

Folketingets arbejdsgruppe
vedrørende datasikkerhed
Birgitte.Toft-Petersen@ft.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 3269 8805
RFJ@HUMANRIGHTS.DK
MENNESKERET.DK

J. NR. 540.10/30991/RFJ/MAF

HØRING OVER BERETNING NR. 3

29. AUGUST 2014

Folketingets arbejdsgruppe om datasikkerhed har ved e-mail af 26. juni 2014 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til beretning nr. 3 afgivet af Kulturudvalget og Retsudvalget den 3. juni 2014 om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse.

Instituttet har følgende bemærkninger:

Institut for Menneskerettigheder hilser den parlamentariske arbejdsgruppe vedr. databeskyttelse velkommen. I takt med den stigende digitalisering er der et øget behov for at sikre et højt niveau af databeskyttelse og informationssikkerhed i Danmark. Som illustreret i beretningen dækker området over en bred række af problemstillinger, der knytter sig til såvel det retlige grundlag, det interne og eksterne tilsyn med området, områdets internationale karakter, borgerens retssikkerhed, mv.

Behovet for øget fokus på databeskyttelse har været fremhævet i instituttets årlige statusrapport i såvel 2012 som 2013. Statusrapportens kapitel om databeskyttelse omhandler blandt andet de danske lovningsregler, kontrol med sociale ydelser, sociale medier, cloud computing, samt reguleringen af, og kontrollen med, politiets efterretningstjeneste. For hvert område er angivet en række anbefalinger til regeringen.

Som supplement til statusrapporten vil instituttet fremhæve følgende tre indsatsområder, som instituttet anser som væsentlige i forbindelse med arbejdsgruppens arbejde.

EN STYRKET INDSATS FOR INFORMATIONSSIKKERHED OG DATABESKYTTELSE

Databeskyttelse og informationssikkerhed behandles ofte som enten juridiske eller tekniske emner, frakoblet hinanden. Hvis informationssikkerhed og databeskyttelse skal gennemsyre praksis i institutioner og virksomheder, kræver det et tæt samspil mellem retlige standarder, organisation og teknologisk løsning. Området bør opprioriteres politisk, og det bør forankres med både teknisk, organisatorisk og juridisk kompetence for eksempel i form af et ressortministerium, en ombudsmand på området eller en offentlig institution. Danmark mangler en stærk tværfaglig instans som kan rådgive, monitorere og tilse det brede område som databeskyttelse og informationssikkerhed dækker over i både offentlige institutioner og private virksomheder.

EN SAMLET STRATEGI FOR INFORMATIONSSIKKERHED OG DATABESKYTTELSE I DEN OFFENTLIGE SEKTOR

Der er igangsat en kortlægning af sikkerheden ved betalingskort. Dette arbejde kan imidlertid ikke stå alene og der er behov for en bredere undersøgelse af, hvordan man kan forbedre sikkerheden ved behandling af personoplysninger i den offentlige sektor. Som led heri bør indgå en kritisk gennemgang af gældende regelsæt, en analyse af interne og eksterne kontrolmekanismer og eventuelt behov for at styrke disse, samt forslag til privatlivsfremmende løsninger, der kan anvendes i den offentlige sektor. Arbejdet bør munde ud i en sammenhængende og tidssvarende strategi for området med pilotforsøg på centrale områder.

PRIVACY KONSEKVENSANALYSE OG BRUG AF PRIVATLIVSFREMMENDE TEKNOLOGIER I OFFENTLIGE IT PROJEKTER

Retlige standarder og tekniske løsninger skal i højere grad sammentænkes. Dette kan blandt andet ske gennem privacy konsekvensanalyser (PIA), der foretages i forbindelse med opstart af nye offentlige IT projekter og lovforslag, der behandler persondata. Konsekvensanalyser indebærer blandt andet en proportionalitetsvurdering, risikovurdering, angivelse af tekniske og organisatoriske forholdsregler, og sikkerhedsforanstaltninger ved påtænkte overførsler til tredjeland, mv.

Privacy konsekvensanalyser er ikke obligatoriske i Danmark, mens de har i flere år været fast praksis for eksempel i Canada. Udgangspunktet i Canada er, at der foretages en risikovurdering med udgangspunkt i borgerens ret til beskyttelse. Det indebærer blandt andet, at borgeren ikke skal identificeres med mindre det er strengt nødvendigt i den

konkrete situation. Der er ligeledes udarbejdet detaljerede krav til, hvorledes disse analyser skal gennemføres og godkendes i samspil med den canadiske privacy kommissær. Den canadiske model kan tjene som inspiration for en dansk skabelon, idet der allerede er udarbejdet et omfattende materiale baseret på flere års erfaringer.

Ligeledes bør privacy som en naturlig og obligatorisk komponent tænkes ind i forbindelse med design af nye IT systemer (såkaldt "privacy by design"). Offentlige IT projekter bør i langt højere grad gøre brug af privatlivsfremmende teknologier, både ved nye IT løsninger men også når man skal gentænke for eksempel CPR løsning eller Nem-id.

For at sikre en reel styrkelse af databeskyttelsen i Danmark er det vigtigt, at arbejdsgruppens indsats munder ud i konkrete tiltag, der kan medvirke til at højne beskyttelsen af personoplysninger i både den offentlige sektor og blandt private virksomheder.

Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder og imødekomme internationale anbefalinger:

- at der udarbejdes en samlet strategi for databeskyttelse og informationssikkerhed i Danmark.
- at tværfaglig rådgivning og tilsyn med databeskyttelse og informationssikkerhed styrkes, inklusiv rådgivning om brug af nye privatlivsfremmende teknologier.
- at privacy konsekvensanalyser indarbejdes som fast obligatorisk praksis i tilknytning til de ISO standarder (ISO27001) og den projektskabelon, som offentlige IT projekter skal følge;
- en styrket kontrol med offentlige IT projekter og leverandørers efterlevelse af de standarder for informationssikkerhed og databeskyttelse, der er foreskrevet i sikkerhedsbekendtgørelsen og ISO27001 standarden; og
- at privacy vurderinger udarbejdes i forbindelse med nye lovforslag på linje med analyse af miljømæssige eller økonomiske konsekvenser af lovforslaget.

Instituttet finder det positivt, at arbejdsgruppen vedr. databeskyttelse aktivt vil inddrage eksterne eksperter. I beretningen nævnes særligt Institut for Menneskerettigheder, Teknologirådet, Forbrugerrådet Tænk, Rådet for Digital Sikkerhed og Forbrugerombudsmanden. Da de nævnte problemstillinger spænder over både jura, tekniske løsninger,

og IT sikkerhed i bred forstand anbefaler instituttet, at der i den kommende proces foretages en bredere inddragelse af interessenter end disse fem organisationer, for eksempel gennem en række åbne, tematiske høringer.

Rikke Frank Jørgensen

FORSKER, PH.D