



CJUK

## Domstolsstyrelsens årsberetning 2015 - persondataloven

### 1. Persondatalovens anvendelsesområde for de danske domstole

Persondataloven – lov nr. 429 af 31. maj 2000 med senere ændringer – har som hovedformål at sikre, at personoplysninger ikke misbruges eller kommer til uvedkommendes kendskab. Loven gælder for alle behandlinger af personoplysninger, der foretages ved elektronisk databehandling, eller som indeholdes i et register.

Loven finder som udgangspunkt anvendelse på alle domstolenes sagsområder, bortset fra visse bestemmelser på det strafferetlige område.

Persondataloven gælder ikke for Færøerne og Grønland. Den færøske persondatalov gælder kun for myndigheder, som er under Færøernes hjemmestyreordning. For rigsmyndighederne på Færøerne, herunder retsvæsnets, gælder således registerloven, der også gælder for Grønland. Det er her Datatilsynet, som fungerer som registertilsyn.

Det fremgår af persondatalovens § 68, stk. 3, at Domstolsstyrelsen offentliggør en årlig beretning om sin virksomhed.

### 2. Domstolsstyrelsens tilsynsopgave

Domstolsstyrelsens kompetence som tilsynsmyndighed er reguleret i persondatalovens §§ 67 og 68. Det følger heraf, at Domstolsstyrelsen fører tilsyn med domstolenes behandlinger af personoplysninger på det administrative område og med overholdelsen af sikkerhedsreglerne både på det judicielle og det administrative område. Tilsynet omfatter også tinglysningssystemet.

Domstolsstyrelsen tilser både af egen drift og efter klage fra en registreret, at den behandling af persondata, der finder sted i forbindelse med domstolenes administrative opgaveløsning, er i overensstemmelse med persondataloven, sikkerhedsbekendtgørelsen<sup>1</sup> og øvrige sikkerhedsforskrifter, herunder øvrig lovgivning samt interne sikkerhedsinstrukser.

Hvis en borger klager over en domstolsbehandling af personoplysninger, træffer domstolen derimod selv afgørelse, når det drejer sig om det *judicielle* område. Domstolens afgørelse kæres til højere ret. Kære sker efter de almindelige regler i retsplejeloven, med en kærefrist på 4 uger.

---

<sup>1</sup> Bkg. nr. 535 af 15/06/2000, Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene

Domstolsstyrelsens tilsynsopgave svarer til den opgave, som Datatilsynet udfører med hensyn til den offentlige forvaltning og det private erhvervsliv. Med udgangspunkt i den sammenlignelige opgave søger Domstolsstyrelsen så vidt muligt at tilrettelægge tilsynsopgaven efter samme retningslinjer, som Datatilsynet fastlægger for sin tilsynsvirksomhed.

### **3. Vejlednings- og tilsynsvirksomheden**

Domstolsstyrelsen lægger vægt på at komme i dialog om databeskyttelsesretlige spørgsmål med såvel de dataansvarlige retter som eksterne databehandlere, der driver et it-system eller på anden måde arbejder for domstolene. Dette gælder også Danmarks Domstoles eget it-center, der udvikler og driver domstolenes sagsbehandlingssystemer.

Domstolsstyrelsens tilsynsvirksomhed udgør således ikke kun en kontrolforanstaltning, men er et væsentligt værktøj i det løbende samarbejde mellem styrelsen og de enkelte retter om at sikre et højt databeskyttelsesniveau i Danmarks Domstole. Domstolsstyrelsen kan således yde generel vejledning til lovforklaring m.v. til retterne, men kan ikke skrive konkrete vejledninger for retterne.

Domstolsstyrelsen har i 2015 gennemført tilsynsbesøg ved Retten på Bornholm, Retten i Roskilde, Retten i Odense, Retten i Holstebro og Retten i Herning.

En konkret henvendelse eller klage over rettens persondatabehandling kan efter omstændighederne udløse et uanmeldt tilsynsbesøg, men udgangspunktet er, at Domstolsstyrelsen afholder anmeldte tilsynsbesøg. Styrelsen har i denne forbindelse en løbende dialog med den ret, besøget vedrører, både før og efter besøget.

I det omfang private databehandlere servicerer domstolenes it-systemer, vil Domstolsstyrelsen kunne foretage tilsynsbesøg hos disse. På samme måde vil der konkret kunne foretages tilsynsbesøg i Danmarks Domstoles eget Center for IT. I udviklingsarbejdet rådgives it-centret så vidt muligt forud for pilotdrift af nyudviklede applikationer, for eksempel brugerstyringsprogrammer og sagsbehandlingsprogrammer.

Et ordinært tilsynsbesøg ved retterne tager normalt udgangspunkt i retternes indberetninger i forbindelse med den årlige informationsindsamling til ledelsesinformation for informationssikkerhed, ligesom der tages særligt udgangspunkt i de krav, som sikkerhedsbekendtgørelsen stiller til behandlingen af personoplysninger.

Der foretages således blandt andet en drøftelse af retternes nærmere fastsatte lokale bestemmelser om sikkerhedsforanstaltninger i overensstemmelse med sikkerhedsbekendtgørelsens § 5, herunder om etablering af en lokal sikkerhedsorganisation og administration af f.eks. autorisationsordninger. Ligesom der sker en indgående drøftelse af organisering af autorisationsordninger, som reguleres i sikkerhedsbekendtgørelsens § 17. Herudover drøftes særligt retternes brug af e-mail og anvendelsen af krypterede mails ved følsomme eller fortrolige oplysninger.

Ovenstående opstilling over emner, som drøftes på et tilsynsbesøg, er ikke udtømmende, da de resterende krav i sikkerhedsbekendtgørelsen og retternes sikkerhedshåndbog ligeledes gennemgås. Ligesom det enkelte embede også har mulighed for selv at tage emner op, som de ønsker drøftet på et tilsynsbesøg.

Et tilsynsbesøg afsluttes som oftest med, at de tilsynsførende får en rundvisning i retsbygningen, hvor særlige fysiske udfordringer i forhold til behandling af personoplysninger drøftes.

Et tilsynsbesøg afsluttes altid med en afrapportering fra tilsynsmyndigheden til det besøgte embede, hvor eventuelle mangler påpeges.

#### Anmeldelse af domstolenes behandling af fortrolige oplysninger

Domstolenes behandling af fortrolige oplysninger skal anmeldes til Domstolsstyrelsen jf. persondataloven § 52.

Behandlingen af personoplysninger ved domstolene foretages som altovervejende hovedregel på samme måde og ved anvendelse af ens it-systemer.

Domstolenes behandlingsanmeldelser er som følge heraf forholdsvis ensartede, og langt den største del af anmeldelserne er foretaget på grundlag af de standarder, som Domstolsstyrelsen har udarbejdet. Domstolsstyrelsen arbejder på at opdatere de nuværende standardanmeldelser.

#### Sikkerhedspolitik

Danmarks domstoles sikkerhedshåndbog, der bygger på DS484, trådte i kraft den 1. juli 2007. Domstolsstyrelsen igangsatte implementeringen af ISO27001 i 2015 som følge af regeringens beslutning om, at alle statslige institutioner skal anvende denne internationale standard i stedet for DS 484.

Det betyder, at Danmarks Domstole overgår til at have en mere ledelsesforankret og risikobaseret tilgang til informationssikkerheden. Det medfører blandt andet, at sikkerhedshåndbogen løbende vil blive opdateret, f.eks. når det besluttes, at uacceptable risici helt eller delvis skal reduceres ved en adfærdsregulering.

#### Generelle og konkrete sager

Nedenfor er gengivet nogle af de sager, som Domstolsstyrelsen har behandlet i løbet af året.

#### *Fremsendelse af personoplysninger til fejladressat*

I efteråret 2015 kom det frem, at det ved tre retskredse i Midt- og Vestjylland var sket fremsendelse af personoplysninger til forkerte adressater. Der var i alle tilfælde tale om beklagelige menneskelige fejl som førte til, at de berørte retskredse overvejede og gennemgik deres interne arbejdsgange for at sikre, at lignende episoder ikke vil opstå igen. Alle de berørte parter i sagerne blev i overensstemmelse med god data-behandlingskik underrettet om episoderne.

Som følge af episoderne foretog Domstolsstyrelsen to ekstraordinære tilsynsbesøg ved to af de berørte retter, hvor der var særligt fokus på behandlingssikkerheden, herunder arbejdsgange og procedurer i forbindelse med afsendelse af fysisk og elektronisk post.

#### *Offentliggørelse af uanonymiserede retslistes*

Et embede blev opmærksomt på, at de ved en fejl ikke have anonymiseret en retsliste, inden denne blev lagt på rettens hjemmeside. Dette medførte, at de tiltaltes navne i straffesager lå tilgængelige på rettens hjemmeside i en kort periode. I overensstemmelse med god databehandlingskik underrettede retten de berørte om episoden. Retten har oplyst, at der var tale om en menneskelig fejl, men har taget episoden til efterretning.

#### *Oplysning om anklage i straffesag til uvedkommende*

En borger klagede over, at en byret ved en fejl have givet oplysninger om vedkommendes indblanding i en straffesag til et af hendes familiemedlemmer. Retten fandt, at der var sket en meget beklagelig fejl i rettens sagsbehandling af sagen, og fandt at der var grundlag for at udbetale godtgørelse for tort.

#### **4. Oversigt over visse love, bekendtgørelser og vejledninger**

- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
- Bekendtgørelse nr. 532 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for domstolene.
- Bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene.
- Bekendtgørelse nr. 546 af 18. juni 2004 som ændret ved bekendtgørelse nr. 1005 af 6. oktober 2006 og nr. 770 af 23. juni 2010 om retslistes og om massemediernes aktindsigt i og opbevaring af kopier af anklageskrifter og retsmødebegæringer m.v.
- Cirkulæreskrivelse af 23. september 2003 om vilkår for offentliggørelse af domsresumeér på hjemmesider.
- Retningslinjer af 15. maj 2009 om anvendelsen af e-mail og internet.
- Domstolsstyrelsens generelle vejledning af februar 2006 om persondataloven.
- Domstolsstyrelsens vejledning af februar 2006 om anmeldelsesordningen m.v. inden for domstolsområdet efter persondataloven.
- Domstolsstyrelsens vejledning af februar 2006 om de registreredes rettigheder efter persondataloven.