Deres ref.	Vår ref.	Dato
200306508-23/ELO		29.09.2004

Persondatautveksling i Norge

Høringsuttalelse fra Norsk Regnesentral

Om avsender

Norsk Regnesentral (NR) ble etablert i 1952 og er et uavhengig institutt for anvendt forskning innen IKT og statistikk. NR driver med forskning og utvikling blant annet innen IKT-sikkerhet, herunder også personvern.

Generelle kommentarer

Vi har i denne høringsuttalelsen valgt å konsentrere oss om problemstillinger knyttet til sikkerhet og personvern, men vil understreke at vi generelt er enige i det målbildet som presenteres i rapporten ”Persondatautveksling i Norge,” såfremt personvern og sikkerhet ivaretas på en fornuftig måte. Når det gjelder personvern har det offentlige et helt spesielt ansvar, og samtidig en unik mulighet til å etablere gode løsninger. Løsninger for å ivareta personvernet er noe som må på plass når en slik stor omlegging skal gjøres. Å løse personvernproblemer etter at systemer er etablert vil være svært dyrt og sannsynligvis håpløst å få til.

Rapporten er et grundig stykke arbeid som gir et godt bilde av en del av de utfordringene man står overfor på persondataområdet i Norge. Vi er imidlertid av den oppfatning at det er vesentlige mangler i diskusjonen av personvernkonsekvensene av forslagene som fremmes, og er bekymret over enkelte nokså lettvinte konklusjoner om at fordelene vil overstige personvernulempene. Det er her viktig å understreke at vi ikke er motstandere av hovedmålet om økt grad av persondatautveksling; det vi savner er en helhetlig analyse av de virkninger forslagene vil ha på personvernet, både når det gjelder fordeler, ulemper og ikke minst hvilke *muligheter* som finnes for å ivareta, eller til og med styrke, personvernet.

Det er viktig å ta inn over seg at beskyttelse av personvern krever mer enn bare ”vanlig” informasjonssikkerhet. Et godt utgangspunkt for en analyse av personvernkonsekvenser vil være å ta tak i de personvernprinsippene som ligger til grunn for lovverket og vurdere forslagene i lys av disse. Viktige grunnleggende prinsipper er følgende (lovbestemte unntak finnes):

- Data skal ikke brukes til annet formål enn de er innsamlet for. Formålet med bruken av data skal spesifiseres ved innsamling, og kan kun endres hvis personen de omhandler samtykker til det.

- Mengden persondata som samles inn og lagres skal minimeres. Man skal ikke samle inn mer enn man trenger, og slette data når de ikke lenger er nødvendige for formålet.
- Individet skal selv kunne ha kontroll med sitt eget personvern. Det innebærer at det i mange tilfeller er krav om samtykke for å få lov til å bruke data, og at individet skal få innsyn i hvilke data som finnes, hva de brukes til, hvem de eventuelt utleveres til og hvordan de sikres. I tillegg skal individet kunne forlange retting eller sletting av data.
- Den som samler inn og bruker persondata har et selvstendig ansvar for datakvaliteten. Det vil si at data skal være riktige, oppdaterte, komplette og relevante for formålet.
- Det er generelt krav til god informasjonssikkerhet. Man må ha gode tekniske løsninger og operasjonelle rutiner for å ivareta sikkerheten, og man må ha dokumentert disse på en måte som gjør at sikkerhetsnivået kan kontrolleres. Man har også et ansvar for å verifisere at alle man utleverer data til kan garantere et tilfredsstillende sikkerhetsnivå.

Et viktig premiss i en personvernanalyse vil være hvem man ønsker å beskytte seg mot. Mot utenforstående, dvs. hackere og andre angripere, bruker man først og fremst tradisjonelle tiltak for informasjonssikkerhet. Imidlertid er insidere den største og alvorligste trusselen, dvs. ansatte og andre som har lovlig tilgang til systemene og som kan bruke sine tilgangsmuligheter til å misbruke persondata, enten med overlegg eller fordi de ikke vet bedre. Mot denne trusselen er det behov for løsninger som sikrer at man oppfyller personvernprinsippene beskrevet over.

Kommentarer til forslag

Å utarbeide en nasjonal metamodell for persondata

NR er enig i at det er helt nødvendig å utarbeide en nasjonal metamodell for persondata.

Gjennom en slik metamodell vil man få god oversikt over hvilke typer data som faktisk brukes, og har da et grunnlag for å vurdere hvilke data som faktisk er nødvendige for det enkelte formål. Videre vil kvaliteten på utvekslede data bli bedre fordi mottaker kan spesifisere nøyaktig hva han trenger og forvente at avgiver forstår hva han ber om.

Metadata som beskriver formål, kilde og eventuelt samtykke er helt nødvendige for å sikre at data kun brukes til det eller de formål de er samlet inn eller godkjent brukt for. Dessuten er gode metadatadefinisjoner nødvendig for å kunne skille policy[1] og systemer på en slik måte at en endring i policyregler ikke krever omprogrammering av systemet.

Det er etter vår mening svært viktig at metamodellen for persondata knyttes tett til metamodeller for andre områder. Da vil man kunne oppnå større fleksibilitet i systemer og arbeidsformer og det blir for eksempel enklere å opprette nye tjenester på

[1] Med policy mener vi i denne sammenheng et sett av regler som sier hvem som har tilgang til hva slags type data under hvilke omstendigheter. Som nevnt, er bl.a. *formålet* med bruk av persondata avgjørende for hvorvidt man får tilgang til data eller ikke.

tvers av gamle skillelinjer. Ved sammenkobling av tidligere atskilte registre vil man kunne koble flere opplysninger til enkeltpersoner, slik at disse opplysningene også faller inn under personopplysningsloven. Hva som regnes som persondata er et policyspørsmål som bør være definert på metadatanivå og ikke "hardkodet" i systemene.

Etablere en offentlig IT-arkitektur for utveksling av persondata

NR er enig i at det er nødvendig å etablere en offentlig IT-arkitektur som standardiserer grensesnittene for utveksling av persondata.

Standardiserte grensesnitt for utveksling vil gi økonomiske fordeler ved at man unngår dobbeltarbeid og kostnader til parvis integrasjon av alle instansene som skal utveksle data, samt at vedlikehold av integrasjonsløsningene vil bli atskillig enklere. En felles arkitektur vil også være viktig for å oppnå tilstrekkelig sikkerhet og å sikre personvernet. Med parvis integrasjon vil det lett oppstå uoversiktlige avhengighetsforhold som gjør at endringer ett sted gir uventede virkninger andre steder, noe som er svært uheldig ut fra sikkerhetshensyn.

Det er imidlertid svært viktig å samordne dette arbeidet med oppfølgingen av forprosjektrapporten "Arkitektur for elektronisk samhandling i offentlig sektor" som nylig har vært ute på høring. Våre argumenter for slik samordning er de samme som argumentene for at metamodellene må knyttes tett sammen, som beskrevet over.

Etablere en utvekslingsportal for persondata

NR er enig i at det kan være en god løsning å opprette en utvekslingsportal for persondata, men vil på det sterkeste understreke viktigheten av at dette gjøres på riktig måte. Dette er et spørsmål som bør utredes mye grundigere enn det er gjort i høringsrapporten.

De største motforestillingene vi har mot å etablere en slik portal er følgende:

- Portalen vil bli et "single point of failure" og et fristende angrepspunkt. Hvis noe går galt i denne portalen vil det kunne få svært alvorlige følger for mange mennesker. Det må derfor stilles svært store krav til sikkerhet.
- Spesielt på små steder kan det bli et problem at offentlige saksbehandlere får tilgang til mye informasjon om enkeltpersoner. Nå er informasjonen spredt på forskjellige etater og det er ikke så lett for enkeltpersoner å få et samlet bilde av andre individer. Det ligger mye god personvernbeskyttelse i måten ting fungerer på i dag med fysiske barrierer mellom ulike dataansamlinger. Mulighetene for misbruk er mye mindre fordi det er krevende å samle inn informasjon og man må gjerne via mennesker som kan stille spørsmålstegn ved hvorvidt informasjonen er nødvendig å gi ut. Dermed blir gode systemer og rutiner for tilgangskontroll og etterkontroll essensielt i en slik portal.
- En sentralisert portal fører til større maktkonsentrasjon. Det fra før skjeve maktforholdet mellom det offentlige og enkeltindivider vil bli enda skjevere. Riktignok vil en slik sentralisering ikke føre til at det offentlige samlet sett får mer informasjon om enkeltpersoner enn de allerede hadde, men det vil bli langt enklere å samle og sammenstille informasjonen.

Etableringen av en portal for uveksling av persondata gir også mange fordeler og muligheter. Det er summen av disse fordelene og mulighetene som gjør at vi

konkluderer med at det kan være en god ide å opprette en slik portal til tross for motforestillingene nevnt over, men da er det viktig at mulighetene utnyttes til fulle. De fordeler og muligheter vi ser er følgende:

- Portalen vil vedlikeholde en samlet oversikt over hvilke data som finnes og hvor de finnes. Det gir flere muligheter:
    - Med utgangspunkt i denne oversikten kan man gjøre grundige vurderinger av hvem som egentlig trenger hvilke data, med det formål å redusere den samlede mengden og bruken av persondata.
    - Individet får ett enkelt sted å henvende seg for å kreve innsyn i data.
- Datakvaliteten kan økes ved at registre kan oppdateres hendelsesstyrt. Dvs. hvis én av instansene (eller individet selv) sender melding om en endring i, eller sletting av, data, så kan endringen propagere raskt til de andre instansene som bruker samme data.
- Endringer hos én aktør kan innpasses ved å gjøre endringer kun i portalen. Hvis alle skal utveksle data parvis, vil endring hos én part kunne føre til uforutsette problemer for mange andre.
- Tilgangsstyring kan skje i portalen ved at man her etablerer systemer for å opprette og vedlikeholde policyregler (om hvem som kan få tilgang til hvilke data i hvilke sammenhenger), og systemer som håndhever disse reglene ved hver forespørsel om data.
- Portalen kan holde oversikt over hvem som faktisk utveksler data for hvilke formål. Dette gir økte kontrollmuligheter:
    - Individet selv kan få innsyn i oversikten over bruken av egne data og har dermed muligheter til å klage på det han/hun eventuelt mener er ulovlig databruk. Et forslag vi vil fremme for å øke bruken av innsynsretten, er at man innfører et system for å registrere hvor ofte data er brukt siden sist personen krevde innsyn, en form for ”prikkbelastning.” Da kan portalen tilby en tjeneste som sender melding til personen når tilgang til data har skjedd et visst antall ganger.
    - Det kan etableres mer eller mindre automatiske løsninger for overvåking av logger og deteksjon av brudd på sikkerhet og personvern.
    - Datatilsynet eller andre kontrollinstanser kan bruke slike logger i sin kontroll av virksomhetenes behandling av personopplysninger.

Andre kommentarer

Vi vil i det følgende knytte noen kommentarer til spesifikke punkter i rapporten.

Kap 1.6, side 10, om pseudonymiserte/anonymiserte data
“Utredningen har ikke behandlet utveksling av anonymiserte og pseudonymiserte data og heller ikke sammenstilt statistikk av persondata.”

Det er synd at man ikke har inkludert en diskusjon av mulighetene som ligger i pseudonymisering av data. I mange tilfeller er en persons identitet helt irrelevant for saksbehandlingen, så lenge alle andre relevante opplysninger er tilgjengelige. Utstrakt

bruk av pseudonymer i stedet for navn eller fødselsnummer kan være en meget god måte å redusere personvernulempene på. Mekanismer for slik pseudonymisering kan legges inn i en personopplysningsportal.

Kap 2.2.4, side 15, om andre grunnregistre
"Andre grunnregistre er Motorvognregisteret, skipsregisteret (NIS, NOR), luftfartøyregisteret og flere. Disse kan inneholde persondata i eierrelasjonen, men disse registrene berøres ikke videre i utredningen."

Dette er et argument for at arbeidet med oppfølgingen av denne høringsrapporten samordnes med arbeidet med oppfølging av forprosjektrapporten "Arkitektur for elektronisk samhandling i offentlig sektor." Personopplysninger er definert som "opplysninger og vurderinger som kan knyttes til en enkeltperson"; hvilket register disse opplysningene finnes i er likegyldig. Derfor er det viktig at løsninger som etableres på andre områder også er i stand til å håndtere personopplysninger på tilfredsstillende måte.

Kap 2.2.4, side 15-16, om etatsregistre
"I tillegg må en ta hensyn til at visse data kun skal brukes til nøyaktig det formålet de er samlet inn for."

Det gjelder ikke bare "visse data;" det gjelder alle personopplysninger. For offentlige etater finnes det svært mange unntak fra denne regelen, slik at det i praksis kanskje har blitt slik at denne formålsbindingen oppfattes som et unntak, men det er i så fall en uheldig misoppfatning som bør korrigeres.

Kap 2.2.6, side 17, om metamodeller og personvern
"[...] det er i hvert fall en personvernulempe at det er vanskelig å se den samlede informasjon som forvaltningen har om en person."

Dette er vi helt enig i. Innsynsretten er meget sentral i personopplysningsloven og er et viktig verktøy for enkeltindividets kontroll med eget personvern. Manglende samlet oversikt over hva det offentlige har av opplysninger er et alvorlig hinder for bruken av innsynsretten. I tillegg gjør den manglende oversikten at det er vanskelig å analysere om forvaltningen som helhet har et tilfredsstillende nivå på beskyttelsen av personvernet.

Kap 2.6.1, side 32, om sikkerhet
"Utviklingen av en sikker infrastruktur, som muliggjør utveksling av sensitive data uten fare for tap eller misbruk, har kommet langt."

Dette stemmer for sikkerhet generelt, men ikke for personvernteknologi. Som vi innledningsvis argumenterer for, så er personvern langt mer enn sikkerhet, og det å tro at man kan løse personvernproblemer med bruk av standard sikkerhetsteknologi er en utopi. Det finnes ulike former for personvernteknologi, men det meste er fremdeles umodent og langt fra hyllevare. Dermed er det nødvendig med grundig analyse for å sikre at man velger de riktige løsningene.

Kap 3.3.2, side 45-46, om standardmeldinger.
"Det bør etableres standardmeldinger for ofte etterspurte persondata."

Vi mener at etablering og utstrakt bruk av standardmeldinger vil være en god ide, også ut fra personvernhensyn. Det vil være mye enklere å definere personvernpolicy for slike standardmeldinger enn for generelle forespørsler. Se dog neste punkt.

Kap 3.3.2, side 47, om standardmeldinger og personvern
"En standardmelding vil i noen tilfeller kunne medføre utlevering av overskuddsinformasjon, eller underskudd på informasjon, i forhold til en individuell vurdering knyttet til en enkelt utlevering/sak etter minste privilegiums prinsipp. [...]Men det vurderes at likebehandlingen og sporbarheten som oppnåes ved å bruke standardiserte meldinger er en bedring av personvernet og vil oppveie personvernulempen."

Dette er ikke bare en "personvernulempe," det er et lovbrudd, og må derfor tas meget alvorlig. (Dette er for øvrig et eksempel på rapportens lite gjennomtenkte personvernvurderinger.)

En løsning på problemet med overskuddsinformasjon vil være å definere standardmeldinger med høy granularitet, dvs. at det defineres mange standardmeldinger som er godt tilpasset til det enkelte formål. Det er da viktig å sikre at systemet er så fleksibelt at disse definisjonene kan justeres så ofte som nødvendig.

Kap 3.3.3, side 47, om metadata for formål og kildesporing
"Metadata bør derfor også ha med seg informasjon om kilde-, formål- og kvalitet, som følger meldingsutvekslingen. Dette vil gjøre det mulig for mottaker å vurdere de mottatte datas juridiske holdbarhet, også etter at de har vært lagret hos mottaker en tid."

Muligheten for å legge slike metadata på informasjonen er en av de største fordelene ved forslagene i rapporten. Metadata som angir godkjente formål og kildeopplysninger er helt nødvendig for å kunne styre tilgang etter personvernlovgivningen. Generelt bør det defineres metadata som gjør det mulig å utlede og evaluere policyregler for tilgangskontroll (f.eks. samtykke fra individet, brukshistorikk for opplysningene, etc.).

Kap 3.3.4, side 48, om nasjonal portal for utveksling av persondata
" Portalen skal gi tilgang til:
[...]
- *Returkanal for korreksjoner*
  (det betyr ikke at alle skal ha rett til å korrigere data direkte)
- *Mekanismer for å styre tilgang og sikre sporing"*

Vi vil understreke viktigheten av at slike mekanismer legges inn i en slik portal hvis den skal realiseres, og av at dette gjøres riktig. Dette vil kreve en god del mer enn hva vanlige sikkerhetsprodukter kan tilby, se neste punkt.

Kap 3.3.5, side 48-49, om tilgangskontroll
"Det er etablert velutviklede mekanismer for å styre tilgangskontroll til persondata. En av distributørene oppgir å ha mer en 100 forskjellige tilgangsnivåer som en bruker kan tildeles."

Det er riktig at det er etablert velutviklede mekanismer for tilgangskontroll, men det gjelder *ikke* for persondata. Kommentaren om 100 tilgangsnivåer høres jo flott ut, men har overhodet ingen relevans i denne sammenhengen. Det som virkelig teller, er om man kan styre tilgang på bakgrunn av *formålet* data er godkjent brukt for, samt annen relevant kontekstinformasjon, og at man har mulighet for å definere regler ut fra ulike adgangskontrollmodeller (som f.eks. "Chinese-wall"-type modeller hvor et viktig poeng er å begrense enkeltpersoners tilgang basert på hva de allerede har gjort).

Man skriver også i rapporten at det er *"vanskelig å utvikle tilgangskontrollsystemer som bare gir tilgang til informasjon som brukeren har rett til under alle forhold,"* og det er helt riktig. Dette er for øvrig et område som NR jobber med, blant annet basert på den foreslåtte standarden EPAL, som nevnes i rapporten på side 49.

Kap 3.3.5, side 49, om sporing av tilgang
"Det bør legges opp til økt etterkontroll eller sporing av tilgang til persondata. [...]Slike sporingsmekanismer vil også bedre personvernet ved at det gir en som er registrert mulighet til innsyn, ikke bare i hvilke data som er registrert, men også hvem som har hatt tilgang til dataene."

Vi er enige i at det er svært viktig at man legger opp til gode løsninger for sporing og etterkontroll. Tilgangskontroll er "førstelinjen" i sikkerhetssystemet, men denne vil erfaringsmessig ikke fange opp alle tilfeller av urettmessig tilgang, enten på grunn av feil eller fordi noen har funnet måter å komme rundt kontrollen på som ingen har tenkt på. Etterkontroll er sikkerhetsnettet som skal fange opp de tilfellene som slipper igjennom.

I denne sammenheng er det viktig å legge til rette for individuelt innsyn i bruken av egne data, men også for annen manuell kontroll, som intern kontroll eller audit fra eksterne (f.eks. Datatilsynet). Videre vil det være mulig å etablere automatiske deteksjonsmekanismer a-la de som brukes til inntrengningsdeteksjon i datasystemer, og til avdekking av svindel og hvitvasking i finanssektoren.

Kap 3.3.6, side 49-50, om personidentifikator
"Fødselsnummeret er i seg selv ikke sensitivt i følge personopplysningsloven, men tradisjonelt har dette nummerert vært ansett som sensitivt da det sees på som "nøkkelen" til annen informasjon."

Det er flere problemer med fødselsnummeret. For det første er det et problem at det ligger meningsbærende informasjon i det. Spesielt fødselsdatoen er for mange en følsom opplysning som man ikke uten videre gir til hvem som helst ("man spør ikke en dame om hennes alder!").

Det alvorligste problemet er imidlertid at fødselsnummeret har vært misbrukt av mange instanser for autentisering og ikke bare for identifisering. Det gjelder f.eks. mange banker som tidligere ga ut kontoopplysninger på telefon hvis man kunne oppgi riktig fødselsnummer. Dermed har folk (med rette) fått en oppfatning av at bruken av fødselsnummeret bør begrenses.

Kap 3.3.7, side 50, om PKI
"Sertifikatets serienummer vil da kunne fungere som en personidentifikator ..."

Dette er etter vår mening ingen god ide på grunn av problemene som vil oppstå hvis et sertifikat blir tilbakekalt. Personidentifikatoren bør være et nummer som ikke endres i personens levetid.

For øvrig ser det ikke ut til at det vil bli utstedt ett sertifikat til hver innbygger slik man ser ut til å anta i rapporten. Tvert i mot går utviklingen i retning av at hver av oss kan ende opp med opptil flere sertifikater, utstedt av ulike kommersielle leverandører.

Kap 4.1, side 53-56, om forslag til tiltak

Her savner vi en grundig gjennomgang av personvernkonsekvensene som en essensiell del av de tiltakene som foreslås, både for å få avdekket trusler og ulemper, men også fordeler og ikke minst muligheter for å styrke personvernet. I avsnitt 4.1.6 nevnes riktignok sikkerhetsmekanismer og mekanismer for sporing, og i avsnitt 4.1.9

nevnes personvern som en av de tingene man må utrede i forbindelse med ny personidentifikator, men disse punktene er ikke i nærheten av å dekke behovet for personvernanalyse.

Kap 4.1.9, side 56 om personidentifikator
"Utredningen bør vurdere:
[...]
- *Nødvendige mekanismer for midlertidige nummer og referanse mellom midlertidige og fast identifikator for et individ."*

Dette er etter vår mening meget viktig å utrede, se vår kommentar til kap 1.6 om bruk av pseudonymer.

Kap 5.4, side 61, om kostnadsfaktorer

Vi vil bemerke at vi her savner en vurdering også av *kvalitative* kostnadsfaktorer, siden man har dekket kvalitative faktorer på nyttesiden.

Oppsummering

NR er positive til endringene som foreslås i rapporten under den forutsetning at man bruker de mulighetene som finnes til å bevare og styrke personvernet.

Hovedpunktene vi har ønsket å få fram i denne høringsuttalelsen er følgende:

- Omlegging av systemene av et slikt omfang som foreslås er en gylden mulighet til å innføre gode løsninger for personvern. Denne muligheten må vi ikke la gå fra oss, for den kommer neppe igjen. Det er behov for en grundig analyse av konsekvenser og muligheter på personvernområdet.
- Det er viktig å benytte muligheten man får ved arbeidet med metamodell for persondata til å gjøre en grundig kartlegging i den enkelte virksomhet av hvilke personopplysninger man faktisk trenger i sin saksbehandling. Kartleggingen må ha som mål å redusere mengden persondata som lagres og brukes til et minimum.
- Bruk av pseudonymer og pseudodomener[2] er et meget lovende og kraftfullt verktøy for reduksjon av personverntruslene, særlig i forhold til truslene fra insidere. Det er imidlertid svært viktig at støtte for dette bygges inn i systemene fra begynnelsen; det vil være vanskelig å innføre slike løsninger etter at systemene er ferdige.
- Sentraliseringen og maktkonsentrasjonen som en portal for persondatautveksling vil føre til kan og bør balanseres med økte muligheter for ekstern kontroll og innsyn fra enkeltindividet. Innsynsretten og klageadgangen er i dag svært lite brukt, noen som antakelig skyldes at rettigheten er for lite kjent og at det er for vanskelig å kreve innsyn. Økt bruk av innsynsretten vil selvfølgelig føre til merarbeid for virksomhetene, men det er etter vår mening helt nødvendig å sørge for at denne retten brukes hvis man vil bevare publikums tillit til systemene.

[2] Oppdeling i domener slik at en person er kjent under ulike pseudonymer i hvert domene. Den enkelte ansatte har ofte ikke behov for å vite identiteten til personen saken omhandler, så lenge man kan innhente nødvendige opplysninger ved bruk av personens pseudonym. Ulike virksomheter, og ulike avdelinger innen en virksomhet kan kjenne personen under ulike pseudonymer.

Med vennlig hilsen

Norsk Regnesentral

Lars Holden
Administrerende direktør

Ragni Ryvold Arnesen
Seniorforsker