Datatilsynet

20 MAR 2019

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse	Vår referanse	Dato
18/6579	18/04264-2/EOL	14.03.2019

Datatilsynets høringsuttalelse - NOU 2018: 14 - IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett

Vi viser til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2018 med to saker på felles høring: 1) Utredning fra IKT-sikkerhetsutvalget, og 2) Regjeringens utkast til lov som gjennomfører NIS-direktivet i norsk rett.

Oppsummering
Datatilsynet mener at situasjonsbeskrivelsen i NOU 2018:14 gir et godt bilde på de viktigste utfordringene vi står ovenfor med hensyn til dagens regulering av IKT-sikkerhet.

Når det gjelder utvalgets anbefalinger til løsninger på disse utfordringene er vi enige i noen av dem, mens andre etter vår mening ikke er like treffsikre.

- Datatilsynet støtter både et initiativ til at det skal stilles krav om IKT-sikkerhet ved anskaffelser og til tettere samarbeid mellom tilsynsmyndigheter som har tilsyn med enheter koblet til internett innenfor sitt myndighetsområde.

- Datatilsynet støtter ikke anbefalingen om etablering av et nasjonalt IKT-sikkerhetssenter. Kompetanse innen IKT-sikkerhet er et knapphetsgode som det allerede er hard konkurranse om. Allerede etablerte fagmiljø og etater trenger denne kompetansen for å utføre sine oppgaver, og etablering av enda et fagmiljø vil bety at det blir enda vanskeligere for disse å skaffe de ressursene de trenger.

  Istedenfor å planlegge et nytt fagmiljø mener Datatilsynet at det må satses på å styrke kompetansen innenfor IKT-sikkerhet og personvern i samfunnet generelt, og i porteføljen til høyere utdanning spesielt. Vi må utdanne flere IKT-sikkerhets eksperter.

- Like viktig som felles og sektorovergripende minstekrav til informasjonssikkerhet er det at offentlige myndigheter stiller tydelige krav til sikkerhet.i nasjonale felleskomponenter. De løsninger og tjenester som skal ivareta større verdikjeder må underlegges et regelverk med tydelige krav til sikkerhetsnivå.

- Datatilsynet mener at bestemmelsen som skal fungere som rettslig grunnlag for behandling av personopplysninger er for lite presis.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 458 Sentrum 0105 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

1. Merknader til IKT-sikkerhetsutvalgets anbefalinger i NOU 2018:14

1.1 Ny lov om IKT-sikkerhet

Vi forstår det slik at utvalgets anbefaling faller sammen med det som er høringens andre del, Regjeringens utkast til lov som gjennomfører NIS-direktivet i norsk rett. Vi kommer derfor med våre merknader til denne anbefalingen under dette punktet

1.2 . Krav om IKT-sikkerhet ved anskaffelser

Datatilsynet støtter et initiativ til at det skal stilles krav om IKT-sikkerhet ved anskaffelser

1.3 Nasjonalt IKT-sikkerhetssenter

Datatilsynet støtter ikke forslaget om å etablere et eget nasjonalt IKT-sikkerhetssenter. Vi betviler ikke behovet for koordinert informasjon og rådgiving innen IKT-sikkerhet, men bakgrunnen for at vi ikke stilles oss bak anbefalingen har utvalget selv pekt på; kompetanse innen IKT-sikkerhet er et knapphetsgode i Norge. Allerede innen dagens organisering av arbeid med IKT-sikkerhet må etablerte fagmiljø og etater konkurrere om de samme, knappe ressurser. Å etablere enda et nytt fagmiljø vil bety enda hardere konkurranse, og som mulig konsekvens at noen fagmiljø/etater ikke vil kunne skaffe den kompetansen de trenger for å føre tilsyn osv.

Utvalget peker på ulike samarbeidsarenaer som er etablert de siste årene i regi av NSM og Difi. Slike arenaer kan fungere etter hensikten uten å tappe de ulike sektorene for ressurser. Datatilsynet mener at et bedre forslag vil være at de ansvarlige departementene gir klare signaler om at denne type samarbeidsarenaer skal prioriteres, samt gir føringer på hvordan samarbeidsforaene formelt skal organiseres for å ha nødvendig legitimitet.

Istedenfor å planlegge et nytt fagmiljø mener Datatilsynet at det må satses på å styrke kompetansen innenfor IKT-sikkerhet og personvern i samfunnet generelt, og i porteføljen til høyere utdanning spesielt. Vi må utdanne flere IKT-sikkerhets eksperter.

Undersøkelser viser at enkeltpersoner har en forventning til at deres personvern og IKT-sikkerhet blir ivaretatt av virksomhetene som behandler deres personopplysninger, men at tillitten til virksomhetene er synkende.[1]

Datatilsynet mener at IKT-sikkerhet og personvern må inn i opplæringen allerede fra grunnskolen av, som en naturlig del av flere fag. Videre må man som et minimum ha IKT-sikkerhet inn som en obligatorisk del av utdanningen innenfor informatikk og andre IKT-fag. Vi anbefaler samtidig å se helhetlig på behovet for kunnskap om informasjonssikkerhet i all utdanning.

---

[1] Datatilsynets rapport *Personvern – tillit og følelser 2018*

1.4 Tingenes internet – ansvar og regulering

Datatilsynet stiller seg bak utvalgets analyse av dagens tilstand hva gjelder et økende antall enheter som blir koblet til internett og som uten krav til sikkerhet kan være en sikkerhetsmessig fare for både enkeltpersoner og virksomheter.

Utvalget foreslår at de myndigheter som har tilgrensende tilsynsmyndighet på området må samarbeide tettere. Dette gjelder Datatilsynet, Forbrukertilsynet, DSB og NKOM.

Datatilsynet har ved flere tilfeller søkt samarbeid med Forbrukerrådet, Forbrukertilsynet og NKOM i saksbehandling og veiledning som gjelder tilkoblede enheter. Erfaringsmessig er det svært nyttig å få flere perspektiver inn i denne type saker. Avgjørelsen av om slikt samarbeid skal søkes gjøres imidlertid fra sak til sak, så noen systematisk tankegang rundt dette har ikke vært på plass.

Datatilsynet har ingen erfaring med samarbeid med DSB. Forutsatt at DSB har, eller blir tilført, den kompetansen som skal til for å koordinere tilsyn, råd og veiledning på dette området er vi åpne for et slikt tiltak.

1.5 Styring og regulering fra departementsnivå

Datatilsynet støtter anbefalingen om å gjennomgå modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt. Vi opplever selv at det i for liten grad er politiske føringer og krav til samarbeid og koordinering på et strategisk/politisk og operativt nivå, og at det samarbeidet som er skyldes initiativ fra fagetatene og privat sektor.

Fra vår side hadde det vært ønskelig om det ble utpekt et ansvarlig departement og at dette departementet sørget for tett koordinering, og kunne bidra til mer strategisk og langsiktig tenkning på tvers av sektorer.

2 Merknader til utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer i norsk rett

2.1 Krav om høyt sikkerhetsnivå i felleskomponenter

Datatilsynet gav i 2016 en høringsuttalelse knyttet til en mulig implementering av samme direktiv. Som uttrykt den gangen mener vi fortsatt at det i hovedsak er positivt med et felles og sektorovergripende minstekrav til informasjonssikkerhet. Vi mener samtidig at det på dette området ikke alltid er flere regler som er løsningen. Mange små og mellomstore virksomheter har et ønske om å etterleve regelverket som gjelder IKT-sikkerhet, men savner tilrettelegging fra det offentlige for at det skal være enkelt for dem å gjøre nettopp det.

IKT-sikkerhetsutvalget er ikke de første som har kommet frem til at IKT-sikkerhetskrav fremstår som fragmenterte. I 2015 kom Digitalt sårbarhetsutvalg til samme konkusjon i sin utredning[2], og de pekte i tillegg på at ulike myndigheter har motstridene prioriteringer med hensyn til sikkerhet. Slik vi ser det handler kjernen i konflikten prinsipielt om forskjellig holdning til risikoaksept. I den ene enden finner vi miljøer hvor hovedprioriteten er å hindre uønskede hendelser. I den andre enden finner vi miljøer hvor hovedprioriteten er tilgjengeliggjøring og effektivisering gjennom digitalisering. Difi og NSM er nevnt som eksponenter for hver sin sikkerhetskultur.

Denne konflikten blir særlig problematisk når sikkerhetsnivå i felleskomponenter, som for eksempel Altinn og ID-porten, skal besluttes. Felleskomponentene er funksjoner som vi har valgt å sentralisere, og som mange virksomheter blir avhengige av. Dersom felleskomponenter som Altinn og ID-porten har dårlig sikkerhet går sårbarheten i arv til de mange som bruker den, og kan få konsekvenser for mange.

Brønnøysundregistrene har ansvaret for å forvalte Altinn og Difi er ansvarlig for drift av ID-porten. Digitalt sårbarhetsutvalg peker på at det er problematisk at offentlige etater alene bestemmer sikkerhetsnivået til felleskomponenter uten at det sikres at de totale verdiene blir tatt hensyn til. Datatilsynet er enig i denne analysen, og mener det er uforsvarlig å ikke regulere krav til sikkerhetsnivå for sentraliserte fellesfunksjoner. De løsninger og tjenester som skal ivareta større verdikjeder må underlegges et regelverk med tydelige krav til sikkerhetsnivå.

Norsk næringsliv består av 99% små og mellomstore virksomheter. De fleste av dem har et ønske om å etterleve regelverket som gjelder IKT-sikkerhet, men har knappe ressurser. Tilrettelegging fra det offentlige ved å sørge for et høyt sikkerhetsnivå i felleskomponenter vil være et tiltak som kan gjøre det enklere for disse virksomhetene å ivareta IKT-sikkerheten på sin side.

2.2 Hjemmel for behandling av personopplysninger må være mer presis

Når det gjelder lovteksten har vi merknader til § 6 som skal være hjemmel for behandling av personopplysninger for formål som inngår i loven. Vi kan ikke se at bestemmelsen er begrunnet og forklart i høringsnotatet, og etterlyser dermed en nærmere redegjørelse for hvordan den tilfredsstiller kravene i personvernforordningen.

Datatilsynet mener at bestemmelsens formulering er for lite presis til å fungere som rettslig grunnlag etter personvernforordningen. Det bør være klare referanser til de bestemmelsene i personvernforordningen som er ment å være grunnlaget for behandlingens lovlighet.

[2] NOU 2015: 13 Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden, pkt. 22.6.3

Vi antar at det for formålet å ivareta IKT-sikkerhet vil artikkel 6 (1) bokstav f og artikkel 9 (2) bokstav g være aktuelle referanser. Begge disse bestemmelsene forutsetter konkrete interesseavveiinger og at det er iverksatt egnede tiltak for å verne de registrertes grunnleggende rettigheter og friheter. Det bør fremgå klart hvilke vurderinger som er gjort av nødvendighet og forholdsmessighet, hvilke momenter som er vektlagt i interesseavveiingen og hvilke tiltak som er iverksatt som vern av grunnleggende rettigheter for de registrerte.

Vi stiller oss til rådighet dersom dere ønsker utfyllende informasjon eller har spørsmål til vårt høringssvar. Dere kan i så fall ta kontakt med Eirin Oda Lauvset på telefon 488 69 369.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO