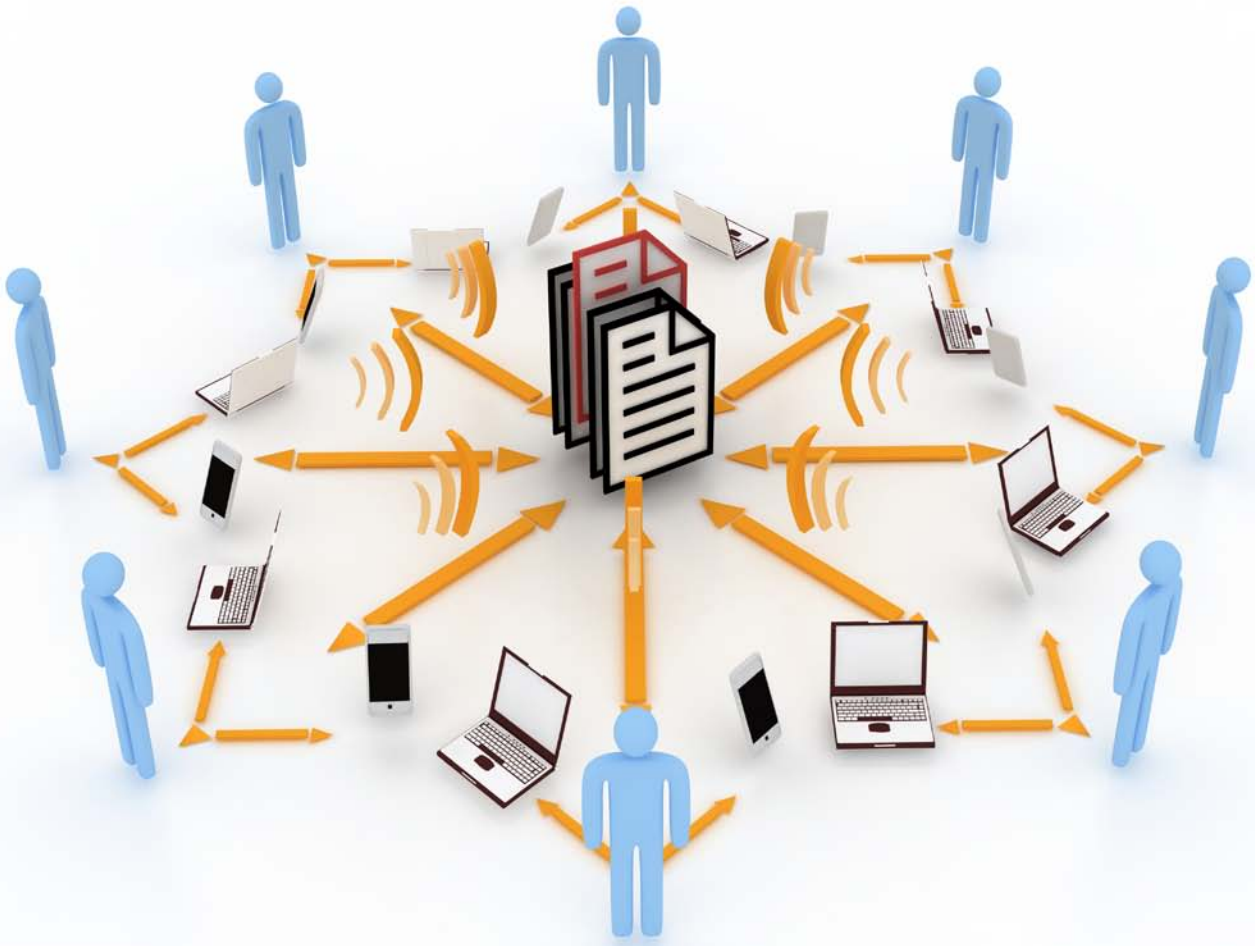
Datatilsynet

Strategi for godt personvern i digitaliseringen av offentlig sektor

Juni 2013



Innhold

Personvernprinsippene

Respekten for privatlivets fred og den enkeltes personlige integritet oppnås først og fremst ved å minimere registrering og bruk av personopplysninger til det strengt nødvendige. Utover dette bør man i størst mulig grad basere seg på samtykke fra den enkelte.

Samtykke eller annet rettslig grunnlag

Behandling av personopplysninger skal i størst mulig grad være basert på frivillig, uttrykkelig og informert samtykke. I mange tilfeller krever imidlertid fellesskapet at det behandles opplysninger om deg enten du vil eller ikke, for eksempel ved ileggelse av skatt og utbetaling av trygd. Dersom behandlingen av personopplysninger ikke baseres på samtykke må det foreligge et annet rettslig grunnlag.

Proporsjonalitet

All innsamling og videre behandling av personopplysninger må skje i overensstemmelse med lovverket, og på en måte som anses rimelig i forhold til den registrerte. Med dette menes at behandlingen ikke må medføre urimelig belastning for den enkeltes selvråderett eller integritet, at man må balansere hensynene til de ulike involverte partene, og at registreringen av opplysninger må være proporsjonal med formålet. I valget av to alternative løsninger ved behandling av personopplysninger skal man velge det alternativet som er minst personverninngripende.

Formålsbestemthet

Personopplysninger må samles inn kun for bestemte formål. Disse formålene må være legitime. Dessuten må formålene for den videre behandling av opplysningene ikke være uforenlige med de formål opplysningene opprinnelig ble samlet inn for. I tråd med dette prinsippet skal personopplysninger heller ikke utleveres til andre uten at det foreligger samtykke eller et annet rettslig grunnlag for utlevering.

Relevans og minimalisering

Personopplysninger skal bare innhentes, lagres og behandles i den grad det er nødvendig for å oppnå det legitime formålet med behandlingen av opplysningene. Har man ikke behov for å registrere personopplysninger skal man heller ikke gjøre det. Overskuddsinformasjon skal unngås. Innsamlede data som ikke lenger er nødvendige for det angitte formål må slettes eller anonymiseres. Under dette prinsippet ligger også det hensyn at enkeltindivider av og til må gis mulighet til å legge fortiden bak seg og begynne med blanke ark, for eksempel når det gjelder straffbare forhold eller betalingsanmerkninger.

Fullstendighet og kvalitet

Personopplysninger må være relevante, korrekte og fullstendige for det formål de skal benyttes til. Dette innebærer at opplysninger som ligger til grunn for behandling skal være oppdaterte og nøyaktige, og ikke inneholde irrelevant informasjon. Opplysninger som er lagret i et register skal ofte brukes som grunnlag til å fatte beslutninger om de registrerte. Dette prinsippet skal dermed sikre at beslutninger ikke blir fattet på et ufullstendig eller feilaktig grunnlag.

Informasjon og innsyn

Prinsippet springer ut av forståelsen om det opplyste individ. I dette ligger det en rett til å bli informert om innsamling og bruk av personopplysninger. Dernest ligger det en rett til kostnadsfritt å få innsyn i de opplysninger som er registrert om seg selv. Det skal også gis mulighet til å få slettet eller korrigert opplysninger som er feilaktige eller misvisende. Den registrerte har videre rett til å få en manuell vurdering av avgjørelser som fullt ut er basert på automatisert behandling av personopplysninger, dersom den avgjørelse som tas er av vesentlig betydning for vedkommende.

Informasjonssikkerhet

De som oppbevarer personopplysninger må treffe nødvendige tiltak for å sikre opplysningene mot uautorisert tilgang, endring, ødeleggelse og spredning. Opplysningene må også beskyttes mot ødeleggelse som følge av uhell.

Særlig strenge regler ved behandling av sensitive personopplysninger

Dette prinsippet sikrer at behandling av sensitive personopplysninger skal være underlagt særlig strenge regler. Personopplysningsloven nevner følgende kategorier av opplysninger som sensitive: rase eller etnisk opphav, politiske oppfatninger, religiøs eller filosofisk overbevisning, medlemskap i fagforeninger, helse og seksualliv.

Anonymitet og sporfri ferdsel

I utgangspunktet skal registreringer begrunnes. Hvis man ikke trenger å registrere identifiserende opplysninger har enkeltindividet rett til å være anonym. Dette følger også av prinsippet om rettslig grunnlag og proporsjonalitet. Individet har krav på at det minst personverninngripende tiltaket anvendes for å oppnå et bestemt formål. Hvis formålet kan oppnås uten bruk av personidentifiserbare opplysninger, er det dette alternativet som skal anvendes.

Personvernutfordringer i offentlig sektor

Personvern er et begrep med mange nyanser. Det finnes derfor ikke én presis og god definisjon på hva personvern er. Enkelt sagt handler det om retten til et privatliv, og retten til å bestemme over egne personopplysninger. Retten til privatliv følger blant annet av den europeiske menneskerettskonvensjon (EMK) artikkel 8, og ligger til grunn for EUs personverndirektiv (95/46 EF).

Retten til vern om egne personopplysninger finnes i blant annet personopplysningsloven, helseregisterloven og politiregisterloven. Personvernhensyn ligger også til grunn for bestemmelser om taushetsplikt, for eksempel i forvaltningsloven.

I forholdet mellom innbygger og det offentlige, er personvern også en rettsikkerhetsgaranti. En innbygger med kontroll over egne opplysninger kan motvirke myndighetsmisbruk, og på den måten skapes det grunnlag for et fritt og demokratisk samfunn. Offentlig sektor har derfor høy prioritet i Datatilsynets arbeid.

Offentlig sektor er storforbruker av alle typer personopplysninger. Opplysningene benyttes ofte i sammenhenger som er av stor betydning for den enkelte, for eksempel for å fastslå rettigheter og plikter. Det er derfor viktig at det offentlige har tilgang på personopplysninger av god kvalitet. Samtidig må det stilles strenge krav til behandlingen.

Den teknologiske utviklingen gir muligheter for å utvikle og effektivisere behandlingen av personopplysninger i offentlig sektor. Det er naturlig at det offentlige benytter seg av disse mulighetene.

Fra et personvernståsted er det viktig at lovbestemt taushetsplikt ikke settes til side eller begrenses på grunn av teknologiske muligheter. Teknologien bør i stedet benyttes til å støtte opp under taushetsplikten.

For å sikre personvernet ved *utveksling og deling av personopplysninger* mellom ulike offentlige instanser, og mellom offentlige og private aktører, må ansvarsforholdene være tydelige. Det må være helt klart hvilken instans som har ansvar for hva eller hvilke deler av behandlingen.

For at den registrerte skal kunne ivareta eget personvern, må vedkommende få informasjon om hvor opplysningene er, og hvilke formål de kan brukes til.

Den elektroniske utviklingen åpner også for *nye kommunikasjonsformer* mellom det offentlige og privatpersoner eller virksomheter. Når personopplysninger blir enklere tilgjengelig for den behandlingsansvarlige, er det viktig å sikre at det ikke hentes inn flere opplysninger enn nødvendig for det konkrete behandlingsformålet.

Retten til privat kommunikasjon er en grunnleggende personvernrettighet. Kommunikasjonsvernet skiller seg fra personopplysningsvernet, fordi det ikke gir rettigheter til de som er registrert i kommunikasjonen, men til de som kommuniserer. Hvilken type opplysninger som kommuniseres har ingen betydning for kommunikasjonsvernet.

Personvernprinsippene gjør seg allikevel gjeldende. Det er derfor nødvendig med klare ansvarsforhold mellom leverandører og eier av kommunikasjonsløsninger som samler inn eller utveksler personopplysninger. I de tilfeller kommunikasjonsformen ikke reguleres av ekomlovgivningen, bør det etableres et selvstendig lovbestemt ansvar for slike tjenesteleverandører. Dette gjelder, særlig for informasjonssikkerhet og internkontroll.

Digitalisering av offentlige tjenester
– *"På nett med innbyggerne"*

I regjeringens digitaliseringsprogram, *"På nett med innbyggerne"*, er ambisjonen at Norge skal ligge i front internasjonalt i utviklingen av en digital forvaltning.

Programmet har fire hovedmålsettinger:

1. Den statlige forvaltningen skal så langt det er mulig, være tilgjengelig på nett
2. Nettbaserte tjenester skal være hovedregelen for forvaltningens kommunikasjon med innbyggere og næringsliv
3. En digital forvaltning skal gi bedre tjenester
4. Digitalisering av forvaltningen skal bidra til å frigjøre ressurser til områder hvor behovet er stort

Hovedstrategien for å oppnå dette, er å etablere fremtidens digitale tjenester på en felles plattform. Det betyr en plattform med felles tekniske løsninger, felles styring, felles organisering og felles finansiering, og et regelverk tilpasset en digital forvaltning. I alle disse skal sikkerhet, robusthet og personvern sikres.

For å oppnå målsettingen forutsettes følgende:

- felles løsning for eID
- Altinn som felles teknisk plattform
- sikker digital postboks
- felles ordning for kontaktinformasjon, og reservasjon mot digital post
- felles offentlige registre skal understøtte den digitale forvaltningen
- felleskomponentene skal ivareta offentlig sektors samlede behov
- IKT-infrastruktur og systemer i staten skal være robuste og sikres godt
- regelverket skal legge til rette for digital post som hovedregel
- lover og forskrifter skal tilpasses digital forvaltning
- innsamlede opplysninger skal kunne gjenbrukes digitalt av andre offentlige myndigheter

I tillegg til disse målsetningene, peker regjeringen på utfordringer knyttet til dagens ansvarsorganisering og samordning av fellesløsninger. En vurdering av organiseringen, styringen og finansieringen av sentrale elementer i den felles IKT-infrastrukturen, er nødvendig for å sikre at den samlede digitaliseringen av offentlige tjenester blir best mulig.

Strategien understreker også at økt digitalisering i offentlig sektor betyr at informasjonssikkerhet blir viktigere. Dette gjelder både for felleskomponentene, og for andre viktige systemer i forvaltningen. Robust drift, og god håndtering av den økte bruk av løsningene må sikres. Samtidig er det viktig å beskytte opplysninger slik at de ikke kommer på avveier, og at det ikke er mulig å manipulere informasjon.

Når teknologien og organiseringen i forvaltningen åpner for nye og mer effektive måter å løse offentlige oppgaver på, bør også aktuelt regelverk vurderes på nytt. Der det er behov, må dette tilpasses til den digitale forvaltningen. Lov- og regelverk må både legge til rette for at det offentlige kan kommunisere digitalt med innbyggere og næringsliv, og gjøre det mulig å gjenbruke informasjon og legge til rette for automatisert saksbehandling der dette er relevant.

Datatilsynets posisjon i digitaliseringsprosessene

Datatilsynets mål er å sikre at det ikke er bare de teknologiske mulighetene som setter rammene for det offentliges behandling av personopplysninger og kommunikasjon med omverdenen. Nye løsninger må etableres i samsvar med personvernhensyn. De nye løsningene må på best mulig måte ivareta ansvar, informasjonssikkerhet, formålsbestemthet og informasjon til de registrerte.

Utviklingen av digitale offentlige løsninger stiller store krav til teknisk, juridisk og organisatorisk kompetanse i forvaltningen. For å sikre at løsningene tas i bruk, må de både fremstå som, og være, trygge og sikre. Hovedregelen for behandling av data i offentlig sektor er formålsprinsippet. Det betyr at det må være klare lovhjemler for – og foretas grundige vurderinger av mulige konsekvenser for personvernet ved – innsamling, videre behandling og eventuell utlevering av personopplysninger. Digitaliseringen åpner for bruk av teknologi som gjør det mulig å ivareta personvernet bedre enn tidligere. Blant annet blir både informasjonsformidling for å oppfylle informasjonsplikten, og å legge til rette for innsyn, lettere enn tidligere.

Strategien omhandler

Datatilsynets strategi tar utgangspunkt i de områdene der forvaltningen er i gang med arbeidet eller strukturene er på plass. Vi legger samtidig til grunn at dette er et dynamisk dokument. Det betyr at vi vil tilpasse dokumentet ettersom nye digitaliseringsinitiativ settes i gang. I denne versjonen har vi konsentrert oss om følgende områder:

- felles registre
- metadata
- offentlige publikumsportaler
- eID
- sikker digital postboks
- felles teknologiplattform (Altinn)

I tillegg til punktene over mener vi at innebygd personvern er nøkkelen til godt personvern og god informasjonssikkerhet. Dette gjelder også i fellesløsninger i offentlig sektor. I strategiens vedlegg II presenteres syv steg for å oppnå innbygd personvern.

Strategien omhandler ikke

Vi går i liten grad inn på organisering av digitaliseringsarbeidet eller de enkelte fellesløsningene, som organisatorisk tilknytning og fordeling av oppgaver. Vi tar heller ikke opp kostnadsspørsmål eller momenter knyttet til gevinstrealisering. Ei heller går vi i særlig grad inn på utfordringer som ligger i generell digital modning hos myndigheter eller hos brukere (innbyggere og næringsliv).

Vi vil likevel understreke at det er viktig med en tydelig og forankret avklaring av ansvarsforholdene, både for selve behandlingen av personopplysninger, og for bruken av kommunikasjonsløsninger.

Digital modning

Som nevnt er digital modning ikke behandlet i stor grad i dette dokumentet. Vi vil likevel understreke at dette bør vurderes konkret for hver enkelt løsning, og hvert enkelt område man ønsker å digitalisere. Det er svært viktig at digitaliseringen ikke blir, eller oppfattes som ekskluderende, men at brukerne oppfatter at det digitale valget best ivaretar hans eller hennes opplysninger, rettigheter og personvern. For Datatilsynet betyr dette at digitaliseringen skal gjøre brukere i stand til å ivareta sitt eget personvern på en best mulig måte. Vi anser dette som særlig viktig fordi det er offentlige myndigheter som står bak digitaliseringen.

Organisering av felleskomponenter og fellesløsninger

Datatilsynet er opptatt av at organiseringen av felleskomponenter og fellesløsninger muliggjør en effektiv og god forvaltning. Videre må organiseringen sikre god informasjonssikkerhet og brukernes personvern. Det krever tydelig fordeling av ansvar og klare ansvarslinjer. Tilsynet vil også foretrekke en organisering som fremmer god kompetanse. Utover dette har vi ingen sterke meninger om organiseringen av ansvaret for, og arbeidet med, de definerte felleskomponentene.

Ansvaret for behandlingen av personopplysninger ligger hos tjenesteeier, uavhengig av organisering. Det må inngås databehandleravtale mellom tjenesteeier og den offentlige forvalteren av felleskomponenten eller fellesløsningen.

Tilgang til andre offentlige etaters opplysninger

Som nevnt tidligere er formålsprinsippet et viktig personvernprinsipp ved digitalisering av offentlig sektor. Det innebærer at data samlet inn til et formål ikke kan brukes til et annet. Vi har gjennom kontroller, og annen kontakt med det offentlige, erfart at mange har en oppfatning om at data som er registrert i et offentlig organ er offentlig felleseie. Vi ser for eksempel at politiet ønsker tilgang til NAVs registre for å avklare bosted for utlendinger som skal transporteres ut av landet.

Når avgjørelser skal automatiseres, er det ofte en forutsetning at en etats system får tilgang til andre etaters data. Et eksempel er ved automatisk innvilgelse av frikort og statsborgerskap. Da vil det være behov for sammenstilling av data fra blant annet Helseøkonomiforvaltningen (HELFO), NAV og Skatt.

På bakgrunn av dette mener vi at det er viktig å holde fast ved formålsprinsippet ved behandling av offentlige data. Før et offentlig organ får tilgang til et annet organs data, må det foretas grundige personvernvurderinger, det må foreligge en klar lovhjemmel, og både tilgangsstyring og regler for hvordan informasjonen kan brukes må være på plass.

Felles offentlige registre

Staten har besluttet at følgende eksisterende registre skal være felles offentlige registre:

- *Det sentrale folkeregisteret* (grunndata og personer)
- *Enhetsregisteret* (grunndata om virksomheter)
- *Matrikkelen* (grunndata om eiendom)

Den viktigste årsaken til å samle grunndata i tre sentrale fellesregistre er å få en felles datakilde for opplysningene. Dette er for å få enhetlige data med bedre kvalitet.

Det sentrale folkeregisteret skal inneholde opplysninger om norske innbyggere og personer bosatt i Norge. De registrerte identifiseres med et unikt fødselsnummer eller et D-nummer. Dette nummeret er entydig knyttet til personen, og gir en entydig identifikator på vedkommende. Registeret inneholder også opplysninger om adresse, men kvaliteten på disse opplysningene er ikke nødvendigvis god nok til at opplysningene kan brukes i alle sammenhenger. Fødselsnummer eller D-nummer er ikke klassifisert som en sensitiv personopplysning, men er en opplysning etater og andre instanser bør begrense eksponeringen av.

Enhetsregisteret er oversikt over alle registreringspliktige enheter i Norge. Alle enheter er identifisert med et unikt organisasjonsnummer. Det finnes en rekke såkalte tilknyttede registre til Enhetsregisteret. Eksempler på tilknyttede registre er SSB sitt Virksomhets- og foretaksregister, og arbeidsgiverdelen av Arbeidsgiver-/Arbeidstakerregisteret hos NAV. Enhetsregisteret har ikke som formål å behandle personopplysninger, men på grunn av knytningen til styreverv og styresammensetninger, prokura, daglig leder og lignende, inneholder registeret likevel en rekke personopplysninger som også er knyttet til roller i næringsliv, frivillige organisasjoner og så videre.

Matrikkelen er en oversikt over fast eiendom i Norge. Den har kartinformasjon om eiendommene, og den inneholder oversikt over hvem som eier disse eiendommene. Matrikkelen har ikke som formål å behandle personopplysninger, men fordi knytningen mellom eiendom og person er en nødvendig del av registeret, inneholder det personopplysninger. Forvaltning av data fra og i registeret er i de fleste sammenhenger en aktivitet som skjer på kommunalt nivå, der hvor også interaksjonen mellom personer og myndigheter skjer.

Utfordringer

Det er spesielle utfordringer knyttet til at opplysninger fra de felles offentlige registrene kan sammenstilles på nye måter. Slike sammenstillinger kan bidra til å skape nye muligheter for bruk av data og nye typer behandlinger. Utfordringen sett fra et personvernperspektiv, er at nye sammenstillinger kan føre til nye behandlinger av personopplysninger. Det er derfor vanskelig å forutse hvilke nye utfordringer sammenstilling av data fra de felles offentlige registrene eventuelt vil skape.

Å samle disse opplysningene i fellesregistre som samtlige aktører i offentlig sektor skal benytte, reiser flere personvernspørsmål. Først og fremst må det avklares hvem som er behandlingsansvarlig for personopplysningene som behandles i fellesregisteret. Etter personopplysningsloven er

behandlingsansvarlig den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette forutsetter at behandlingsansvarlig har ansvar for, og kontroll over, opplysningene. Den behandlingsansvarlige er ansvarlig for beslutningene som fattes, og er den innbyggeren og øvrige aktører skal forholde seg til hvis det har skjedd feil. Den behandlingsansvarliges formål med, og behov for behandling av personopplysningene, avgjør hvilke opplysninger som kan registreres, og hvordan de kan håndteres videre, jf. personopplysningsloven § 11.

Det kan være vanskelig å peke på en enkelt behandlingsansvarlig for opplysninger i offentlige virksomheters fellesregistre. Et felleregister kan ha en behandlingsansvarlig for innsamlingen, en for selve registerføringen og forvaltningen, og en tredje for den videre behandlingen i virksomheten som benytter opplysningene.

I noen tilfeller vil det offentlige opprette nye registre for å tilrettelegge for det digitale førstevalg. Slike registre kan være en strukturering av opplysninger hentet fra ulike fellesregistre. I noen tilfeller kan det være samme behandlingsansvarlig for grunndataregisteret og det nye registeret, men dette avhenger av formålet. Før nye offentlige registre kan opprettes, må registerets formål avklares. Dette vil gjøre det lettere å avklare hvem som er behandlingsansvarlig for registeret.

Når formålet med det nye registeret er avklart, må dette vurderes opp mot formålsprinsippet. Det innebærer at opplysninger som er samlet inn til ett formål ikke kan brukes til senere, uforenelige formål, uten at den registrerte samtykker. Samtidig skal opplysningene være tilstrekkelige og relevante for formålet med behandlingen, korrekte og oppdaterte, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen.

Aktørene

- Registerførerne
    - Brønnøysundregistrene (Enhetsregisteret)
    - Skatteetaten (Det sentrale folkeregisteret)
    - Statens Kartverk (Matrikkelen)
- Andre offentlige virksomheter som benytter seg av opplysninger fra fellesregistre
- Overordnede departementer
    - Nærings- og handelsdepartementet (Enhetsregisteret)
    - Finansdepartementet (Det sentrale folkeregisteret)
    - Miljøverndepartementet (Matrikkelen)
    - Fornyings-, administrasjons og kirkedepartementet (IKT- departement)

Datatilsynets posisjon

Fellesregistrene vil ofte behandle personopplysninger, og må derfor forholde seg til personopplysningslovens krav til behandling av personopplysninger. Loven skiller også mellom behandling av personopplysninger hos den enkelte offentlige virksomhet, og behandling av personopplysninger i fellesregisteret.

For å sikre etterlevelse av personopplysningsloven må følgende sentrale personvernrettslige problemstillinger avklares ved digitalisering av offentlig sektor, og videre bruk av fellesregistre:

- Hvordan skal rollene og ansvaret for personopplysningene fordeles mellom aktørene?
- Hva er formålet eller formålene med behandlingen av personopplysningene?
- Hvilke personopplysninger skal behandles?
- Hva er det rettslige grunnlaget for behandlingen av personopplysninger?
- Hvilke kvalitets- og sikkerhetskrav stilles til behandlingen av personopplysninger?

Det er viktig at det kartlegges hvilken offentlig virksomhet som har behov for hvilke opplysninger, og i hvilken grad behovene er sammenfallende. En forutsetning for samling og bruk av opplysninger fra flere felles registre, må være at det er et faktisk behov for dette. Tilgangen til opplysninger må styres slik at den enkelte bruker ikke har tilgang til flere opplysninger enn nødvendig, og det må legges til rette for at innbyggeren har kontroll med opplysninger om seg selv.

Hver virksomhet som benytter felles registre for behandling av personopplysninger, må være behandlingsansvarlig for behandling av personopplysninger innenfor egen virksomhet.

For grunndataregistre er det naturlig at behandlingsansvaret ligger hos den som etter lov er registeransvarlig.

Datatilsynets strategi

Datatilsynet skal:

- innlede samarbeid med registerførere for grunndataregistre gjennom kontaktmøter på toppledernivå
- bidra til at registerførerne for grunndataregistre er mer bevisste på at registrene inneholder personopplysninger
- stille krav om at formål, behandlingsansvar og databehandlerrolle er avklart og dokumentert, før opplysninger fra registrene benyttes til nye felles formål
- delta aktivt i arbeidet med endringer i lover og forskrifter som regulerer innhold og bruk av data fra fellesregistrene
- fortsette engasjementet i prosjektet for ”nytt folkeregister”
- fortsette engasjementet i arbeidet med elektronisk tinglysning av eiendomsinformasjon
- delta i råd utvalg eller andre forum der innhold, bruk og forvaltning av fellesregistre er tema
- være proaktive med råd og veiledning til aktører knyttet til fellesregistrene

Korrekt og oppdatert informasjon, metadata og interoperabilitet

Ved deling av informasjon og gjenbruk av data fra felles grunndataregistre, er det tre hovedfaktorer som sikrer kvaliteten på data som deles og at dataene faktisk bidrar til raskere og bedre beslutninger:

- Oppdatering av opplysninger – ansvar, frekvens (hvor gamle er data) og validering.
- Metadata – beskrivelse av data (data om data).
- Interoperabilitet – den evne IT-systemer med tilhørende forretningsprosesser har til å utveksle data og dele informasjon og kunnskap.

Oppdatering av data er i dag et ansvar som i sin helhet ligger hos den myndigheten som er satt til å forvalte det aktuelle registeret. Dette gjelder også for fellesregistrene. Hvordan oppdatering foregår, og hvordan data eventuelt deles, er regulert av lov og forskrift. Ryddig og god regulering er avgjørende for tillit til offentlige etater som forvaltere av registre, kanskje særlig i et digitalt perspektiv.

Metadata, eller data om data, brukes for å sikre at to samhandlende aktører (menneske/maskin eller maskin/maskin) har lik forståelse av det de samhandler om.

Fornyings-, administrasjons og kirkedepartementet sier at felles *metadatadefinisjoner for grunndata,* er et tiltak for å etablere felles forståelse av *data*. Offentlig sektor har utviklet SERES (Semantikkregisteret for elektronisk samhandling). Registeret inneholder metadata som beskriver semantikk og informasjonsstrukturer for data som skal utveksles innenfor offentlig sektor. Målet med SERES er å etablere felles definisjoner for informasjon som skal gjenbrukes på tvers av fagområder og mellom aktører. Samtidig skal aktørene fortsette å eie egne data og egne datastrukturer.

Interoperabilitet handler om at data kan utveksles og gjenbrukes av andre parter. Dette forutsetter at forståelsen av data er den samme, og at data både teknisk og rettslig kan utveksles og forstås likt. Interoperabilitet deles gjerne opp i følgende:

- *Semantisk interoperabilitet* omfatter etablering av lik forståelse for prosesser, tjenester og presentasjon, i tillegg til lik forståelse av informasjon eller data, definering av begreper, samordning av betydningen av data og etablering av metadatamodeller.
- *Organisatorisk interoperabilitet* er samordning av arbeidsprosesser og endringer av organisatoriske forhold som er nødvendig for ønsket samhandling.
- *Teknisk interoperabilitet* er samspillet mellom tekniske løsninger.
- *Juridisk interoperabilitet* omtaler det rettslige grunnlaget for samhandling mellom parter. Det viktigste med juridisk interoperabilitet er ”harmoniserte lover og regler”, det vil si at de er enhetlige på tvers av sektorer. Bruk av fellesregistre som knytter sammen bruk og saksbehandling hos ulike myndigheter, er også avhengig av et felles sikkerhetsnivå. Juridisk interoperabilitet er nødvendig for implementering av felles prinsipper på sikkerhetsområdet.

Utfordringer

Det er mange utfordringer knyttet til deling og gjenbruk av data og personopplysninger. Hvis det er usikkerhet om hvorvidt innholdet i dataene er korrekt, oppfattes likt og/eller er oppdatert, vil situasjonen være utfordrende både for den som deler og den som gjenbruker dataene.

Deling og gjenbruk av personopplysninger utfordrer personvernet fordi den registrerte ikke har kontroll med hvilke opplysninger som behandles av hvem. Begrensinger i informasjonsplikten gjør det i mange tilfeller enda vanskeligere for den registrerte å ha kontroll på egne opplysninger.

Uten felles etablerte definisjoner og oppfatninger av hva informasjonen betyr, kan man ikke være sikker på hvordan den skal tolkes. Dermed reduseres informasjonskvaliteten, selv om informasjonen i seg selv er riktig. Dette kan føre til at det fattes feil beslutninger. For eksempel må man for en lønnsmottaker kunne skille mellom netto- og bruttolønn, for å sikre at riktig betalingssats settes.

I enkelte sammenhenger kan data representeres og presenteres forskjellig i ulike deler av løsningen, selv om dataene innholdsmessig betyr det samme. Andre ganger vil tilsynelatende lik informasjon brukes ulikt i forskjellige etater. I slike tilfeller må informasjonen tilpasses til oppgaven og til det enkelte fagsystem. Forskjell i bruk, representasjon og presentasjon av informasjonen, gjør det vanskelig å oppdage fellestrekk (overlapp) på tvers av ulike bruksområder og fagsystemer.

Aktørene

- Offentlige virksomheter som skal samhandle om data (eiere og brukere av metadata).
- Brønnøysundregistrene – som eier og forvalter av semantikkregisteret SERES.
- Nærings- og handelsdepartementet – som har ansvar for SERES.
- Difi – som IKT-direktorat og ansvarlig for felleskomponentprogrammet.
- Semicolon II – et samarbeidsprosjekt mellom offentlige aktører, Forskningsrådet, universiteter og konsulentmiljøer.
- Fornyings-, administrasjons og kirkedepartementet – som er IKT-departement.

Datatilsynets posisjon

Personopplysningsloven stiller krav til behandling av personopplysninger, det vil si opplysninger som *kan knyttes* til én fysisk person. Det er store muligheter for at dataene i fellesregistrene inneholder personopplysninger. Datatilsynet er derfor opptatt av "reglene" for hvordan man oppdaterer, oppbevarer og kvalitetssikrer dataene i fellesregistrene. Det vil si informasjonen som senere kan deles.

Sentrale personvernrettslige problemstillinger er:

- Hvilke opplysninger behandles, oppdateres og deles?
    - Ansvar, metadata og interoperabilitet?
- Hvordan skal rollene og ansvaret fordeles mellom aktørene?
    - SERES sin rolle?
- Hvem er behandlingsansvarlig og hvem er databehandler for hvilke behandlinger?
- Hva er det rettslige grunnlaget for behandlingen eller behandlingene?
- Hva er formålet med behandlingen eller behandlingene?
- Hvilke kvalitets- og sikkerhetskrav stilles til behandlingen?
- Hvordan sikre at den registrerte i størst mulig grad har kontroll over egne opplysninger?

Det er viktig å kartlegge hvilke offentlige virksomheter som har behov for hvilke opplysninger, og i hvilken grad behovene er sammenfallende. Herunder må det avklares hvem som oppdaterer opplysninger og hvordan det gjøres. Samme metadatakilde skal benyttes, og *interoperabilitet* – både teknisk, organisatorisk og juridisk – må avklares.

Datatilsynets strategi

Datatilsynet skal:

- innlede samarbeid med samtlige aktører på området gjennom kontaktmøter på toppledernivå
- bidra til avklaring av hvilke metadatakilder som benyttes, samt delta i arbeidet med endringer i lover og forskrifter som regulerer innhold og bruk av data, både for fellesregistrene og for metadata knyttet til disse
- være proaktive i råd og veiledning til aktører knyttet til fellesregistrene, metadata og interoperabilitet
- bidra til at de som har ansvar for å bygge felles metadatakilder og for utbredelse og bruk av disse, tenker informasjonssikkerhet og innebygd personvern (se vedlegg II)

Offentlig ID-forvaltning (eID)

Elektronisk ID (eID) er en generell betegnelse for noe som både kan identifisere en bestemt person, og som kan sendes elektronisk. eID har tilnærmet samme funksjon som et vanlig papirbasert identifikasjonskort, slik som for eksempel et pass, bankkort eller et sertifikat.

Elektroniske sertifikater er dokumenter som kan brukes som eID. Disse sertifikatene er knyttet til unike identiteter som entydig kan knytte personer til dette sertifikatet. Sertifikatene kan benyttes til autentisering (verifisere at du er du) ved for eksempel innlogging til offentlige tjenester. Sertifikatene kan også muliggjøre digitale signaturer, som gir en kobling mellom undertegners identitet og dokument.

På samme måte som eID kan brukes til å identifisere en bestemt person, kan det også benyttes til å identifisere en bestemt virksomhet. Da brukes såkalte virksomhetssertifikater. Disse virker på samme måte som elektroniske sertifikater knyttet til personer, men identiteten knyttes entydig til en virksomhet. Virksomheter kan utstede personlige virksomhetssertifikater til sine ansatte som knytter dem til virksomheten, og som gir den enkelte personen rettigheter på vegne av aktuell virksomhet.

Det har i mange år vært jobbet med planlegging og innføring av et "borgerkort" eller nasjonalt ID-kort, for alle innbyggere i Norge. Kortet skal kunne brukes som reisedokument i Schengenområdet, og skal inneholde en chip som kan gjøre det til en eID for både autentisering og signering.

Offentlig ID-forvaltning og eID reguleres av en rekke lover, forskrifter, kravspesifikasjoner og rammeverk:

- Lov om elektronisk signatur (*eSignaturloven*).
- Forskrift om krav til utsteder av kvalifiserte sertifikater.
- Forskrift om elektronisk kommunikasjon med og i forvaltningen *(eForvaltningsforskriften*).
- Kravspesifikasjon for PKI (Public Key Infrastructure) i offentlig sektor *(kravspesifikasjonen)*.
- Forskrift om frivillig selvdeklarasjonsordning for sertifikatutstedere.
- Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor *(rammeverket)*.

Løsningene offentlig sektor bruker i dag er i hovedsak basert på kravene fra *kravspesifikasjonen*. Inndelingen i løsningene benytter sikkerhetsnivåer fra *rammeverket*, og forutsetter at sertifikatutstederne er selvdeklarert etter *Forskrift om frivillig selvdeklarasjonsordning for sertifikatutstedere*. Dette betyr at det i dag ikke kreves at kommersielle tilbydere av elektroniske sertifikater oppfyller kravene til utstedere av kvalifiserte sertifikater i *Forskrift om krav til utsteder av kvalifiserte sertifikater*.

Dette kan bety at sertifikatene ikke oppfyller forskriftens krav til teknologi. Det betyr også at de ikke må oppfylle de kravene som er stilt til for eksempel erstatningsansvar og som forskriften hjemler. Dette kan føre til usikkerhet knyttet til ansvar ved for eksempel ID-tyverier for den offentlige aktøren.

ID-porten er den største og meste utbredte løsningen for pålogging til offentlige tjenester. Den er samtidig definert som en av felleskomponentene. Målsettingen for det offentlige er at dette skal

være innloggingsportalen til samtlige offentlige tjenester. Så langt har ID-porten kun tilbudt autentiseringstjenester, og ikke lagt til rette for signering eller kryptering. Dersom ID-porten skal bli en effektiv, god og sikker felles plattform, må den i fremtiden også tilby signering og mulighet for kryptert kommunikasjon. Så vidt Datatilsynet forstår, er dette opsjoner til fremtidige leveranser fra dagens tilbydere av ID-porten. For at personvernhensyn skal ivaretas best mulig ved implementering av signering i ID-porten, vil kravene som stilles i *Forskrift om krav til utsteder av kvalifiserte sertifikater* være viktige.

Det er også viktig at det legges til rette for løsninger der innbyggerne kan være anonyme eller under et pseudonym. De kan være anonyme når det ikke er behov for å vite hvem man kommuniserer med, og pseudonym kan brukes når man kun trenger å vite at det er samme person, men ikke hvem.

Utfordringer

Selv om vi har stor forståelse for at digitaliseringsprogrammet gjennomføres så raskt som mulig uten omfattende endringer i dagens løsninger, kan dette gå på bekostning av brukernes personvern.

ID-kriminalitet og ID-tyverier er et problem for dem som blir utsatt for dette. Offentlige data og løsninger vil bli mer og mer attraktive for ID-tyver etter hvert som dataene digitaliseres, fordi større mengder informasjon og flere tjenester blir lettere tilgjengelig. Informasjonen vil blant annet kunne brukes til å skaffe falske identiteter og gjennomføre svindel, samt føre til andre ulemper for dem som rammes.

Etablering av et borgerkort á la Schengen-kort, som også har elektronisk ID og nøkler for konfidensialitetsbeskyttelse, vil kunne bidra til å øke sikkerheten i felles offentlige løsninger. Da vil det offentlige være premissgiver, og derfor kunne forvalte både sikkerhet og personvern i løsningen. Offentlige etater, private organisasjoner og landets innbyggere kan bruke kortet med sterk autentisering og konfidensialitetsbeskyttelse for å sikre seg ved bruk av elektroniske tjenester på Internett.

Mangelen på utbredelse av virksomhetssertifikater er en utfordring for næringslivet og næringslivsaktører. Den største utfordringen for personvernet er at dette medfører at ansatte må bruke sin personlige eID for å kunne utføre nødvendige deler av sin jobb. Dette betyr at man ikke nødvendigvis kan skille mellom privat og jobb.

De offentlige fellesløsningene har også en utfordring med begrepsapparat og terminologi.

Rammeverket beskriver fire sikkerhetsnivå for eID som er tatt med i de offentlige fellesløsningene. Samtidig vises det i andre sammenhenger til *kravspesifikasjonen* og begrepene *Person Standard* og *Person Høy* for å beskrive sikkerhetsnivåer. Når signeringstjenester skal inn i fellsløsningene, blir det viktig at man kan tilby sertifikater i henhold til *Forskrift om krav til utsteder av kvalifiserte sertifikater*, særlig med tanke på behandling av sensitive personopplysninger.

Aktørene

- Nærings- og handelsdepartementet – som er ansvarlig for lov om digital signatur med forskrifter.
- Fornyings-, administrasjons og kirkedepartementet – som har ansvar for *Kravspesifikasjonen for PKI* og *Rammeverk for uavviselighet*.
- Difi – som har ansvar for ID-porten, og som står for det vesentlige av eID-forvaltning og bruk.
- Post- og teletilsynet – som forvalter tilsyn og kontroll med eID-ordninger.
- Brønnøysundregistrene, Skatteetaten og Lånekassen – som er store aktører på bruk i det offentlige.
- Leverandører av digitale sertifikater og tjenester, slik som Buypass, Comfides og BankID.

Datatilsynets posisjon

- Behandling av sensitiv informasjon skal skje ved kvalifiserte sertifikater.
- Individets behov må vektlegges på lik linje med virksomhetens behov ved valg av løsninger.
- Omfattende logging av innbyggernes handlinger skal begrenses.
- Forholdene skal legges til rette for at ansatte slipper å benytte privat eID i jobbsammenheng.
- Sikker autentisering skal kun gjøres når dette er nødvendig.
- Forholdene skal legges til rette for bruk av pseudonym der det kun er behov for å vite at man kommuniserer med den samme som tidligere.
- Vi skal bidra til at det skal lages løsninger som hindrer ID-kriminalitet i form av falske identiteter.

Datatilsynets strategi

Datatilsynet skal

- samarbeide tett med Difi (forvalter av ID-porten) både på toppledernivå og på operativt nivå.
- samarbeide med offentlige brukere av eID-tjenester
- bidra til at det offentlige leverer kvalifiserte sertifikater som kan brukes ved sensitive opplysninger
- samarbeide med Post- og teletilsynet for å gjøre flere aktører gode på personvern, samt forbedre sikkerheten i eID-løsninger
- jobbe aktivt for at det etableres et borgerkort á la Schengen-kort, og som samtidig er bærer for elektronisk ID og nøkler for konfidensialitetsbeskyttelse
- bidra til innføring av virksomhetssertifikater, slik at ansatte slipper å benytte privat eID i jobbsammenheng
- bidra til at det legges til rette for bruk av pseudonym der dette er godt nok
- bidra til at det utvikles og tas i bruk hensiktsmessige løsninger og nivåer, både for publikum og brukersteder

Sikker digital postboks

Det offentlige sin kommunikasjon med private og virksomheter er i dag i varierende grad elektronisk. Noe informasjon, som for eksempel ligningsinformasjon, formidles elektronisk til innbyggerne. Utover dette er det helst standarddokumenter med stor utbredelse som formidles elektronisk. Det er i dag mulig for det offentlige å sende informasjon på en sikker måte til både private og virksomheter. Det kan gjøres gjennom private leverandører av postbokløsninger slik som Digipost og eBoks. Per i dag er bruken av disse varierende.

I regjeringens digitaliseringsprogram *"På nett med innbyggerne",* legges det opp til at det offentlige skal etablere en sikker digital postboks. Denne skal opprettes for alle innbyggere som ikke har reservert seg, samt for alle virksomheter. Når det kommer post i den digitale postboksen, skal eieren motta beskjed om dette på e-post eller SMS. Postboksen skal brukes til å sende brev, meldinger og annen relevant informasjon fra det offentlige og i første omgang til innbyggerne.

Utfordringer

Den digitale postboksen skal opprettes automatisk uten den enkeltes samtykke. Denne praksisen kan føre til at det opprettes flere postbokser som aldri blir tatt i bruk. Fordi postboksene skal brukes til å sende ut offentlig informasjon, kan dette føre til en opphopning av elektroniske postbokser med sensitivt innhold som eieren ikke har lest eller kjenner til.

En løsning som dette samler informasjon fra flere behandlingsansvarlige som igjen videreformidles til én innbygger. Dette kan føre til utfordringer knyttet til behandlingsansvaret og databehandlerrollen. Roller og ansvar må være tydelig for alle involverte.

En samling av brev og skjema sendt fra det offentlige, vil totalt sett kunne inneholde en betydelig mengde personopplysninger. Fastsettelsen av sikkerhetsnivået i løsningen må ta høyde for dette, og man kan ikke kun se på beskyttelsesnivået til hver enkelt forsendelse. Flere opplysninger med moderat beskyttelsesnivå kan i sum kreve høy sikkerhet.

Sendte og mottatte dokumenter må håndteres på en forsvarlig måte. Det må avklares om dokumenter kan lagres på ubestemt tid, eller om de automatisk slettes etter en viss tid. Det må også fastsettes sletterutiner for feilsendt post.

Datatilsynet anbefaler at området særreguleres. Da kan ansvar, ansvarsoverganger, roller, funksjonalitet og sikkerhet reguleres på en langt bedre måte enn i dagens regulering. Andre områder som i dag har tilsvarende særregulering er telekomtjenester og posten.

Aktørene

- Fornyings-, administrasjons og kirkedepartementet – som er IKT-departement, styrer IKT-politikken og er oppdragsgiver for opprettelsen av sikker digital postboks
- Samferdselsdepartementet – som er eier og forvalter av forskrift, og eventuell særlov, og som forvalter IKT-politikken på departementsnivå
- Difi – som forvalter av IKT-politikken, og kan ha en styrende rolle eller eie en løsning
- Altinn – som mulig leverandør av digital postboks
- Digipost og eBoks – som er private leverandører av elektroniske postbokser i dag

Datatilsynets posisjon

- Tjenester av denne typen bør reguleres rettslig.
- Behandlingsansvaret skal være tydelig og avtalefestet.
- Det må avklares om det skal opprettes latente postbokser til dem som ikke aktivt skaffer seg en avtale med en leverandør. Dersom dette skal gjøres må innbyggerne informeres om at det gjøres og hvorfor.
- Post som er åpnet og lest av innbyggeren, eies av innbyggeren.
- Innbyggeren bestemmer selv hva som skal slettes eller lagres.
- Det må avklares hvordan det kan etableres sletterutiner for ulest informasjon.
- Videresending av post fra den digitale postboksen, kan ha negative konsekvenser og føre til at sensitive opplysninger sendes i usikre kanaler (e-post).
- Bruk av postboksen må være et forhold mellom innbyggeren og den aktuelle postboksleverandøren.
- Det må finnes et reservasjonsregister der innbyggere kan velge å reservere seg mot digital post.
- Et kontaktregister som skal brukes i sammenheng med en digital postboks, trenger kun å inneholde opplysninger om hvilken postboksleverandør en innbygger har.
- Ved fastsettelse av sikkerhetsnivå for bruk av løsningen, skal det legges vekt på at sammenstilling av flere ikke-sensitive opplysninger, kan føre til behov for sterkere autentisering.
- Meldinger med sensitivt innhold må kunne krypteres fra avsender til mottaker (meldingskrypteres), og autentiseringsnivået må følge kvalifiserte sertifikater.

Datatilsynets strategi

Datatilsynet skal

- Jobbe for at digitale postbokser blir underlagt særregulering
- Bidra til at det blir etablert klare ansvarslinjer mellom avsender, meldingsformidler, postboksleverandør og mottaker
- Bidra i arbeidet med spesifisering av løsningen. Dette gjelder spesielt innenfor følgende områder:
    - lov og forskriftsreguleringer
    - behandlingsansvar og roller
    - lagring og sletting av informasjon
    - fastsettelse av sikkerhetsnivå
    - autentisering
    - innebygd personvern

Felles offentlig teknologisk plattform (Altinn)

Altinn er en felles teknologisk plattform og samhandlingstjeneste for offentlig sektor. Den har egen felles portal for at innbyggerne skal nå ulike offentlige tjenester. En slik felles plattform reiser flere spørsmål knyttet til personvern. Det viktigste spørsmålet er hvem som er behandlingsansvarlig for det som skjer på plattformen eller i portalen.

Så langt har utfordringene rundt behandlingsansvar vært løst gjennom avtaler mellom Altinn som forvalter, og virksomhetene som har brukt løsningen til sine tjenester. Disse avtalene har til en viss grad også fungert som databehandleravtaler. Dette bygger på en forutsetning om at den behandlingsansvarlige har ansvar for, og kontroll over, opplysningene. Tydelig avklaring av hvem som er ansvarlig for beslutningene som fattes, og hvem innbyggeren eller påtalemyndigheten skal forholde seg til hvis det skjer en feil, er viktig. Kompleksiteten i dette ansvaret øker etter hvert som flere og flere tjenester samles på Altinn-plattformen.

Altinn er en komplisert løsning med mange samarbeidspartnere. Det kan derfor være vanskelig å beskrive behandlingsansvaret entydig. Brønnøysundregistrene har gjennomgått løsningen mange ganger for å kartlegge og tydeliggjøre dette. Det er utarbeidet databehandleravtaler med alle databehandere. Disse ligger som vedlegg i de enkelte samarbeidsavtalene.

Nærings- og handelsdepartementets ønske om at Altinn primært skal være en løsning for næringslivet, skaper utfordringer når løsningen i stadig større grad brukes i tjenester rettet mot innbyggere. Avviklingen av MinSide har ført til at flere innbyggertjenester flyttes til Altinn, noe som igjen har forsterket innbyggernes bruk av, og behov for, Altinn.

Siden dette er en plattform (og portal) som brukes til flere ulike formåk og av flere offentlige virksomheter, er det vanskelig å peke på en enkelt behandlingsansvarlig. I en løsning som kun brukes av én etat, er det normalt oversiktlig å fastsette både formål og behandlingsansvarlig. Når løsningens formål er å bidra til samordning og dialogtjenester som på ulike vis håndterer personopplysninger, blir bildet mer sammensatt. På samme måte som for fellesregistre, kan det være én behandlingsansvarlig for forvaltningen, og en annen for den videre behandlingen i virksomheten som benytter opplysningene.

Kort oppsummert har Altinn følgende hovedfunksjoner:

- databehandler
- skjemabehandler, både å bygge opp skjemaer og å formidle skjemaer
- leverandør av *"sikker postboks"* (meldingstjeneste fra etaten)
- innsynstjenester mot etatens system eller data i Altinn
- leverandør og bruker av eID og autorisasjonsløsninger
- portalløsning

- eDialog, som har hjelpesystem for å lede brukerne gjennom en prosess i flere trinn, også hos flere virksomheter

Utfordringer

Teknologiplattformen består av standardiserte komponenter som kan velges og settes sammen på ulike måter. Noen av disse ivaretar personvern og personvernsikkerhet på en god måte, mens andre ikke gjør det. Det er en utfordring at det ikke er tydelig for brukerne hvilke muligheter som gir godt og hvilke som gir mindre godt personvern.

Når det gjelder autentisering er det i dag seks ulike mekanismer for dette, fordelt på fire nivåer. Disse mekanismene bygger på standardprodukter. Etatene som eier tjenestene som tilgjengeliggjøres i Altinn, beslutter selv nivået på autentisering til sine tjenester. Altinn er, som alle andre offentlige portaler med påloggingsbehov, pålagt å benytte ID-porten og avvikle sine egne løsninger. Altinn har også en rollebasert autorisasjon, men denne har liten betydning for publikumstjenester. Den kan imidlertid ha betydning for virksomhetsbruk.

Fastlegging av behandlingsansvarlig i Altinn er ikke tydelig beskrevet, men dette antas å være mulig ved bruk av begrepet tjenesteeier. I de samarbeidsavtalene som finnes, er rollen som databehandler utydelig ivaretatt. Databehandleravtale med nødvendig innhold omtales ikke i samarbeidsavtalene.

Aktørene

- Nærings- og handelsdepartementet og departementenes kontaktforum (DKF) for Altinn
- Brønnøysundregistrene – som forvalter av både drift, applikasjonsforvaltning og utvikling av Altinn
- Altinn styringsråd – som består av blant annet Skatteetaten, NAV, SSB og Difi

Datatilsynets posisjon

- Autentisering
    - Altinn bør, som alle andre offentlige portaler med påloggingsbehov, benytte ID-porten
    - Altinn må tilby mulighet for bruk av kvalifisert sertifikat
    - Altinn må støtte bruk av virksomhetssertifikater
- Behandlingsansvaret ved bruk av portalen skal være klarlagt
- Hovedrollen som databehandler må bli tydelig ivaretatt, og gode databehandleravtaler må være på plass
- Innbyggerens rett til informasjon bør være ivaretatt, spesielt er dette være viktig der Altinn sørger for at informasjon deles mellom ulike etater
- Regler for sensitive opplysninger må innarbeides

Datatilsynets strategi

Datatilsynet skal:

- Innlede tett samarbeid med Altinns forvalter Brønnøysundregistrene gjennom kontaktmøter på toppledernivå
- Bidra til at den enkelte forvalteren blir mer bevisst på behandling av personopplysninger
- Stille krav om at formål, behandlingsansvar og databehandlerrolle er avklart og dokumentert, før opplysninger fra forskjellige virksomheter brukes til felles formål gjennom Altinn
- Følge opp at det etableres databehandleravtaler i alle ledd, både mellom etater (tjenesteeiere) og Altinn-forvalter (Brønnøysundregistrene), samt mellom Altinn-forvalter og de kommersielle leverandørene
- Bidra til at de som har ansvar for å bygge felles teknologisk plattform (Altinn) og for utbredelse og bruk av denne, tenker informasjonssikkerhet og innebygd personvern
- Være pådriver for at virksomhetssertifikater tas i bruk
- Sikre at innbyggerens rett til informasjon ivaretas

Vedlegg I: Begrepsavklaringer

"På nett med innbyggerne"

Regjerings plan for flere og mer bruk av elektroniske løsninger i kommunikasjonen mellom myndighetene og innbyggerne.

Digitaliseringsprogrammet

Et annet begrep for *"På nett med innbyggerne"*.

Digitalt førstevalg

Innbyggerne skal oppmuntres til å velge digitale tjenester der disse er tilgjengelige.

eID

Elektronisk identifikator, en metode for å identifisere innbygger i bruk av elektroniske tjenester. eID kan brukes til å autentisere (hvem er du), til elektronisk signering og til å kryptere.

Altinn

Det offentliges teknologiske plattform for samhandlingstjenester. Altinn er også en portal.

Sikker digital postboks

En løsning for å motta og sende sikker elektronisk post. Dette kan løses enten ved bruk av kommersielle aktører, eller ved hjelp av eksisterende offentlige løsninger.

Felleskomponenter

Regjeringen har definert felleskomponenter som digitaliseringen skal bygge på og bygges rundt. Disse er:

- Altinn
- eID
- Det sentrale folkeregisteret
- Enhetsregisteret
- Matrikkelen

eSignatur

Metode for å signere elektronisk (for eksempel offentlige dokumenter) med samme sikkerhet som ved en vanlig signatur på papir. Dette er regulert i eSignaturforskriften.

Fødselsnummer

En unik identifikator for personer født i Norge, eller som har fått permanent opphold i Norge.

D-nummer

Tilsvarende som fødselsnummer, men brukes som unik identifikator for utenlandske personer som oppholder seg i Norge der det er behov for at disse er oppført i Det sentrale folkeregisteret.

Organisasjonsnummer

En unik identifikator for alle enheter som er registrert i enhetsregisteret.

SERES

Semantikkregisteret for elektronisk samhandling (SERES) inneholder metadata som beskriver semantikk og informasjonsstrukturer for data som skal utveksles med og innenfor offentlig sektor. SERES forvaltes av Brønnøysundregistrene.

Semicolon

Prosjektets hovedmål er å utprøve og etablere metoder, verktøy og måleindikatorer som kan legges til grunn for forvaltningsanbefalinger og standarder. Dette er for at norsk offentlig sektor skal kunne samarbeide bedre på tvers av etater, og settes i stand til å tilby framtidsrettede og kosteffektive tjenester til innbyggere og næringsliv. Semicolon er et samarbeidsprosjekt mellom både private aktører, universitets- og forskningsmiljø og offentlige etater.

ID-porten

Felles påloggingsportal for å nå alle offentlige tjenester.

MinID

En påloggingsmetode for offentlige tjenester.

Sikkerhetsnivå for eID

Offentlig sektor har besluttet å dele inn sikkerhetsnivåene for innlogging i fire nivåer. Dette er nedfelt i *Rammeverk for uaviselighet*, som er et dokument utgitt av Fornyings-, administrasjons og kirkedepartementet. I noen sammenhenger snakkes det om *Person Standard* og *Person Høy*.

Kvalifisert sertifikat

Såkalte sertifikater for bruk av offentlige påloggingsmekanismer. Disse brukes etter forskriften for kvalifiserte sertifikater.

Selvdeklarasjon

En forskriftsordning der utstedere av sertifikater kan deklarere seg selv for leveranser av sertifikater som oppfyller kravene til det som er definert som person høy eller nivå fire. Det er viktig å være oppmerksom på at dette ikke er det samme som kvalifiserte sertifikater.

PKI

Public Key Infrastructure er et rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater over datanettverk.

PKI kravspesifikasjon

Er et dokument som regulerer kravene som stilles til bruk av PKI, og til kvalitet for leveranser av PKI for bruk i det offentlige.

Buypass

En kommersiell leverandør av sertifikater.

Comfides

En kommersiell leverandør av sertifikater.

BankID

En kommersiell leverandør av sertifikater.

Vedlegg II: Prinsipper for innebygd personvern (privacy by design)

Innebygd personvern, eller Privacy by Design, betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Det er både kostnadsbesparende og mer effektivt enn å endre et ferdig system.

Brukerne forventer personvern

I dagens teknologiske samfunn, utfordres grensene mellom personvern, brukervennlighet og tilgjengelighet. Datatilsynet ser at brukere av nettbaserte tjenester forventer at løsningene både er sikre, og ivaretar personopplysningene på en god måte. Personvern er ikke bare forventet, men også et mulig konkurransefortrinn for mange virksomheter. Dersom en virksomhet kan vise at de forvalter personopplysninger på en bedre måte enn en konkurrent som har tilsvarende løsning, vil brukerne foretrekke virksomheten med fokus på personvern.

Lekkasjer eller misbruk av personopplysninger kan bety svekket tillit, noe som ofte fører til tap av omdømme. Det er viktig å unngå slike hendelser, og det viser seg ofte kostbart å rette opp feilen og endre løsningen i etterkant.

Syv steg til innebygd personvern

De syv stegene er ment for deg som er bestiller, kravstiller, utvikler, er leverandør eller på annen måte er involvert i utvikling av IT-verktøy som behandler personopplysninger.

1. Vær i forkant, forebygg fremfor å reparere

For å lage en personvernvennlig løsning, er det viktig å vurdere risikoene for personvernet så tidlig som mulig i utviklingsprosessen. Kostnadene ved å rette feil og mangler ved et ferdig system kan være høye. Dersom du tar hensyn til personvernet tidlig i utviklingen kan du unngå unødvendige krenkelser av personvernet. Eksempler på krenkelse av personvernet er manglende tilgangsstyring, at det samles inn flere personopplysninger enn nødvendig, samt lekkasje av, og manglende sletting av, personopplysninger.

Eksempel:
En skoleeier skal utvikle et skoleadministrasjonssystem. Før selve utviklingen begynner, gjør man en vurdering av personvernkonsekvensene (Privacy Impact Assessment). Det vil si å gjøre en vurdering for å identifisere mulige risikoer for personvernet. I risikovurderingen forutser man problemer og foreslår løsninger. Skoleeieren vil med denne vurderingen kunne utvikle et system som i best mulig ivaretar elevenes, foreldrenes og de ansattes personvern.

2. Gjør personvern til standardinnstilling

Standardinnstillinger er førende for hvordan et system blir brukt, og for hvordan personopplysninger blir lagret. For at et system skal ha innebygd personvern, må standardinnstillingene settes opp slik at ikke flere personopplysninger enn nødvendig samles inn eller vises, at det finnes et lovlig formål med innsamlingen, at det er satt tekniske begrensninger for bruken av opplysningene, at opplysningene slettes når formålet er oppnådd og at man bare får tilgang til å se hvilke opplysninger som er registrert på seg selv. Et slikt system vil automatisk styre brukeren til en arbeidsmåte som gir bedre personvern.

Eksempel:
Noen nettlesere er utviklet med *"Do Not Track"* som standardinnstilling. Det betyr at nettleseren automatisk sier i fra til de ulike nettstedene at brukeren ikke ønsker å bli sporet. Dersom brukeren ønsker at nettaktiviteten skal spores må hun endre innstillingene.

3. Bygg personvern inn i designet
Personvern skal være innebygd i IT-systemets design og arkitektur, samt i forretningspraksisen. Det bør ikke være en funksjon lagt til i etterkant. Dermed blir personvernet en viktig del av kjernefunksjonaliteten. Det vil si at personvern er en integrert del av systemet uten at det går på bekostning av funksjonaliteten.

Eksempel:
Det er lett å gi fra seg for mye informasjon dersom en løsning legger til rette for det. For å unngå unødvendig innsamling av personopplysninger, kan nettbaserte skjema, for eksempel et skjema som skal sendes til et legekontor, lages med valg fra en nedtrekksliste i stedet for fritekstfelt.

4. Skap full funksjonalitet: både-og, ikke enten-eller
Gjennom innebygd personvern ivaretar virksomheten både brukerens personvern og sine egne behov. Det er viktig å ta hensyn til personvernet fra start for å unngå reparasjoner som går utover funksjonaliteten til løsningen. Noen ganger er det ikke mulig å gjøre endringer i etterkant uten at systemet blir dårligere. Målet er en både-og-tilnærming fremfor en enten-eller, for å ivareta virksomhetens behov og interesser og samtidig ta hensyn til de registrertes personvern.

Eksempel:
En kunde ringer teleleverandøren sin fra sitt registrerte telefonnummer. Systemet styrer kundebehandleren slik at han automatisk får tilgang til kundens registrerte opplysninger. Prosessflyten i systemet er tilgangsstyrt. Dette betyr at kundebehandleren har tilgang til den aktuelle kundens opplysninger uten å se resten av kunderegisteret.

5. Ivareta informasjonssikkerheten fra start til slutt
Informasjonssikkerhet må være del av løsningen fra vugge til grav. Det betyr at alt som skjer i systemet på forhånd er risikovurdert og hensiktsmessig sikret, helt fra før personopplysningene samles inn, mens de behandles og til de er slettet. Personopplysningene skal sikres mot uautorisert tilgang, endring, ødeleggelse og spredning.

Eksempel:
Et system er satt opp til å følge sikkerhetsstandardene for å sikre konfidensialitet, integritet og tilgjengelighet av personopplysninger gjennom hele livssyklusen. Dette inkluderer metoder for sikker sletting, hensiktsmessig kryptering, og sterk tilgangskontroll og logging. Systemet kan kun samle inn de mest nødvendige personopplysningene, og skrivetilgangen er kun tilgjengelig der det er nødvendig. Systemet inneholder dessuten rutiner for automatisk sletting av data når de ikke lenger trengs.

6. Vis åpenhet
Det skal være åpenhet om hvordan systemet fungerer, og hvordan personvernet blir ivaretatt. Virksomheten skal sørge for at brukerne får god informasjon og at det legges til rette for innsyn i egne opplysninger. Det skal være mulig å kontrollere at systemet ivaretar personvernet slik leverandøren oppgir.

Eksempel:
I en netthandelsløsning informeres kunden om hvordan opplysningene hans behandles i løsningen. Dette gjøres ved å lage en god og brukervennlig personvernerklæring som er lett tilgjengelig for kunden, både før han registrerer seg, men også etter at han er registrert. Kunden blir informert om hvilke opplysninger som samles inn, hvordan de brukes, hvem som har tilgang til dem, hvordan og hvor lenge de lagres, kundens muligheter for å endre og slette dem, og eventuelt hvilke andre instanser opplysningene kan bli utlevert til.

7. Respekter brukerens personvern
Fremfor alt krever innebygd personvern at utviklerne, bestillerne og administratorene gir brukerens personvern høy prioritet. Dette vil si å sørge for at personvernet ivaretas gjennom standardinnstillinger, tydelige brukervilkår og løsninger for at brukeren skal kunne kontrollere opplysningene sine selv.

De syv stegene til innebygd personvern er fritt oversatt og tilpasset fra *"7 foundational principles for privacy by design"* by Ph. D. Ann Cavoukian, Information & Privacy Commissioner in Ontario, Canada.

Les mer og se sjekkliste for innebygd personvern på:
www.datatilsynet.no/teknologi/innebygd-personvern

Gateadresse: Tollbugata 3, Oslo

Postadresse: Pb 8177 Dep, 0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50