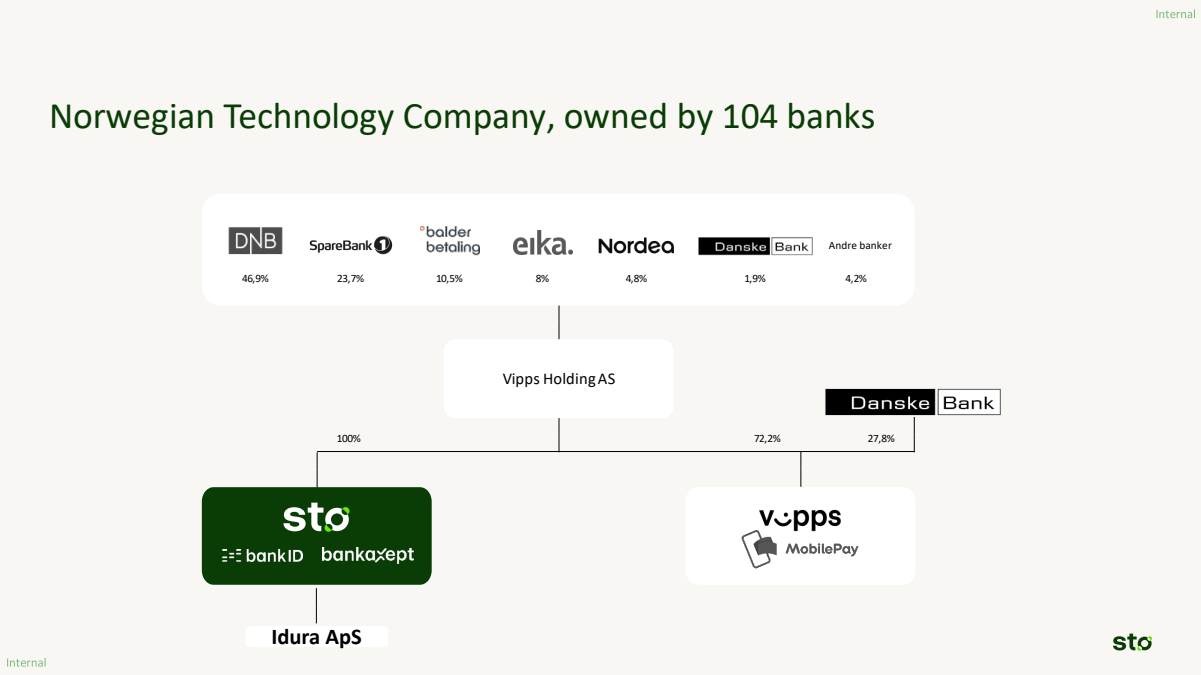
Stø var én av fem søkere som ble tatt opp i sandkassen med løsningen BankID Antisvindel 2.0, som forvalter svindelhåndtering i BankID-tjenestene. Hensikten med antisvindelsystemet er å forbedre ivaretakelsen av BankID-sluttbrukere sin bruk av BankID, både i form av sikkerhetsmonitorering, analysering, profilering, ved å gi sluttbrukeren informasjon i transaksjonsøyeblikket og i etterkant, og gi alarm og risikoscore til brukersteder.

BankID Antisvindel 2.0 er en vesentlig oppgradering av tidligere antisvindelsystem og forutsetter utvidet innsamling av data, dvs mer informasjon fra brukersteder enn tidligere.

Denne sluttrapporten – utarbeidet av Stø – oppsummerer de vurderingene og funnene som er gjort i prosjektet, med faglig støtte og veiledning fra Finanstilsynet og Datatilsynet gjennom det regulatoriske sandkassearbeidet.

[1] Fra Finanstilsynets invitasjon 14. november 2024 - Invitasjon til regulatorisk sandkasse – prosjekter om datadeling - Finanstilsynet.no

Om Stø AS, utstederrollen og BankID



Stø AS (tidligere BankID BankAxept AS) eies av bankene i Norge og leverer – på vegne av bankene, elektroniske ID- og betalingsløsninger. Selskapets hovedprodukter er BankID og det nasjonale betalingssystemet BankAxept, samt kundesjekk-løsninger (KYC) for rapporteringspliktige foretak etter hvitvaskingsregelverket.

Endring av utstederrollen

Bankene i Norge har fra 2004 vært utstedere av BankID. Rammebetingelsene for elektronisk ID er i endring, blant annet gjennom rask teknologisk utvikling, revidert eIDAS-regelverk fra EU og nasjonal eID-strategi.

For å møte fremtidige forventninger og krav jobber bankene og Stø med å forenkle og modernisere BankID's utstedermodell og styringsstruktur. Partene tar sikte på å være i mål med nødvendige endringer i BankID-avtaler og BankID-regelverket i løpet av 2026.

Når endringene er gjennomført vil Stø bli eneste formelle og juridiske utsteder av BankID person- og brukerstedssertifikater. Dette involverer etableringen av en bankuavhengig modell for utstedelse av BankID. En slik modell legger igjen til rette for at flere kan få BankID.

Hva er BankID?

BankID-tjenestene tilbyr sluttbrukere og brukersteder både elektronisk autentisering- og signeringsløsning. BankID er utstedt til 4,6 millioner sluttbrukere for sikker innlogging og autentisering på om lag 12.000 offentlige tjenester gjennom ID-porten Altinn og 4.000 private brukersteder som nettbanker og kommersielle tjenestetilbydere. I sum medfører dette at BankID brukes omtrent 1 milliard ganger per år, noe som betyr at tjenesten i snitt har over 200 transaksjoner per sluttbruker.

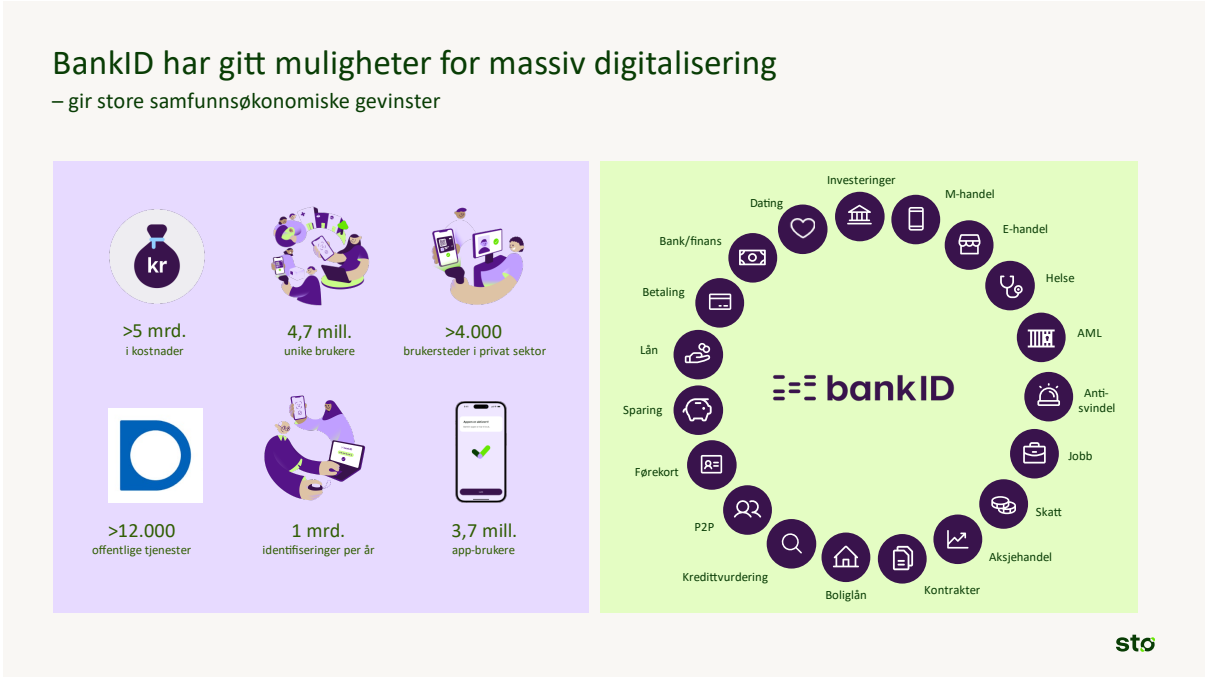
BankID som autentiseringsløsning (heretter «eID») er notifisert på høyeste sikkerhetsnivå i

Europa (såkalt «Level of Assurance High») og signeringstjenesten står på EUs tillitsliste[2].

BankID app

BankID app er en digital ID-lommebok som blant annet inneholder BankID-tjenester og erstatter kodebrikken. Appen gir også tilgang til en rekke andre tjenester – som ID-kort, ID-sjekk og kvalifiserte signeringstjenester. BankID app er lastet ned av mer enn 3,7 millioner BankID-sluttbrukere.

Les mer om Stø AS sine tjenester her.



Digital identitet – en sårbar suksess

BankID fra bankene i Norge har vært en fantastisk digitaliseringsreise som har gitt store samfunnsøkonomiske gevinster, men utbredelsen av digitale identiteter har også brakt med seg sårbarheter. De tekniske og organisatoriske sikkerhetstiltakene må derfor legge til rette for at sluttbrukere, brukersteder og systemet som helhet kan hindre og oppdage uønsket bruk. Når truslene endres, bør også forståelsen av utsatte sårbarheter og verdier endre seg.

Sluttrapporten fra SODI-prosjektet (Societal Security and Digital Identities) undersøkte hvordan juss og teknologi kan samvirke for å avdekke og redusere sårbarheter og risiko knyttet til bruk og misbruk av elektroniske identifikasjonssystemer i Norge. På side 6 i rapporten skrives det:

> *«Den digitale identitetsforvaltningen i Norge er en suksess og en katastrofe på samme tid. God utbredelse av private, markedsbaserte løsninger for elektronisk identifisering (eID), særlig BankID, har lagt til rette for digitalisering av både privat og offentlig sektor. Det har gitt enklere tilgang til en rekke digitale tjenester for store deler av befolkningen og kostnadsbesparelser for mange offentlige og private*

[2] Stø AS (tidligere BankID BankAxept AS) har kvalifisert status i den norske tillitslisten hos Nkom (https://nkom.no/internett/elektronisk-id-og-tillitstjenester/tillitsliste-trusted-list) og er oppført som en kvalifisert tillitstjenesteleverandør i EUs tillitsliste (https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/NO/tsp/16)

aktører.

Universalnøkkelfunksjonen som gjør bruk av eID nyttig og kostnadsbesparende, fører imidlertid samtidig med seg alvorlige utfordringer og sårbarheter knyttet til utenforskap, ID-misbruk og sviktende rettssikkerhet. Når en eID kan brukes i tusenvis av ulike sammenhenger, er det også potensiale for identitetsmisbruk i alle disse sammenhengene. Kriminelle som tilegner seg andres eID kan manipulere informasjon i offentlige registre, overføre penger, søke om lån, opprette selskaper og få utbetalt offentlige stønader på feilaktig grunnlag. Dette fører til enorme tap for individer, selskaper og offentlige myndigheter. I verste fall kan mennesker bli utsatt for strafferettslig forfølgning, justismord og/eller økonomisk ruin som følge av handlinger begått av andre med deres digitale identitet, og samfunnets tillitsgrunnlag kan forvitre.»[3]

BankID Antisvindel 2.0

Finanstilsynet viste i sin Risiko- og sårbarhetsanalyse (ROS) 2025[4] at «*tap som følge av svindel fortsetter å øke og utgjorde i sum 1227 millioner kroner i 2024, en økning på 32 prosent fra 2023. Økningen i svindelaktiviteten tilsier at foretakene fortsatt må legge ned betydelig innsats i antisvindelarbeidet.»*

Trusselbildet for digitale identiteter har endret seg. Telenors rapport «*Digital sikkerhet 2025*»[5] beskriver et trusselbilde som ikke lenger er begrenset til tekniske svakheter, men som omfatter en helhetlig og sammensatt trusselstruktur. De peker på at angrepene er både målrettede og masseproduserte, og utnytter alt fra mobiltelefoner og skyplattformer til QR-koder og KI. Trusselaktørene kombinerer teknologier og metoder for å manipulere, lure og skade både enkeltpersoner og samfunnskritisk infrastruktur. Dette viser at det digitale trusselbildet nå er komplekst og dynamisk, og krever en bredere forståelse enn bare teknisk sårbarhet.

Dagens trusselbilde tilsier derfor at det er nødvendig med tiltak for svindelforebygging, også for elektroniske identiteter. Økende trusler som bedrageri og misbruk, særlig med økt bruk av KI og avanserte phishing-angrep understreker behovet for bedre sikkerhetstiltak og svindelforebygging.

Stø har hittil generert 60.000 alarmer i året som sendes til bank som utsteder og bidrar med det sterkt til å begrense omfanget av svindel. Likevel er det for mye svindel som ikke oppdages.

Økningen i digitale bedragerier har gjort det nødvendig med mer avanserte og koordinerte tiltak. Stø har derfor, på oppdrag fra bankene, utviklet Antisvindel 2.0 for å møte dagens og fremtidens trusselbilde, og for å sikre at BankID fortsatt kan brukes trygt i både offentlig og privat sektor.

Den største forbedringen som kommer med Antisvindel 2.0 er funksjonaliteten til å analysere BankID-transaksjoner i sanntid, fremfor etter at transaksjoner har blitt fullført.

[3] Fra SODI rapporten, side 6: sodi-rapport-5-2025.pdf
[4] Risiko- og sårbarhetsanalyse (ROS) 2025 - Finanstilsynet.no
[5] Telenors Sikkerhetsrapport: Digital Sikkerhet 2025

Systemet kan stanse transaksjonene før de gjennomføres, gi alarmer og risikoscore til brukersteder, og i nødvendige tilfeller sperre BankID og på den måten stanse svindlerne.

Stø vil også kunne bruke BankID-appen til å kommunisere med sluttbrukeren i mye større grad enn tidligere, basert på innsikt fra antisvindelsystemet. Det kan være å informere om kontekst for transaksjonen som er i ferd med å gjennomføres, gi beskjed om at BankID har blitt sperret, eller at transaksjoner har blitt avbrutt på grunn av mistanke om svindel.

Juridisk problemstillinger og målene i sandkassen

I sandkassen har Stø, med veiledning fra Datatilsynet og Finanstilsynet, vurdert noen juridiske problemstillinger ved bruk av BankID Antisvindel 2.0.

Problemstillingene tar utgangspunkt i BankID som en elektronisk identifikasjon (eID) etter lov om elektroniske tillitstjenester – og med Stø i rollene som tredjepartsleverandør av IKT-tjenester, tilbyder av eID-ordninger og fra 2026 eneste utsteder av BankID til både fysiske og juridiske personer.

Målet for Stø var å kartlegge muligheten til å avtaleregulere forpliktelser for BankID brukersteder om innsendelse av flere datapunkter til BankID infrastruktur, til bruk i BankID antisvindelsystem, med utgangspunkt i rammebetingelsene i finansforetaksloven, lov om elektroniske tillitstjenester og personvernregelverket.

I sandkassen diskuterte Stø fire rettslige vurderingstemaer med Datatilsynet og Finanstilsynet;

1. **Taushetsregler**
   Vurdere mulighetsrommet for innsamling av datapunkter fra finansforetak – innenfor rammene av lovbestemt taushetsplikt.
2. **Behandlingsansvar**
   Hvem er behandlingsansvarlig for antisvindelfunksjonen, og innsamling og utlevering av nye datapunkter?
3. **Behandlingsgrunnlag**
   Rettslig grunnlag for behandling av personopplysninger i BankID Antisvindel 2.0, inkludert innsamling og utlevering til/fra brukersted.
4. **Nye datapunkter**
   Diskutere omfanget av innsamling av datapunkter i henhold til taushetsregler og personvernprinsipper.

I de påfølgende kapitlene vises til vurderingene Stø har gjort på disse problemstillingene, i samråd med Datatilsynet og Finanstilsynet.

Juridisk problemstilling 1: Taushetsregler

Vurdere mulighetsrommet for innsamling og utlevering av datapunkter fra finansforetak - innenfor rammene av lovbestemt taushetsplikt.

En grunnforutsetning for at Stø skal kunne innhente kundeopplysninger (benevnt «datapunkter») fra banker og andre finansforetak til bruk i antisvindelsystemet, er at finansforetakenes lovbestemte taushetsplikt ikke står formelt i veien for slik deling. Med andre ord må datapunktene kunne deles med Stø uhindret av taushetsplikt.

Med dette bakteppet har Stø sett på gjeldende taushetsregler i finansforetaksloven og analysert det rettslige mulighetsrommet for deling av datapunkter som beskrevet nedenfor under Vurderingstema nr. 3 – i samråd med Datatilsynet og Finanstilsynet.

Mulighetsrommet for deling av kundeopplysninger under finansforetaksloven
I henhold til finansforetaksloven §§ 9-6 (Taushetsplikt om kundeforhold mv), 9-7 (Taushetsplikt om finansforetaket) og 16-2 (Finansforetaks taushetsplikt, behandling av kundeopplysninger mv) er banker og andre finansforetak samt deres ansatte, tillitsvalgte og oppdragstakere, pålagt lovbestemt taushetsplikt om kunde- og forretningsforhold overfor uvedkommende.

De relevante deler av disse taushetsreglene lyder:

> **«§ 9-6 Taushetsplikt om kundeforhold**
> *(1) Ansatte og tillitsvalgte i et finansforetak plikter å hindre at uvedkommende får adgang eller kjennskap til opplysninger om kunders og andres forretningsmessige eller personlige forhold som de under utførelsen av sitt arbeid eller verv for foretaket blir kjent med, med mindre de etter lov eller forskrifter gitt med hjemmel i lov enten har plikt til å gi opplysninger eller er gitt adgang til å gi ellers taushetspliktbelagte opplysninger. Tilsvarende gjelder enhver som utfører oppdrag for et finansforetak, selv om vedkommende ikke er ansatt i foretaket. Når særlige hensyn tilsier det, kan Finanstilsynet helt eller delvis oppheve taushetsplikten.*
> *(2) ….»*
>
> **«§ 9-7 Taushetsplikt om finansforetaket**
> *(1) Ansatte, tillitsvalgte og enhver annen som utfører oppdrag for foretaket, plikter å følge styrets retningslinjer om taushetsplikt for opplysninger om foretaket og dets virksomhet. Finanstilsynet kan ved enkeltvedtak helt eller delvis oppheve taushetsplikten i enkelttilfeller.*
> *(2) ….»*
>
> **«§ 16-2 Finansforetaks taushetsplikt, behandling av kundeopplysninger mv.**
> *(1) Et finansforetak plikter å hindre at uvedkommende får adgang eller kjennskap til opplysninger om kunders og andres forretningsmessige eller personlige forhold som foretaket mottar under utøvelsen av virksomheten, med mindre foretaket etter lov eller forskrifter gitt med hjemmel i lov har plikt til å gi opplysninger eller er gitt adgang til å gi ellers taushetspliktbelagte opplysninger. Når særlige hensyn tilsier det, kan Finanstilsynet helt eller delvis oppheve taushetsplikten.*
> *(2) ….»*

Som det fremgår av bestemmelsene foran er det angitt noen unntak fra taushetsplikten:

1. At det etter særlovgivningen foreligger opplysningsrett eller -plikt overfor myndighetene og andre finansforetak,
2. At Finanstilsynet ved enkeltvedtak helt eller delvis har opphevet taushetsplikten når særlige hensyn tilsier det, eller
3. At det foreligger utleveringssamtykke fra berørte personkunder.

I samråd med Finanstilsynet, har Stø vurdert at ingen av disse unntakene er anvendelige for finansforetakenes deling av kundeopplysninger (datapunkter) med Stø som tilbyder av eID-ordninger.

To praktisk viktige unntak fra taushetsplikten for deling av kundeopplysninger er nedfelt i finansforetaksloven § 13-21 (Adgangen til behandling og utveksling av betalingsinformasjon) og tredje ledd i § 16-2 (Finansforetaks taushetsplikt, behandling av kundeopplysninger mv);

Etter unntaksbestemmelsen i § 13-21 kan tilbydere av betalingstjenester dele betalingsinformasjon med andre tilbydere av betalingstjenester *«når dette er nødvendig for å sikre forebygging, etterforskning eller avsløring av betalingsbedragerier»*. Stø vurderte, med veiledning fra Finanstilsynet, det dithen at denne lovbestemte retten til deling av ellers taushetsbelagte kundeopplysninger, ikke kan påberopes som følge av at Stø i denne sammenheng ikke anses som tilbyder av betalingstjenester.

Et nokså likt unntak fra taushetsplikten følger av § 16-2 (3) med et kriminalitetsforebyggende formål. Bestemmelsen gir finansforetak adgang til å utlevere ellers taushetsbelagte opplysninger til et annet finansforetak *«med formål å motvirke og avdekke betalingsbedragerier samt annen alvorlig kriminalitet»*. Heller ikke denne opplysningsretten gir banker og andre finansforetak adgang til å dele kundeopplysninger med Stø.

Stø er ikke en virksomhet som er omfattet av finansforetaksloven. Ingen av de ovennevnte unntaksbestemmelser gir derfor banker og andre finansforetak rett til å dele kundeopplysninger med Stø. Innhenting av frivillig og informert skriftlig samtykke fra berørte sluttbrukere ved indikasjon eller mistanke om misbruk av BankID under en konkret svindelsituasjon, er heller ikke hensiktsmessig eller gjennomførbart.

Taushetsplikten om kunde- og forretningsforhold gjelder imidlertid overfor «uvedkommende». Som redegjort for i punktet nedenfor kan Stø i rollen som oppdragstaker og leverandør av eID-ordningen BankID og tilhørende antisvindelsystem, til banker og andre finansforetak under DORA-loven, ikke anses som uvedkommende.

Oppsummering: Stø som oppdragstaker
For å kunne motta nødvendige kundeopplysninger (valgte datapunkter) fra finansforetak uhindret av lovbestemt taushetsplikt vil Stø, som tilbyder og leverandør av BankID og det obligatoriske antisvindelsystemet, videreføre rollen som en avtalebasert tredjepartstilbyder av IKT-tjenester og «oppdragstaker» i taushetsreglenes forstand.

I henhold til mangeårig praksis er det legitimt for banker og andre finansforetak å dele taushetsbelagte kundeopplysninger med sine oppdragstakere så lenge oppdragstakeren har et saklig og begrunnet behov for kundeopplysningene med formål å gjennomføre den avtalebaserte ytelsen/tjenesten.

Ved mottak av taushetsbelagte opplysninger blir oppdragstakeren omfattet av lovbestemt taushetsplikt[6]. Finansforetaksloven § 9-6 bestemmer at plikten til å bevare taushet etter § 16-2 også omfatter foretakets oppdragstakere. Sammenhengen mellom disse

[6] Se Prop. 125 L (2013-2014) om §§ 9-6 og 16-2, samt Finanstilsynets Rundskriv 2019-3, punkt 5.

bestemmelsene er at finansforetakets taushetsplikt ikke er til hinder for at de som har taushetsplikt etter § 9-6, gis de opplysninger om kunders forhold som vedkommende oppdragstaker har behov for ved utførelsen av sine arbeidsoppgaver for finansforetaket.

Behovsbegrensningen innebærer en plikt for foretaket til å sørge for at bare personer hos oppdragstaker som har saklig behov for opplysningene, gis tilgang. Finansforetaksloven § 16-2 sjette ledd krever at finansforetaket har kontrollordninger som sikrer dette. Foretakene må ha et bevisst forhold til hvilke ansatte, både i eget foretak og hos oppdragstakere, som til enhver tid skal ha tilgang til taushetsbelagte opplysninger (basert på prinsippet om «need to know»), herunder vurdere om det bør være særlige begrensninger med hensyn til hvilke ansatte som skal ha tilgang til opplysninger om enkelte kunder eller kundegrupper.

Finansdepartementets høring om endringer i finansforetaksloven og – forskriften om taushetsplikt og informasjonsdeling

I Finansdepartementets høring 17. september 2025 av Finanstilsynets notat av 29. august 2025 «Nærmere regler om informasjonsdeling for finansforetak», med bl.a. forslag til endringer i finansforetaksloven § 16-2 og i finansforetaksforskriften ny § 16-17, er det foreslått å åpne for mer utstrakt deling av informasjon mellom finansforetak, politi og tilbydere av elektroniske kommunikasjonstjenester.

Stø støtter endringsforslagene med utvidede hjemler for datadeling, ikke bare begrenset til mellom finansforetak og overfor telekomtilbydere, men også til eID-tilbydere som er omfattet av lov om elektroniske tillitstjenester, se høringsuttalelse fra Stø, datert 4. november 2025[7]

[7] Høring - finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet - regjeringen.no

Juridisk problemstilling 2: Behandlingsansvar

Hvem er behandlingsansvarlig for antisvindelfunksjonen, og innsamling og utlevering av nye datapunkter?

Behandlingsansvar er et sentralt begrep i GDPR, og handler om hvem som har det overordnede ansvaret for hvordan personopplysninger behandles etter personvernprinsippene i GDPR artikkel 5 og for å overholde personvernforordningen ellers.

GDPR artikkel 4 nr. 7 definerer behandlingsansvarlig slik:

> *«en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett»*

Formålet og midlene for behandling av personopplysninger kan fastsettes i lov, og når det er tilfelle kan slik lov utpeke den behandlingsansvarlige eller angi kriterier for dens utpeking.

Lov om elektroniske tillitstjenester gjennomfører i norsk rett europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked («eIDAS»). Ett av formålene med eIDAS er å oppnå et egnet sikkerhetsnivå for elektroniske identifikasjonsmidler og tillitstjenester. Stø vil i løpet av 2026 bli en utsteder av BankID og må oppfylle gjeldende krav fastsatt i eIDAS i forbindelse med eID-tjenesten.

eIDAS artikkel 8 fastslår kriterier for elektroniske identifikasjonsmidler som BankID må oppfylle for sikkerhetsnivåene «betydelig» og «høyt». Slike midler skal ha som formål å oppnå en betydelig redusert risiko for (for «betydelig») eller å hindre (for «høyt») misbruk eller endring av identiteten, og som skal kjennetegnes på grunnlag av tekniske spesifikasjoner, standarder og framgangsmåter, herunder tekniske kontroller. EU-kommisjonen har fastsatt slike tekniske minstespesifikasjoner, minstestandarder og minstekrav til framgangsmåter i gjennomføringsforordning 2015/1502. Disse inneholder krav til påliteligheten og kvaliteten av autentiseringsordningen som gjør det mulig å bruke BankID-tjenesten til å bekrefte sin identitet overfor et brukersted.

Stø har argumentert i sandkassen for at BankID Antisvindel 2.0 er et nødvendig tiltak og er en obligatorisk del av BankID-tjenesten, i dagens trusselbilde. Kildene til kravene er identifisert og kravene vurdert av Stø slik at tiltakene som er implementert for BankID Antisvindel 2.0 svarer opp kravene i eIDAS artikkel 8 og gjennomføringsforordningen, med hjelp av veilederen ”Guidance for the application of the levels of assurance which support the eIDAS Regulation”. Dette fremkommer nærmere under kapittelet nedenfor om «Er behandling av personopplysninger i BankID Antisvindel 2.0 nødvendig?».

I lys av dagens trusselbilde, som preges av avansert svindel og identitetstyveri, må tiltakene være tilstrekkelige for å oppnå ovennevnte formål. Dette innebærer at BankID Antisvindel 2.0, som bl.a. analyserer avvik fra normal adferd, er ansett nødvendig for å oppfylle lovens krav. Behandlingen av personopplysninger i løsningen er derfor en forutsetning for å sikre at

autentiseringsordningen oppfyller eIDAS-kravene og gir et forsvarlig sikkerhetsnivå.

Formål med å behandle personopplysninger i BankID Antisvindel 2.0
Formålene med å behandle personopplysninger i BankID Antisvindel 2.0 fremgår i det vesentlige av eIDAS artikkel 8, og er ytterligere spesifisert i gjennomføringsforordning 2015/1502 som beskriver nærmere fastsatte krav for de forskjellige sikkerhetsnivåer i en ordning for elektronisk identifikasjon. Dette kan oppsummeres slik:

- å oppnå en betydelig redusert risiko for misbruk eller endring av identiteten (for sikkerhetsnivået betydelig).
- å hindre misbruk eller endring av identiteten (for sikkerhetsnivået høyt).

Det er likevel slik at Stø - som en tilbyder av eID under eIDAS – har et handlingsrom i å bestemme hvordan disse formålene skal oppnås.

Midler som skal brukes i BankID Antisvindel 2.0
Stø mener at følgende midler er helt nødvendig å ta i bruk for å oppnå formålene:

- bygge en profil av sluttbrukerens normal BankID-transaksjonsatferd
- analysere BankID-transaksjoner mot normal brukerprofil for å oppdage uvanlige eller mistenkelige autentiseringsmønstre
- gi kontekstinformasjon til sluttbruker
- utlevere alarmer og risikoscore til brukersteder, eventuelt suspendere eller sperre BankID
- drifte, forvalte og utvikle løsningen i overenstemmelse med formålet.

Behandlingsansvar
Som det fremgår av nedenstående drøftelse under vurderingstema nr 3 – Behandlingsgrunnlag, anses BankID Antisvindel 2.0 som et nødvendig sikkerhetstiltak etter lov om elektroniske tillitstjenester for å møte dagens digitale trusselbilde, hvor identitetstyveri og digital svindel stadig blir mer avansert. Antisvindelløsningen er ikke eksplisitt påkrevd i loven, men følger av krav om hensiktsmessige tekniske og organisatoriske tiltak under eIDAS og tilhørende regelverk.

Forståelsen av eIDAS regelverket er gitt i veilederen «LoA Guidance[8]» som gir en detaljert forklaring på hva Level of Assurance (LoA) betyr, og hvordan de tre nivåene (Low, Substantial og High) skal anvendes, samt praktiske eksempler og krav til hvordan identitetskontroll og autentisering bør foregå. Veilederen er utarbeidet som et felles arbeid mellom EU-kommisjonen (DG CNECT – eGovernment and Trust Unit) og medlemmer av eIDAS Cooperation Network.

Når loven bestemmer formål og krav til de ulike sikkerhetsnivåene, er det påkrevd at utsteder av eID må bestemme virkemidlene, hvor Stø har vurdert at BankID Antisvindel 2.0 er et slikt nødvendig virkemiddel. eIDAS-forordningen nevner heller ikke eksplisitt at utsteder er behandlingsansvarlig, men at personopplysninger skal behandles i tråd med personvernforordningen, jf eIDAS artikkel 5.

Stø vurderer derfor, i samråd med Datatilsynet og Finanstilsynet, at utsteder av BankID vil

[8] https://ec.europa.eu/digital-building-blocks/sites/download/attachments/40044784/LoA%20guidance.docx?version=1&api=v2

ha rollen som behandlingsansvarlig for behandling av personopplysninger i BankID Antisvindel 2.0.

Felles behandlingsansvar?
Sandkassen diskuterte også om det kunne foreligge et felles behandlingsansvar etter GDPR artikkel 26 mellom utsteder og brukersted, når brukersted utleverer nye datapunkter til utsteder. Spørsmålet er ikke endelig avklart og utgjør ikke det mest sentrale punktet i sandkasseprosjektet. Datatilsynet vil kunne veilede Stø om temaet på et senere tidspunkt.

Juridisk problemstilling 3: Behandlingsgrunnlag

Rettslig grunnlag for behandling av personopplysninger i BankID Antisvindel 2.0, inkludert innsamling og utlevering til/fra brukersted.

For all behandling av personopplysninger krever GDPR artikkel 6 at det foreligger et rettslig grunnlag. Artikkel 6 gir en uttømmende oversikt over seks mulige grunnlag, hvor både utsteder og brukersteder må vurdere og dokumentere hvilket som oppfylles for enhver behandling av personopplysninger. Hvis bestemte personopplysninger behandles for flere formål, må det foreligge et gyldig behandlingsgrunnlag for hvert formål. Manglende rettslig grunnlag innebærer at behandlingen er ulovlig og kan resultere i strenge sanksjoner.

Vurderingene tar utgangspunkt i å lage en oversikt over alle behandlingsaktiviteter og hvorfor de skal utføres, og deretter se nærmere på hvilke av de seks behandlingsgrunnlagene som kan være aktuelle, og begrunne valget.

I sandkassen så vi nærmere på behandlingsgrunnlagene (1) «rettslig forpliktelse» og (2) «berettiget interesse» for personopplysninger som behandles i BankID Antisvindel 2.0, for henholdsvis utsteder og brukersted. I det tilfelle rettslig forpliktelse er aktuelt må det også finnes et supplerende rettsgrunnlag.

Stø har strukturert vurderingene om behandlingsgrunnlag både fra perspektivet til utsteder og brukersted. Stø vurderte også om BankID Antisvindel 2.0 behandler særlige kategorier av personopplysninger etter GDPR artikkel 9 og hvilket unntak i GDPR artikkel 9 nr. 2 som i så fall kan være aktuelt å benytte for henholdsvis utsteder og brukersted.

Om behandlingsgrunnlagene «rettslig forpliktelse» og «berettiget interesse».

Rettslig forpliktelse
En virksomhet kan behandle personopplysninger dersom det er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige, jf. GDPR artikkel 6 nr. 1 bokstav c. Med andre ord, dersom virksomheten må behandle personopplysninger for å oppfylle en rettslig forpliktelse, har den også lov til det.

Krav til supplerende rettsgrunnlag
Den rettslige forpliktelsen må vise til en hjemmel i en supplerende lov eller forskrift. Det vil si at behandlingsgrunnlaget må fastsettes i en lov eller forskrift som den behandlingsansvarlige er underlagt. GDPR artikkel 6 nr. 3 inneholder noen vilkår som må oppfylles for at behandling av personopplysninger kan hjemles i GDPR artikkel 6 nr. 1 bokstav c. Formålet med behandling må være fastsatt i det supplerende rettsgrunnlaget, og

behandlingen må stå i et rimelig forhold til det berettigede målet som det supplerende rettsgrunnlaget søkes oppnådd. Den rettslige forpliktelsen må være klart nok formulert. Det må være klart at det er en plikt, altså at det ikke foreligger valgfrihet.

I fortalepunkt 45 til GDPR skrives det at det ikke kreves en særlig lovbestemmelse for hver enkelt behandling. En lov kan være tilstrekkelig som grunnlag for flere behandlingsaktiviteter som bygger på en rettslig forpliktelse som påhviler den behandlingsansvarlige.

Ifølge fortalepunkt 41 til GDPR og forarbeidene[9] til personopplysningsloven følger det at kravene til det supplerende rettsgrunnlaget må tolkes i lys av EMK artikkel 8 og Grunnloven § 102, i tillegg til legalitetsprinsippet i Grunnloven § 113. Dette innebærer at rettsgrunnlaget må oppfylle kravet til klarhet, nødvendighet og forholdsmessighet.

Hvorvidt det foreligger et tilstrekkelig supplerende rettsgrunnlag beror på en konkret vurdering, herunder av hvor inngripende behandlingen av personopplysninger er. En inngripende behandling, eksempelvis behandling av særlige kategorier av personopplysninger, tilsier strengere krav til utformingen av det supplerende rettsgrunnlaget når det gjelder tydelighet og forutberegnelighet.

For å sikre en god vurdering av om det supplerende rettsgrunnlaget er tilstrekkelig klart, må den behandlingsansvarlige ha oversikt over alle behandlingsaktiviteter, herunder hvilke personopplysninger som behandles, hvem det behandles personopplysninger om og behandlingens omfang, se nærmere om dette nedenfor under avsnittet «Er behandling av personopplysninger i BankID Antisvindel 2.0 et nødvendig tiltak?».

Berettiget interesse
I det tilfelle det benyttes berettiget interesse må det foretas en interesseavveining. Det vil si en vurdering av om den behandlingsansvarliges eller en tredjeparts interesser veier tyngre enn den enkeltes personvern.

For at berettiget interesse skal være et gyldig behandlingsgrunnlag, må tre kumulative vilkår være oppfylt:

1. Berettiget interesse: At den behandlingsansvarlige eller en tredjepart forfølger en berettiget interesse.
2. Nødvendighet: Behandlingen må være nødvendig for å forfølge den berettigede interessen – det skal ikke finnes mindre inngripende alternativer.
3. Avveining: En dokumentert interesseavveining må vise at den registrertes interesser eller grunnleggende rettigheter ikke går foran den behandlingsansvarliges eller tredjepartens berettigede interesse.

Dette behandlingsgrunnlaget er fleksibelt og brukes ofte i forbindelse med f.eks. IT-sikkerhetstiltak og forebygging av svindel utover når dette er påkrevd av lov.

Behandlingsgrunnlag for utsteder

For utsteders tilfelle er alle behandlingsaktivitetene i BankID antisvindel identifisert og samlet for følgende formål:

[9] Prop. 56 LS (2017–2018) – punkt 6.3.2 «Supplerende rettsgrunnlag», siste avsnitt, side 33.

- å oppnå en betydelig redusert risiko for misbruk eller endring av identiteten (for sikkerhetsnivået betydelig).
- å hindre misbruk eller endring av identiteten (for sikkerhetsnivået høyt).

Stø identifiserte deretter «rettslig forpliktelse» i GDPR artikkel 6 nr. 1 bokstav c som et relevant og aktuelt behandlingsgrunnlag basert på nedenstående drøftelse om behandling av personopplysninger i BankID antisvindel 2.0 er nødvendig, gitt at det er et nødvendig tiltak for en eID-utsteder etter lov om elektroniske tillitstjenester (eIDAS);

Er behandling av personopplysninger i BankID Antisvindel 2.0 et nødvendig tiltak?
På bakgrunn av veiledning fra Datatilsynet, vurderte Stø nødvendigheten av å behandle personopplysninger i BankID Antisvindel 2.0 som et tiltak for å oppfylle lovkrav i eIDAS-regelverket, med fokus på sikkerhetskrav og trusselbilde. Det ble drøftet om BankID Antisvindel 2.0 kan hjemles som en rettslig forpliktelse iht. eIDAS, om behandling av personopplysninger er nødvendig for Stø for å oppfylle den rettslige plikten og hvordan det bidrar til å opprettholde tillit og sikkerhet i elektroniske identifikasjonsmidler.

Økende bedrageri og AI-utvikling utfordrer digitale identiteter, noe som krever bedre sikkerhetstiltak som antisvindelløsninger for å opprettholde tillit.

eIDAS-rammeverkets sikkerhetskrav krever tekniske og organisatoriske tiltak tilpasset risiko for å sikre elektroniske identiteter på tvers av EU/EØS med høyt sikkerhetsnivå. eIDAS gjennomføringsforordning 2025/1502 spesifiserer minstekrav for eID-sikkerhet på nivå høyt, inkludert beskyttelse mot kopiering, manipulering og avanserte angrep.

EU-kommisjonen har utarbeidet en veileder;"*Guidance for the application of the levels of assurance which support the eIDAS Regulation*" som understreker at sikkerhetstiltak må tilpasses risiko og trusler som «phishing», «spoofing» og «session hijacking», og at løpende vurdering av trusselbildet er nødvendig, noe BankID Antisvindel 2.0 adresserer.

BankID Antisvindel 2.0 innebærer behandling av flere kategorier personopplysninger enn tidligere som følge av dagens trusselbilde. Stø må likevel sørge for at slik behandling er forholdsmessig og ikke er mer enn nødvendig for å oppnå sine rettslige forpliktelser etter eIDAS og GDPR. Til sammenligning uttalte Justis- og beredskapsdepartementet til forarbeidene til digitalsikkerhetsloven at det er opp til den enkelte tilbyderen å vurdere hvilke tiltak som bør iverksettes, herunder tiltak som kan innebære behandling av personopplysninger.

Stø gjennomførte en grundig vurdering av nødvendigheten med et antisvindelsystem med utgangspunkt i rammebetingelser, krav og veiledninger. Selv om antisvindelsystemer ikke eksplisitt nevnes i eIDAS, mener Stø at løsningen implisitt er nødvendig som teknisk og organisatorisk tiltak for å håndtere risiko og opprettholde tillit til eID, og BankID Antisvindel 2.0 kan derfor hjemles som en rettslig forpliktelse. Behandlingsgrunnlaget "berettiget interesse" ble for utsteder følgelig ikke behandlet videre i sandkassen.

Behandlingsgrunnlag for brukersted

For finansforetaks muligheter for deling av taushetsbelagte opplysninger med utsteder vises til vurderingstema nr 1 Taushetsplikt, ovenfor.

Finanstilsynet har også i sitt høringsnotat «*Nærmere regler om informasjonsdeling for*

finansforetak»[10] argumentert for et behov for klarere rettsgrunnlag enn det som i dag kan utledes av finansforetaksloven, og foreslår utvidet deling av personopplysninger gjennom delingsplattformer når dette er nødvendig for å forebygge eller avdekke økonomisk kriminalitet og annen alvorlig kriminalitet, se høringsnotatets punkt 7 om endringer i finansforetaksloven og finansforetaksforskriften. Høringsnotatet hadde høringsfrist 14. november 2025.

Stø ga i sitt høringssvar innspill på at finansforetak også bør kunne dele taushetsbelagte opplysninger med virksomheter som er omfattet av lov om elektroniske tillitstjenester. Dette omfatter tilbydere som tilfredsstiller en eID-ordning i forskrift 21. november 2019 nr. 1578 om selvdeklarasjon av ordninger for elektronisk identifikasjon § 3 og som er oppført på publisert liste i henhold til § 13 første ledd i nevnte forskrift, og ikke begrenset til kun tilbydere av elektroniske kommunikasjonstjenester (telekom-tilbydere).

Forslaget til lovendringen nevnt ovenfor kan gi finansforetak bedre hjemmel til utvidet deling og behandling av opplysningstyper, men nye hjemler gir ingen *plikt* til å utlevere. Behandlingsansvarlige finansforetak må fortsatt foreta en vurdering etter GDPR og definere formål og finne et rettslig behandlingsgrunnlag i artikkel 6 for å utlevere personopplysningene, innenfor rammene av lovpålagt taushetsplikt.

Merk: Brukerstedet inngår brukerstedsavtale med utsteder for å ta i bruk BankID-tjenesten, og integrerer seg mot BankID-infrastruktur via BankID OIDC (OpenID Connect), inkludert spesifiserte API'er (avhengig av brukerstedskategori) slik at utsteder mottar visse kategorier av opplysningstyper for formålet å forebygge eller avdekke økonomisk kriminalitet og annen alvorlig kriminalitet. Data vil heller aldri utleveres til BankID-tjenesten med mindre det er en pågående autentisering eller signering med BankID og som er aktivt initiert av sluttbruker. Brukerstedet er også behandlingsansvarlig for all behandling av personopplysninger hos brukersted, før utlevering finner sted. Brukersted må selv vurdere hvilke av de seks behandlingsgrunnlagene i GDPR artikkel 6 som er relevante for brukerstedets utlevering av opplysninger, og utsteder kan bistå i vurderingen ved behov.

Det tvingende behovet for en forbedret antisvindel til fordel for sluttbrukere, utstedere og brukersteder, vil være avgjørende på vektskålen for at en berettiget interesse kan anvendes som behandlingsgrunnlag for brukerstedets utlevering av nye datapunkter til BankID Antisvindel 2.0, jf GDPR artikkel 6 nr. 1 bokstav f.

Brukerstedet må selv dokumentere en interesseavveining der de berettigede interessene angis, hvoretter det må vurderes om de registrertes interesser eller grunnleggende rettigheter og friheter går foran, eller om grunnene til å foreta behandlingen er så gode at personvernulempene behandlingen medfører kan aksepteres.

Kort oppsummert er de berettigede interessene det tvingende behovet for forbedret antisvindel til fordel for sluttbrukere, utstedere og brukerstedene, jf. grunnlaget og temaet for sandkasserapporten.

[10] Høring - finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet - regjeringen.no

Behandles det særlige kategorier av personopplysninger?

Hvis så, hvilket lovlig behandlingsgrunnlag kan man benytte?

For utsteder:
Bruken av eID, herunder antisvindeltiltak, reiser også spørsmål om det behandles særlige kategorier av personopplysninger.

Sluttbruker kan i prinsippet velge å bruke BankID til autentisering hos enhver type brukersteder, også brukersteder som indirekte kan avsløre opplysninger om f.eks. helse, tilhørighet til religion, fagforening eller politisk parti.

Etter lov om elektroniske tillitstjenester, som gjennomfører eIDAS-forordningen i norsk rett, er formålet i loven å sikre et velfungerende marked og et tilstrekkelig sikkerhetsnivå for digitale identitetstjenester. Antisvindeltiltak er et sentralt virkemiddel for å oppnå dette, ettersom tiltaket bidrar til å forebygge misbruk og identitetstyveri.

Samtidig kan slike tiltak innebære behandling av personopplysninger som gir innsikt i sluttbrukerens adferd, type brukersted og transaksjonsmønstre. Selv om formålet med behandlingen i BankID Antisvindel 2.0 er å hindre misbruk og endring av identiteten, må det vurderes om opplysningene – direkte eller indirekte – kan avsløre særlige kategorier personopplysninger etter GDPR artikkel 9, for eksempel helserelaterte data eller religiøs tilknytning gjennom mønstre i bruk.

EU-domstolen har avsagt flere avgjørelser om GDPR artikkel 9 de seneste år[11] og har presisert at artikkel 9 skal tolkes vidt, slik at artikkel 9 også dekker informasjon som indirekte kan utlede særlige kategorier og at det ikke er avgjørende om behandlingen ikke har som intensjon å utlede slike opplysninger.

Det legges derfor til grunn at behandling av opplysningstyper i BankID, herunder BankID Antisvindel 2.0 *kan* avsløre særlige kategorier personopplysninger. Dette innebærer at utsteder som tilbyr eID og implementerer antisvindelløsninger må foreta en grundig vurdering av nødvendighet og forholdsmessighet, samt sikre at behandlingen omfattes av ett av unntakene i GDPR artikkel 9 nr. 2 og eventuelle supplerende hjemler.

For utsteder som har et behandlingsgrunnlag i GDPR artikkel 6 nr. 1 bokstav c kan unntaket i GDPR artikkel 9 nr. 2 bokstav g benyttes for behandling av særlige kategorier personopplysninger;

GDPR artikkel 9 nr. 2 bokstav g regulerer et unntak fra hovedregelen om forbud mot behandling av særlige kategorier personopplysninger. Når en behandlingsansvarlig allerede

[11] C-184/20 (1. august 2022)
C-252/21 (4. juli 2023)
C-21/23 (4. oktober 2024)

Søk på sakene her: CURIA - Search form

har et behandlingsgrunnlag etter artikkel 6 nr. 1 bokstav c, kan artikkel 9 nr. 2 bokstav g brukes dersom;

- behandlingen er nødvendig av hensyn til viktige allmenne interesser, og
- den skjer på grunnlag av unionsrett eller nasjonal rett, som:
    - er forholdsmessig i forhold til formålet
    - respekterer de grunnleggende prinsippene for personvern, og
    - inneholder egnede og spesifikke tiltak for å verne den registrertes rettigheter og interesser.

Lov om elektroniske tillitstjenester kan for utsteder være et slikt supplerende rettsgrunnlag, men kan ikke fastsettes generelt. Det må vurderes konkret, blant annet basert på hvor inngripende behandlingen av personopplysninger er. For behandlinger som anses særlig inngripende, slik som behandling av særlige kategorier personopplysninger, stilles det strengere krav til utforming av det supplerende rettsgrunnlaget når det gjelder både tydelighet og forutsigbarhet.

Loven angir at utsteder skal sikre tjenestens sikkerhet og forebygge misbruk. Stø begrenser behandlingen til det som er nødvendig for å oppnå formålet fastsatt i lov, ved å benytte tiltak som dataminimering, pseudonymisering og slettefrister. Det er gjennomført risikovurderinger, tilgangskontroller, krypteringsmekanismer og transparens overfor sluttbrukere.

Stø vurderer det slik at behandlingen er nødvendig av hensyn til viktige allmenne interesser for forebygging av identitetstyveri og svindel. Dette er vurdert under temaet «Er BankID Antisvindel 2.0 et nødvendig tiltak?» ovenfor og er av sentral samfunnsinteresse fordi misbruk av eID kan undergrave tillit til digitale tjenester, finansielle transaksjoner og offentlige digitale tjenester. Lov om elektroniske tillitstjenester pålegger også utstedere å sikre tjenestens integritet og forebygge misbruk. Behandlingen vurderes forholdsmessig i forhold til formålet, hvor formålet med antisvindel er legitimt og klart definert, dataminimering er vurdert, det er begrenset lagringstid og tilstrekkelige andre beskyttelsestiltak er på plass (logging og tilgangskontroll). Disse tiltakene reduserer risiko for urimelige konsekvenser for sluttbruker, hvor det supplerende rettsgrunnlaget oppfyller kravene til proporsjonalitet og garantier, og forutberegnelighet for sluttbruker hvor behandlingen er klart regulert og kommunisert til sluttbruker.

Stø anser at behandlingen er nødvendig og forholdsmessig også for opplysningstyper som anses som særlige kategorier av personopplysninger, hvor unntaket i GDPR artikkel 9 nr. 2 bokstav g kan anvendes som behandlingsgrunnlag for utsteder.

For brukersted:
Datatilsynet veiledet Stø i dette spørsmålet;

Personvernforordningen artikkel 9 nr. 1 fastsetter at behandling av særlige kategorier personopplysninger er forbudt med mindre det foreligger et unntak i henhold til alternativene i artikkel 9 nr. 2. Type brukersted og transaksjonsmønstre kan bidra til å avsløre særlige kategorier av personopplysninger. Det kan derfor ikke utelukkes at opplysninger som utleveres fra brukersteder til Stø for bruk i BankID Antisvindel 2.0 kan omfatte særlige kategorier av personopplysninger.

Ved utlevering av særlige kategorier av personopplysninger til Stø må brukerstedene, i tillegg til et rettslig grunnlag etter artikkel 6 nr. 1, altså også oppfylle et av unntakene i artikkel 9 nr. 2 for den aktuelle utleveringen.

I denne sammenhengen er det er kun alternativene i artikkel 9 nr. 2 bokstav a (samtykke) og g (viktige allmenne interesser) som potensielt kan oppfylles av brukerstedene. Ettersom alternativet med samtykke er lite praktisk for brukerstedene, er ikke samtykke vurdert nærmere i sandkassen.

Det aktuelle unntaket som ble diskutert i sandkassen er derfor artikkel 9 nr. 2 bokstav g, som gir adgang til å behandle særlige kategorier av personopplysninger dersom "[b]ehandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett […]".

I motsetning til for eksempel ordlyden i artikkel 6 nr. 1 bokstav c og e, eller artikkel 9 nr. 2 bokstav b, oppstiller ikke ordlyden i artikkel 9 nr. 2 bokstav g et uttrykkelig krav til at lovgrunnlaget må være direkte rettet mot den behandlingsansvarlige.

I denne forbindelse har det i sandkassen blitt reist spørsmål ved om lovgrunnlaget som artikkel 9 nr. 2 bokstav g viser til (unionsretten eller medlemsstatenes nasjonale rett) må rette seg mot den behandlingsansvarlige direkte. Spørsmålet er relevant fordi eIDAS-forpliktelsene er rettet mot utstederen (Stø), og ikke eksplisitt mot brukerstedene.

Denne problemstillingen har ikke tidligere kommet på spissen i saker for Datatilsynet, og Datatilsynet var heller ikke kjent med at spørsmålet er avklart i rettspraksis eller andre autoritative rettskilder. Basert på bestemmelsens ordlyd, forordningens systematikk og formålsbetraktninger utelukker ikke Datatilsynet en tolkning av artikkel 9 nr. 2 bokstav g som tilsier at lovgrunnlaget *ikke* direkte må rette seg mot den behandlingsansvarlige.

Datatilsynet understreket imidlertid at uavhengig av om det åpnes for en tolkning av bokstav g som nevnt, må den behandlingsansvarlige på vanlige vilkår vurdere hvorvidt hjemmelsgrunnlaget er klart nok for den konkrete behandlingen, og om den aktuelle behandlingen oppfyller kravene om nødvendighet og forholdsmessighet, slik disse fremgår uttrykkelig av artikkel 9 nr. 2 bokstav g så vel de generelle prinsippene i artikkel 5. I tillegg må den behandlingsansvarlige alltid oppfylle kravet om et eget rettslig grunnlag som følger av artikkel 6 nr. 1.

Juridisk problemstilling 4: Nye datapunkter

«Diskutere omfanget av innsamling og utlevering av datapunkter under regulatoriske krav til taushetsplikt og i henhold til personvernprinsippene.»

Innledning
I arbeidet med å utvikle en antisvindelløsning under eIDAS-regelverket oppstår et sentralt spørsmål: hvor langt kan man gå i innsamling og utlevering av datapunkter uten å bryte grunnleggende personvernprinsipper og krav til taushetsplikt?

Krav til taushetsplikt er behandlet under Vurderingstema nr. 1 – Taushetsplikt, men krav til formålsbegrensning, dataminimering, nødvendighet og forholdsmessighet gjelder for alle, både for utsteders innsamling og brukersteders utlevering, også utlevering fra finansforetak.

Oversikt over datapunkter som blir behandlet i BankID infrastruktur og BankID Antisvindel 2.0 ble presentert og gjennomgått i sandkassen, men ikke vurdert konkret hver for seg.

Reguleringene i eIDAS og personvernforordningen krever at en eID-løsning ivaretar både krav til sikkerhet og forebygger misbruk, samtidig som løsningen må respektere individets rett til privatliv. Denne balansen også utfordrer noen grunnleggende prinsipper i GDPR:

- dataminimeringsprinsippet,
- nødvendighetsvilkåret og
- forholdsmessighetsprinsippet

som Stø som utsteder av en eID og behandlingsansvarlig må hensynta i sine vurderinger.

Først litt om inngrep i personvernet
BankID og BankID Antisvindel 2.0 krever mer innsamling av data enn tidligere. Dette omfatter data som gir mer informasjon om hva sluttbruker anvender sin BankID til, ved opprettelse av normal adferdsprofil for BankID-transaksjoner. Selv om omfanget av data gir en teknisk profil, kan datapunktene likevel gi en detaljert innsikt i adferd, bevegelsesmønstre og digitale vaner. Slik innsikt kan innebære en risiko for direkte identifisering og overvåkning av sluttbrukers digitale liv.

Selv om formålet er legitimt og tungtveiende for å forhindre misbruk eller endring av en identitet, innebærer likevel behandlingen et inngrep i sluttbrukers personvern. Det kan f.eks. være at sluttbruker ikke har kontroll eller informasjon om omfanget av behandling av sine egne personopplysninger, at det samles inn mer data enn nødvendig, og når sluttbruker blir profilert er det begrenset informasjon om hvordan risiko scores eller at det er en risiko for feil analysebehandling.

Når sluttbruker blir profilert i antisvindelløsningen kan dette oppleves som inngripende fordi sluttbrukers BankID-transaksjon kategoriseres etter risiko og vurderes gjennom automatiske analyser, noe som kan medføre suspendering eller sperring av et BankID sertifikat.

Risiko- og analysemodellene kan feiltolke legitime BankID-transaksjoner som mistenkelige. Feilaktige avgjørelser kan føre til kontosperring i bank, avvist tilgang til offentlige tjenester som fører til ulemper eller forsinkelser i viktige, kanskje livsviktige offentlige tjenester. Slike konsekvenser er et inngrep i sluttbrukers rettigheter og risikoen for uriktige antisvindelanalyser er derfor en sentral del av personverninngrepet.

Det legges til grunn at sluttbruker forventer en høy grad av sikkerhet for en eID på nivå «høyt» og «betydelig». Det skilles ikke på sikkerhetstiltak i BankID infrastruktur på de ulike sikkerhetsnivåene. Per i dag må sluttbruker ha et gyldig BankID sertifikat på nivå «høyt» for å ta i bruk BankID på nivå «betydelig». Antisvindeltiltakene benyttes for begge nivåer. Det er brukersted som beslutter hvilket sikkerhetsnivå som skal benyttes. Sluttbruker forventer likevel at en eID brukes primært til å autentisere en identitet, og ikke benyttes til overvåkning utover det som er strengt nødvendig for formålet.

Bruk av datapunktene i lys av formålet med BankID Antisvindel 2.0
Som nevnt ovenfor er formålene med å behandle personopplysninger i BankID Antisvindel 2.0 spesifisert i det vesentlige av eIDAS artikkel 8, som oppsummeres slik:

- å oppnå en betydelig redusert risiko for misbruk eller endring av identiteten (for sikkerhetsnivået betydelig).
- å hindre misbruk eller endring av identiteten (for sikkerhetsnivået høyt).

Dataminimeringsprinsippet
Dataminimeringsprinsippet ble vurdert i sammenheng med nødvendighetsvilkåret og forholdsmessighetsprinsippet, som omtales nedenfor.

Dataminimeringsprinsippet er fastsatt i GDPR artikkel 5 nr. 1 bokstav c, som pålegger at personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålet med behandlingen. For BankID og BankID Antisvindel 2.0 betyr dette at utsteder kun skal innhente og behandle personopplysninger som er strengt nødvendige for å oppnå det angitte formålet.

De aktuelle datapunktene er tett koblet til deteksjon av mistenkelige mønstre og risikosignaler. Kun datapunkter som direkte bidrar til svindeldeteksjon benyttes, mens andre opplysninger som ikke er adekvate eller relevante, er utelatt.

Nødvendighetsvilkåret
GDPR artikkel 5 nr. 1 bokstav c og artikkel 6 stiller krav om at personopplysninger som behandles skal være nødvendige i forhold til det angitte formålet. Dette innebærer at det må foreligge en tydelig og legitim sammenheng mellom hvert enkelt datapunkt og formålet med behandlingen, at tiltaket er virkningsfullt i å oppnå formålet og det ikke finnes mindre inngripende, men like virkningsfulle alternativer.

Samtlige datapunkter behandlet i BankID Antisvindel 2.0 er grundig dokumentert, vurdert og ansett som nødvendige for å oppfylle formålet. Formålet er både lovpålagt og samfunnskritisk, og det er utarbeidet et dokumentert risikobilde som tilsier behov for tiltak. Mindre inngripende alternativer er vurdert som utilstrekkelige sett i lys av gjeldende krav og dagens trusselbilde, jf. vurderingen «Er behandling av personopplysninger i BankID Antisvindel 2.0 nødvendig?».

Forholdsmessighetsvurdering
Selv om innsamling av tekniske og atferdsbaserte datapunkter innebærer et inngrep i sluttbrukers personvern, vurderes tiltakene som er implementert i BankID Antisvindel 2.0 som forholdsmessige med utgangspunkt i formålet om å forhindre misbruk og endring av identitet.

Forholdsmessighetsvurderingen baserer seg på en balansert analyse mellom inngrepets karakter og formålets betydning, samt etablerte tiltak for ivaretakelse av personvernet.

Formålet anses som vesentlig og av stor samfunnsmessig verdi. BankID gir tilgang til både offentlige og private tjenester, hvor de fleste av disse tjenestene er digitalisert. Misbruk og endring av identitet kan medføre alvorlige konsekvenser for både sluttbrukere og brukersteder som benytter eID. Forebygging av slike hendelser anses dermed som legitimt, nødvendig og viktig for sluttbruker og fra et samfunnsperspektiv.

Databehandlingen er strengt begrenset til sikkerhetsformål, hvilket styrker forholdsmessigheten ved at de innsamlede datapunktene kun benyttes til forebygging og identifisering av svindel. Tilgangen er begrenset til autorisert analysepersonell og driftsroller, og datapunktene benyttes ikke til andre formål.

Antisvindeltiltakene påvirker verken brukeropplevelsen eller tilgang til tjenesten, med mindre det avdekkes en risiko. Datapunkter behandles i separate IT-løsninger med strenge tilgangsbegrensninger, tilgangslogger og kryptering. Analysemodeller og regelverk kvalitetssikres jevnlig, og lagringstiden er definert og begrenset.

Effektiv bekjempelse av svindel ivaretar i stor grad sluttbrukers interesser, beskytter mot økonomisk tap, opprettholder tilliten til BankID og sikrer adgang til nødvendige digitale tjenester.

Sluttbrukere mottar utfyllende informasjon om bruk av BankID og behandling av personopplysninger gjennom sluttbrukervilkår og personvernerklæring.

Samlet vurdert anses behandling i BankID Antisvindel 2.0 som nødvendig, rimelig og i samsvar med forholdsmessighetsprinsippet.

Veien videre

I rapporten peker Stø til behovet for et tydeligere nasjonalt regelverk for svindelforebyggende tiltak, særlig gjennom nye forskriftsbestemmelser om informasjonsutveksling innen sektorer som finans og telekommunikasjon der elektroniske ID-er benyttes, hvor dagens taushetsregler setter begrensninger.

Videre understreker Stø at eksisterende rammeverk for tilbydere av eID og tillitstjenester må vurderes i sammenheng med dagens trusselbilde og teknologiske utvikling. Innføringen av en antisvindelløsning fremheves som et nødvendig og sentralt virkemiddel for å opprettholde tilliten til digitale identiteter.

De viktigste refleksjonene som Stø sitter igjen med fra sandkassen er at det er et behov for klarere delingshjemler for både finansforetak og brukersteder tilknyttet tilbydere av tillitstjenester, med henvisning også til arbeidet med og behovet for ny regulering om antisvindeltiltak på betalingstjenesteområdet i EU. For formålet å forhindre økonomisk kriminalitet, bør derfor aktører i betalings-, telekom- og tillitstjenestene gis bedre hjemmelsgrunnlag til utlevering gjennom informasjonsdelingsordninger.

Ifølge Stø er ikke personvern den primære utfordringen for mer effektiv datadeling i arbeidet mot økonomisk kriminalitet. Det største hinderet er behovet for tydeligere delingshjemler for det samfunnsnyttige formålet, samt at dagens taushetsregler for finansforetak og telekommunikasjon begrenser delingsadgang.

Overfor tilbydere etter lov om elektroniske tillitstjenester er det også konkrete utfordringer som må adresseres bedre fremover.

Lov om elektroniske tillitstjenester er en viktig del av Norges digitale infrastruktur, som sikrer at elektroniske transaksjoner kan gjennomføres trygt og effektivt. Loven gir et rammeverk for både offentlige og private aktører (brukersteder) til å bruke elektroniske autentiseringstjenester og signaturer i samsvar med europeiske standarder, men mangler klarere hjemmel for tilbyders innsamling av datapunkter og utlevering av datapunkter fra brukersteder for å forhindre misbruk eller endring av identitet.

Personopplysninger skal behandles i samsvar med GDPR, jf. eIDAS artikkel 5 nr. 1. Autentiseringsordningen forutsetter at det behandles personopplysninger (identifikasjonsdata) om sluttbruker, og sluttrapporten viser at det er nødvendig med sikkerhetstiltak for en eID etter lov om elektroniske tillitstjenester og behov for nye datapunkter fra brukersted, i dagens trusselbilde, for det nevnte formålet.

Lov om elektroniske tillitstjenester bør derfor få en klarere hjemmel for utsteders innsamling og brukersteds utlevering av nødvendige opplysninger til nevnte formål, som også omfatter personopplysninger nevnt i personvernforordningens artikkel 9 og 10, dvs en klarere adgang til datadeling for brukersteder av tillitstjenester, som også har behov for enten et supplerende rettsgrunnlag eller en mer presis tolkning av artikkel 9 nr. 2 bokstav g når informasjonen potensielt omfatter særlige kategorier av personopplysninger.

Dette bør tydeliggjøres både ved at tilbydere av elektroniske tillitstjenester skal etablere og forvalte en mekanisme for transaksjonsovervåkning for å forhindre misbruk eller endring av

identitet, samt for å styrke effektiviteten av slike mekanismer dele og motta informasjon for samme formål, med tilknyttede brukersteder til tillitstjenestene, innenfor rammene av personvernprinsippene.

Etter levering av sandkasserapporten om BankID Antisvindel 2.0, vil Stø videreføre sitt arbeid med å forebygge, avdekke og forhindre misbruk og endring av identitet i tett samarbeid med både private og offentlige aktører. Arbeidet vil bygge videre på innsikten, anbefalingene og erfaringene fra sandkasseprosessen, og har som mål å bidra til mer helhetlige, effektive og fremtidsrettede tiltak mot svindel i Norge.

Stø vil særlig legge vekt på tverrsektorielt samarbeid mellom finansnæringen, telekom, offentlige myndigheter og relevante tilsynsmyndigheter. Stø har initiert dialog med Digitaliseringsdirektoratet og telekomleverandørene for å utforske et potensielt samarbeid på antisvindelområdet. Ved å legge til rette for deling av kunnskap, erfaringer og relevante data innenfor gjeldende rammebetingelser, kan aktørene sammen utvikle bedre forståelse av trusselbildet, identifisere nye svindelmetoder tidligere og koordinere tiltak på tvers av sektorer.

En sentral del av det videre arbeidet vil være å bidra til dialog mellom aktører og regulatoriske myndigheter om rammebetingelser, regelverksforståelse og eventuelle behov for tilpasninger som kan muliggjøre mer effektiv svindelbekjempelse, samtidig som hensyn til personvern, rettssikkerhet og tillit ivaretas. Stø AS kan her fungere som en brobygger og pådriver for balanserte løsninger som forener innovasjon og ansvarlighet.

Gjennom dette arbeidet søker Stø å bidra til å styrke samfunnets samlede motstandskraft mot økonomisk kriminalitet og svindel, redusere tap for både privatpersoner og virksomheter, og understøtte tilliten til digitale identitets- og betalingstjenester i Norge.

***

Til sist ønsker Stø å rette en stor takk til Finanstilsynet og Datatilsynet for et konstruktivt samarbeid i sandkassen. Tilsynene er løsningsorienterte, solide diskusjonspartnere og har gitt god veiledning om relevante rettslige spørsmål. Det har medført at Stø står trygt i de vurderingene som er foretatt.

Vedlegg

Begrep	Definisjon
Avtale om BankID	Standardisert avtale mellom utsteder og sluttbruker om BankID.
BankID	En elektronisk identitet (eID) som brukes for autentisering, innlogging og signering i digitale tjenester. BankID er notifisert på høyeste sikkerhetsnivå i EU.
BankID Antisvindel 2.0	En oppgradert løsning for svindelforebygging i BankID som innebærer utvidet datainnsamling og informasjonsutveksling mellom aktører.
BankID OIDC (OpenID Connect)	Teknisk grensesnitt og integrasjonspunkt mellom utsteder og brukersteder for leveranse av BankID-tjenesten.
BankID Sertifikat	En datastruktur som inneholder sertifikatholders offentlige nøkkel, signert med en sertifikatutsteders private nøkkel. Brukes til autentisering og integritet i elektronisk kommunikasjon.
BankID Tjenesten	Samlebetegnelse på alle BankID-relaterte tjenester, inkludert Person BankID og Brukersted BankID.
BankID Transaksjon	Meldingsutveksling mellom sluttbruker, brukersted og utsteder sikret med BankID.
Bedrageri	Handlinger der kriminelle skaffer seg uberettiget vinning ved å lure eller forlede noen til å foreta en handling som medfører eller kan føre til tap.
Behandlingsansvarlig	Den eller de som bestemmer formålet med og midlene for behandling av personopplysninger, jf. GDPR artikkel 4(7).
Behandlingsgrunnlag	Det rettslige grunnlaget som gir lov til å behandle personopplysninger, for eksempel samtykke, avtale, lovpålagt plikt eller berettiget interesse.
Brukersted	Juridisk enhet som har inngått avtale om BankID-tjenesten.
Brukersted BankID	BankID utstedt til et brukersted (f.eks. finansforetak, telekom, ID-porten, andre kategorier av foretak).
Brukerstedsavtalen	Avtale mellom utsteder og brukerstedet om bruk av BankID-tjenesten.
Dataminimering	Prinsippet om å begrense innsamling og behandling av personopplysninger til det som er nødvendig for formålet.
Datapunkter	Informasjonselementer som behandles i

	BankID, som også benyttes for å forebygge og avdekke svindel.
eIDAS	EU's forordning for elektronisk identifikasjon og tillitstjenester. Norge har inkorporert forordningen i lov om elektroniske tillitstjenester.
Gyldig BankID sertifikat	Et sertifikat som ikke er tilbakekalt eller suspendert, og hvor gyldighetstiden ikke er utløpt.
Kundeautentisering	Prosessen for å bekrefte identiteten til en bruker før tilgang til tjenester eller gjennomføring av transaksjoner.
Person BankID	BankID utstedt til en fysisk person (sluttbruker).
Personopplysninger	Enhver opplysning som direkte eller indirekte kan knyttes til en identifisert eller identifiserbar fysisk person.
Regulatorisk sandkasse	Virksomheter kan teste nye produkter og tjenester under veiledning fra relevante myndigheter. Dette gir en felles økt forståelse av gjeldende regelverk, eventuelt behov for regelverksendringer, samtidig som det muliggjør effektiv identifisering av risikoer og utvikling av hensiktsmessige løsninger gjennom samarbeid.
Risikovurdering	Systematisk analyse av sannsynlighet og konsekvens for uønskede hendelser, som f.eks. svindel.
Sertifikatholder	Sluttbruker eller virksomhet som har fått utstedt BankID.
Svindel med elektronisk ID	Svindel og misbruk av eID kan bl.a. føre til økonomisk kriminalitet, manipulering av offentlige registre, bedrageri, hvitvasking og sosial manipulering og phishing.
Svindelmønster	Typiske kjennetegn eller indikatorer som brukes til å identifisere forsøk på bedrageri.
Taushetsplikt	Lovpålagt plikt til å hindre at fortrolige opplysninger blir kjent for uvedkommende.
Utsteder (tilbyder)	En aktør som utsteder og forvalter en eID til fysiske eller juridiske personer. Utsteder (tilbyder) har ansvar for å etterleve alle kravene etter eIDAS.