

Innspill Digitaliseringsstrategien – personvern

Jeg heter Knut Soelberg ønsker å gi noen innspill ift Digitaliseringsstrategien relatert til personvern.

Under følger også nærmere omtale av min erfaringer ift personvern.

Overordnet utfordringer personvern per i dag

- De store internasjonale «tech»-aktørene utvikler digitale tjenester rettet mot private forbrukere (og virksomheter) som i for begrenset grad følger personopplysningsloven/GDPR tilstrekkelig per i dag.
 - o Årsakene til dette er flerdelte, men viktige årsaker er leverandørens forretningsmodell og at de har forankring (hovedkontor) i land med en «svakere» personvernlovgivning enn Norge/EU
 - o Omtaler ikke tiltak/mål her, men Datatilsynets arbeid ift saken med Meta er et godt eksempel på et viktig tiltak
- For mange norske virksomheter, både innen det offentlige og private, har per i dag for svak kompetanse, kapasitet og fokus til at de i tilstrekkelig grad sørger for at deres tjenester (både som behandlingsansvarlig og databehandler) i tilstrekkelig grad etterlever personopplysningsloven/GDPR generelt og ift personvernprinsippene spesielt
 - o Ja, heldigvis finnes det også virksomheter som er «gode» innenfor dette området
 - o Årsakene til dette er mange, men blant viktige årsaker er
 - En av de store utfordringene per i dag er at det dessverre ikke er noe fokus på at virksomheten (les de som er ansvarlig for aktuelle tjeneste) **alltid** må
 - Beskrive behandlingen
 - Påse at personvernprinsippene etterleveresfor alle formål med behandling av personopplysninger.
De færreste har dessverre en god forståelse per i dag av hva en DPIA bør inkludere og hvordan den bør utformes.
 - GDPR oppleves som «vanskelig»
 - Etterlevelse av personopplysningsloven forankres ikke tilstrekkelig hos de som «eier» de aktuelle tjenestene (som behandler personopplysninger)

- For ensidig forankring i juridisk avd / it-sikkerhet
 - Tjeneste-/produktutviklingsmiljøene har ikke personvern som en iboende aktivitet i deres produkt/tjeneste utvikling (gjelder både behandlingsansvarlig og databehandler)
 - Personvern er et tverrfaglig fagområde – det er lite forståelse for dette
 - Jeg har for øvrig møtt på overraskende mange tilfeller hvor det er åpenbart utført feilvurderinger ift hvem som er behandlingsansvarlig. Erfaringen er også at det viser seg å være veldig vanskelig å endre dette i etterkant. Har flere eksempler fra offentlige virksomheter
 - Det er per i dag en tendens til at personvern kobles for sterkt og ensidig opp mot it-sikkerhet. Ja, it-sikkerhet der definitivt viktig, men de fleste av personvernprinsippene er faktisk koblet opp mot virksomhetens/tjenestens domene (forretningsområde). Uten tilstrekkelig fokus på domene/forretningsområde, vil man ikke kunne etterleve personvernprinsippene tilstrekkelig, man vil heller ikke identifisere hva som er rette sikkerhetsnivå ift «behandlings art»
- Utdanningen innenfor personvern er per i dag for snever
- Personvern har først og fremst fokus innenfor juridiskutdanning per i dag
 - Innenfor juridisk utdanning blir det for lite fokus på hvordan etterlever man personopplysningsloven generelt og personvernprinsippene spesielt når man utvikler digitale tjenester
 - Juridisk utdanning har ofte fokus på koblingen jus, samfunn og teknologi, men det er lite fokus på koblingen mot virksomhetsutøvelse (i privat og offentlig sektor). Det er jo her de digitale tjenestene som behandler personopplysninger utvikles og leveres til publikum og andre virksomheter
 - Det finnes også kurs/emner innenfor informatikk/databehandling og lederutdanninger, men dette er meget begrenset og har lite eller ingen fokus på hvordan sikrer vi at digitale tjenester som utvikles og leveres etterlever personvernprinsippene. (For ordensskyld inkluderer jeg også her det å sikre et de registrertes rettigheter og friheter etterleveres, at behandlingen har et juridisk grunnlag og at relevante databehandleravtaler inngås med tilstrekkelig kvalitet)
 - Har sett at flere at de kursene som dekker personvern er et kombinert kurs innenfor sikkerhet og personvern

Her er forslag til mål med 5 års perspektiv, for å håndtere personvernutfordringene og sikre en videre god digitalisering.

1. Alle tjenester i offentlig og privat sektor som krever behandling av personopplysninger skal utvikles og forvaltes med «personvern som en iboende del» av tjenesteutviklingen og forvaltningen. Ideelt sett bør man ha en form for «sertifisering» kombinert med tilsyn også av «tjenesteutviklingsprosessen».
2. Dagens veiledere for behandling av personopplysninger fra Datatilsynet og andre må forenkles og inkludere gode eksempler som tydeliggjør hvordan behandling av personopplysninger kartlegges, personvernprinsippene etterleves og gode risikovurderinger gjennomføres. Dagens veiledere fungerer i praksis ikke godt nok.
3. Det bør utarbeides forhåndsutfylte maler for personvern vurderinger for alle tjenester som behandler personopplysninger og som er vanlig i en kommune. Tilsvarende gjelder også for andre sektorer. Dette vil forenkle arbeidet for den enkelte kommune og sikre høyere kvalitet og et bedre personvern.
 - Et eksempel her er Husbanken og deres løsning for søknad om kommunal bolig hvor de har laget en forhåndsutfylt mal for vurdering av personvernkonsekvenser (DPIA) som kan spisses.
4. Det bør utarbeides maler/veiledninger for ulike typer verdikjeder som tydeliggjør aktørene, samhandlingen, lovligheten, mm.
 - Eksempel på verdikjede: Sivil luftfart er en verdikjede som inkluderer bla. lufthavner, flyselskaper, reisebyråer og andre aktører på lufthavnen. Disse aktørene utveksler personopplysninger om flypassasjerene slik at disse kan få gjennomført sin flyreise.
5. Personvern må innarbeides som del av de utdanningene som yrker innen digitalisering rekrutterer fra
6. Forberedende statlig arbeid i forbindelse med tilsynsordninger for AI Act må starte tidlig, dvs før forordningen er implementert i norsks lovgivning for å sikre en forsvarlig bruk av kunstig intelligens
7. Personvern, risikovurderinger (ROS) og etterlevelse av AI Act må inkluderes som en iboende del av norsk forskning innen kunstig intelligens / maskinlæring
8. Personvern vurderinger og krav må bli en iboende del av arbeidet med utforming av lover hvor de nye eller reviderte lovene og forskriftene medfører behandling av personopplysninger
9. Det må gjøres gjennomgang og revideringer av relevante lover og forskrifter hvor det er sannsynlig at bruk av kunstig intelligens vil gi verdi for samfunnet

Jeg har også gitt noen likende innspill til Datatilsynet i våres. Jeg vedlegger disse

Under følger litt informasjon om min bakgrunn og erfaring med personvern

Jeg jobber som konsulent hos Bouvet og jobber hovedsakelig med oppdrag ut hos kunder. Jeg har de siste årene bistått flere store virksomheter med i større grad å etterleve

personopplysningsloven og har i løpet av disse årene fått en omfattende praktisk erfaring. Denne erfaringen har jeg benyttet da jeg for 2,5 år siden ble spurt av kursavdelingen i Bouvet om å holde kurs i anvendt personvern. Jeg har holdt kurset i ulike versjoner rettet mot ulike roller. Kursene jeg har holdt har både vært åpne kommersielle kurs, bedriftsinternt kurs og interne kurs i Bouvet.

Jeg er for øvrig informatiker, ikke jurist, men kjenner etter hvert personopplysningsloven veldig godt. Jeg har som regel oppdrag hvor jeg er leid ut på kundesiden hos store (offentlige) virksomheter over flere år. Når jeg er ute i oppdrag er jeg opptatt av å lære så mye som mulig bla. om virksomhetens (kjerne)prosesser og organisering. Jeg omtaler meg selv som prosjektleder og rådgiver, men **«Personvern som del av digital produktutvikling» er et av mine spesialområder.** Jeg har også omfattende it-sikkerhetsbakgrunn.

En av mine viktigste erfaringer fra personvernoppdrag er at personvern er et **tverrfaglig fagområde** og at fokus på denne tverrfagligheten er et viktig suksesskriterie. Jeg fokuserer derfor på at personvern bør være en iboende del av produktutviklingen hvilket betyr at det er behov for både breddekompetanse og noe dybdekompetanse i alle produktteam som utvikler digitale produkter som inkluderer formål med behandling av personopplysninger.

Mvh
Knut Soelberg
Mobil 91 58 33 84