STYRELSEN FOR
PATIENTSIKKERHED

Databeskyttelsesforordningen – gammel vin på nye flasker?

eSundhedsobservatoriet 2017

Birgitte Drewes, Kontorchef, Styrelsen for Patientsikkerhed

11. oktober 2017

Gammel vin på nye flasker?

- I høj grad videreførelse af gældende regler (ISO 27001, persondatalov og sikkerhedsbekendtgørelse)

Men

- Større ansvar for databehandlere
- Større fokus på dokumentation
- Tungere sanktioner
  - Offentlige myndigheder stadig uafklaret

Ny vejledning pr. 10. oktober 2017:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/Captia_Generel_informationspjece__formateret___DOK446249_.pdf

Hvornår finder forordningen anvendelse?

- Stadig automatisk behandling af oplysninger (og manuelle registre)
- Dataansvarlig etableret i Danmark og behandling indenfor EU, men også
  - Udbud af varer eller tjenester til personer i Danmark
  - Overvågning af personers adfærd i Danmark
- Offentlige: Ikke rigets sikkerhed, ikke strafferetten
- Private: Ikke rent private aktiviteter

Hvad er personoplysning?

- Stadig enhver form for information, der kan henføres til bestemte personer
- Stadig sondring
  - Almindelige oplysninger
  - Oplysninger om strafbare forhold
  - Følsomme oplysninger
    - Race eller etnisk oprindelse
    - Politisk, religiøs eller filosofisk overbevisning
    - Fagforeningsmæssigt tilhørsforhold
    - Genetiske data
    - Biometriske data med det formål entydigt at identificere en fysisk person
    - Helbredsoplysninger
    - Seksuelle forhold eller seksuel orientering
- CPR-numre stadig fortrolige, men lagt op til lempelse ift. privates brug, jf. § 11 i lovforslag

Hvad er behandling af personoplysninger?

- Som i dag: Enhver håndtering af personoplysninger.
  - Indsamling
  - Registrering
  - Systematisering
  - Opbevaring
  - Søgning
  - Brug
  - Videregivelse
  - Sletning
  - Osv.
- Husk: enkeltmandsvirksomheder er stadig også personer

Hvem er dataansvarlig hhv. databehandler?

- Dataansvarlig: Stadig den der afgør
  - Hvilke data?
  - Hvilke formål?
  - Hvordan?
  - Hvor længe?
- Databehandler: Stadig den, der handler efter instruks fra den dataansvarlige

Hvad er behandling af personoplysninger?

- Som i dag: Enhver håndtering af personoplysninger.
    - Indsamling
    - Registrering
    - Systematisering
    - Opbevaring
    - Søgning
    - Brug
    - Videregivelse
    - Sletning
    - Osv.

Betingelser for at behandle personoplysninger

- Stadig
  - Lovlighed, rimelighed og gennemsigtighed
  - Formålsbegrænsning
  - Dataminimering
  - Rigtighed
  - Opbevaringsbegrænsning
  - Integritet og fortrolighed

- NB: Samtykke
  - Nye særlige regler for børn
  - Offentlige myndigheder ikke bero alene på samtykke

Den registreredes rettigheder

- Stadig oplysningspligt (der behandles oplysninger)
    - NB: kan begrænses af ressourcemæssige hensyn
- Stadig indsigtsret
- Stadig rettelse/sletning
    - NB: nye regler om sletning/"retten til at blive glemt".
    - NB: særlige regler offentlige myndigheder.
    - NB: retten til at blive glemt trumfer ikke fx journalpligt
- Dataportabilitet – krav på at tage eget indhold med sig
    - NB: Gælder ikke ved myndighedsudøvelse

- Vejledning kommer primo 2018

Behandlingssikkerhed

- ”Betryggende og passende niveau” ift. den konkrete risiko
- Konsekvensanalyse (”Privacy Impact Assessment”) før igangsættelse af høj risiko aktiviteter
  - Nogle tilfælde pligt til at høre Datatilsynet
- Skal tænkes med fra start – ”Privacy by design and default”
- Underretningspligt
  - Dataansvarlig => Datatilsynet
  - Databehandler => Dataansvarlig

Artikel 29 gruppen har udgivet vejledning om DPIA

Men er der slet ikke noget nyt?

- Dokumentationskrav udtrykkelige
  - Hvis det ikke er dokumenteret, findes det ikke
- Anmeldelsessystemet nedlægges
  - I stedet dataansvarlig og databehandler føre fortegnelser (minder om fællesanmeldelser)
- Konsekvensanalyser nye som pligt
  - Artikel 29 gruppe vejledning
- Databeskyttelsesrådgiver (DPO) hos offentlige myndigheder og visse private
  - Artikel 29 gruppe vejledning & Datatilsyns vejledning
- Selvstændigt ansvar for databehandler
- Adfærdskodekser & certificering
  - Skal udvikles

Så gammel vin på nye flasker?

- Kendt smag
- Spædet op
- Vil udvikle sig over tid…

Tjekliste – kan I svare på og dokumentere følgende?

- Kender I forordningen?
- Hvilke personoplysninger behandler I (datastrømme)?
- Hvilken information giver I den registrerede?
- Hvordan opfylder I den registreredes rettigheder (sagsgange)?
- Hvad er jeres hjemmel/lovgrundlag til at behandle oplysningerne?
- Hvordan indhenter I samtykke?
- Behandler I oplysninger om børn?
- Hvordan håndterer I sikkerhedsbrud?
- Medfører jeres behandling særlige risici for den registrerede?
- Tænker I databeskyttelse ind i systemerne?
- Hvem har ansvaret for databeskyttelse hos jer?
- Driver I virksomhed i flere lande – og har I styr på reglerne om data over grænser?

Gode links

Ny vejledning pr. 10. oktober 2017 (opdateres i foråret 2018, når ny persondatalov vedtaget):

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/Captia_Generel_informationspjece__formateret___DOK446249_.pdf

12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf

Betænkningen fra Justitsministeriet om forordningen og forslag til ny persondatalov (for den særligt interesserede):

http://jm.schultzboghandel.dk/publikationer/publikationsdetaljer.aspx?PId=d4caa501-e175-4859-945e-74fe990460f2

http://www.hoeringsportalen.dk/Hearing/Details/60828

Artikel 29 gruppens vejledninger: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Tak for opmærksomheden

Spørgsmål?

Birgitte Drewes – bidr@sst.dk