NIFS-møte tirsdag 6. november 2018

Risikobasert arbeid med personvern

Martha – Datatilsynet

Spørsmål fra salen: Er det lov å drive med innovative prosjekter på automatiserte avgjørelser uten å be om samtykke?
For eksempel legevakt der hastegrad av legehjelp er bestemt av en maskin.
Svar fra Martha: Dette må jeg høre med juristene om. Man har uansett krav på "manuell" behandling om man ber om det.

Kommentarer til tiltak om å bruke brevpost istf e-post for å hindre at man sender personopplysninger til feil mottaker på epost:
Mange hadde flere hendelser når man brukte brevpost. Det er viktig å gjøre risikovurdering for alle typer tjenester, ikke bare de digitale.

Spørsmål fra salen: Hva betyr sannsynlig? (kontekst: risikovurdering)
Svar: Virksomheten må gjøre denne vurderingen selv

Spørsmål fra salen: Får Datatilsynet avviksmeldinger på integritet- og tilgjengelighetsbrudd?
Svar fra Martha: DT får også avvik om integritet- og tilgjengelighetsbrudd, typisk sykehusopplysninger som ikke er tilgjengelige i en helsesituasjon. Det er ofte en annen myndighet som også blir involvert.

Spørsmål fra salen: Hva er det som skal dokumenteres i forbindelse med et avvik, må alt dokumenteres?
Svar fra Martha: Har man et system for å håndtere avvik så er det greit. Ikke alt må dokumenteres, man må bruke litt sunn fornuft.

Spørsmål fra salen: Hva skjer i Datatilsynet når en avviksmelding kommer inn? Hvor lang tid tar det før den er behandlet?
Svar fra Martha: Det er en egen innsatsgruppe som er involvert, de fleste sakene blir avsluttet ganske raskt hvis DT ser at den ble håndtert. Svaret i sånne tilfeller kommer i løpet av noen dager.

Diskusjonsoppgave 1

- Viktig å vite hvor mange personer som har vært inne på siden
- Koblingen personnummer pluss navn er uheldig i seg selv, men det kommer an på hvor mange som har vært inne på siden.
- Kobling person og etat kan være problematisk, men det finnes id-kontroll-løsninger. Hvis man for eksempel kan få kreditt uten id-kontroll da er det etaten som ikke har en bra nok løsning. Man skal ikke basere seg på at personnummer kan gi tilgang til hva som helst.
- Tiltak:
    - rutiner for oppdatering og testregimer før man publiserer, samt logging.
    - Innebygd personvern
    - Man kan vurdere om i det hele tatt er nødvendig å ha med personnummer
    - Lenken ble slettet
    - Informere om at det er ulovlig å spre opplysningene (om det er relevant)
- Skal avviket meldes til DT: Flere meninger om dette:

    - Saken ble håndtert fort og dersom det ikke er store konsekvenser så trenger man ikke å melde det inn til DT. Særlig hvis man har tilgang til logger og ser at ikke mange har sett opplysningene.
    - Martha sier at saken burde rapporteres og meldes inn
    - Hva er de største konsekvensene i saken? Ta med i vurderingen om det har noen konsekvenser i det hele tatt for de registrerte

- Skal man informere de berørte:
    - Det kommer an på etat og type søknad
    - Hvis man kan se hvilke dokumenter som ble lest, så kan man informere bare de som ble berørt og ikke alle i systemet.
    - Vurder dette grundig, dersom å informere de berørte gjør mer skade så bør man ikke informere.

Diskusjonsoppgave 2

K, I, T - hva som er viktig er avhengig av type virksomhet.

Betraktninger fra salen:

Etterlevelse: vi har de overordnede dokumentene, men ligger det i ryggraden til de som jobber med dette? Risikovurdering for ny funksjonalitet, oppdatering underveis. Jobber agilt med utvikling, følger med risiko og tiltak.

Hvor er den største utfordringen på **personvernområdet**? Vi vet ikke, har laget risiko og sårbarhetsanalyser, men har ikke aggregert og prioritert på virksomhetsnivå. Før dette er gjort, så har man ikke oversikt.

Må gå tilbake til **risikostyringen**, bruker trekantmodellen til NSM og bruker verdivurderingen til å si hva vi bør gjøre på DPIA. Ser på helheten og rapporterer til departementet.

Hvilket **omfang** skal man legge seg på? Dette er en utfordring spesielt når man har et stort omfang av ulike personopplysninger.

Vi har folk til slikt nedover i organisasjonen. Ledelsen er fornøyd når prosesser er dokumentert. **Fravær av hendelser** er ikke et bevis på at ting er godt nok.

Diskusjonsoppgave 3

Eksempler på sikkerhetsbrudd:

Uthenting av skattekort til tidligere ansatte – dette skader omdømmet til etaten
Det er lett å hente ut informasjon siden man har lov til det, så med automatiserte prosesser så skjer slike uhell.

Melding i elektronisk meldingsbok som ved et uhell går ut til alle foreldre

Innovasjonsprosjekt med personopplysninger som ble lagt i skyen og ble tilgjengelig for alle

Hendelse med langvarig nedetid som ikke varsles pga at konsekvensene ikke er så store. Har redundante systemer. Kan være ressurssløsing men betyr ikke så stor risiko for den registrerte.

Det er stor variasjon på opplysninger som blir behandlet og også på kunnskapsnivået til de som behandler det. Det er stort rom for subjektive vurderinger. Prøver å gå over på anonyme data. Er det riktig at det er opp til den enkelte å definere hva som er godt nok anonymisert. Hva er innenfor særlige kategorier. Det bør være en felles vurdering på dette.

Hvordan dokumenterer dere sikkerhetsbrudd?

Kan noteres i saksbehandlingssystemet