Personvern: En forutsetning for samhandling og nye tjenester

Ragni Ryvold Arnesen
Seniorforsker
Norsk Regnesentral

Jerker Danielsson
Forsker
Norsk Regnesentral

Introduksjon

Ny teknologi gir uante muligheter når det gjelder innsamling og utnyttelse av store mengder informasjon. Utviklingen går i retning av individuell tilpasning, selvbetjening og mange tjenester samlet på samme sted. Virksomheter omorganiseres og fusjoneres, tidligere atskilte datasystemer og databaser kobles sammen og nye tjenester tilbys, også på tvers av tidligere organisatoriske skillelinjer. Begrunnelsen er ofte brukervennlighet og effektivitet.

Den økte informasjonsmengden som blir tilgjengelig for stadig flere inneholder også mye informasjon som kan knyttes til enkeltpersoner, og som dermed er å betrakte som personopplysninger i lovens forstand. Hensynet til personvernet kan lett bli en showstopper i utviklingen av nye tjenester og arbeidsformer. Dette skyldes både lovpålagte krav som er vanskelige å tilfredsstille og at man kan få problemer med lav sosial aksept av løsninger og håndtering av publikums subjektive oppfatninger av hva som er et tilstrekkelig personvern.

Med økt utnyttelse av informasjon øker dessverre også mulighetene for misbruk av informasjonen. Den teknologiske utviklingen er det neppe verken mulig eller ønskelig å stanse, og dermed blir det desto viktigere å sørge for at systemene er godt forberedt på å motstå truslene. For å oppnå tilstrekkelig sikkerhet og personvern uten altfor høye økonomiske kostnader, er det viktig at sikkerhets- og personvernløsninger designes inn i systemene fra begynnelsen av.

Vi ønsker med denne artikkelen å skape forståelse for nødvendigheten av – og fordelene ved – å ivareta personvernet til kunder eller klienter. Ikke minst vil vi peke på de mulighetene som finnes til å ivareta, eller til og med styrke, personvernet.

Hva er personvern?

Interessen for personvern og erkjennelsen av at det ligger store utfordringer på dette området er økende, men forståelsen av hva det egentlig innebærer å ivareta personvernet er ikke like stor. Sikkerhet er noe mange begynner å få en rimelig god forståelse av, og et høyt sikkerhetsnivå er en selvfølgelig forutsetning for personvern, men det er viktig å være klar over at beskyttelse av personvern krever en god del mer enn bare ”vanlig” informasjonssikkerhet.

Så hva er egentlig personvern? En enkel definisjon er at personvern er summen av de rettigheter, forbud og påbud som finnes i lovverk som angår personopplysninger, særlig i personopplysningsloven. Et godt utgangspunkt for forståelse av lovverket, er å se på de personvernprinsippene som ligger til grunn for både det norske lovverket og EU-direktivet. Det finnes som alltid mange lovbestemte unntak fra de generelle prinsippene, men

intensjonen bak lovverket er å følge disse prinsippene så langt det er mulig. I det følgende gir vi en oppsummering av disse prinsippene og en diskusjon av hva de innebærer.

Persondata 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. Dette er en av de store utfordringene innen personvern siden vanlige systemer for tilgangskontroll ikke tar hensyn til slike ting som formål eller samtykke.

Mengden persondata som samles inn og lagres skal minimeres.
Man skal ikke samle inn mer persondata enn man trenger. Det innebærer at man må gå nøye gjennom sine systemer og arbeidsrutiner for å vurdere hvilke data som faktisk er nødvendige. Dernest skal man slette data når de ikke lenger er nødvendige for formålet. For eksempel kan det være krav om at man skal slette data etter et visst antall dager eller etter at fakturaen er betalt. Videre bør man, så langt det er mulig, minimere graden av identifiserbarhet. Man kan for eksempel vurdere om det er nødvendig for en saksbehandler å kjenne identiteten, adressen eller eksakt fødselsdato til den personen saken omhandler. Hvis ikke, kan man sørge for at saksbehandleren ikke får se slike identifiserende data eller man kan erstatte dem med et pseudonym eller mindre nøyaktige data (f.eks. oppgi et intervall i stedet for eksakt fødselsdato).

Individet skal selv kunne ha kontroll med sitt eget personvern.
Tidligere lovverk la i stor grad opp til at Staten skulle både bestemme og kontrollere på vegne av borgerne, men i dagens lovverk er individets rett til selv å bestemme over bruken av personopplysninger viktig. Du skal med andre ord selv kunne velge hva du anser som tilstrekkelig personvern, veid opp mot de tjenestene du kan få ved å åpne for bruk av dine persondata. Dette innebærer at det i mange tilfeller er krav om samtykke for å få lov til å bruke data, samt 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. Ved å legge til rette for utstrakt bruk av innsynsretten kan man få et meget kraftfullt verktøy for kontroll, kvalitetssikring og bygging av tillit.

Den som samler inn og bruker persondata har et selvstendig ansvar for datakvaliteten.
Det vil si at man har plikt til å sørge for at personopplysninger som man lagrer og bruker er riktige, oppdaterte, komplette og relevante for formålet. Store databaser har en lei tendens til å inneholde mange feil, og det kan påvirke kvaliteten av de tjenester som benytter seg av databasen. Det mange nok ikke er klar over, er at når det gjelder personopplysninger så er slike feil faktisk også brudd på loven. Hvis feil oppdages så har man også plikt til å sørge for å minimere skadevirkningene det kan få for individet, f.eks. som følge av at uriktige opplysninger er gitt videre til andre parter. Sikring mot feil kan skje på mange måter, f.eks. validering av input i forhold til gitte regler, vasking mot andre registre, eller ved at man oppfordrer individene til selv å kontrollere opplysningene og gjøre det enkelt å få rettet feil som oppdages.

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. Det er svært viktig å være klar over at man også har et ansvar for å verifisere at alle man utleverer data til kan garantere et tilfredsstillende sikkerhetsnivå.

Et viktig spørsmål i en personverndiskusjon er 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 insidertrusselen er det behov for løsninger som sikrer at man oppfyller personvernprinsippene beskrevet over.

Hvorfor trenger vi personvern?

Personvernprinsippene over beskriver idealsituasjonen for enkeltindividet. Fra individets ståsted er det ikke vanskelig å argumentere for hvorfor man trenger personvern. Men det mest interessante å diskutere i denne sammenhengen er i hvilken grad det er nødvendig eller

fordelaktig for en *virksomhet*, det være seg offentlig eller privat, å beskytte personvernet til sine kunder eller klienter. Lovpålagte krav bør selvfølgelig etterleves, men på grunn av Datatilsynets altfor begrensede kapasitet til kontroll, er det svært mange virksomheter som enten lever i lykkelig uvitenhet om sine plikter eller som tilnærmet risikofritt satser på at de ikke blir oppdaget. Vi vil på ingen måte hevde at personvernet skal beskyttes for enhver pris, men vi mener det er mange gode grunner utover det å følge loven til å sørge for en sterk beskyttelse av personvernet.

For private virksomheter er det viktig å bygge tillit til egne merkevarer, og oppnå høy grad av kundeaksept og lojalitet. Et viktig poeng når det gjelder bruk av personopplysninger og beskyttelse av personvern er at kundene antakelig stoler på at selve virksomheten ikke har uærlige hensikter med bruken av data, men de stoler ikke nødvendigvis på alle virksomhetens ansatte. Videre stoler de ikke nødvendigvis på at virksomheten er godt nok rustet til å beskytte persondata mot utenforstående. For å bygge tillit er det derfor viktig å overbevise kundene om at man har gode systemer for å håndtere trusler både fra utsiden og fra egne ansatte. Dette kan man gjøre ved å informere godt om hvilke systemer og rutiner man har (forutsatt at man faktisk har slike!), og ved å gjøre det enkelt for kundene å benytte sin rett til innsyn i egne data og i hvordan de brukes av virksomheten. For både private og offentlige virksomheter vil en generell policy om åpenhet om hva virksomheten driver med også bidra til å øke den generelle tilliten og sosiale aksepten i befolkningen for øvrig.

Personalisering og utstrakt kjennskap til kundenes behov og preferanser åpner for verdiskapning gjennom nye tjenester eller forbedring av eksisterende tjenester. Videre er personalisering et verktøy for å oppnå økt kundelojalitet. Kunder liker generelt ikke å bli glemt, men de kan bli skremt om man husker for mye om dem. Da må man ha kundens aksept for at opplysninger om preferanser kan brukes til dette formålet, ellers vil tilliten til virksomheten og dens merkevarer raskt synke. Slik aksept får man neppe om kundene ikke fra før har tilstrekkelig tillit til at personprofiler ikke blir misbrukt enten av virksomheten selv, eller av andre som en personprofil kunne tenkes å bli utlevert til. Tilstrekkelig personvern er en forutsetning for å lykkes med utstrakt personalisering av tjenester, men det er også omvendt; godt personvern krever en viss grad av personalisering. Hva som er et tilstrekkelig personvern varierer fra person til person, og fra situasjon til situasjon.

De offentlige virksomhetene eksisterer for borgernes skyld og har et spesielt ansvar for å ivareta borgernes rettigheter på en best mulig måte, ellers kan de rett og slett miste sin legitimitet. Planene om modernisering, dvs. økt elektronisk samhandling og derav følgende økt utveksling av persondata, har potensielt store innvirkninger på personvernet. 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. Dessuten må man gjerne via mennesker som kan stille spørsmålstegn ved hvorvidt informasjonen er nødvendig å gi ut. Spesielt på små steder hvor samfunnet er mer gjennomsiktig og folk i stor grad kjenner (til) hverandre, kan det oppleves som et problem at offentlige saksbehandlere får tilgang til mye informasjon om enkeltpersoner.

Det er meget viktig å adressere personvern hvis man skal få aksept fra befolkningen for den utstrakte utvekslingen og gjenbruken av data som trengs for å effektivisere offentlig sektor. Samtidig har det offentlige gjennom planene for modernisering og økt elektronisk samhandling en unik mulighet til nettopp å ta tak i personvernproblematikken. Når systemer likevel skal legges om, har man en gylden sjanse til å få på plass gode og fornuftige løsninger helt fra starten av.

Hvordan oppnå personvern?

For å oppnå god beskyttelse av sine kunders personvern må man gjennom visse trinn. Som i så mange andre sammenhenger er det viktig å basere sine handlinger på rasjonelle begrunnelser. Den største trusselen mot personvernet i et organisasjonsperspektiv er ureflektert innsamling og bruk av persondata.

I personvernssammenheng trenger man å analysere hvilken persondata man har behov for å samle inn, basert på organisasjonens arbeidsprosesser og det behov som finns for persondata av juridiske grunner, f.eks. lovpålagt innsamlingskrav eller et behov for identifisering ved kriminalitet. Videre trenger man å analysere hvilket behov for aksess personer med forskjellige arbeidsoppgaver har til persondata, og om man eventuelt kan

erstatte identifiserende data med et pseudonym eller mindre nøyaktige data. En slik analyse resulterer i et målbilde.

I tillegg til å formulere et målbilde bør man analysere nåværende innsamling og bruk av persondata. Målsettingen må være at man over tid minsker det gap som eventuelt eksisterer mellom målbilde og nåværende situasjon.

Om ikke organisasjonen har en dokumentert personvernpolicy bør en slik forfattes og håndheves. Den må som et minimum oppfylle lovpålagte krav. Personvernpolicyen skal kommuniseres både internt og eksternt; eksternt fungerer den som et løfte og internt fungerer den som retningslinjer. Ettersom organisasjonen forflytter seg mot målbildet må man oppdatere og detaljere organisasjonens personvernpolicy. I tillegg til organisasjonens egen policy kan det finnes et behov for å la kundene ha innflytelse gjennom å gjøre visse valg med hensyn til hvordan deres persondata kan brukes.

Et *vokabular* som beskriver datakategorier, roller, formål, betingelser og forpliktelser er en forutsetning for anvendbare personvernpolicyer. Et slikt vokabular kan være generelt eller domenespesifikt. Det pågående metadataprosjektet til Oppgaveregistret i Brønnøysund, hvor man har som mål å utvikle en metadatamodell for informasjon som samles inn og brukes i offentlig sektor, er et eksempel på et arbeid for å ta fram et domenespesifikt vokabular av datakategorier.

Organisasjonens personvernpolicy må håndheves gjennom rutiner og bruk av tekniske løsninger. Dette innebærer etablering av aksesskontroll til persondata og å sikre at forpliktelser, slik som sletting av data etter en viss tid, blir overholdt. I tillegg må man etablere etterkontroll for å forsikre seg om at persondata kun har blitt brukt til gyldige formål.

For å implementere målbildet trengs det nye systemer eller modifisering av gamle. Det er ofte vanskelig og dyrt å modifisere eksisterende systemer. Det er derfor mest praktisk å innføre personvernøkende teknologiske løsninger (f .eks. pseudonymer og aksesskontroll) i forbindelse med utvikling av nye systemer. I takt med at organisasjonen applikasjoner oppgraderes bør også organisasjonens systeminfrastruktur utvides med personvernsfunksjonalitet, f. eks. system for innsyn og sikring av datakvalitet.

NRs personvernprosjekt

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.

NR startet i 2002 opp et strategisk instituttprosjekt innen personvern finansiert av Norges forskningsråd. Prosjektet gjennomføres i samarbeid med Avdeling for forvaltningsinformatikk (AFIN) ved Universitetet i Oslo. Gjennom dette prosjektet har NR etablert seg som det ledende kompetansemiljøet i Norge på de teknologiske aspektene ved personvern. Kompetanseoppbygging, og ikke minst anvendelse og spredning av kompetansen, er det overordnede målet med denne typen prosjekter.

Prosjektets hovedfokus er hvordan organisasjoner kan beskytte sine kunders persondata mot misbruk både fra utenforstående og egne ansatte. Når et datasubjekt, dvs. personen informasjonen gjelder, tillater en organisasjon å samle inn persondata, må datasubjektet nødvendigvis stole på at organisasjonen ikke har uærlige hensikter med bruken av informasjonen, men denne tilliten gjelder ikke nødvendigvis alle organisasjonens ansatte. Det er derfor behov for beskyttelsesmekanismer som kan håndheve det løftet om personvern som en organisasjon gir sine kunder når persondata samles inn. Videre er personvern også subjektivt. Ulike personer har forskjellig oppfatning av hva som er personvernkrenkende og hva som ikke er det, og også om hvem man kan stole på. Med andre ord har man ulike personvernpreferanser, og disse bør man få lov til å uttrykke og få respektert. For en organisasjon som har tusenvis av kunder med ulike personvernpreferanser, er det nødvendig med automatiserte løsninger. Et system for automatisk håndheving av personvernpolicy og -preferanser vil bidra til økt tillit til organisasjonen.

NR har definert et rammeverk for håndheving av personvernpolicy, og jobber med videreutvikling og implementering av dette. Målet er å få kunnskap om, og erfaring med, de spesielle problemstillingene som oppstår i praksis. Særlig viktige problemer som vi har jobbet

med ulike løsninger på, er hvordan man enklest mulig kan få til integrasjon av personvernteknologi i forretningsapplikasjoner og hvordan man skal sikre at ikke data brukes for andre formål enn de er godkjent brukt for. Andre sentrale aspekter ved personvern er minimering av mengden persondata som lagres, anonymisering og pseudonymisering, håndtering av innsynsrett, samtykke og personlige preferanser, krav til datakvalitet, forpliktelser i forhold til sletting av data når det ikke lenger er behov for dem, og deteksjon av brudd på personvernet.

Vi har jobbet mye med teknologiske løsninger, men har også erfart at det i tillegg til teknologi er et stort behov for metodikker både for analyse av risiko og behov, og for design av personvern i systemer. Ikke minst er det et presserende behov for å fylle gapet mellom analyse og design. Med andre ord: når man har identifisert et behov for tiltak; hvordan går man fram for å finne de riktige tiltakene? På dette området mangler det fremdeles mye, og dette er noe vi vil jobbe med framover i samarbeid med både offentlige etater og private selskaper.