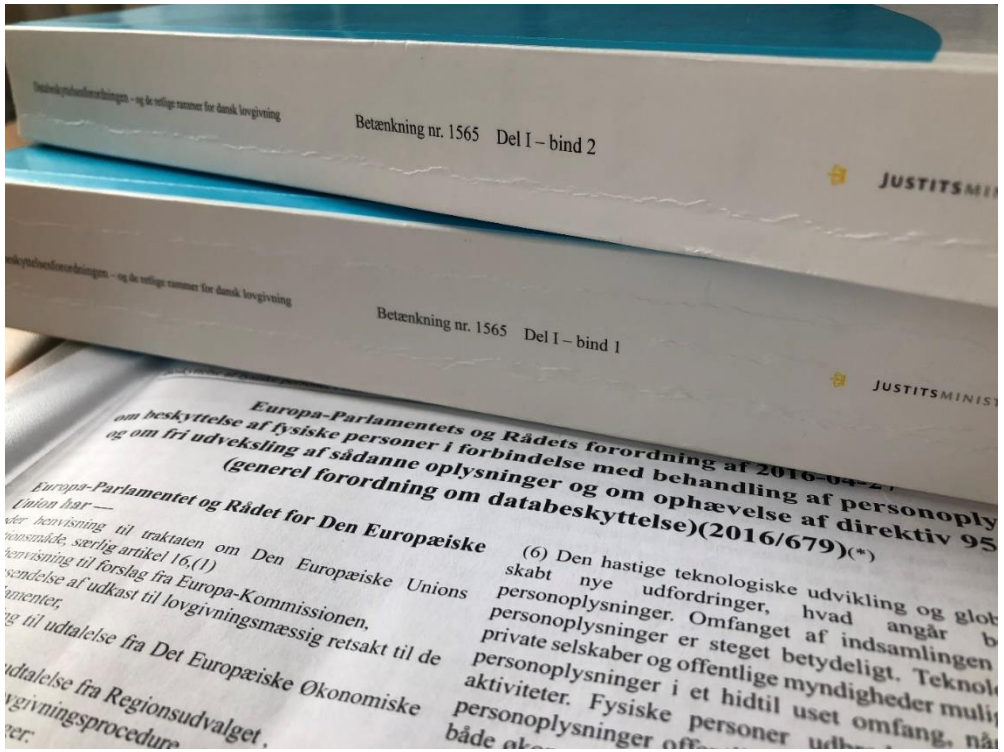
DATATILSYNET

Når Datatilsynet banker på Databeskyttelsdagen 2019

IT-sikkerhedsspecialist & cand.jur. Allan Frank
Datatilsynet
17. januar 2019

Nyt fra Datatilsynet



Forordningen kom !
Og hvad skete der så ?

DATATILSYNET

Dejligt travlt ☺

- Som det tidligere er sagt:
- En ca. 4 dobling af sagsantallet
- Mange nye personer i berøring med området
- Ca. 3500 anmeldelser om sikkerhedsbrud siden 25. maj

Hvad er det for nogle sikkerhedsbrud ?

Altovervejende

- menneskelige fejl
    - fejlindtastninger
    - klippe klistre fejl
    - manglende fjernelse af peronoplysninger ved ”anonymisering”
    - autocorrect/autocomplete
    - flettebreve
    - diverse fejl 40

DATATILSYNET

Tekniske fejl teknisk sikkerhed

- dårlig kode
- URL'er hvor person oplysninger (telefon, cpr-nummer el. lign.) er en del af en offentliggjort URL
- manglende kryptering
- manglende validering af brugere
- manglende patchning
- Ingen eller kun dårligt konfigureret firewall
- manglende hærdning af eksponerede komponenter
- "test"systemer med livedata
- manglende segmentering af netværk/krydscontaminering

RISIKOVURDERINGER!!

- Forretningsindragelse af forskellige kompetencer.

Få dem på plads de giver hele organisationen et billede af den eksponering der er, plus hvor der skal sættes ind.

DATATILSYNET

En Tilgang der virker

- Databeskyttelses livscyklus
- Risikobaseret tilgang
- Med udgangspunkt i forretningsudvikling tænk holistisk

- Generelt, artikel 24
- Konsekvensanalyse, artikel 35
- Høring af Datatilsynet, artikel 36
- Databeskyttelse gennem design, artikel 25, stk. 1
- Databeskyttelse gennem standard indstillinger, artikel 25, stk. 2
- Behandlingssikkerhed, artikel 32
- Anmeldelse af brud, artikel 33
- Underretning, artikel 34

DATATILSYNET

Datatilsynets tilsynsvirksomhed

Hvem og hvad har DT ført tilsyn med i efteråret 2018

Tilsyn vedr. behandlingssikkerhed:

- Region Hovedstaden: Sundhedsplatformen - behandlingssikkerhed
- Region Sjælland: Sundhedsplatformen - behandlingssikkerhed
- Arp-Hansen Hotel Group A/S: Sletning
- Taxa 4x35: Sletning
- IDdesign A/S: Sletning

Juridiske tilsyn:

- Den Uafhængige Politiklage-myndighed: Registreredes rettigheder efter retshåndhævelsesloven
- Auditørkorpset: Registreredes rettigheder efter retshåndhævelsesloven
- Dating.dk ApS: Behandlingshjemmel og sikkerhed
- Matas A/S - Club Matas og tilhørende underklubber: Behandlingshjemmel og sikkerhed
- Gyldendal A/S - bogklubber: Behandlingshjemmel og sikkerhed
- Varde Kommune: Fortegnelsen
- Holstebro Kommune: Fortegnelsen
- Ringkøbing-Skjern Kommune: Fortegnelsen

DATATILSYNET

Datatilsynets tilsynsvirksomhed

Hvem og hvad har DT ført tilsyn med i efteråret 2018

Juridiske tilsyn fortsat:

- Randers Kommune: Anvendelse af databehandlere
- Viborg Kommune: Anvendelse af databehandlere

Internationale tilsyn:

- SIS (Schengen Informations System)
- VIS (Visa Informations Systems)

DPO-tilsyn:

- Alle ministerier (departementer), kommuner, regioner samt seks privathospitaler (Aleris Hamlet Hospitaler A/S, Aleris Hamlet Hospitaler Ringsted A/S, Capio CFR A/S, GHP Gildhøj Privathospital ApS, Kysthospitalet Skodsborg A/S og Privathospitalet Danmark A/S): Udpegelse af databeskyttelsesrådgiver

Datatilsynets tilsynsvirksomhed

Generelt om typer af tilsyn og antal

- Tilsyn kan ske ved oplysningsindsamling , egentlige tilsynsbesøg og kombinationer deraf. Herudover har det også karakter af en slags tilsyn, når DT behandler klager.

- Hjemmel: Databeskyttelsesforordningens artikel 58 (beføjelser) og databeskyttelseslovens § 29 =) kan ”kræve enhver oplysning” og ”har adgang til alle lokaler” (uden retskendelse). Hvis konkret mistanke =) selvinkriminering (private)

- Nyt at Datatilsynet har fået generel adgang til at udføre tilsynsbesøg hos alle private -) er blevet indtænkt.

- Forordningen indeholder regler om fælles tilsyn -) andre datatilsyn kan f.eks. bede Datatilsynet om at foretage tilsyn hos en dansk virksomhed og kan også i vist omfang deltage i et sådan tilsyn.

- Antal: Datatilsynet vil bestræbe sig på – under hensynstagen til tilsynets ressourcer – at gennemføre så mange tilsyn som muligt. Tilsyn bliver prioriteret!

Datatilsynets tilsynsvirksomhed

Hvordan forløber et planlagt tilsyn typisk

- **Tilsyn ved oplysningsindsamling (fx DPO tilsynene)**
  - Spørgeskemaer
  - Eventuelle supplerende spørgsmål (dialog)
  - Endelig udtalelse – eventuelt kombineret med politianmeldelse, påbud, forbud mv.
  - Eventuel opfølgning på afgørelse

- **Fysisk tilsyn**
  - Typisk varsling 4 uger før tilsynsbesøget
  - Varsling ofte suppleret med anmodning om oplysninger
  - Fysisk besøg – samtale og besigtigelse
  - Referat til gennemsyn
  - Endelig afgørelse – eventuelt kombineret med politianmeldelse, påbud, forbud mv.
  - Eventuelt opfølgning på afgørelse

Datatilsynets tilsynsvirksomhed

Hvad bliver der typisk fokuseret på ved udvælgelsen af tilsynsemner?

- Områder hvor der har vist sig at være udfordringer (f.eks. påseelse af sikkerhed hos databehandlere)
- Datatilsynets ”sorte bog” (henvendelser fra borgere og medier mv.)
- Geografi (skal være hele DK’s datatilsyn).
- Om dataansvarlige behandler følsomme oplysninger i stort omfang (f.eks. kommuner, regioner mv.)
- Behandlinger som indebærer brug af nye teknologier

Datatilsynets tilsynsvirksomhed

Hvad bliver der typisk fokuseret på ved udvælgelsen af tilsynsemner?

- Ubekendt faktor: De fælles europæiske tilsyn -) hvor mange anmodninger vil der komme om sådanne? Indtil videre ikke modtaget nogen.

- Nyt at Datatilsynet får en generel adgang til at foretage tilsyn hos alle private -) indgår i overvejelserne -) nye muligheder.

Datatilsynets tilsynsvirksomhed

Mulige konsekvenser af et tilsyn

- Der er med forordningen lagt op til, at overtrædelser skal sanktioneres.

- Vil som noget nyt kunne opleve, at tilsyn kan resultere i politianmeldelse og eventuel bøde (formentlig både til private virksomheder og offentlige myndigheder). Der vil formentlig blive indgivet politianmeldelse i forbindelse med nogle af efterårets tilsyn.

- Ellers fortsat kritik og offentliggørelse på Datatilsynets hjemmeside.

Datatilsynets tilsynsvirksomhed

Læren af efterårets tilsyn (indtil videre)

- Det er DT's indtryk, at det er kommet bag på nogen, at man skal kunne dokumentere, at man rent faktisk lever op til reglerne. Dette følger af forordningens artikel 5, stk. 2, og artikel 24.

- Det er med andre ord ikke tilstrækkeligt, at man kan fremlægge en fin persondatapolitik man skal også efterleve politikken i praksis og kunne dokumentere dette.

- *Eksempel*: Hvis man har fastsat en slettefrist til 2 år, vil det blive kontrolleret, om man rent faktisk har slettet efter 2 år.

Datatilsynets tilsynsvirksomhed

Læren af efterårets tilsyn (indtil videre)

- *Eksempel:* Hvis man siger, at man baserer en behandling på et samtykke, vil det blive kontrolleret, om man rent faktisk har et gyldigt samtykke.

- *Eksempel:* Man kan blive bedt om at redegøre for, hvordan data, der udveksles mellem- og benyttes af flere forskellige it-systemer, stadig er retvisende ved de transformationer og dataudvekslinger der sker systemerne imellem (Sundhedsplatformen) v vil fx kunne efterprøves ved en it-teknisk gennemgang af datamodeller, services og ved konkrete stikprøver.

Datatilsynets tilsynsvirksomhed

Ny tilsynsplan på vej

- Ny tilsynsplan for foråret/sommeren 2019 forventes offentliggjort (emner) ultimo januar eller primo februar.

- Et pt. under udarbejdelse.

DATATILSYNET

??????????????????????????

Spørgsmål