ADVODAN

# Aktuel GDPR-praksis


## Karsten Holt, advokat og certificeret databeskyttelses-rådgiver, CIPP/E, CIPM, CIPT, FIP
## formand for Fagudvalget for Databeskyttelse


24. august 2022

# Agenda

Temaer:

- Behandlingssikkerhed, herunder
  - Kryptering
  - Adgangsbegrænsning – internt og eksternt
  - Multifaktor login
- Dataminimering
- Sletning: Strukturerede og ustrukturerede data
- Oplysningspligt ctr. Tavshedspligt
- Kontrol med databehandlere
- Interne compliance-kontroller
- Awareness-træning

# Behandlingssikkerhed - kryptering

Kryptering af e-mails med følsomme/fortrolige oplysninger:

- Minimum TLS, ver. 1.2
- Forced TLS nødvendigt
- Ved større mængder persondata/mange registrerede er TLS ikke nok - brug end-to-end kryptering

Kryptering af USB-nøgler:

- Data må ikke udveksles på USB-nøgler (eller andet mobilt device), hvis der ikke er effektiv kryptering på

Passwords skal altid opbevares krypteret

# Behandlingssikkerhed - adgangsbegrænsning

*”En advokat kan dele fortrolige oplysninger med advokater og andre, der er beskæftiget i samme advokatfirma som advokaten, hvis det åbenbart er i klientens interesse. ”*
*(Advokatetiske regler, artikel 17)*

Overvej adgangsbegrænsning internt i firmaet – evt. på sagstyper:

- I advokatsystemet
- På minretssag.dk

Hvor tit tjekkes adgangsrettighederne?

Deling eksternt kræver som hovedregel klientens samtykke (undtaget retslig forpligtelse eller åbenbar almeninteresse)

# Behandlingssikkerhed – Multifaktor login (MFA)

En ekstra faktor – f.eks. NemID, sms-kode, ansigtsgenkendelse mv. Anbefalet af CfCS siden sommeren 2021 på alle systemer med følsomme eller fortrolige oplysninger, der kan tilgås eksternt (f.eks. Fra bærbar eller mobil)

I nylig afgørelse har Datatilsynet indstillet et advokatfirma til bøde på 500.000 kr. for manglende MFA i forbindelse anmeldt databrud (hackerangreb). Elementer i begrundelse:

1. Mange oplysninger, som kræver særlig beskyttelse
2. Høj risiko for de registrerede (klienterne)
3. Fjernadgange stiller krav om særlige foranstaltninger, f.eks. MFA

# Dataminimering

Eksempel: bilag til retssag

- Kun det for sagen relevante skal med
- Vær opmærksom på, hvordan sletning/anonymisering foregår rent teknisk (anvendes PDF-editor, så tjek, at maskeringen ikke han fjernes eller at metadata ikke afslører oprindeligt indhold, f.eks. links – afgørelse Finanstilsynet, whistleblowerordning)

Eksempel: Lejeroplysninger ved opfyldelse af tilbudspligt (afgørelse vedr. boligselskab – Privatbo)

# Sletning

- Er der slettepolitik for advokatsystemet mv.? (strukturerede data) – og gennemføres det konsekvent?
- Hvad kan gemmes aht. andre pligter (f.eks. interessekonflikttjek) – og hvor længe?
- Slettepolitik for mailsystemet (ustrukturerede data) – anbefales kraftigt (undgå dobbeltopbevaring)
- Øvrige opbevaringssteder; fildrev, intranet mv. – fastsæt retningslinjer (afgørelser)

# Oplysningspligt ctr. tavshedspligt

- Overfor klienten – klares ofte med hjemmeside/e-mail-signatur
- Overfor modparter – hvornår og hvor meget/lidt? – afgrænsning aht. tavshedspligten
- Overfor tredjeparter – bipersoner og parter

Meget lidt afklaring på dette område

- Enkelt afgørelse om oplysningspligt ifm. advokatundersøgelse (TV2/Norrbom Vinding)

# Kontrol med databehandlere

Vejledning fra Datatilsynet i oktober 2021

- Pointsystem til risikovurdering (1-10 point tildeles ud fra antal registrerede samt typen af oplysninger – følsomme og fortrolige)
- 6 tilsynskoncepter
- Årligt tilsyn på de mest centrale databehandlere (ofte IT-revisionserklæring)

Det skal dokumenteres, at der er foretaget risikovurdering af alle databehandlere, der skal lægges en tilsynsplan – og den skal følges

# Interne compliance-kontroller

Artikel 30-fortegnelser, risikovurderinger, politikker og retningslinjer skal være på plads

MEN det er mindst lige så vigtigt, at der føres kontrol med, at reglerne de facto efterleves – og kontrollerne skal dokumenteres, f.eks.:

- Kontrol af sletning
- Kontrol af adgangsrettigheder
- Kontrol af lagring af data på drev mv.

# Awareness

**Sidst, men ikke mindst:**

HUSK at medarbejderne regelmæssigt skal trænes i korrekt håndtering af persondata.

Gennemfør regelmæssig undervisning, og dokumentér den, herunder deltagelse

ADVODAN

# Spørgsmål?