DATATILSYNET

Folketinget
Udvalgssekretariatet
Christiansborg
1240 København K

Sendt til: Birgitte.Toft-Petersen@ft.dk

29. august 2014

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2014-19-0041
Sagsbehandler
Maiken Christensen
Direkte 3319 3224

Vedrørende høring over beretning nr. 3

1. I e-mails af 26. juni 2014 har arbejdsgruppen vedrørende medieetik og medieansvar under Folketingets Kulturudvalg samt arbejdsgruppen om datasikkerhed under Folketingets Retsudvalg anmodet om bemærkninger til beretning nr. 3 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".

2. I den anledning kan Datatilsynet oplyse følgende:

2.1. Det fremgår af beretningen, at arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg konkret forventes at se på bl.a. eksternt tilsyn med overholdelse af gældende lovgivning, herunder Datatilsynets kompetencer og ressourcer, samt andre tilsynsorganer af relevans for området og behovet for eventuel oprettelse af nye organer.

Datatilsynet skal bemærke, at tilsynets opgavevaretagelse og medarbejdersammensætning i høj grad afspejler den lovgivning, der findes på området for persondatabeskyttelse. Således er langt størstedelen af tilsynets opgaver i dag lovbundne.

Datatilsynet har bl.a. følgende opgaver og funktioner:

- Generel vejledning og rådgivning af offentlige myndigheder og private vedrørende behandling af oplysninger
- Behandling af klagesager og sager, der tages op af egen drift
- Behandling af anmeldelser fra offentlige myndigheder, der behandler fortrolige oplysninger
- Behandling af ansøgninger om tilladelse fra private virksomheder mv., der behandler følsomme oplysninger
- Behandling af ansøgninger fra private virksomheder mv. om tilladelse til behandling af oplysninger i forbindelse med stillingsbesættende virksomhed, kreditoplysningsvirksomhed, advarselsregistre og retsinformationssystemer
- Behandling af ansøgninger om tilladelse til overførsel af oplysninger til tredjelande

- Udførelse af inspektioner hos offentlige myndigheder, private virksomheder, forskere mv.
- Afgivelse af udtalelse ved udarbejdelsen af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger
- Nationalt tilsyn med internationale informationssystemer, f.eks. den nationale del af Schengen Informationssystemet (SIS)
- Deltagelse i internationalt samarbejde, f.eks. i de fælles tilsynsmyndigheder nedsat i henhold til Schengen- og Europolkonventionerne og i EU-regi

Herudover har Datatilsynet opgaver i henhold til anden lovgivning. F.eks. modtager tilsynet anmeldelser i henhold til lov om massemediers informationsdatabaser. Endvidere er Datatilsynet Registertilsyn for Grønland og i forhold til rigsmyndighederne på Færøerne i medfør af de dér gældende registerlove.

Datatilsynet skal pege på, at overvejelser om en styrkelse af Datatilsynet ikke alene bør fokusere på omfanget af ressourcer, men også på indholdet af de opgaver, som Datatilsynet forventes at varetage.

Det kan f.eks. overvejes, om tilsynet fortsat i samme udstrækning som i dag skal udstede tilladelser til virksomheder, der behandler oplysninger, samt behandle anmeldelser fra offentlige myndigheder, der behandler fortrolige oplysninger som naturlig følge af deres myndighedsudøvelse.

Datatilsynet skal i øvrigt bemærke, at tilsynet udøver sine funktioner i fuld uafhængighed, jf. persondatalovens[1] § 56. Bestemmelsen har sin baggrund i databeskyttelsesdirektivets[2] artikel 28, stk. 1, 2. afsnit.

2.2. Af beretningen fremgår endvidere, at arbejdsgruppen vedrørende datasikkerhed under Folketingets Retsudvalg konkret forventes at se på bl.a.

- internt tilsyn, herunder sikkerhedsgodkendelse af personer med adgang til personfølsomme data, samt opdeling af medarbejdere i flere sikkerhedsniveauer, der regulerer adgangen til oplysninger
- muligheden for at stille yderligere krav til både offentlige og private dataansvarlige, herunder anvendelse af privacy by design, logning af opslag i registre, forbud mod unødvendig sammenkøring af oplysninger og lign.

Datatilsynet skal i den forbindelse bemærke, at for *offentlige myndigheder* er persondatalovens sikkerhedskrav nærmere udmøntet i sikkerhedsbekendtgørelsen[3] og sikkerhedsvejledningen[4].

---

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer

[2] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

Sikkerhedskravene for offentlige myndigheder omfatter – afhængigt af den konkrete behandling af personoplysninger – navnlig følgende:

- forpligtelsen til at fastsætte nærmere retningslinjer, der beskriver, hvordan de fornødne sikkerhedsforanstaltninger konkret er etableret i organisationen,
- kravet om instruktion af medarbejderne,
- kravet om skriftlige aftaler med eventuelle databehandlere til sikring af, at datasikkerheden lever op til persondataloven og sikkerhedsbekendtgørelsen, samt at den dataansvarlige påser dette,
- kravet om særlige retningslinjer ved adgang til personoplysninger ved brug af it-udstyr uden for den dataansvarliges lokaliteter (hjemmearbejdspladser og lign.),
- kravet om fysisk sikkerhed
- kravet om iagttagelse af de fornødne sikkerhedsforanstaltninger i forbindelse med reparation og service samt ved salg og kassation af anvendte datamedier,
- kravet om formel autorisationsprocedure, der sikrer, at kun personer, som autoriseres hertil, har adgang til personoplysninger, og at der kun autoriseres personer, for hvem adgangen er nødvendig som led i deres jobfunktion, at disse tildeles et individuelt personligt login, samt at den udstedte autorisation ændres eller lukkes ved medarbejderens fratræden eller flytning inden for organisationen,
- kravene om, at der ved transmission via internettet (eller andre åbne net) foretages en risikovurdering omfattende alle elementer i løsningen, at der implementeres de fornødne sikkerhedsforanstaltninger til imødegåelse af de foreliggende risici, herunder brug af kryptering, hvis fortrolige eller følsomme personoplysninger overføres via internettet (eller andre åbne net), og om sikring af sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger,
- kravet om kontrol med afviste adgangsforsøg, herunder blokering for yderligere forsøg efter et antal afviste adgangsforsøg samt
- kravet om registrering (logning) af alle anvendelser af personoplysninger.

I den *private sektor* er der ikke på samme måde fastsat mere præcise regler om behandlingssikkerheden. For den private sektor gælder derfor rammebestemmelsen i persondatalovens § 41, stk. 3.

Af denne bestemmelse fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger

---

[3] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

[4] Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Datatilsynet kan dog i forbindelse med udstedelse af tilladelser til behandling af personoplysninger hos private virksomheder mv. stille krav om, at der træffes konkrete sikkerhedsforanstaltninger. Det kan f.eks. være krav om autorisation og adgangskontrol og i enkelte tilfælde om registrering (logning) af alle anvendelser af personoplysninger.

Datatilsynet har endvidere på visse områder fastsat egentlige krav til datasikkerheden i den private sektor. Det gælder bl.a. ved overførsel af følsomme oplysninger via hjemmesider, hvor tilsynet stiller krav om kryptering.

2.3. Vedrørende den konkrete sag, der har givet anledning til nedsættelsen af arbejdsgrupperne, kan det oplyses, at Datatilsynet af egen drift har iværksat flere undersøgelser.

Datatilsynet blev via presseomtale den 28. april 2014 bekendt med, at Se og Hør angiveligt systematisk skulle have indsamlet og brugt oplysninger fra Nets (tidligere PBS) om kendte danskeres brug af kreditkort. Datatilsynet anmodede samme dag Se og Hør om en redegørelse til brug for tilsynets overvejelser om, i hvilket omfang der kan have været tale om behandling af personoplysninger i strid med persondataloven. Datatilsynet gjorde samtidig opmærksom på, at Se og Hør ikke var forpligtet til at afgive oplysninger, idet der kunne være risiko for, at der blev afgivet oplysninger om, at der var begået noget strafbart.

Aller Media A/S besvarede ved brev af 15. juli 2014 Datatilsynets henvendelse. Aller Media A/S oplyste, at Aller Media A/S er sigtet af politiet og derfor ikke ønsker at udtale sig til tilsynet.

På den baggrund har Datatilsynet oversendt sagen til Københavns Vestegns Politi med anmodning om, at spørgsmålet om eventuel overtrædelse af persondataloven i stedet inddraget i politiets sag mod Aller Media A/S.

Tilsynet har ligeledes af egen drift iværksat undersøgelser af SAS og Rigshospitalet (Region Hovedstaden), idet det af medieomtale er fremgået, at Se og Hør fra medarbejdere hos SAS og Rigshospitalet skal have modtaget oplysninger om kendte personer.

Sagerne vedrørende Rigshospitalet og SAS er på nuværende tidspunkt endnu ikke afsluttede hos Datatilsynet.

Det bemærkes, at Datatilsynet er bekendt med, at Finanstilsynet undersøger forholdene hos Nets og i den forbindelse har indhentet en redegørelse fra Nets. På den baggrund har Datatilsynet på nuværende tidspunkt ikke iværksat en selvstændig undersøgelse af Nets.

Se og Hør-sagen har i øvrigt affødt en henvendelse til Datatilsynet fra Danske Medier om mediernes anmeldelse til tilsynet af redaktionelle informationsdatabaser, ligesom tilsynet har modtaget et stort antal af sådanne anmeldelser fra danske massemedier.

2.4. Datatilsynet skal afslutningsvis bemærke, at der i beretningen flere gange anvendes begrebet "personfølsomme oplysninger".

Datatilsynet kan i den forbindelse oplyse, at begrebet "personfølsomme oplysninger" ikke anvendes i persondataloven eller i tilsynets praksis.

I persondataloven findes begrebet "personoplysninger". Det dækker alle typer af oplysninger om personer, både følsomme og ikke-følsomme oplysninger.

Følsomme oplysninger er de oplysninger, som er nævnt i persondatalovens §§ 7-8, herunder f.eks. helbredsoplysninger og oplysninger om strafbare forhold. En betalingsoplysning vil normalt ikke være en følsom oplysning, men vil som udgangspunkt være omfattet af reglerne i lovens § 6 om almindelige ikke-følsomme oplysninger.

Personnummer er heller ikke en følsom oplysning efter persondataloven, men det er en oplysning, der nyder en særlig beskyttelse efter persondatalovens § 11.

Datatilsynet skal på den baggrund foreslå, at der i arbejdsgruppernes videre arbejde – bl.a. for at undgå tvivlsspørgsmål i relation til persondataloven – anvendes en terminologi svarende til persondatalovens, herunder at der som overordnet begreb anvendes betegnelsen "personoplysninger".

3. Datatilsynet står naturligvis til rådighed, hvis det videre arbejde skulle give anledning til konkrete spørgsmål af persondataretlig karakter eller spørgsmål om tilsynets virksomhed.

Med venlig hilsen

Birgit Kleis
Kst. direktør