Dansk Epidemiologisk Selskabs årsmøde og generalforsamling – den 27. og 28. april 2017

SUNDHEDSDATA-
STYRELSEN

Håndhævelse af databeskyttelsesforordningen – udvalgte highlights

v/chefkonsulent Anja Sofie Nielsen

Sidste gang……

Materielle regler (behandlingsregler)	Sikkerhed	Databehandlere	Registreredes rettigheder
Samme behandlingsregler (stort set – mulighed for at fastsætte nationale regler for alle behandlingsartikler)	Risikobaseret tilgang	Kun anvende databehandlere, der kan stille fornødne garantier…	Samme pligter og rettigheder (stort set)
MEN: Videreførsel af persondatalovens § 10? Artikel 9, stk. 4	Ingen anmeldelse (men mulighed for at fastsætte særregler herom), dog konsekvensanalyse og mulig høring af tilsynsmyndighed	Krav til indhold af databehandleraftale	Udvidelse: Indsigelsesret, artikel 21
MEN: Samtykke-kravet ses skærpet (artikel 4, nr. 11)	Data Protection Officer (DPO) og data protection by design and by default	Skærpelse af selvstændigt ansvar	MEN: Mulighed for at fastsætte fravigelser fra rettigheder
MEN: Private dataansvarlige og forskning i art. 10-opl.?	Underretningspligt af tilsynsmyndighed ved brud på datasikkerheden	Underretningspligt til dataansvarlig hvis brud på sikkerhed mv.	Underrettes ved brud på persondatasikkerheden, artikel 34
Derudover: Yderligere krav til forsknings- og statistik i artikel 89	Politikker, procedurer, dokumentation	Også krav om DPO	(Afdøde er ikke omfattet af databeskyttelsesforordningen – præambel 27)

Highlight 1 – brug af forskningsdata

Persondataloven

- § 6-oplysninger (almindelige oplysninger):
  - Samtykke
  - Behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse
- §§ 7 og 8-oplysninger (følsomme og semi-følsomme oplysninger):
  - Samtykke
- § 10, stk. 1:
  - §§ 7 og 8-oplysninger må behandles, hvis dette **alene** sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne

Databeskyttelsesforordningen

- Artikel 6 (almindelige oplysninger):
  - Samtykke
  - Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse….
- Artikel 9 (særlige kategorier af personoplysninger):
  - Samtykke
  - Behandling er nødvendig til …. Videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-rettelsen eller medlemsstaternes nationale ret
- Medlemsstaterne kan opretholde eller indføre nye betingelser for behandling af bla. helbredsoplysninger…

Highlight 1 – brug af forskningsdata

Persondataloven

- § 10, stk. 2:
  - De af stk. 1 omfattede oplysninger (dvs. §§ 7 og 8-oplysningerne) **må ikke senere behandles i andet end statistiske eller videnskabeligt øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed, jf. §** 6.
- § 10, stk. 3:
  - De af stk. 1 og 2 omfattede oplysninger må kun videregives til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden. Tilsynsmyndigheden kan stille nærmere vilkår for videregivelsen.

Databeskyttelsesforordningen

- Præambel 159:
  - "…Hvis resultatet af videnskabelig forskning navnlig inden for sundhed giver grund til yderligere foranstaltninger i den registreredes interesse, **bør de generelle regler i denne forordning finde anvendelse med henblik på disse foranstaltninger.**"

Highlight 1 – brug af forskningsdata

Persondataloven

Databeskyttelsesforordningen

- Præambel 162:
  - "….Ved statistiske formål forstås enhver indsamling og behandlingen af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater. Disse statistiske resultater kan videreanvendes til forskellige formål, herunder videnskabelige forskningsformål. **Det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personoplysninger, men aggregerede data, og at dette resultat eller personoplysningerne ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer**."

Highlight 2 – Data Protection Officer (DPO)

- Nye vejledninger fra artikel 29-gruppen
  - **Guidelines on Data Protection Officers ('DPOs') – vejledning om databeskyttelsesrådgivere**
  - Guidelines on the right to data portability – vejledning om dataportabilitet
  - Guidelines for identifying a controller or processor's lead supervisory authority – vejledning om identificering af den ledende tilsynsmyndighed

- Hvad er artikel 29-gruppen?
  - Arbejdsgruppe nedsat i medfør af databeskyttelsesdirektivet (95/46/EF af 24. oktober 1995)
  - Et rådgivende og uafhængigt nævn med repræsentanter fra bl.a. medlemsstaternes tilsynsmyndigheder m.fl.
  - Holder jævnligt møder i Bruxelles, hvor de vedtager henstillinger, udtalelser og notater, der bl.a. bliver offentliggjort på nettet.
  - Disse er ikke juridisk forpligtende, men de har betydelig indflydelse på retsudviklingen og er en vigtig retskilde

Highlight 2 – Data Protection Officer (DPO)

- Guidelines on Data Protection Officers ('DPOs') - vejledning af 13. december 2016, revideret og endeliggjort den 5. april 2017
  - Vedrører databeskyttelsesforordningens artikel 37 – 39:
    - Udpegelse af en DPO
    - DPO'ens stilling
    - DPO'ens opgaver

- Artikel 37, stk. 1, litra a: Obligatorisk at udpege en DPO, hvis man er en offentlig myndighed eller et offentligt organ (undtagen domstolene)
  - En virksomhed, der varetager offentligretlige tjenester eller som arbejder på offentligretligt grundlag, kan også være underlagt kravet om en DPO

- Artikel 37, stk. 1, litra b: Hvis kerneaktiviteten består af behandlingsaktiviteter, der kræver regelmæssig og systematisk overvågning af registrerede i stort omfang
  - Hvad er en kerneaktivitet?
  - Hvad er stort omfang?

Highlight 2 – Data Protection Officer (DPO)

- Artikel 37, stk. 1, litra c: Hvis kerneaktiviteten består af behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, og personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10.
  - Kerneaktiviteten igen…
  - Stort omfang….?

- I vejledningen står følgende om kerneaktivitet (core activities):
  - ”Core activities can be considered as the key operations necessary to achieve the controller´s or processor’s goals. **However, ‘core activities’ should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller’s or processor’s activity.**
  - For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing heath data, such as patients’ health records. Therefore, processing these data should be considered to be one of any hospital’s core activities and hospitals must therefore designate DPOs.”

Highlight 2 – Data Protection Officer (DPO)

- I vejledningen står følgende om stort omfang (large scale):
  - "….the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
    - The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
    - The volume of data and/or the range of different data items being processed
    - The duration, or permanence, of the data processing activity
    - The geographical extent of the processing activity

- Vejledningen kommer (heldigvis) med eksempler på hvad der er "stort omfang" – her udvalgte eksempler:
  - processing of patient data in the regular course of business by a hospital
  - processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
  - processing of personal data for behavioural advertising by a search engine
  - processing of data (content, traffic, location) by telephone or internet service providers

Highlight 2 – Data Protection Officer (DPO)

- Vejledningen kommer også med eksempler på, hvad der ikke er "stort omfang":
  - "processing of patient data by an individual physician
  - processing of personal data relating to criminal convictions and offences by an individual lawyer"

- Behandling af personoplysninger på hospitaler =
  - + stort omfang
  - + krav om DPO

- Behandling af personoplysninger af de enkelte praktiserende læger =
  - ÷ stort omfang
  - ÷ krav om DPO

- Hvad med forskere? Hvad med eksempelvis Kræftens Bekæmpelse?

Highlight 2 – Data Protection Officer (DPO)

- Artikel 37, stk. 5: Databeskyttelsesrådgiveren udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og –praksis samt evne til at udføre de opgaver, de er omhandlet i artikel 39.

  - Det er ikke defineret, hvilke faglige kvalifikationer DPO'en skal have, men følgende fremgår af vejledningen:
  - "Relevant skills and expertise include:
    - expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
    - understanding of the processing operations carried out
    - understanding of information technologies and data security
    - knowledge of the business sector and the organisation
    - ability to promote a data protection culture within the organization"
    - Der udbydes mange kurser, så man kan blive klædt på til rollen som DPO
  - Af vejledningen fremgår det, at personlige kvalifikationer også bør inddrages ved udpegelsen: "Personal qualities should include for instance integrity and high professional ethics."

Highlight 2 – Data Protection Officer (DPO)

- Artikel 37, stk. 6: Databeskyttelsesrådgiveren kan være den dataansvarliges eller databehandlerens medarbejder eller kan udføre hvervet på grundlag af en tjenesteydelseskontrakt
  - Intern DPO: Klar adskillelse af opgaver og ingen interessekonflikter
  - Man må godt bruge en ekstern DPO – igen klar adskillelse af opgaver og ingen interessekonflikter

- Artikel 37, stk. 7: Den dataansvarlige eller databehandleren offentliggør kontaktoplysninger for databeskyttelsesrådgiveren og meddeler disse til tilsynsmyndigheden
  - Kontaktoplysningerne skal være tilgængelige internt og eksternt
- Det fremgår af vejledningen, at man bør dokumentere beslutningen om udpegelse af en DPO
- Det fremgår også af vejledningen, at hvis man frivilligt beslutter at udpege en DPO, så gælder reglerne om en DPO også denne (bordet fanger)

Highlight 2 – Data Protection Officer (DPO)

- Artikel 38: DPO'ens stilling
  - En DPO skal kunne agere uafhængigt
    - Så man er ikke underlagt noget over/underordnelsesforhold i forhold til opgaven som DPO
  - En DPO skal inddrages i alle sager (og i alle stadier af en sag) vedrørende databeskyttelse, og det skal gøres rettidigt
  - DPO'ens rådgivning skal altid gives relevant vægt, og hvis man er uenig i rådgivningen, bør man dokumentere, hvorfor man ikke har fulgt DPO'ens råd
  - En DPO skal altid underrettes ved et brud på datasikkerheden o.lign.
  - En DPO skal have de fornødne ressourcer til at kunne udføre sit arbejde
    - Aktiv støtte fra "senior management"
    - Nok tid
    - Kontinuerlig efteruddannelse
    - Det kan lige frem være nødvendigt med et helt team alt afhængig af størrelsen og strukturen af organisationen
  - Man kan ikke blive fyret eller "straffet" for at have udført sit job som DPO
    - Straffet kan også være udelukkelse af goder, som andre medarbejdere får, ingen lønstigning mv. Trusler herom er også nok

Highlight 2 – Data Protection Officer (DPO)

- Artikel 39: Databeskyttelsesrådgiverens opgaver
  - Underretning og rådgivning af dataansvarlig eller databehandler om deres forpligtelser i helhold til forordningen og anden EU-ret eller national ret om databeskyttelse
  - Overvåge overholdelsen af forordningen, anden EU-ret eller national ret
  - At rådgive om konsekvensanalyser – når der anmodes herom – og overvåge dens opfyldelse i henhold til artikel 35
  - At samarbejde med tilsynsmyndigheden, herunder at fungere som dennes kontaktpunkt

Highlight 2 – Data Protection Officer (DPO)

- Præambel 97 kommer også krav til DPO'en:
  - "Hvis behandling foretages af en offentlig myndighed [.....], **bør en person med ekspertise i databeskyttelsesret og -praksis bistå den dataansvarlige eller databehandleren med at overvåge den interne overholdelse af denne forordning**."

- Vejledningen kommer med eksempler på, hvad denne interne overvågning især kan bestå af:
  - Samle oplysninger for at identificere databehandlingsaktiviteter
  - Analysere og kontrollere compliance med databehandlingsaktiviteter
  - Informere, rådgive og udstede anbefalinger til den dataansvarlige eller databehandleren

Highlight 2 – Data Protection Officer (DPO)

- Rent praktisk kan en DPO rådgive om:
  - Hvorvidt en konsekvensanalyse vedrørende databeskyttelse efter artikel 35 skal udføres og måden denne udføres på
  - Hvilke sikkerhedsforanstaltninger der kan implementeres for at "dæmme op" for identificerede risici
  - Hvorvidt konsekvensanalysen er udført rigtigt, og hvorvidt konklusionerne er forenelige med forordningen

- Hvis ansvar er det at leve op til forordningen?
  - DPO'ens?
  - Den dataansvarliges eller databehandlerens?
    - **Det er den dataansvarliges og databehandlerens ansvar…..**

Mange tak for jeres opmærksomhed!

Spørgsmål?

Kontakt mig gerne ved opfølgende spørgsmål:

Anja Sofie Nielsen
Chefkonsulent, cand.jur.
Compliance, Informationssikkerhed og Internationale relationer - Direktionssekretariatet
Sundhedsdatastyrelsen
Ørestads Boulevard 5, 2300 København S
www.sundhedsdata.dk

E: asni@sundhedsdata.dk
T: +45 3268 9232
M: +45 2552 8186

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk