Kandidatnummer og emnekode vil bli lagt inn automatisk etter at du har levert.

Eksamensbesvarelse DRI2020 høst 2016

Oppgave 1

Når Stortinget vedtar en lov så er det etter en lang lovgivningsprosess som resulterer i en innstilling fra en fagkomité som tok utgangspunkt i departementets proposisjon som igjen tok utgangspunkt i en utredning. Stortinget mottar innstillingen, så voteres den over, dersom forslaget får flertall, går den til annen gangs behandling, hvis ikke, henlegges den. Dersom det ved annen gangs behandling stemmes ja, har de da vedtatt lovforslaget. Dersom flertallet her stemmer nei, følger det at det må skriver anmerkninger til loven, altså hva som burde endres. Tredje gangs behandling vil innebære at det voteres over det originale lovforslaget med de foreslåtte endringene. Dersom det får flertall, er det lovforslaget med endringer som er vedtatt, ved dissens henlegges forslaget.

Spørsmålene oppgaven reiser ble for min del litt uklare, slik det ikke sjeldent blir innenfor jussen, men jeg velger her å forstå «bruk av lovvedtak» som en anvendelse av loven etter at den er vedtatt i Stortinget, en annen tolkning kunne være å se på bruk av lovvedtak som hvorvidt Stortinget benytter seg av vedtak under behandling av innstilling til lov.

Dette var litt generelt om hvordan Stortinget vedtar lovene. Når lovvedtak må anvendes er ved myndighetenes inngrep ovenfor den enkelte, da må dette inngrepet ha grunnlag i lov iflg. Legalitetsprinsippet jf. Grunnlovens § 113. I tillegg er Stortinget nødt til å rette seg etter regler som omhandler deres egen struktur og organisering samt plikter og oppgaver. Da som regel rettsreglene som fremgår av Grunnloven del C om borgerrett og lovgivende makt. I tillegg er Stortinget underlagt Stortingets forretningsorden 7 juni 2012 nr. 518

I tillegg kan det være hensiktsmessig av Stortinget å benytte seg av lovvedtak selv når det ikke strengt talt er nødvendig mht. lov. Dette kan bl.a. være pga. at det vil styrke folkets tillit til Stortinget og vise at de, selv om de ikke er nødt, underretter seg loven. Det vil også gi en slags trygghet for folk flest på samme måte som at meroffentlighet i forvaltningen gir tillit og skaper trygghet. Det er sjeldent det oppstår situasjoner der Stortinget vil nekte å bruke lovvedtak som de har mulighet til å bruke, da bruk av dette vil bidra til å styrke rettssikkerheten ved at det oppstår forutberegnelighet, altså at man har et forventet utfall av en handling eller hendelse.

Oppgave 2

Innebygget personvern, eller privacy by design, er viktig når det kommer til utvikling av systemer. Hovedpoenget med innebygget personvern er at man skal ha personvern «innbakt» i systemet, ikke som noe man legger til på slutten. Derfor følger syv prinsipper for innebygget personvern for at det skal kunne realiseres i systemutviklingen.

De syv prinsippene er:

Embedded privacy – dette innebærer at man fra starten av prosessen tenker på personvernet. Altså at personvernet ligger i kjernen av selve systemet. Allerede i arkitektur-stadiet eller ved design-studiet av utviklingen skal det ta hensyn til personvern og det skal gjennomgående ligge inne i systemet.

Preventive – En god metafor for preventivt personvern er at man låser døren før man har opplevd innbrudd i stedet for å prøve å jakte på tyvene. Altså vil det si at man tar høyde for og legger inn personvernhensynene før det skjer en feil i systemet. Det er ofte dyrt og tidkrevende å rette opp i feil

eller legge til funksjoner i systemet i ettertid, det er derfor viktig at det tidlig i prosessen vil være gode personvernløsninger. Altså, man setter en personvernlås på systemdøra før tyvene kan stjele personopplysninger, i stedet for å måtte spore ned tyvene etterpå.

Privacy as a default setting – dette betyr at man slipper å aktivt velge å skru på personverninstillingen. Altså såkalt opt. in. I følge dette prinsippet skal en heller måtte opt. Out, eller «skru av», dersom man ikke ønsker å ha disse personverninstillingene. Et eksempel er om man på Facebook skal legge inn telefonnummer fordi å kunne motta et nytt passord dersom man hadde glemt det gamle. Da burde Facebook som en default setting ikke la nummeret ditt være synlig for andre. Derimot skal du ha muligheten til å si at man vil ha telefonnummer som en del av den synlige profilen din. Dette er en slags sikkerhet for at du skal ha kontroll på dine opplysninger og at informasjon ikke blir spredt ved uhell.

End-to-end privacy (full security lifecycle) – End-to-end security vil si at det ikke er noe svakt ledd når systemet brukes. Personvernet skal ikke være svekket i deler av systemet, men skal ivaretas fra en ende til en annen. Et eksempel er kryptering av meldinger. Dersom meldingene er krypterte når de er på hver sin telefon, men ikke er krypterte idet de sendes, er det svekket sikkerhet akkurat da meldingen sendes, og den kan derfor «snappes opp». Derfor er det viktig at det tas hensyn til personvern i hver del av utviklingen og at man ikke kun prøver å ta inn personvernhensynene i siste del av utviklingen.

High functionality (positive-sum not zero-sum) – dette prinsippet handler om at man skal være forsiktig med å gå på

kompromiss med personvernet for andre hensyn, som f.eks. sikkerhet, effektivitet, budsjett mv. Det er noen ganger at man velger å veie andre hensyn tyngre enn personvern. Det som viser seg er at dersom en avveining oppstår, er det i mange tilfeller mulig å ivareta begge hensyn uten at de skal måtte innskrenkes. Derfor er det ikke noen unnskyldning å si at man måtte velge effektivitet framfor personvern dersom det ikke blir en konflikt mellom de to hensynene.

Transparency and visibility – Prinsippet om åpenhet og gjennomsiktighet er et gjennomgående prinsipp flere steder, særlig i forvaltningen. Dette er fordi vi ønsker å kunne se hvordan vår data behandles, vi ønsker å se hvilke prosesser som fører til hvilket resultat og vi ønsker å kunne se hvem som er ansvarlig dersom det skulle skje en feil.

User-centered - brukeren skal være i sentrum, derfor vil det være viktig å ha brukerens beste i tankene. Ettersom at det skal være brukerorientert, vil det bl.a. måtte være brukervennlig og lett å forstå slik at brukeren har kontroll og oversikt og ikke godkjenner en handling som han eller hun ikke ønsker. Dette er sentralt da det skal handle om sikkerhet for bruker.

Dette er en slags oppskrift på innebygget personvern, den er ikke bindende, men er allikevel en god oppskrift som kanskje vil kunne spare tid og penger ved at den har som hensikt å hindre feil. Som nevnt over er det både tid- og ressurskrevende å endre systemet etter at det er oppdaget feil, og derfor vil denne oppskriften kunne hindre disse feilene.

Derimot mener mange at det ikke vil lønne seg ettersom at å gjøre personvern innebygget i systemet vil føre med seg

kostnader og tidkrevende oppgaver slik at sluttresultatet vil være at en taper tid og penger på innebygget personvern.

I tillegg er en kritikk at systemutviklere generelt ikke har kunnskap og kompetanse nok til å innføre personvern i så stor grad i systemet. Derfor mener noen at denne oppskriften på innebygget personvern er for ambisiøs og at en ikke kan forvente at en systemutvikler vil følge den.