Datatilsynet

Justis- og politidepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	11/00697-3/HVE	22. desember 2011

Supplerende høringsuttalelse - Forslag til politiregisterforskriften - Del I - Informasjonssikkerhet og internkontroll

Det vises til vår høringsuttalelse på politiregisterforskriftens del I av 18. oktober 2011 hvor det gikk frem at Datatilsynet ville komme med en supplerende uttalelse knyttet til forskriftens kapitler 39 og 40 om internkontroll og informasjonssikkerhet. Datatilsynet gir i det følgende sine merknader til disse kapitlene.

Som det fremgår av høringsnotatet har Datatilsynet igangsatt et revisjonsarbeid for personopplysningsforskriftens kapittel 2 og 3 om hhv. informasjonssikkerhet og internkontroll. Datatilsynet slutter seg til departementets merknad om at det er ønskelig at bestemmelsene i personopplysningsforskriften og politiregisterforskriften i størst mulig grad er harmonisert.

Kapittel 39 – Internkontroll
Som det fremgår av kommentarene til forskriftsutkastet ga Datatilsynet innspill ved utformingen av kapitlet om internkontroll om at dette burde utformes mer utfyllende enn tilsvarende regulering i personopplysningsforskriften, noe Departementet har hensyntatt.

Datatilsynet finner imidlertid at strukturen i kapittelet kan bedres vesentlig. Tilsynet legger derfor ved et forslag til omstrukturering av kapitlet. Omstruktureringen innebærer en flytting av innhold fra forslagets § 39-4 til foregående bestemmelser, og en strukturering av kapitlet i en innledende bestemmelse med påfølgende bestemmelser om styrende-, gjennomførende- og kontrollerende deler.

Kapittel 40 – Informasjonssikkerhet
Forslaget harmonerer med bestemmelsene i personopplysningsforskriften, og Datatilsynet har kun mindre kommentarer til foreslått § 40-13.

Bestemmelsen er en kombinasjon av personopplysningsforskriftens § 2-14 om sikkerhetstiltak og nytt materiell innhold om logging. Datatilsynet foreslår følgende justeringer til § 40-13:

- 2. ledd flyttes ned slik at det blir tredje ledd.
  Dette for å strukturere innholdet slik at sikkerhetstiltak generelt behandles først, deretter sporing spesielt

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

- 4. ledd foreslås endret til "Hver bruk av opplysningene skal registreres og kunne spores for å ...".
  Dette siden registrering faktisk skal finne sted, jf. foregående bestemmelser.

Nærmere om § 2-3 og forskriftens kapittel 40
Det vises generelt til våre kommentarer til § 2-3 i høringsuttalelse av 18. oktober.

§ 2-3 om delegering av det daglige ansvaret, 2. ledd omhandler delegering av det daglige behandlingsansvaret for informasjonssikkerhet til PDMT. Siden det her gis kommentarer til kapittel 40, gis det også enkelte tilleggskommentarer til § 2-3.

I kommentarene til kapittel 40[1] fremgår det at kapittel 40 "for alle praktiske formål retter seg til Politiets Data- og materielltjeneste (PDMT)...". Med bakgrunn i tidligere høringsuttalelse slutter ikke Datatilsynet seg til denne merknaden. Dette må også ses i lys av høringsnotatets kommentarer til § 2-3, hvor det understrekes at det faktiske ansvaret ligger hos den behandlingsansvarlige.

I foregående høringsuttalelse er det problematisert hvorledes kravene til sikkerhetsrevisjon vil forholde seg mellom behandlingsansvarlig og PDMT. Tilsvarene vil kravene i § 40-7 om personell (som blant annet innebærer kunnskap hos ansatte (opplæring)) vanskelig kunne ivaretas fullt ut av PDMT.

Bruk av logger i oppfølging av sikkerhetsrelaterte hendelser som har blitt aktualisert lokalt (eksempelvis mistanke om lekkasjer i en konkret sak), vil naturlig forutsette at det er lokal kompetanse og myndighet til å gjennomføre tiltak som følger av forskriftens § 2-13.

Som tidligere påpekt innebærer den uklare delegeringen i § 2-3 etter Datatilsynets syn en fare for mangelfull ivaretakelse av regelverkets krav.

Datatilsynet forstår at argumentasjonen for ikke å definere PDMT som databehandler dels baseres på at det innebærer, etter departementets syn, en uhensiktsmessig avtaleplikt. Datatilsynet mener at et tilsvarende avtalekrav følger etter § 40-14 om regulering av forholdet til leverandører og kommunikasjonspartnere hva gjelder informasjonssikkerhet. Dette underbygger at det er nødvendig å tydeliggjøre PDMTs rolle, og eventuelt tilpasse § 40-14 til dette.

Det bemerkes videre at en mulig løsning på utfordringene som følger av foreslått § 2-3 er å i større grad benytte forskriften til å sette rammer for forholdet mellom PDMT og de behandlingsansvarlige.

[1] Høringsnotatet kapittel 6.6, 3. avsnitt

Om behov er Datatilsynet tilgjengelig for dialog om utformingen av forskriften eller utdypning av merknadene her.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Helge Veum
senioringeniør

Kopi: Fornyings- administrasjons- og kirkedepartementet,
v/Statsforvaltningsavdelingen, Postboks 8004 Dep, 0030 OSLO

Vedlegg: Endringsforslag kapittel 39 - internkontroll