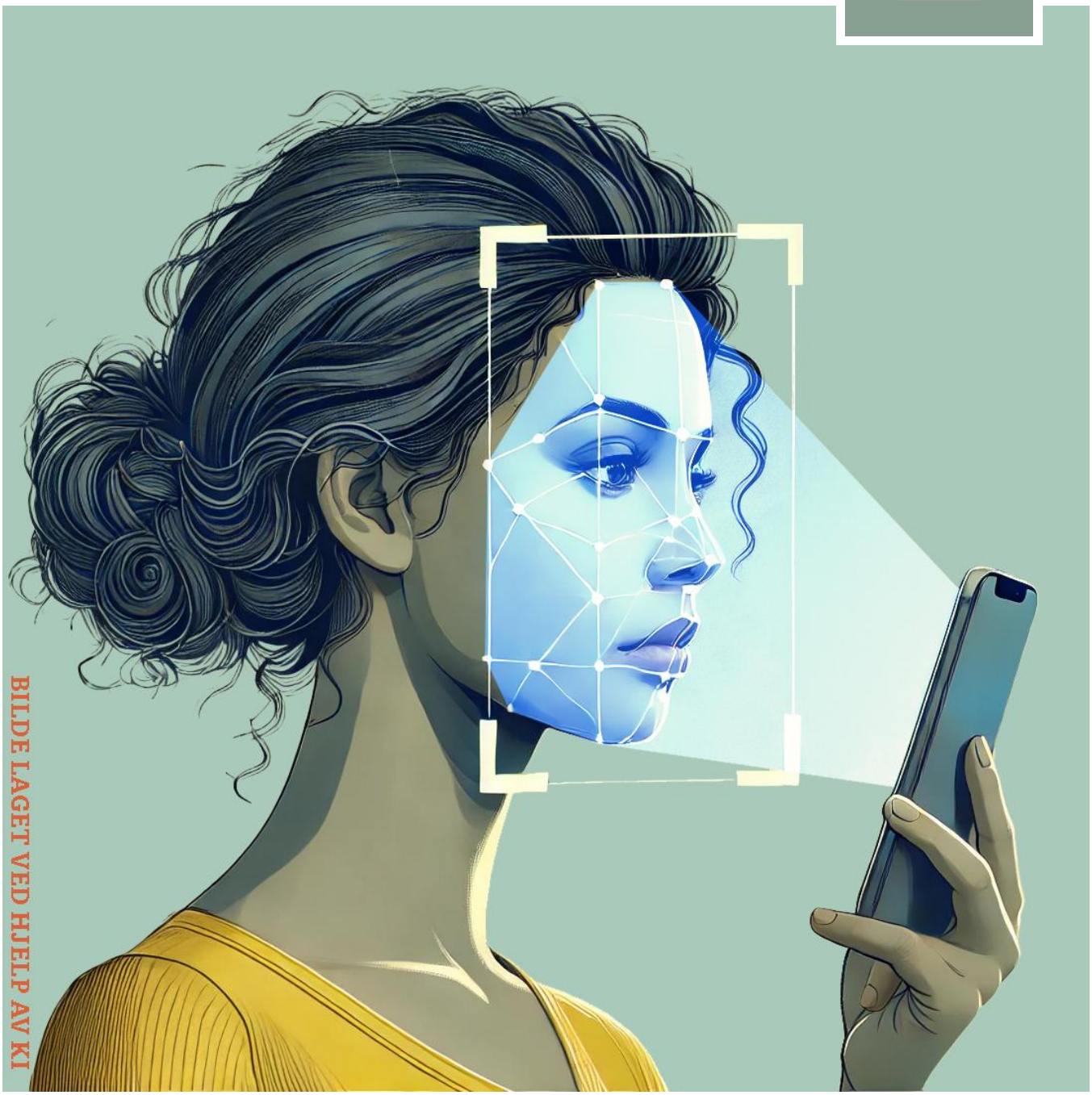


Sikring av digitale identiteter

Biometriske opplysninger og beskyttede maler i eID-løsninger

Sluttrapport fra sandkasseprosjektet med Mobai m. fl.

Datatilsynet

Innhold

Sammendrag

Digitale tjenester er en integrert del av våre liv. For at vi skal bruke og ha tillit til disse tjenestene, er det avgjørende at de er sikre og effektive.

Digitale tjenester tilbyr vanligvis flere måter for en person å verifisere sin identitet på, som regel med krav om flere faktorer. Dette kan inkludere informasjon om noe du vet (passord eller PIN-koder), noe du har (en spesifikk enhet eller en fysisk nøkkel) eller noe du er (biometri).

Vi ser en dreining hos virksomheter mot mer bruk av biometri for å øke sikkerheten ved identitetsverifisering. Biometriske opplysninger omfatter unik informasjon om våre fysiske, fysiologiske eller atferdsmessige egenskaper – oftest med henvisning til våre fingeravtrykk eller ansiktsbilder.

Biometriske opplysninger er unike for hver enkeltperson, og det kan ha store negative konsekvenser hvis de blir stjålet. Samtidig må risikoen ved å bruke biometriske opplysninger sees i lys av at sosial manipulering har blitt mer vanlig, hvor ondsinnede aktører lurer brukere til å gi fra seg informasjonen som trengs for å få tilgang til nettbaserte tjenester. Derfor er slike opplysninger underlagt strenge personvernregler, som skal begrense innsamling, lagring og bruk av slike opplysninger.

Mobai ønsker med SALT-løsningen sin å redusere risikoen forbundet med behandling av biometriske opplysninger. De tar sikte på å gjøre dette ved å utnytte kunstig intelligens og innovative maskinlæringsmetoder. Slik ønsker de å redusere personvernrisikoen for brukeren samtidig som de utvider hvordan biometrisk informasjon kan bli brukt til digital verifisering.

I denne rapporten tar Datatilsynet for seg sentrale juridiske utfordringer knyttet til "SALT" – inkludert om løsningen kan utvide hvordan biometrisk informasjon kan brukes for verifiseringsformål.

Vårt mål med denne sluttrapporten er å gi verdifulle og generaliserbare juridiske innsikter som kan være til nytte for Mobai og deres samarbeidspartnere, samt andre aktører som jobber med lignende problemstillinger.

Merk

Teknologien og jussen er stadig i utvikling, og det vil kunne ha skjedd justeringer og presiseringer etter at denne rapporten ble skrevet.

Hovedfunn

I dette sandkasseprosjektet tar vi tak i noen sentrale juridiske utfordringer knyttet til hvordan SALT-løsningen fungerer, som også er relevante for andre selskaper i lignende felt og med lignende juridiske problemstillinger.

Våre vurderinger av disse utfordringene er som følger:

- **Er ansiktsbilder biometriske opplysninger?**

Et ansiktsbilde kvalifiserer seg ikke alltid som en biometrisk opplysning slik det er definert i personvernregelverket. Datatilsynet vurderer imidlertid at biometriske maler er biometriske opplysninger. Vi anser også operasjonene som utføres på ansiktsbildet for å generere den biometriske malen (dvs. uttrekkingen av biometriske egenskaper fra bildet) som behandling av biometriske opplysninger.

Selv om ansiktsbilder i seg selv ikke er ansett som biometriske opplysninger etter forordningen, kan altså behandling av ansiktsbilder være underlagt samme nivå av sikkerhetskrav som behandling av biometriske opplysninger.

- **Er beskyttede maler (Protected Templates) basert på biometriske opplysninger personopplysninger etter personvernforordningen?**

Datatilsynet har diskutert med Mobai om biometriske beskyttede maler – laget ved homomorfisk kryptering – kan anses som anonyme, eller om de fortsatt er ansett som personopplysninger.

Selv om homomorfisk kryptering og beskyttede maler gjør informasjonen uforståelig for parter som ikke har krypteringsnøkkelen, garanterer dette ikke nødvendigvis anonymitet. Så lenge krypteringsnøkkelen kan brukes til å koble malen til en fysisk person, omfattes den etter vår vurdering av personvernforordningens definisjon av personopplysninger.

- **Anses biometriske opplysninger som brukes til verifisering som en særlig kategori av personopplysninger?**

Det er knyttet juridisk usikkerhet til om biometrisk verifisering innebærer en behandling av særlige kategorier av personopplysninger etter artikkel 9 nr. 1. Spørsmålet kan ikke løses i dette sandkasseprosjektet. Men basert på diskusjonene vi har hatt, anser Datatilsynet det som sannsynlig at biometrisk verifisering er omfattet av artikkel 9 nr. 1. Vi anbefaler derfor de involverte i SALT-prosjektet å behandle de biometriske opplysningene som brukes til verifiseringsformål som en særlig kategori av personopplysninger.

- **Hva er forskjellen mellom den primære behandlingen av personopplysninger i SALT-løsningen og behandlingen for sekundære formål?**

Det primære formålet med SALT-løsningen er å verifisere identitet. Datatilsynet anser at visse operasjoner som skjer i forkant av verifiseringen er omfattet av dette formålet, men bare når de er

strengt nødvendige for å oppnå formålet. I Mobais tilfelle knytter dette seg til genereringen og sammenligningen av beskyttede maler.

Vi anser behandling av personopplysninger til forbedringer av algoritmene og systemet som sådan, som behandling for sekundære formål. Denne behandlingen krever et selvstendig rettslig grunnlag.

- **Er det lov å lagre biometrisk informasjon på en sentral server?**

Mobais tilnærming til lagring og behandling av biometriske opplysninger krever sentralisert lagring. Dette er fordi de anser det som nødvendig for å forbedre sikkerheten.

Sentralisert lagring muliggjør avansert kryptering, tilgangskontroll og robuste sikkerhetstiltak, men reiser også bekymringer rundt storskala innsamling av biometriske opplysninger – og andre type opplysninger – som kan brukes til verifisering av digitale identiteter.

Mobai hevder at de kan balansere sikkerhet og personvern ved å bruke innovativ teknologi for å generere biometriske, beskyttede maler som gjør det mulig å kombinere egenskapene til desentraliserte enheter med sentral lagring og behandling.

I tillegg lagrer Mobai krypterte bilder sentralt for trening av KI-modellene, mens de har på plass strenge dataminimeringspraksiser. Formålet med dette er å balansere sikkerhet og regelverksetterlevelse ved håndteringen av sensitive opplysninger.

I dette prosjektet har Datatilsynet vurdert at Mobais løsning kan gjøre det mulig med sentral lagring og behandling av biometriske opplysninger i tilfeller hvor det tidligere ikke ble ansett som sikkert nok til å adressere de betydelige bekymringene forbundet knyttet til sentral lagring.

Hva er Datatilsynets sandkasse?

I sandkassa jobber deltakere sammen med Datatilsynet for å løse spørsmål om personvern. Målet er at tjenesten eller produktet deres følger loven og gir godt personvern.

Datatilsynet gir råd til deltakerne, men konklusjonene er ikke offisielle avgjørelser, vedtak eller godkjenninger. Deltakerne velger selv om de vil følge rådene.

Sandkassa er nyttig for å se på spørsmål der jussen har få praktiske eksempler å vise til. Vi håper rapporten kan hjelpe andre med liknende utfordringer.

Om prosjektet

Mobai er et selskap med bakgrunn fra Norges teknisk-naturvitenskapelige universitet (NTNU). De utvikler biometri-teknologi for digitale tjenester. Teknologien brukes særlig i innrullerings- og verifiseringsprosesser for digitale tjenester.

I dette sandkasseprosjektet er fokuset rettet mot deres løsning kalt "SALT" ("Secure privacy preserving authentication using facial biometrics to protect your identity"). SALT er utviklet av Mobai i samarbeid med BankID BankAxept AS og Sparebank 1 Østlandet.

Kripos påpekte i sin årsrapport for 2023 at digitalt bedrageri er et utbredt problem i Norge, og at det er en økning i identitetsbedrageri knyttet til eID-løsninger. Det er spesielt utstedelse, nyutstedelse og bruk av eIDer som er sårbare for ulike angrep, som potensielt kan føre til at påloggingsinformasjon blir stjålet eller misbrukt.

Ambisjonen med SALT er å utvikle en løsning for digital ansiktsverifisering som betydelig reduserer risikoen for identitetstyveri av digitale kontoer. Samtidig har løsningen som mål å beskytte biometriske opplysninger mot misbruk og tyveri. For å forhindre dette utvikler Mobai SALT som en sikkerhetskomponent – som kan komplementere eksisterende sikkerhetstiltak – i eID-løsninger.

eID

«eID» står for elektronisk identifikasjon. Begrepet viser spesifikt til de som leverer tjenester knyttet til identifisering, slik som verifisering og digital signering.

eID-tjenester i Norge følger kravene i eIDAS-forordningen, som skal sikre et velfungerende marked og oppnå et passende sikkerhetsnivå for elektronisk identifikasjon og tillitstjenester.

Om SALT-løsningen

Den sentrale komponenten i SALT er en innovativ krypteringsteknikk kalt "homomorfisk kryptering". I motsetning til andre krypteringsmetoder tillater homomorfisk kryptering analyse av krypterte data – uten at de først blir dekryptert.

I ansiktsbiometriske systemer som SALT, verifiseres identiteter ved å sammenligne to ansiktsbilder. Sammenligningen genererer ett “likhetspoeng” som indikerer graden av samsvar mellom ansiktene. I SALT utføres denne sammenligningen innenfor et kryptert domene ved hjelp av homomorfisk kryptering, og også resultatet av sammenligningen forblir kryptert gjennom hele prosessen.

For å sammenligne ansiktsbilder blir biometriske egenskaper hentet ut fra bilder av brukerens ansikt. Alle biometriske egenskaper på bildet får så en vektor-representasjon i form av et

datasett. Dette datasettet kalles en "biometrisk mal", og er maskinlesbart og egnet for ansiktsgjenkjenning. Likhetspoenget genereres ved å sammenligne settet av biometriske egenskaper i de biometriske malene.

De biometriske malene inneholder kun klartekst, og ikke selve bildet. Det har imidlertid blitt demonstrert at noe informasjon om ansiktet, og visse ansiktstrekk, kan rekonstrueres fra biometriske maler. For å forhindre dette er det nødvendig å iverksette sterke sikkerhetstiltak for å beskytte dem.

Beskyttede maler er et slikt sikkerhetstiltak. Beskyttede maler er – kort fortalt – et sikkerhetstiltak hvor malene som finnes i klartekstform, blir transformert og kryptert. I "SALT" skjer dette ved bruk av homomorfisk kryptering.

Fordelene med disse beskyttede malene er at de kan brukes til ansiktsgjenkjenning – akkurat som klartekstmaler. Men med dagens teknologi antas det å være praktisk talt umulig å regenerere malen i klartekst fra en beskyttet mal, og det er derfor ikke mulig å gjenopprette ansiktsbilder (eller andre karakteristikker) som tilhører brukeren.

Krav til beskyttende maler

I henhold til Den internasjonale standardiseringsorganisasjonen (ISO/IEC 24745:2022) må en beskyttet mal oppfylle følgende krav:

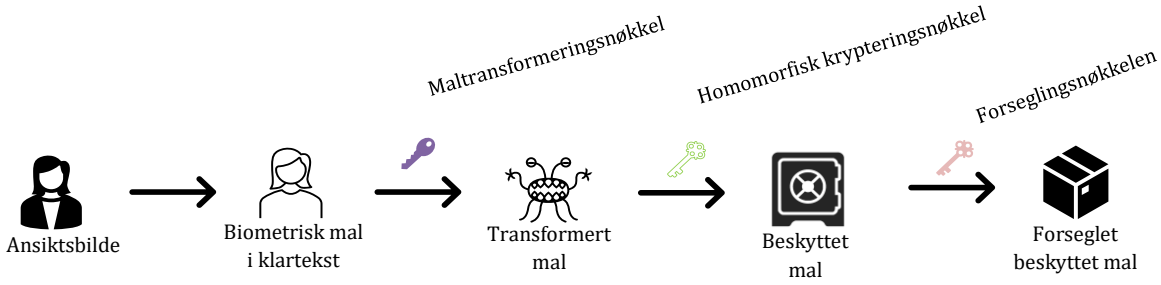
- **Mulighet for tilbakekalling og fornyelse:** Et system må kunne tilbakekalle kompromitterte beskyttede maler, slik at de ikke kan brukes/misbrukes videre. Følgelig må systemet kunne generere en ny, ukompromittert beskyttet mal og erstatte den opprinnelige slik at sluttbrukeren fortsatt kan bruke løsningen.
- **Ikke reverserbar:** Ansiktsbildet eller ansiktsmalen skal behandles med irreversibel transformasjon før lagring.
- **Ikke sporbart mellom systemer:** De lagrede ansiktsmalene skal ikke kunne kobles på tvers av applikasjoner eller databaser

Hvordan fungerer krypteringen?

I dette kapittelet beskriver vi hvordan krypteringsnøkler fungerer i SALT-løsningen. Håndteringen av nøkler er en essensiell del av løsningen, ettersom opprettelse og bruk av beskyttede maler involverer bruk av flere krypteringsnøkler som gir ulike egenskaper knyttet til sikkerhet og personvern.

Markert med farger i figuren nedenfor finner du en oversikt over nøkler som brukes i opprettelsen av beskyttede maler. Det er tre krypteringsnøkler: "maltransformeringsnøkkel", "homomorfisk krypteringsnøkkel" og "forseglingsnøkkel".

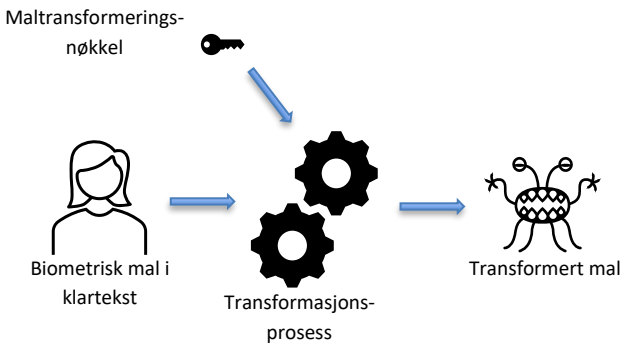
Forseglingsnøkkelen brukes for å sikre systemets integritet i det krypterte domenet, men tilfører ikke personvernegenskaper til den beskyttede malen.



Figur 1: Oversikt over nøkler som brukes i opprettelsen av en beskyttet mal

Maltransformeringsnøkkelen

Den første nøkkelen ("maltransformeringsnøkkelen") brukes til å transformere en klartekst biometrisk mal til en transformert mal. Den gjør dette ved å kombinere et "frø" med transformasjonsprosessen for å generere en ny og unik versjon av en klartekstmal hver gang prosessen utføres. Mobai hevder at denne transformasjonen sikrer personvernet ved å gjøre informasjonen irreversibel og ikke-sporbar, i samsvar med ISO/IEC 24745:2022.



Figur 2: Malgenerering-prosessen tar den biometriske klartekstmalen og kombinerer den med maltransformeringsnøkkelen for å lage den transformerte malen

Med dagens teknologi, antas det å være praktisk umulig å rekonstruere ansiktstrekk fra en transformert mal. Dette kan sikre dataenes irreversibilitet. Ikke-sporbarheten (et annet krav i

henhold til ISOen) mellom to beskyttede mal som er generert fra samme person, sikres ved å bruke forskjellige transformeringsnøkler for hver registrering.

Videre, hvis en transformert mal blir kompromittert, kan den gamle maltransformeringsnøkkelen kastes, noe som gjør den transformerte malen ubrukelig. Dette betyr at det er mulig å muliggjøre informasjonens tilbakekallbarhet. Videre kan en ny transformert mal opprettes ved bruk av en ny maltransformeringsnøkkel, som sikrer dens fornybarhet.

Den transformerte malen er et mellomtrinn i prosessen med å generere beskyttede maler. Den transformerte malen brukes ikke til ansiktssammenligning og lagres ikke.

Den homomorfiske Krypteringsnøkkelen

Det andre trinnet er å kryptere den transformerte malen med en homomorfisk krypteringsnøkkel. Resultatet av denne krypteringen er den «beskyttede malen».

Krypteringen sikrer konfidensialiteten til den beskyttede malen, både ved lagring og ved bruk. Den sikrer også konfidensialiteten til resultatet av ansiktssammenligningen. I dette systemet er det kun resultatet som dekrypteres.

Det homomorfiske krypteringssystemet er basert på asynkron kryptering. Dette vil si at det er to nøkler – et nøkkelpar – hvor et dataelement kryptert med den første nøkkelen (dvs. den beskyttede malen) kun kan dekrypteres med den andre nøkkelen.

Et viktig sikkerhetsprinsipp som er gjort mulig av asynkron kryptering er nøkkelseparasjon. Dette vil si at ingen enhet har tilgang til begge nøkler. I SALT-løsningen vil innehaveren av den andre nøkkelen kun ha tilgang til resultatet. Dette systemet muliggjør faktisk seperasjon mellom lagring og bruk av de beskyttede malene, og deres dekrypteringsnøkkel. Dermed unngås enkeltstående kompromitteringspunkter i løsningen.

Forseglingsnøkkelen

Forseglingsnøkkelen fungerer som en digital signatur og sikrer integriteten til den beskyttede malen og resultatet fra sammenligningen. Dette trinnet bruker et etablert system for elektroniske signaturer. Verifiseringsprosessen bør validere denne signaturen før hver bruk av en beskyttet mal.

Nøkkelhåndtering

Mobai har til hensikt å håndtere nøklene på en måte som sikrer konfidensialiteten til de overnevnte prosessene. Nøkkelhåndteringssystemet vil generere og håndtere nøkler i sikre miljøer. Maltransformeringsnøkkelen genereres ved bruk av en sterk tilfeldig tallgenerator med tilstrekkelig lengde, og den homomorfiske krypteringsnøkkelen genereres ved bruk av det nyeste homomorfiske krypteringssystemet. En kryptografisk nøkkelhåndteringspolicy vil bli implementert ved å følge standardene som følger av ISO 27001.

Hvordan fungerer løsningen?

Nedenfor gir vi en forenklet trinnvis forklaring av hvordan SALT-løsningen fungerer i praksis. Forklaringen skisserer et scenario hvor en sluttbruker samtykker til å bruke SALT-løsningen for å få tilgang til en nettbasert tjeneste levert av en bank.

Prosessen består av to faser: en innrulleringsfase og en verifiseringsfase.

Det er også en siste fase, hvor personopplysninger behandles for sekundære formål, inkludert forbedring av svindeldetektor-modulen og maskinlæringsalgoritmene. Vi vil utforske sekundære formål nærmere i neste kapittel.

Innrulleringsfasen

1. **Initiering:** Inrulleringsfasen initieres når brukeren sender inn et "referansebilde". Referansebildet er ansiktsbildet hentet fra et nasjonalt utstedt ID-dokument, som et nasjonalt ID-kort eller et pass. Spesifikt, så er det bildet fra Radio Frequency Identification (RFID)-brikken i dokumentet som hentes.
2. **Malgenerering**: En malgenereringsmodul konverterer referansebildet til en "klartekstmal".
3. **Nøkkelgenerering**: En nøkkelhåndteringsserver vil generere en unik "transformeringsnøkkel" som er spesifikk for hver bruker. Den vil også generere en "homomorfisk krypteringsnøkkel", som er spesifikk for hver eID-leverandør.
4. **Sikker behandling**: Klartekstmalen sikres gjennom en transformasjonsprosess ved bruk av transformeringsnøkkelen, etterfulgt av en krypteringsprosess ved bruk av den homomorfiske krypteringsnøkkelen. Denne prosessen resulterer i genereringen av en beskyttet mal. Den beskyttede malen forsegles deretter ved bruk av forseglingsnøkkelen. Dette sikrer integriteten til den beskyttede malen.
5. **Lagring**: Den forseglede beskyttede malen lagres i en lagringsserver. Denne beskyttede malen er referansemalen, og den brukes til ansiktssammenligningen i verifiseringsfasen.
6. **Verifisering**: For å sikre at innrulleringen utføres av innehaveren av det nasjonale ID-dokumentet, må brukeren verifisere sin identitet ved å følge trinnene i "verifiseringsfasen", beskrevet nedenfor. Hvis verifiseringsavgjørelsen er positiv, har brukeren blitt innrullert for videre bruk (dvs. løpende verifiseringer).

Verifiseringsfasen

For å få tilgang til en tjenesteleverandørs/forhandlers tjenester, må brukeren gjennomgå en verifiseringsfase, detaljert nedenfor:

1. **Bildeopptak**: Brukeren tar et livebilde av seg selv (en "selfie") på sin mobile enhet og laster opp dette bildet til SALT-løsningen.
2. **Svindeldetektor-modul:** En svindeldetektor-modul (se infoboks) analyserer bildet for å vurdere om det ble tatt live fra en tilstedeværende person uten noen bildemanipulasjon eller fabrikasjon.
3. **Generering av klartekstmal:** Hvis svindeldetektor-modulen konkluderer med at bildet er autentisk, genererer malgenereringsmodulen en klartekstmal.

4. **Generering av beskyttet mal:** En beskyttet mal vil bli generert fra denne klartekstmalen ved bruk av samme prosedyre som beskrevet tidligere, ved bruk av samme transformeringsnøkkel og homomorfiske krypteringsnøkkel som ble brukt for opprettelsen av brukerens referansetemplate. Den beskyttede malen forsegles deretter ved bruk av forseglingsnøkkelen.
5. **Ansiktsverifisering og sammenligning:** Den forseglede beskyttede malen sendes til ansiktsverifiseringsmodulen hvor den vil bli sammenlignet med brukerens beskyttede referansemal.
6. **Sammenligning av poeng fra malene:** Sammenligningen genererer en likhetspoengscore og tar deretter en verifiseringsavgjørelse basert på om poengsummen møter en forhåndsdefinert terskel. Resultatet fra prosessen er verifiseringsavgjørelsen, som er tilgjengelig for leverandøren.
7. **Autorisasjon:** Hvis verifiseringsavgjørelsen er positiv, vil brukeren bli autorisert til å bruke den digitale tjenesten.

Hvilke personopplysninger vil bli behandlet?

Hva er komponentene i ansiktsverifiseringssystemet?

Ansiktsverifiseringssystemet involverer følgende moduler:

- **Opptaksmodul:** Denne modulen kjøres i mobilapplikasjoner på brukernes smarttelefoner og kommuniserer med kameraapplikasjonen og brukeren når de tar en selfie. Mobilapplikasjonen vil typisk være levert av en bank eller BankID. Opptaksmodulen er en programvarekomponent i disse mobilapplikasjonene.

- **Ansiktsverifiseringsmodul:** Denne modulen sammenligner et referansebilde (hentet fra et ID-dokument under innrulleringsfasen), og et livebilde av ansiktet som brukeren tar av seg selv under verifiseringsfasen. Modulen genererer en likhetspoengscore som indikerer sannsynligheten for at bildene kommer fra samme person.

- **Svindeldetektor-modul:** Denne modulen analyserer livebilder for å vurdere om de ble tatt live fra en tilstedeværende person, eller om det er en forfalskning eller manipulasjon. Svindeldeteksjon inkluderer følgende undermoduler:

    - **Deteksjon av ansiktspresentasjonsangrep:** Denne modulen kan oppdage om livebildet er ekte, eller om det er en digital overflate eller en maske. Denne modulen forhindrer svindlere fra å presentere digitale bilder av andre brukere for å få fjerntilgang.
    - **Deteksjon av angrep via deepfakes:** Denne modulen oppdager om livebildet er en deepfake, dvs. et syntetisk bilde som er generert gjennom maskinlæring eller som har blitt byttet ut.
    - **Deteksjon av angrep via ansiktsmorfing:** Denne modulen oppdager om referansebildet er bevisst "morfet". Et morfing-angrep består av to eller flere ansiktsidentiteter som er digitalt kombinert for å skape et enkelt ansiktsbilde som representerer multiple identiteter. I et vellykket morfing-angrep kan et ID-dokument brukes av flere ulike svindlere.

Alle disse modulene involverer forhåndstrente modeller som bruker kunstig intelligens.

I Mobai sin løsning vil personopplysninger om brukeren bli samlet inn og behandlet. Disse personopplysningene inkluderer:

- Ansiktsbilder tatt med sluttbrukerens enhet.
- Klartekstmaler som genereres fra referansebildet (dvs. et nasjonalt utstedt ID-dokument).
- Beskyttede maler, som omfatter klartekstmaler og er beskyttet av homomorfisk kryptering.
- Ansiktsbilde hentet fra «Radio Frequency Identification» (RFID)-brikken i sluttbrukerens ID-dokument (for eksempel pass eller nasjonalt utstedt ID-kort).
- Data fra den maskinlesbare delen av nasjonalt utstedte ID-er, i henhold til den elektroniske maskinlesbare reisedokumentstandarden (ICAO 9303).
- Data fra den maskinlesbare sonen ("MRZ") på ID-dokumentet, nødvendig for å få tilgang til informasjonen på RFID-brikken.
- Informasjon om brukerenheten.

Mobai knytter formålet med behandlingen av disse opplysningene til registrering til digitale tjenester og påfølgende verifiseringer.

Hvem er de mest relevante interessentene?

I SALT-løsningen er det fire aktører som spiller distinkte roller i løsningen. Disse er:

1. **eID-leverandør:** Denne aktøren utsteder eID-en (som BankID, Buypass, Commfides og MinID) til sluttbrukeren og leverer eID-tjenestene til en digital tjeneste.
2. **Mobai:** Mobai er underleverandør til eID-leverandører, og leverer komponenter til e-ID-tjenestene. Disse komponentene inkluderer tjenester som 1) fjern-innrullering for å utstede en eID, 2) ny-utstedelse av en eID, 3) tilbakestilling av passord eller 4) bekreftelse av "liveliness" (dvs. at rett person har tilgang).
3. **Tilbydere av digitale tjenester (som SpareBank 1 Østlandet):** Denne tredjeparten er avhengig av eID-leverandøren, og følgelig Mobais komponenter som et ekstra sikkerhetslag, for å sikre at de gir tilgang til rett sluttbruker.
4. **Sluttbrukeren:** Motivasjonen for sluttbrukeren til å bruke løsningen er å fjernverifisere sin identitet til en tjeneste uten risikoen for at "svindlere" bruker deres eID med eller uten deres kunnskap.

Behandling av personopplysninger for sekundære formål

Om primærformål og sekundære formål

I konteksten av dette prosjektet refererer "sekundære formål" til bruken av personopplysninger utover det primære formålet – som er registrering til eID-tjenesten og de påfølgende identitetsverifiseringene.

Alle de sekundære formålene nevnt i denne rapporten er kjent for behandlingsansvarlig på tidspunktet når informasjonen først samles inn. Vi antar derfor at personopplysningene innledningsvis vil bli samlet inn for både det primære og sekundære formål nevnt i denne rapporten. Dermed vil ikke personvernforordningen artikkel 6 nr. 4 som regulerer behandling for nye formål komme til anvendelse.

I dette kapittelet beskriver vi bruken av personopplysninger for sekundære formål.

Mobais sekundære formål inkluderer:

- Forbedringer i prediksjonsriktighet for opptaksmoduler, ansiktssammenligning og svindeldeteksjonsalgoritmer, inkludert:
  - trening av algoritmer,
  - identifisering av ukjente type svindler for å forbedre algoritmer og
  - forbedring av sikkerhet og generelle forbedringer av tjenesten
- Gjennomføring av svindeletterforskning etter sanntidsøkter – for eksempel i tilfelle av en tvist
- Fremlegging av bevis for rettshåndhevelse (hvis og når det kreves ved lov)
- Reduksjon av skjevheter

Informasjonen som lagres for sekundære formål inkluderer:

- Sanntidsbildet, dvs. en "selfie"
- Diverse enhets- og sesjonsrelaterte data

Mobai anser seg selv som behandlingsansvarlig for de sekundære formålene som er knyttet til å gjøre forbedringer i algoritmene og reduksjon av skjevheter. For de sekundære formålene knyttet til svindeletterforskning i tilfelle av en tvist, og fremlegging av bevis for rettshåndhevelse, anså Mobai seg innledningsvis som databehandler.

I et senere kapittel av denne rapporten ser vi nærmere på forskjellene mellom primær og sekundær behandling i SALT-løsningen. I den forbindelse ser vi på formålet knyttet til trening og forbedringer av algoritmene og systemet som sådan (det første av de fire kulepunktene ovenfor).

Formålene nevnt i de andre tre kulepunktene har ikke vært en del av omfanget til dette sandkasseprosjektet. Når det gjelder reduksjon av skjevheter, har det imidlertid vært et relevant prosjekt i det regulatoriske sandkasseprosjektet til Information Commissioner's Office (ICO) i Storbritannia om dette temaet. For videre lesing, se Onfido Regulatory Sandbox Final Report (ico.org.uk).

Sentral lagring

Mobai vil lagre dataene som brukes for sekundær behandling i et sikkert servermiljø som beskyttes med blant annet fysiske sikkerhetstiltak. Dataene vil bli kryptert ved bruk av konvensjonelle metoder (ikke homomorfisk kryptering) og lagret i et dedikert miljø som er atskilt fra tjenestetilbudene – og hvor risikoen for misbruk og datalekkasje er redusert. Formålet med dette er å sikre at kun autorisert personell har tilgang. Mobai kan tilby deling av sesjonsdata med forretningspartnere i sanntids-operasjoner.

Lagringstid

I SALT-løsningen vil Mobai beholde personopplysninger i 180 dager fra det øyeblikket hvor det innledende resultatet av en verifiseringstransaksjon sendes til forhandleren. Formålet med dette er å legge til rette for maskinlæring og forbedringer i systemene for svindeldeteksjon.

Et unntak er dataene som samles inn for trening av algoritmer. Disse vil bli lagret i et helt år, for å oppnå et høyt nok antall eksempler til å sikre effektiv trening.

Prosjektets mål

Mobai og Datatilsynet har i felleskap identifisert to mål i dette prosjektet:

1. **Å vurdere den juridiske statusen til ansiktsbilder og beskyttede maler i en KI-basert løsning for identitetsverifisering:** Denne problemstillingen fokuserer på den juridiske statusen til ansiktsbilder og beskyttede maler, samt behandling for primærformålet (knyttet til biometrisk verifisering) og for sekundære formål.

2. **Å vurdere de tekniske sikkerhetstiltakene for lagring av beskyttede maler (som skal brukes av KI-en) og ansiktsbilder for treningsformål:** Utformingen og bruken av tekniske sikkerhetstiltak i SALT-løsningen vil delvis være avhengige av resultatene av diskusjonene i #1.

   Disse problemstillingene anses også som relevante for andre utviklere og virksomheter som ønsker å bruke lignende maskinlæringsteknikker og teknologier.

Rettslig grunnlag og rettslig status

Kunstig intelligens krever ofte behandling av store mengder data, ofte personopplysninger, som samles inn og analyseres i et omfang som ikke lar seg gjøre på andre måter.

For at behandling av personopplysninger skal være lovlig, trengs det et rettslig grunnlag. Personvernforordningen artikkel 6 nr. 1 bokstav a-f inneholder en uttømmende liste over seks rettslige grunnlag for lovlig behandling av personopplysninger.

Det er naturlig å dele opp spørsmålet om rettslig grunnlag og se på de to hovedfasene i et KI-prosjekt hver for seg: anvendelsesfasen og utviklingsfasen. Utviklingsfasen kommer ofte både før, under og etter fasen da tjenesten er i bruk, og personopplysninger blir ofte brukt på ulike måter i de to fasene.

I dette sandkasseprosjektet har vi ikke tatt stilling til om Mobai eller tilbyderne av elektronisk identifisering har rettslig grunnlag for å behandle personopplysninger ved hjelp av KI-verktøyet som Mobai tilbyr (SALT-løsningen). Dette gjelder både for løsningens primære formål, som er å digitalt verifisere en persons identitet, og eventuell bruk av personopplysninger til de sekundære formål som er nevnt i rapporten.

Drøftelsene i dette sandkasseprosjektet er basert på en antagelse om at de behandlingsansvarlige – som kan være Mobai selv eller tilbyderne av eID – finner et rettslig grunnlag for å behandle personopplysninger ved bruk og videreutvikling av SALT-løsningen.

Hvorfor er det relevant å drøfte rettslig status?

Det er viktig for Mobai å avklare den rettslige statusen til sentrale data som utgjør en del av løsningen. Dette gjelder blant annet ansiktsbilder, klartekstmaler og beskyttede maler.

Begrepet «rettslig status» sikter til flere ulike spørsmål, blant annet: Er opplysningene som blir behandlet, å anse som personopplysninger som faller inn under personvernforordningen? Når blir opplysningene regnet som «biometriske»? Og når blir de ansett som særlige kategorier av personopplysninger som faller inn under artikkel 9? Det er viktig å få avklart disse spørsmålene, særlig i forhold til krypteringsteknikker og maskinlæring, siden personvernforordningen ikke gjelder for data som er fullstendig anonymiserte.

Er beskyttede maler personopplysninger eller anonyme opplysninger?

Skillet mellom personopplysninger og anonyme opplysninger kan være uklart. Det er svært høy terskel for når opplysninger kan anses som anonyme.

Det er enklere å pseudonymisere opplysninger, det vil si å erstatte direkte identifiserbare parametere med pseudonymer, som fremdeles vil være entydig identifiserbare. Pseudonymisering kan gjøre det vanskeligere å koble et datasett til den personen opplysningene gjelder, og kan derfor være en nyttig teknikk for å styrke personvernet. I motsetning til anonyme

data blir pseudonymiserte data imidlertid fremdeles definert som personopplysninger etter personvernforordningen.

Se våre generelle retningslinjer for mer informasjon om anonymisering og pseudonymisering.

Når det gjelder beskyttede maler, må Mobai vurdere om opplysningene det gjelder, er anonymiserte, pseudonymiserte eller ganske enkelt vanlige personopplysninger.

Homomorfisk kryptering og beskyttede maler gjør riktignok opplysningene uforståelige for utenforstående som ikke har tilgang til krypteringsnøkkelen, men dette garanterer ikke nødvendigvis anonymitet. Så lenge det er mulig å koble malen til en fysisk person ved hjelp av nøkkelen, er det rimelig å si at den faller inn under personvernforordningens definisjon av personopplysninger.

Personvernforordningen artikkel 4 støtter dette synspunktet. Artikkelen definerer personopplysninger som opplysninger om en direkte eller indirekte identifiserbar person. Selv om det ikke er mulig å direkte identifisere noen på grunnlag av den beskyttede malen, vil selve nøkkelen gjøre indirekte identifikasjon mulig.

Er ansiktsbilder biometriske opplysninger?

I personvernforordningen artikkel 4 nr. 14 defineres biometriske opplysninger som «personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger».

I sandkasseprosjektet ble det drøftet hvordan formuleringen «som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person» i artikkel 4 nr. 14 skal forstås. Særlig vekt ble lagt på om denne formuleringen betyr at definisjonen bare dekker personopplysninger som brukes for det spesifikke formål å entydig identifisere et individ. Datatilsynet mener at dette er en i overkant restriktiv tolkning av definisjonen, og at data som egner seg til slik entydig identifikasjon også må falle inn under definisjonen i artikkel 4 nr. 14. Personvernforordningens definisjon av biometriske opplysninger tilsvarer altså stort sett definisjonen i EUs KI-forordning.

Et ansiktsbilde vil ikke nødvendigvis være regnet som biometriske opplysninger i personsonvernforordningens forstand. Dette går fram av punkt 51 i fortalen til personvernforordningen, der det står:

«(...) Behandling av fotografier bør ikke systematisk anses som behandling av særlige kategorier av personopplysninger, ettersom fotografier omfattes av definisjonen av biometriske opplysninger bare når de behandles ved hjelp av et særskilt teknisk middel som gjør det mulig entydig å identifisere eller autentisere en fysisk person. (...)»

Begrepet «særskilt teknisk behandling» er verken definert i personvernforordningen eller fortolket i rettspraksis. Etter vår mening oppfyller imidlertid de biometriske malene fra malgenereringsmodulen (som konverterer brukerens referansebilde til en "klartekstmal") definisjonen i personvernforordningen artikkel 4 nr. 14 og bør derfor regnes som biometriske

opplysninger. Vi mener også at behandlingen av ansiktsbildet for å generere den biometriske malen (som involverer uttrekking av biometriske trekk) skal anses som behandling av biometriske opplysninger etter personvernforordningen.

Selv om ansiktsbilder i seg selv ikke systematisk blir regnet som biometriske opplysninger, kan behandling av ansiktsbilder underlegges like strenge sikkerhetskrav som biometriske opplysninger. For eksempel vil det å bygge opp en database som inneholder et stort antall ansiktsbilder av høy kvalitet av personer med verifisert identitet, sannsynligvis innebære en stor risiko for rettighetene og frihetene til personene som er registrert i databasen. Se neste avsnitt om sentralisert lagring av biometriske opplysninger for mer informasjon om denne problemstillingen.

Hva er forskjellene mellom behandlingen for primærformål og sekundære formål?

Biometrisk digital verifisering av identitet ved hjelp av SALT-løsningen innebærer en rekke ulike operasjoner. Det blir tatt et bilde (ansiktsbilde/selfie) ved hjelp av en mobilapp på brukerens enhet. Det gjøres en «forbehandling» av bildet før en biometrisk mal blir generert. Denne «forbehandlingen» består av ulike operasjoner, blant annet en sjekk av bildekvaliteten og tiltak for å avsløre presentasjonsangrep, «deepfakes» og ansiktsmorfing. Formålet med disse operasjonene er å være sikker på at det mottatte bildet er ekte.

Når ansiktsbildet har bestått «forbehandlingen», blir det generert en beskyttet mal som så blir sammenlignet med referansemalen. Sammenligningen gir en poengsum som viser hvor like bildene er.

Det ble drøftet i sandkassen om denne rekken av operasjoner kunne sies å utgjøre en «behandling» etter definisjonen i personvernforordningen artikkel 4 nr. 2.

Her bør man merke seg at artikkel 4 nr. 2 definerer «behandling» som:

«enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke (…)» (vår understreking)

Operasjonene som er nevnt over, er alle knyttet til utførelsen av en enkelt verifiseringsforespørsel. Når man skal avgjøre om disse operasjonene kan regnes som én behandling etter personvernforordningen artikkel 4 nr.2, er det naturlig å ta i betraktning formålet med behandlingen. I dette tilfellet er hovedformålet å gjøre en digital verifisering av brukerens identitet.

Operasjonene som vi har kalt «forbehandling», er nødvendige for å sikre at ansiktsbildet – som skal sammenlignes med referansebildet – er ekte. Dette er ikke unikt for slik digital verifisering. Ved en fysisk verifisering av identitet, for eksempel i en bank, vil den bankansatte automatisk sjekke at personen som vedkommende har foran seg er ekte – det vil si at personen ikke har på seg en maske eller lignende.

Datatilsynet anser operasjonene som utgjør «forbehandlingen» for å være en naturlig del av verifiseringsprosessen og strengt nødvendig for å oppnå formålet med identitetsverifiseringen.

På bakgrunn av dette mener vi at det er naturlig å regne «forbehandlingen», malgenereringsfasen og sammenligningen mellom den beskyttede malen og referansemalen som «en rekke av operasjoner» som utføres med det hovedformål å gjennomføre en digital verifisering av identitet.

Mobai mener at selskapet kvalifiserer som databehandler når det gjennomfører en forespørsel om identitetsverifisering. Mobai vil imidlertid også behandle personopplysninger samlet inn under innrullerings- og verifiseringsprosessen for å trene og forbedre maskinlæringsmodellene

sine, i tillegg til å ivareta sikkerheten og gi generell forbedring av tjenesten. Mobai mener at selskapet kvalifiserer som behandlingsansvarlig når det gjennomfører disse prosessene.

I motsetning til operasjonene som utgjør «forbehandlingen», blir trening og forbedring av maskinlæringsmodellene og resten av systemet utført i etterkant av at identitetsverifiseringen er fullført. I dette steget i prosessen har systemet allerede bekreftet brukerens identitet eller forkastet forespørselen. Behandlingen som gjennomføres for trenings- og forbedringsformål har ikke den samme koblingen til utførelsen av en enkelt verifiseringsforespørsel som «forbehandlingen» har. Disse prosessene er imidlertid nært knyttet til tjenestens hovedfunksjon, siden trenings- og forbedringsprosessene er nødvendige for at KI-modellen skal fungere over tid. Behandlingen utføres imidlertid ikke for å fullføre en identitetsverifisering, men for å forbedre algoritmene og selve systemet. Vi anser derfor dette som behandling for sekundære formål.

Som allerede nevnt anser Mobai at selskapet kvalifiserer som behandlingsansvarlig for sekundære behandlingsformål knyttet til forbedring av algoritmene og selve systemet, men som databehandler for den primære behandlingen (innrullering og gjennomføring av verifiseringsforespørsler). Mobai kan ikke være både behandlingsansvarlig og databehandler for behandlingsaktiviteter som faller inn under samme formål. Dette argumentet støtter også konklusjonen om at behandling for å forbedre algoritmene og selve systemet ikke faller inn under det primære behandlingsformålet.

Behandling av biometriske opplysninger – når gjelder artikkel 9?

Behandling av biometriske opplysninger blir ikke alltid ansett som behandling av særlige kategorier av personopplysninger. Grunnen til dette er at behandling av biometriske opplysninger bare regnes som behandling av særlige kategorier av personopplysninger når opplysningene blir behandlet «med det formål å entydig identifisere en fysisk person», se personvernforordningen artikkel 9 nr. 1.

Den rettslige betydningen av formuleringen «å entydig identifisere en fysisk person» har vært gjenstand for omfattende debatt. Noen argumenterer for at formuleringen bare dekker biometrisk identifisering (1:n), mens andre mener at den også dekker biometrisk verifisering (1:1). Ettersom Mobai har tenkt å behandle biometriske opplysninger for verifiseringsformål, er tolkningen av dette vilkåret avgjørende for vurderingen av hvorvidt den planlagte behandlingen vil falle inn under personvernforordningen artikkel 9 eller ikke.

I denne rapporten skiller vi mellom:

«Biometrisk identifisering», som er en en-til-mange-sammenligning (1:n) der en biometrisk mal tilhørende en person med ukjent identitet blir sammenlignet mot en database med maler for å finne personens identitet, og

«Biometrisk verifisering», som er en en-til-en-sammenligning (1:1) mellom en persons biometriske mal og én enkelt referansemal for å verifisere en påstått identitet.

En tolkning av ordlyden i artikkel 9 nr. 1 gir ikke tilstrekkelig klarhet til å fastslå artikkelens virkeområde når det gjelder biometriske opplysninger. Noen vil påstå at formuleringen «å entydig identifisere» bare dekker biometrisk identifisering, mens andre påpeker at det også er nødvendig å entydig identifisere noen i den biometriske verifiseringsprosessen for å bekrefte en påstått identitet. Den siste tolkningen finner en viss støtte i definisjonen av biometriske opplysninger i personvernforordningen artikkel 4 nr. 14, som gjelder personopplysninger som stammer fra en særskilt teknisk behandling «som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person» (vår understreking).

I det første forslaget til personvernforordning som EU-kommisjonen la fram, inneholdt ikke artikkel 9 noen referanse til biometriske opplysninger. Denne referansen ble lagt til under trepartsforhandlingene på oppfordring fra EU-parlamentet. Det framgår av en skriftlig rapport fra trepartsforhandlingene datert 24. november 2015, at lovgivernes hensikt var å regulere behandlingen av biometriske opplysninger i tråd med Europarådets moderniserte konvensjon 108, som bare definerer biometriske opplysninger som sensitive opplysninger hvis de «entydig identifiserer en person». Imidlertid framgår det ikke helt klart i forarbeidene hverken til

personvernforordningen eller til den moderniserte konvensjon 108 om biometrisk verifisering skal regnes som behandling av sensitive opplysninger.

Bruken av systemer for en-til-mange biometrisk identifisering har generelt større påvirkning på grunnleggende rettigheter enn en-til-en biometrisk verifisering. Denne forskjellen mellom biometrisk identifisering og biometrisk verifisering ser vi tydelig i forslaget til KI-forordning (versjon av 13. juni 2024), som setter strenge krav for bruk av KI-baserte systemer for biometriske identifisering. Dette kan tas til inntekt for å tolke personvernforordningens artikkel 9 nr. 1 slik at bare biometrisk identifisering (1:n) vil være regnet som behandling av sensitive opplysninger.

Rettspraksis fra EU-domstolen støtter imidlertid en videre tolkning av artikkel 9, se sak C-184/20 (avsnitt 125).

Det europeiske personvernrådet kom nylig med en uttalelse der det ble antydet at artikkel 9 nr. 1 også gjelder for behandling av biometriske opplysninger for verifiseringsformål, se Uttalelse 11/2024: «on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR)». I dette dokumentet uttaler Personvernrådet:

"Facial recognition technology can fulfil two distinct functions – authentication and identification. While both functions are distinct, they both rely on the processing of biometric data related to an identified or identifiable natural person and, therefore, constitute processing of special categories of personal data under Article 9 GDPR." (se avsnitt 21)

Tidligere retningslinjer fra Personvernrådet tyder også på at artikkel 9 nr. 1 gjelder for behandling av biometriske opplysninger for verifiseringsformål, (se Guidelines 05/2022: «on the use of facial recognition technology in the area of law enforcement» | Det europeiske personvernrådet (europa.eu), avsnitt 12; Det europeiske personvernrådets Guidelines 3/2019 «on processing of personal data through video devices», avsnitt 78).

Som vist over råder det betydelig rettslig usikkerhet når det gjelder hvorvidt biometrisk verifisering faller inn under artikkel 9 nr. 1. Dette spørsmålet kan ikke avgjøres i dette sandkasseprosjektet. På bakgrunn av diskusjonene vi har hatt i dette sandkasseprosjektet, anser vi det imidlertid som sannsynlig at biometrisk verifikasjon vil falle inn under artikkel 9 nr. 1. Vi anbefaler derfor SALT-prosjektet å behandle biometriske opplysninger brukt til verifiseringsformål som en særlig kategori av personopplysninger.

Den mest åpenbare følgen av dette er at Mobai eller deres kunder, alt etter hvilken part som er behandlingsansvarlig, må kunne vise til et gyldig unntak etter artikkel 9 nr. 2 og et rettslig grunnlag etter artikkel 6 nr. 1 som tillater behandling av personopplysninger for dette formålet.

Om behandlingen av biometriske opplysninger faller inn under artikkel 9, vil ikke nødvendigvis ha noe å si for hvilket sikkerhetsnivå personvernforordningen krever for behandlingen. Selv om direktiv 95/46/EF, som personvernforordningen erstattet, ikke definerte biometriske data som en særlig kategori av personopplysninger, stilte direktivet likevel strenge krav til sikkerhet når det gjaldt behandling av biometriske opplysninger. Etter vårt syn er det ingenting som tyder på at

dette har endret seg med innføringen av personvernforordningen. Representantene for SALT-prosjektet deler denne oppfatningen.

Gjelder artikkel 9 også behandling for sekundære formål?

Som nevnt over er ikke biometriske opplysninger i seg selv ansett som en særlig kategori av personopplysninger. Det er formålet med behandlingen som avgjør om artikkel 9 gjelder.

Når det gjelder de ulike behandlingsoperasjonene i dette prosjektet, har vi anbefalt at Mobai anser operasjonene som involverer å forbedre nøyaktighet i innsamlingsmodulen, algoritmen for ansiktssammenligning og algoritmer for å avdekke svindel, i tillegg til etterforskning av svindel etter sanntidsøkter, som behandling for sekundære formål.

I dette tilfellet er de sekundære formålene knyttet til trening og forbedring av KI-modellene og selve systemet. Som vi har påpekt tidligere, er ikke formålet med denne behandlingen å verifisere en identitet. Vi anser derfor ikke dette for å være behandling «med det formål å entydig identifisere en fysisk person».

Vi mener derfor at artikkel 9 ikke gjelder for behandling av personopplysninger for disse sekundære formålene.

Som nevnt over vil dette ikke nødvendigvis ha noe å si for hvilket sikkerhetsnivå personvernforordningen krever for behandlingen. Den primære konsekvensen er derfor at Mobai kun trenger et rettslig grunnlag etter artikkel 6 nr. 1 for slik behandling, med mindre opplysningene de behandler faller inn under en eller flere av de andre særlige kategoriene opplysninger nevnt i artikkel 9 nr. 1. Vær oppmerksom på at sandkasseprosjektets drøftinger av artikkel 9 har begrenset seg til biometriske opplysninger som en særlig kategori av personopplysninger. Denne rapporten vil derfor ikke ta for seg andre særlige kategorier av personopplysninger. Mobai må likevel vurdere dette før firmaet behandler personopplysninger for sekundære formål.

Personvernforordningen artikkel 9 nr. 4 fastslår at «Medlemsstatene kan opprettholde eller innføre ytterligere vilkår, herunder begrensninger, med hensyn til behandling av (…) biometriske opplysninger (…).». Den norske personopplysningsloven setter i § 12 tilleggsvilkår for behandling av «entydige identifikasjonsmidler» som f.eks. biometriske data:

«Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.»

Konsekvensen av denne nasjonale reguleringen for behandling av biometriske data knyttet til trening og forbedring av KI-modeller og selve systemet, har ikke blitt drøftet i dette sandkasseprosjektet.

Sentral lagring av biometriske opplysninger

Behandling av digitale data som representerer trekk ved en fysisk person, i rå og ukryptert form (f.eks. ansiktsbilder, fingeravtrykk eller irisskanninger) utgjør en stor risiko for individet, siden dataene er statiske og ikke kan endres eller erstattes. Behandlingsansvarlige må derfor sette inn passende sikkerhetstiltak når de behandler ansiktsbilder og biometriske maler.

Personvernforordningen anser lagring av biometriske opplysninger som særlig sensitivt, og dette medfører utfordringer og forpliktelser for organisasjoner. På grunn av opplysningenes sensitive natur framhever både personvernforordningen og den norske personopplysningsloven (§ 12) hvor viktig det er å ha strenge sikkerhetstiltak på plass når biometriske opplysninger blir behandlet og lagret.

SALT-løsningen har to ulike implementeringskonsepter avhengig av hvorvidt sluttbrukernes enheter er tiltrodde eller ikke tiltrodde:

- «Tiltrodde enheter» vil gjøre det mulig å behandle og lagre biometriske opplysninger lokalt
- For «ikke tiltrodde enheter» vil behandlingen og lagringen av biometriske opplysninger måtte deles mellom lokale enheter og sentrale systemer.

Sentral lagring og behandling av biometriske data begrunnes først og fremst med at Mobai ikke anser brukernes personlige enheter som konsekvent «tiltrodde» for sitt bruksmønster. Denne rapporten har derfor et spesielt fokus på sentral lagring og behandling. Den vil imidlertid også drøfte den underliggende begrunnelsen for sentralisert behandling og risikoene slik behandling fører med seg.

Det er viktig å skille mellom to ulike typer lagring av biometriske opplysninger:

- sentral lagring, som betyr at en stor mengde biometriske opplysninger er samlet i en database, og
- desentralisert, eller lokal, lagring, vanligvis på brukernes personlige enheter, for eksempel mobiltelefoner, datamaskiner eller smartkort/sikkerhetsnøkler.

Lokal lagring gjelder bare brukerens egne biometriske opplysninger og er innhentet lokalt på brukerens egen enhet, slik at brukeren har fysisk kontroll over opplysningene med mindre plattformen/enheten/tjenesteyteren har rutiner for sikkerhetskopiering som medfører at dataene også lagres eksternt. Slike enheter lagrer vanligvis lokale data på spesielle beskyttede maskinvarekomponenter som moderne enheter er utstyrt med, for eksempel en TPM (Trusted Platform Module) eller TEE (Trusted Execution Environment). Slike løsninger er ofte allerede i bruk på mobiltelefoner som et alternativ til PIN-koder for skjermlås.

Det finnes mange bruksområder for lokal lagring. Mange bruker allerede ulike typer lokal autentisering eller verifisering der en bruker identifiserer seg ved hjelp av mobiltelefonens eget system for ansiktsverifisering.

Viktige hensyn å ta ved sentral lagring av biometriske opplysninger

Sentral lagring av biometriske opplysninger fører med seg ulike risiko:

- Sikkerhetsbrudd får større konsekvenser: Sentralisering av biometriske opplysninger innebærer å samle sensitive opplysninger på ett sentralt sted eller system. Dette skaper et større mål og større konsekvenser ved cyberangrep eller uautorisert tilgang. Et sikkerhetsbrudd kan gi tilgang til et stort antall personers biometriske opplysninger på en gang og føre til betydelige personvernkrenkelser.
- Lovstridig formålsendring: Sentral lagring kan gjøre det lettere å bruke biometriske opplysninger til annet enn det tiltenkte formålet. Sentral datalagring uten streng kontroll kan for eksempel føre til at data blir brukt til andre formål enn de registrerte personene opprinnelig ønsket eller samtykket til.
- Tap av kontroll for de registrerte: Sentral lagring kan gjøre det vanskelig for personer å kontrollere sine biometriske opplysninger. Hvis data blir samlet og lagret sentralt, kan det være utfordrende for enkeltpersoner å utøve rettighetene som personvernforordningen gir dem, f.eks. retten til tilgang til, retting eller sletting av opplysninger.

Det finnes ulike varianter av sentralisert lagring av biometriske opplysninger, for eksempel ved å fordele databasens innhold på flere databaser eller dele opp hver registrering i flere deler som kan lagres på ulike steder. Avbøtende tiltak kan settes inn ved sentral lagring for å redusere risiko og konsekvenser.

Lokalt lagrede biometriske data kan også være sårbare for ulike typer angrep. Samtidig er det en viktig fordel ved lokal lagring på brukerens personlige enheter at det gir en lavere risiko for omfattende brudd på konfidensialitet. Lokal lagring gjør det også vanskeligere å systematisk samle biometriske opplysninger og gjenbruke dem i et omfang som kan brukes til 1:n (en-til-mange-) identifisering.

Det stilles derfor omfattende sikkerhetskrav til sentral lagring. Nedenfor beskriver vi kravene som gjelder for de ulike tilnærmingene:

- Kryptering: Biometriske data som lagres sentralt, må være krypterte, både under lagring og under overføring og om mulig under bruk. Dette sikrer at opplysningene ikke vil være leselige eller brukbare i tilfelle uautorisert tilgang. Denne tilnærmingen krever god og effektiv håndtering av krypteringsnøkler. Den krever også effektive og sikre krypteringsalgoritmer og nøkkellengder.
- Tilgangskontroll: Streng tilgangskontroll kreves for å sikre at bare autoriserte personer har tilgang til sentralt lagrede biometriske opplysninger. Dette inkluderer flerfaktorautentisering, rollebasert tilgangskontroll og regelmessig gjennomgang av tilgangslogger.
- Pseudonymisering: Om mulig bør biometriske opplysninger pseudonymiseres før de blir lagret sentralt. Pseudonymisering innebærer å endre dataene slik at de ikke kan knyttes til en bestemt person uten mer informasjon.

- Dataminimering og sletting: Organisasjoner bør begrense mengden personopplysninger som hentes inn og behandles til det som er strengt nødvendig for å oppnå formålet. Dette prinsippet taler for at man aktivt skal avstå fra å samle inn og lagre mer data enn nødvendig. Dessuten skal alle data som ikke lenger er nødvendige for å oppnå det oppgitte formålet, inkludert sikkerhetskopier, slettes så snart som mulig i henhold til retningslinjer basert på prinsippene om forholdsmessighet og nødvendighet.
- Regelmessige sikkerhetsgjennomganger og samsvarskontroll: Organisasjoner må regelmessig gjennomgå sine sikkerhetsrutiner og tilhørende infrastruktur for å sikre at deres sentrale lagring av biometriske opplysninger fremdeles er sikker. Dette innebærer en gjennomgang av krypteringsmetoder, tilgangskontroll, prosedyrer for sletting og eventuelle endringer i trusselbildet.

Viktige motforestillinger mot sentral lagring av biometriske opplysninger

Spørsmålet om sentralisert lagring av biometriske opplysninger er gjenstand for omfattende debatt i EU. Hovedspørsmålet som diskuteres er hvorvidt slik lagring i det hele tatt bør være tillatt, og, hvis ja, hvilke spesifikke aktører som bør få lov til å lagre data på denne måten. Det finnes ingen formell konsensus om disse spørsmålene.

Det europeiske personvernrådet (EDPB) har utgitt retningslinjer som framhever hvor viktig det er å minimere risiko knyttet til behandling av biometriske opplysninger. Selv om personvernrådet ikke forbyr sentral lagring av biometriske opplysninger, så understreker rådet at det må settes strenge vilkår og foreslår lokal lagring som et tryggere alternativ i mange tilfeller. Personvernrådet går inn for at biometriske data bare skal behandles og lagres på de måter som er strengt nødvendige og forholdsmessige med tanke på formålet med behandlingen. Sentral lagring blir ofte sett på som en siste utvei som bare kan forsvares hvis det ikke finnes noe mindre risikabelt alternativ.

Det franske datatilsynet (CNIL – Commission Nationale de l'Informatique et des Libertés) har kommet med kraftige advarsler mot sentral lagring av biometriske opplysninger. Tilsynet anbefaler at slike data lagres desentralisert eller på enkeltenheter for å redusere risikoen for personvernbrudd. Flere regionale datatilsynsmyndigheter i Tyskland har tatt sterke standpunkt mot sentral lagring av biometriske data, særlig innenfor offentlig forvaltning og rettshåndhevelse. De argumenterer med at desentralisert lagring i kombinasjon med sterk kryptering og lokal behandling (på enheter) gir bedre beskyttelse mot uautorisert tilgang og misbruk.

Enkelte medlemmer av EU-parlamentet og komiteer, særlig de som fokuserer på borgerretter, har uttrykt bekymring over sentral lagring av biometriske opplysninger, særlig i forhold til statlig overvåkning og masseinnhenting av data. Noen har kommet med krav om strengere regulering eller til og med forbud mot sentral lagring, særlig statlige databaser. Borgerrettighetsgrupper, blant andre nettverket European Digital Rights (EDRi), argumenterer mot sentral lagring av biometriske opplysninger ved å vise til at det fører med seg iboende sårbarheter og risikoer som det er vanskelig å gjøre noe med. De arbeider for desentraliserte alternativer som tar vare på personvernet, med vekt på prinsippene om dataminimering og brukerkontroll.

Den europeiske menneskerettighetsdomstolen (EMD) påvirker EUs politikk. I noen saker har domstolens kjennelser gått mot sentralisert lagring av sensitive personopplysninger, inkludert biometriske opplysninger, særlig når slik lagring ikke er begrunnet med vektige allmenne interesser eller mangler tilstrekkelige sikkerhetstiltak.

EU har ikke noe absolutt forbud mot sentral lagring av biometriske opplysninger, men det råder en sterk preferanse for desentraliserte tilnærminger i store deler av rettsvesenet så vel som blant datatilsynsmyndigheter og personvernforkjempere. Disse organisasjonene argumenterer med at sentralisert lagring medfører betydelig risiko og at biometriske data så langt det lar seg gjøre bør lagres på en måte som redusere disse risikoene, for eksempel på personlige enheter eller i krypterte, desentraliserte systemer.

Mobais argumenter for sentral lagring av biometriske opplysninger

EUs tekniske spesifikasjoner for eID prioriterer flerfaktorautentisering og legger vekt på hvor viktig det er at biometriske opplysninger blir behandlet i sikre, kontrollerte miljøer. Dette beskrives i standarder, blant annet ETSI TS 119 461.

Mobai framholder at det følger sikkerhetsutfordringer med å skulle behandle biometriske opplysninger utelukkende på enkeltenheter (som personlige datamaskiner eller mobiltelefoner). Moderne enheter har riktignok avanserte sikkerhetsfunksjoner, men de er fremdeles sårbare for manipulering, noe som etter Mobais mening gjør det nødvendig med pålitelige sentrale miljøer for sikker lagring og behandling.

For å oppnå et høyt nivå av sikkerhet kreves det altså en kombinasjon av enhetsspesifikke sikkerhetstiltak og ekstern behandling som til sammen gir et ekstra lag med beskyttelse som gjør det vanskeligere for potensielle angripere å oppnå uautorisert tilgang. Sosial manipulering, der brukere blir lurt til å gi fra seg innloggingsinformasjon som er basert på noe brukeren vet eller har, blir stadig vanligere. Dette utgjør en stor risiko, særlig for bankkontoer, elektronisk identifisering og andre digitale tjenester. Effektiv biometrisk verifisering avhenger av sikker lagring og behandling av brukerspesifikke biometriske referanser.

Å sikre den biometriske referansens integritet gjennom sammenligningsprosessen er en sentral utfordring. Mange elektroniske enheter, inkludert bærbare datamaskiner og mobiltelefoner, kan være sårbare for manipulering og uautorisert tilgang. Smarttelefoner lagrer biometriske data med sikker lagring beskyttet av kryptering og isolerte miljøer, men tilgangen er også plattformstyrt (f.eks. av Google, Apple, Microsoft osv.).

Mobais løsning tar sikte på å styrke beskyttelsen av biometriske opplysninger både under lagring og behandling ved å legge til egne sikkerhetstiltak, blant annet homomorfisk kryptering. Den beskyttede biometriske malen (Protected Biometric Template, forkortet PBT) gir personvernfunksjoner som går ut over standardfunksjonene man finner i vanlig identifisering eller biometribruk i smarttelefoner. Ved hjelp av homomorfisk kryptering støtter Mobai egenskaper som annullerbarhet, irreversibilitet og ikke-koblbarhet i henhold til kravene i ISO/IEC

24745:2022. Gitt den beregningskapasiteten homomorfisk kryptering krever, anser Mobai sentral behandling for å være veien framover for å sikre pålitelige resultat fra ansiktssammenligning.

PBT-lagring kan være sentralisert eller desentralisert. Etter Mobais mening gir sentral lagring store sikkerhetsfordeler, blant annet raskere oppdatering og bedre trusseldeteksjon. Den sentraliserte tilnærmingen innebærer også kvanteresistent kryptering gjennom SALT, mens desentraliserte systemer vil være basert på konvensjonell kryptering (som betyr at data må dekrypteres for mønstersammenligning).

I korte trekk hevder Mobai at sentral lagring gir dem bedre kontroll over sikkerheten, inkludert nøkkelhåndtering, og over personvernet ved hjelp av nye krypteringsmetoder. En desentralisert tilnærming, derimot, ville gjøre tjenesteleverandører som BankID avhengige av plattformeiernes sikkerhetstiltak og gi mindre direkte kontroll over PBT-lagringens sikkerhet, integritet og personvern.

Datatilsynets vurdering av muligheten for sentral lagring

I denne rapporten har vi tatt opp viktige motforestillinger mot sentral lagring av biometriske opplysninger og lagt fram Mobai's argumenter for sentral lagring. Vi har pekt på at det ikke finnes noe absolutt forbud mot sentral lagring av biometriske opplysninger og at det finnes en vei framover for selskaper som ønsker å benytte slik lagring. Det Datatilsynet har pekt på i denne rapporten, er at selskap må vurdere om sentral lagring av biometriske opplysninger er nødvendig og forholdsmessig og grundig dokumentere begrunnelsen for dette med gode risikovurderinger for konkrete avbøtende beskyttelsestiltak.

Med tanke på Mobais løsning vurderer Datatilsynet at sentral lagring og behandling av biometriske opplysninger kan være mulig i tilfeller der det tidligere ikke var ansett som sikkert nok i lys av motforestillingene mot sentral lagring.

Trening og forbedring av KI-modeller og systemer

For å bruke data – som representerer en fysisk person – til å verifisere en persons identitet må man bruke metoder og algoritmer som faller inn under de generelle begrepene «KI» og «maskinlæring» (ML). Det ligger i ML-modellers natur at de krever trening, kvalitetskontroll og justering for å fungere godt over tid og for å forbedre kvaliteten og gjøre dem mer effektive. Disse kontinuerlige justeringene og forbedringene krever tilgang til treningsdata.

Mobai lagrer krypterte ansiktsbilder i en sentral database for en periode som begrenses av interne prosedyrer for å oppfylle sekundære formål. Mobai har gitt til kjenne at de bare trenger noen av bildene til treningen. Det har ikke blitt fastsatt noen prosedyre for å avgjøre hvilke bilder og hvilken andel av opplysningene som trengs, men ifølge Mobai kan det være snakk om så lite som en tidel av alle de potensielt tilgjengelige bildene. Imidlertid kan denne andelen forandre seg basert på behov, det vil si når det oppstår situasjoner eller hendelser som tilsier at det er behov for å justere eller trene modellene på et konkret grunnlag. Det er viktig å ha en aktiv og godt dokumentert praksis for dataminimeringsprinsipper for modelltreningen for at både innebygd personvern og personvern som standardinnstilling skal kunne anses som implementert i løsningen.

Fra et teknisk synspunkt er hovedforskjellen mellom primærformålet og sekundærformålene, at det primære formålet involverer flere aktører og bruk av de biometriske dataene på tvers av organisasjonsgrenser. Dette er også bakgrunnen for bruken av utvidede sikkerhetstiltak (blant annet homomorfisk kryptering) for primærformålet.

Datatilsynet forstår det slik at Mobai ikke vil lagre biometriske opplysninger for det sekundære formålet, siden ansiktsbilder som ikke er behandlet spesifikt for å bli maler, ikke regnes som biometriske opplysninger. De sentralt lagrede opplysningene (ansiktsbildene) utgjør imidlertid en risiko tilsvarende biometriske opplysninger, siden de utgjør en samling av data. Det stilles derfor betydelige krav til beskyttelse av disse opplysningene. Datatilsynet har ikke vurdert de konkrete sikkerhetstiltakene for lagring av opplysninger for sekundær bruk i denne rapporten.

Den behandlingsansvarlige må gjennomføre en tilstrekkelig risikovurdering og sette inn tilstrekkelige sikkerhetstiltak for lagring og behandling av ansiktsbilder for det sekundære formålet. Dette inkluderer en ordentlig vurdering av nødvendighet og forholdsmessighet.

Veien videre

Mobai og partnere viser med SALT et forsøk på å ta tak i den økende risikoen for misbruk i digitale løsninger for identitetsverifisering, inkludert veksten i sosial manipulering.

Framover vil geopolitisk usikkerhet, framveksten av KI-drevet svindel, og potensialet til kvanteberegninger (som potensielt kan svekke visse utbredte krypteringsalgoritmer) føre med seg nye risikoer. Dette vil gjøre det nødvendig å utvikle sikrere løsninger med bedre personvern for våre digitale identiteter.

En mer utstrakt bruk av biometriske data i slike løsninger vil imidlertid også medføre risiko for den enkelte. Spørsmålet om sentral lagring av biometriske opplysninger som vi har tatt for oss i denne rapporten, har skapt mye debatt. Dersom kriminelle aktører skulle lykkes i å bryte seg inn i en database som inneholder ubeskyttede biometriske opplysninger, vil resultatet være mer enn et tyveri – de kan potensielt tilegne seg hele den digitale identiteten til et stort antall personer.

Dette er grunnen til at de fleste myndigheter foretrekker desentraliserte tilnærminger og krever ekstraordinære beskyttelsestiltak dersom sentral lagring blir brukt, selv om det ikke eksisterer noe absolutt forbud mot sentral lagring av biometriske opplysninger.

Det finnes imidlertid en vei framover for selskaper som tar sikte på å benytte seg av sentral lagring av biometriske opplysninger. Det Datatilsynet har pekt på i denne rapporten, er at virksomheter må vurdere om sentral lagring av biometriske opplysninger er nødvendig og forholdsmessig, og deretter grundig dokumentere begrunnelsen for dette med gode risikovurderinger for konkrete avbøtende beskyttelsestiltak.

Et annet viktig drøftingspunkt i rapporten er bruken av nokså ny og nyskapende teknologi som homomorfisk kryptering. Dette er en nøkkelkomponent i SALT-løsningen og presenterer et innovativt bruksområde for denne type kryptering. Datatilsynet ser at den har potensial for å gi bedre sikkerhet for krypterte data og potensielt kan brukes på andre områder der det kan være nyttig å kunne analysere og behandle data mens konfidensialiteten opprettholdes.

Besøksadresse:
Trelastgata 3, Oslo

Postadresse:
Postboks 458 Sentrum,
0105 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no