

Planlagte tilsyn indtil udgangen af 2018

Datatilsynet er den centrale uafhængige myndighed, der fører tilsyn med, at reglerne om databeskyttelse bliver overholdt. Vores arbejdsfelt er bredt og varieret og spænder fra at vejlede og rådgive til at behandle klagesager og ansøgninger om tilladelse til at behandle personoplysninger, ligesom vi også hvert år gennemfører forskellige typer af tilsyn hos myndigheder og virksomheder og deltager i bl.a. det fælles europæiske samarbejde om databeskyttelse.

Når det gælder de forskellige typer af tilsyn, så foretager Datatilsynet hvert år et antal planlagte tilsyn, hvor vi i første omgang finder frem til, hvilke temaer og myndigheder/virksomhedsbrancher tilsynene skal dække, og herefter finder vi så frem til de enkelte dataansvarlige, som skal være genstand for vores tilsyn. Vi tager hvert år også altid et antal ekstra sager op på eget initiativ (ad hoc tilsyn) som følge af konkrete hændelser. I 2018 har vi således indtil videre taget 27 sager op til behandling, efter at vi bl.a. var blevet kontaktet af journalister, bekymrede borgere mv.

Når det gælder de planlagte tilsyn, har Datatilsynet indtil udgangen af i år valgt at fokusere på følgende temaer:

- Behandlingsgrundlag og persondatasikkerheden hos private virksomheder
- Sletning af personoplysninger hos private virksomheder
- Anvendelse af databehandlere hos kommunerne
- Persondatasikkerheden i større it-systemer på sundhedsområdet
- Udpegning af databeskyttelsesrådgiver – offentlige myndigheder og en række private virksomheder
- Udarbejdelse af en fortegnelse hos kommunerne
- De registreredes rettigheder efter retshåndhævelsesloven
- Databehandlingsaktiviteter i forhold til en række EU-informationssystemer

Nærmere om baggrunden for de enkelte temaer

Behandlingsgrundlag og persondatasikkerheden hos private virksomheder

I tiden frem mod den 25. maj 2018, hvor databeskyttelsesforordningen¹ begyndte at finde anvendelse i Danmark og resten af EU, og hvor samtidig den danske databeskyttelseslov² afløste persondataloven, oplevede tusindvis af danskere at få fyldt deres indbakker med e-mails fra navnlig private virksomheder, der under henvisning til de nye databeskyttelsesregler enten bad om et (fornyet) samtykke til fortsat at kunne behandle personoplysninger eller gerne ville orientere om indholdet af deres persondatasikkerhedspolitik. Spørgsmålet er imidlertid, om indholdet af disse e-mails i alle tilfælde var og er i overensstemmelse med databeskyttelsesreglerne og anden relevant lovgivning som f.eks. markedsføringsloven.

¹ Europa-Parlamentets og Rådets forordnings (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

² Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

Datatilsynet har derfor besluttet – i et samarbejde med Forbrugerombudsmanden – at undersøge dette nærmere hos en række private virksomheder. Fokus vil især være rettet mod en datingside og et par kundeklubber hos private virksomheder.

Sletning af personoplysninger i private virksomheder

Ét af de grundlæggende principper for behandling af personoplysninger i databeskyttelsesforordningen er, at virksomheder ikke må behandle personoplysninger længere end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Det vil med andre ord sige, at når personoplysningerne ikke længere er nødvendige for virksomheden, skal denne sørge for, at oplysningerne slettes. Reglen bidrager til at sikre mod en unødvendig ophobning af oplysninger. En sådan ophobning indebærer nemlig principielt altid en vis forøget risiko for krænkelse af de registrerede, f.eks. ved at oplysninger kommer uvedkommende i hænde.

Sletning af oplysninger har været et stort tema i perioden op til 25. maj i år. Datatilsynet ønsker derfor at følge op på, om private virksomheder har fået styr på deres sletterutiner, således at de sletter personoplysninger, når der ikke længere er grundlag for at opbevare dem. Datatilsynet har for at kontrollere dette besluttet at føre tilsyn med sletning hos en hotelkæde, en møbelkæde og et taxaselskab.

Persondatasikkerheden i større it-systemer på sundhedsområdet

Når Datatilsynet vælger at fokusere netop på sundhedsområdet, så skyldes det, at myndighederne på dette område er blandt de myndigheder herhjemme, som behandler flest følsomme personoplysninger. Myndighederne på sundhedsområdet skal sikre, at disse data opbevares, så de ikke kommer til uvedkommendes kendskab, men også at de er tilgængelige og pålidelige, så patienter kan få den rette behandling til den rette tid.

Datatilsynet har derfor besluttet at føre en række tilsyn med persondatasikkerheden i offentlige myndigheders it-systemer på sundhedsområdet, hvor der bl.a. anvendes ny teknologi. Datatilsynet vil derfor bruge disse tilsyn til at få indblik i, om de udvalgte myndigheder passer på borgernes (følsomme) personoplysninger, og om de gør det godt nok.

Udpegning af databeskyttelsesrådgiver

Databeskyttelsesforordningen stiller krav om, at alle offentlige myndigheder og visse private virksomheder skal udpege en databeskyttelsesrådgiver (kaldes ofte også DPO, som er den engelske forkortelse for Data Protection Officer). Efter forordningen skal den dataansvarlige eller databehandleren endvidere offentliggøre kontaktoplysninger for databeskyttelsesrådgiveren og meddele disse til Datatilsynet.

Databeskyttelsesrådgiverens funktion er bl.a. at understøtte, at myndigheden eller virksomheden overholder databeskyttelsesreglerne. Herudover har databeskyttelsesrådgiveren en særlig stilling i forhold til Datatilsynet, idet databeskyttelsesrådgiveren er kontakttled til og skal samarbejde med Datatilsynet.

Det er således meget vigtigt, at alle offentlige myndigheder og alle relevante virksomheder har sørget for at få udpeget de databeskyttelsesrådgivere, som de er forpligtede til.

Hertil kommer, at de nordiske datatilsyn på et møde den 7.-8. maj 2018 aftalte, at man vil gennemføre et fælles tilsynsinitiativ i forhold til, om alle offentlige myndigheder har udpeget en databeskyttelsesrådgiver.

Initiativet er nærmere omtalt i den "København-erklæring", der var resultatet af mødet, og som kan læses [her](#).

På baggrund af ovennævnte har Datatilsynet besluttet, at der skal føres tilsyn med, om alle offentlige myndigheder og en række private virksomheder har udpeget en databeskyttelsesrådgiver og meddelt kontaktoplysninger på denne til Datatilsynet.

Anvendelse af databehandlere hos kommunerne

Det er meget vigtigt for bl.a. persondatasikkerheden, at der bliver indgået de fornødne databehandler-aftaler. Dette skyldes, at det netop er i databehandleraftalen, at det skal fastslås, hvilken sikkerhed der skal være hos databehandleren.

Endvidere er det meget vigtigt, at den dataansvarlige påser, at databehandleren rent faktisk lever op til det aftalte. Dette er også nødvendigt for at leve op til databeskyttelsesforordningens krav om ansvarlighed, hvorefter en dataansvarlig skal kunne påvise, at en behandling af personoplysninger er i overensstemmelse med reglerne i databeskyttelsesforordningen.

Datatilsynet gennemførte i 2016 en række tilsyn med, om kommuner, regioner og statslige myndigheder havde indgået de fornødne databehandleraftaler med deres databehandlere, og om de i tilstrækkeligt omfang påså persondatasikkerheden hos deres databehandlere. I den forbindelse kunne Datatilsynet konstatere, at der var store udfordringer i forhold til at leve op til kravene. I februar 2018 har Datatilsynet udarbejdet en skabelon til en standard-databehandleraftale, ligesom tilsynet i maj 2018 har offentliggjort en ny vejledende tekst om tilsyn med databehandlere og underdatabehandlere.

Datatilsynet har derfor besluttet igen i år at føre tilsyn med en række kommuners anvendelse af databehandlere. Vi har i den forbindelse en forhåbning om, at ovennævnte skabelon og vejledende tekst fører til, at resultaterne af tilsynene bliver mere positive, end hvad der var tilfældet med tilsynene fra 2016. Årets tilsyn er således også en opfølgning på de tidligere konstaterede udfordringer.

Kommunernes fortegnelser

Som noget nyt, stiller forordningen krav om, at alle dataansvarlige og databehandlere fører interne fortegnelser over deres behandling af personoplysninger. Fortegnelseskravet skal ses som en forlængelse af databeskyttelsesforordningens øgede fokus på ansvarlighed ("accountability").

Denne ansvarlighedstanke indebærer for det første, at den dataansvarlige – og i visse tilfælde databehandleren – har ansvaret for at efterleve forordningens regler. For det andet, skal den dataansvarlige også kunne påvise, at de behandlinger, som denne har ansvaret, for lever op til forordningens regler. Fortegnelseskravet skal således ses som en naturlig indgangsvinkel til at kunne løfte denne opgave.

Ved at føre en fortegnelse får den dataansvarlige og databehandlerne et overblik over de behandlinger, som er iværksat. Et sådant overblik er en nødvendig forudsætning for at kunne overholde en række forpligtelser i databeskyttelsesforordningen, såsom: overvejelser om, hvilke oplysninger man kan behandle, håndtering af indsigtsbegæring og anmeldelser af brud på persondatasikkerheden. Fortegnelseskravet er i vidt omfang udtryk for, at den dataansvarlige og databehandleren skal dokumentere de overvejelser, som de i medfør af forordningens øvrige regler i forvejen skal gøre sig.

Datatilsynet har besluttet at føre tilsyn med, om udvalgte kommuner har de påkrævede fortegnelser. Kommunerne vil derfor blive bedt om at indsende deres fortegnelser til Datatilsynet, som herefter vil gennemgå fortegnelserne og stille supplerende spørgsmål til kommunernes behandling af personoplysninger.

Registreredes rettigheder efter retshåndhævelsesloven

Den 30. april 2017 trådte retshåndhævelsesloven³ i kraft i Danmark. Loven gælder for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Datatilsynet har valgt at føre tilsyn med, om udvalgte retshåndhævende myndigheder overholder reglerne om de registreredes rettigheder, hvilket f.eks. kunne være oplysningspligten og indsigtsretten.

Internationale tilsyn

På en række særlige områder er Datatilsynet udpeget som tilsynsmyndighed og deltager derfor også i internationalt samarbejde herom. Det drejer sig om:

- Schengen-informationssystemet (SIS), hvor Datatilsynet fører tilsyn med behandlingen af informationer om efterlyste personer, savnede personer og personer, der er nægtet indrejse til Schengen-området
- Visuminformationssystemet (VIS), hvor Datatilsynet fører tilsyn med behandlingen af informationer om visumansørgeres fingeraftryk og ansigtsbilleder
- EU-fingeraftryksregisteret (Eurodac), hvor Datatilsynet fører tilsyn med behandlingen af oplysninger om asylansørgeres fingeraftryk
- Toldinformationssystemet (CIS), hvor Datatilsynet fører tilsyn med behandlingen af informationer i den danske del af det fælleseuropæiske toldinformationssystem.

Datatilsynet vil derfor i 2018 også gennemføre en række internationale tilsyn, herunder i forhold til visse EU-informationssystemer.

³ Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer.