SIXTUS

COMPLIANCE

Agenda

- Databehandleraftaler – Do’s and Dont’s
- Certificeringer – Hvis man er Databehandler
- Audits og Inspektioner - Hvis man er Dataansvarlig
- Organisatorisk og Teknisk understøttelse af krav i en DBA

SIXTUS
COMPLIANCE

7 GRUNDPRINCIPPER FOR GDPR

GDPR pålægger alle organisationer, der tilbyder varer og tjenester til mennesker i EU, nye forpligtelser, uanset hvor virksomheden ligger.

Her er de 7 nøgleprincipper vedr. indsamling og lagring af data under GDPR.

1. Lovlighed, rimelighed og gennemsigtighed

Data skal behandles lovligt og retfærdigt og på en gennemsigtig måde.

Databehandler

2. Rigtighed

De indsamlede data skal være præcise og fri for fejl.

Dataansvarlig

3. Klart kommunikeret

Formålet og den tilsigtede anvendelse af data, skal være tydeligt specificeret for personerne og indsamlet med deres udtrykkelige godkendelse.

Dataansvarlig

4. Specifikt og relevant

Indsaml kun relevante data, der er specifikke for den tilsigtede anvendelse.

Dataansvarlig

5. Sikker opbevaring

Personlige oplysninger om personer eller brugere skal opbevares sikkert og i krypteret format.

Databehandler

6. Integritet og fortrolighed

Personlige oplysninger skal holdes fortrolige, og dataintegriteten skal opretholdes.

Dataansvarlig Databehandler

7. Den dataansvarliges ansvar

Den dataansvarlige skal være ansvarlig for sikkerheden for brugernes personlige data.

Dataansvarlig

Hvem styrer data?
Den part, der indsamler og bruger dataene

Dataansvarlig

Hvem behandler data?
Den part, der behandler data på vegne af den ansvarlige

Databehandler

Databehandleraftaler – Do’s and Dont’s

7 vigtige punkter i en DBA

- Databehandleren's Instruks
- Hvilken underdatabehandlere benyttes der
- Overførsler til 3. lande og Int. Organisationer
- Registreredes rettigheder og henvendelser
- Databrud
- Sikkerhed omkring behandlingen
- Tilsyn med databehandlere

Vi tager fremadrettet udgangspunkt i Datatilsynets Databehandlerskabelon.

https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/vejledninger-i-pdf-format

7 vigtige punkter i en DBA

- Databehandleren's Instruks i Bilag A

  •Formålet med behandlingen
  •Karakteren af behandlingen
  •Typer af personoplysninger
  •Kategorier af registrerede
  •Varighed af behandlingen

7 vigtige punkter i en DBA

Hvilken underdatabehandlere benyttes der til behandling af data – Afsnit 7, Bilag B og C
Man kan overveje at lave en liste der har følgende info.

- Typen af personoplysninger der er omfattet
- Mængden af personer (cirka tal), der behandles oplysninger om
- Geografisk lokation, underdatabehandlerens hjemland og hostingland
- Underdatabehandlerens mulighed for at ændre eller tilføje nye underunderdatabehandlere
- Tilsynsmuligheder med underdatabehandleren
- Underdatabehandlerens overblik over egne tekniske og organisatoriske sikkerhedsforanstaltning

Dette er overvejelser, men mindre kan gøre det.

Kontrol Spørgsmål!

Hvad sker der hvis vi behandler data der ikke er beskrevet i databehandleraftalen?

1. Vi bliver data ansvarlige
2. Der kan være tale om et databrud
3. Vi har pligt til at melde det

Kort sagt – Stop behandlingen, undersøg det sammen med den dataansvarlige og opdater aftalen om nødvendigt

7 vigtige punkter i en DBA

Overførsler til 3. lande og Int. Organisationer

- Dette kan være overførsler internt til moder eller datterselskab uden for EU/EØS
- Hosting uden for EU
- Man må ikke overføre data uden en instruks fra den dataansvarlige
- Lokaliteter skal fremgå af Bilag C afsnit 5
- Instruksen skal fremgå af Bilag C afsnit 6
- Overførsler skal have et grundlag som kan være via en SCC med en TIA og evt. ekstra sikkerhedsforanstaltninger

7 vigtige punkter i en DBA

Registreredes rettigheder og henvendelser

- Som databehandler skal man kunne bistå den dataansvarlige med henvendelser
  - F.eks. Retten til indsigt, sletning osv.

- Der er en liste over pligterne i afsnit 9 pkt 1.

- Her kan man inkludere en instruks f.eks. en mailadresse man kan skrive til, eller hvilken oplysninger der skal med ved en henvendelse.

7 vigtige punkter i en DBA

Databrud!

- Man skal bistå den dataansvarlige ved en hændelse
- Er man i tvivl oplyser man om det alligevel
- Det er en dataansvarliges ansvar at melde til DT.
- Husk eventuelle deadlines!
- Forpligtelserne er beskrevet i afsnit 6, punkt 3 og afsnit 9, punkt 2
- Afsnit 10 definere en specifik tidsramme for hvornår man skal underrette den dataansvarlige.

BRUG JERES RÅDGIVER ELLER DPO

7 vigtige punkter i en DBA

Sikkerhed omkring behandlingen

- I Bilag C afsnit 2 tages der stilling til sikkerhedsniveauet ved behandlingen
- Ofte listes et minimum af tekniske og organisatoriske krav til databehandleren.
- Man kan også selv udfylde den, men sørg for at den passer med virkeligheden.
- Være opmærksom på ublu krav!

7 vigtige punkter i en DBA

Tilsyn med databehandleren

- Vigtigt og ofte glemt punkt.
- Beskriver hvordan man skal føre tilsyn med jer, som databehandler
- Kig på de 6 tilsynskoncepter i DT's vejledning om tilsyn med databehandlere
- Bilag C afsnit 7 beskriver tilsynsmulighederne.

Vigtigt at man kontrollere om man kan understøtte kravene og ikke bare underskriver for at få kunden i hus.

Do's and Dont's

- Brug jeres rådgiver eller DPO
- Læs aftalen igennem og vurder om man kan leve op til kravene.
- Forhandl om nødvendigt, evt. via jeres rådgiver eller DPO.
- Lad være med at lukke øjnene og bare skrive under.
- Sørg altid for at Datatilsynets skabelon bliver brugt.
- Lov ikke mere end i kan holde.
- Forsøg ikke at have for mange forskellige aftaler

Certificeringer

Certificeringer

Kig I Datatilsynets vejledning for tilsyn med databehandlere

- Oftest brugt er ISAE3000
- ISO27001 kan også bruges.
- ISAE3402 kan en sjælden gang bruges.
- ISO og SOC/2 er oftest brugt I udlandet
- D-Mærket
- Uafhængig rådgiver inspektion, IT Sikkerhedsinspektion….kært barn har mange navne
- Disse skal I også selv indsamle når I inspicerer jeres underdatabehandlere.

- Nogle virksomheder sender også spørgeskemaer ud, med alt fra 3 til 200 spørgsmål.

Teknisk og organisatorisk understøttelse

Teknisk Implementering

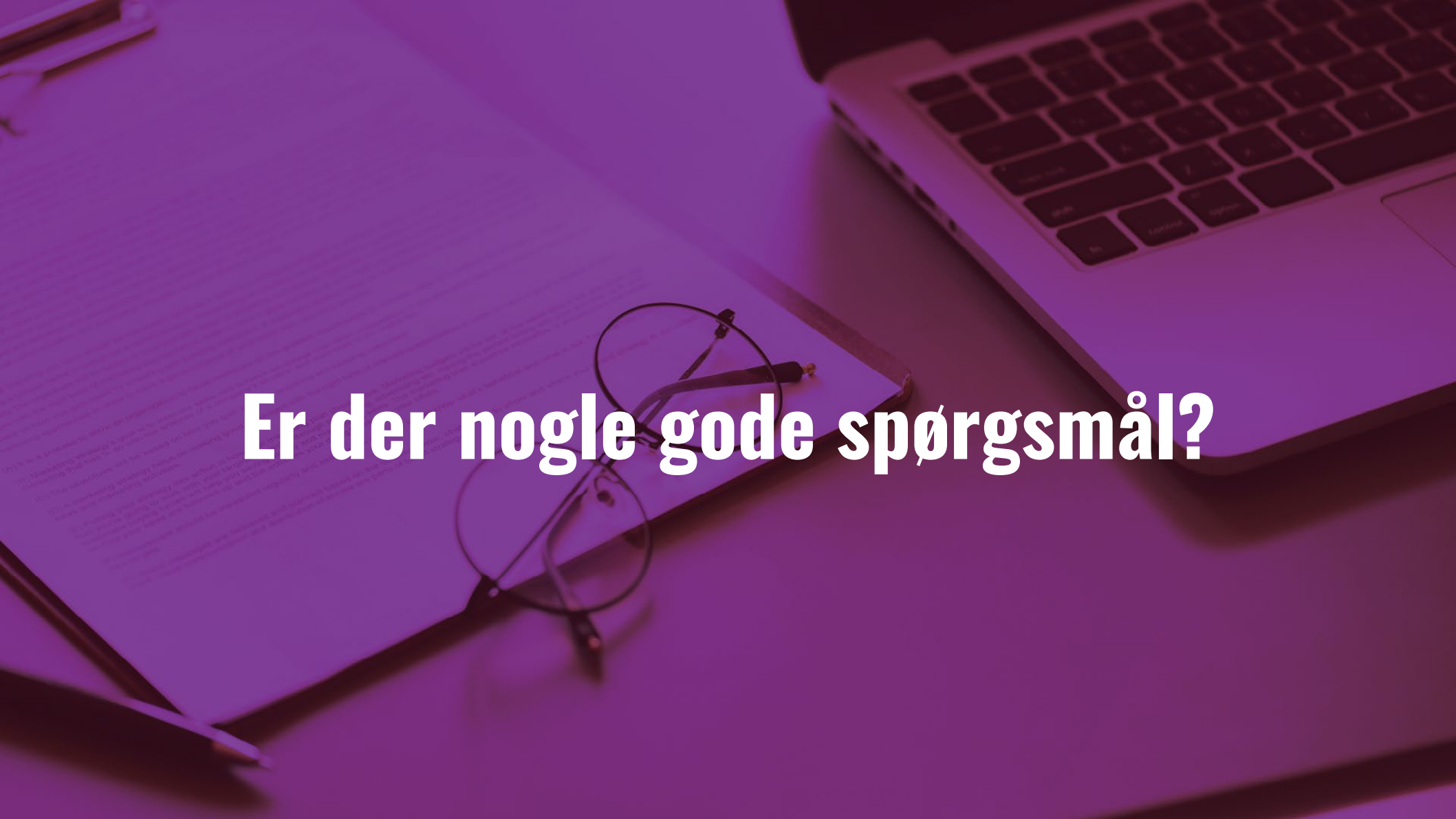
Altså bør vi have et system hvor vi kan holde styr på GDPR og være i stand til at dokumentere at vi har styr på det

I Danmark er der mange systemer om buddet

+Excel, Word, Sharepoint, Onenote, Google Sheets mm.

Teknisk Implementering

- Vi skal dokumentere at de krav der er stillet i en databehandleraftale overholdes og kan vises ved en inspektion – Også fra Datatilsynet.
- Dette kan gøres via de førnævnte certificeringer
- Egenkontroller
- Dokument revisioner
- Vær opmærksom på eventuelle afvigelser, og noter dem i jeres compliance system.


Er der nogle gode spørgsmål?

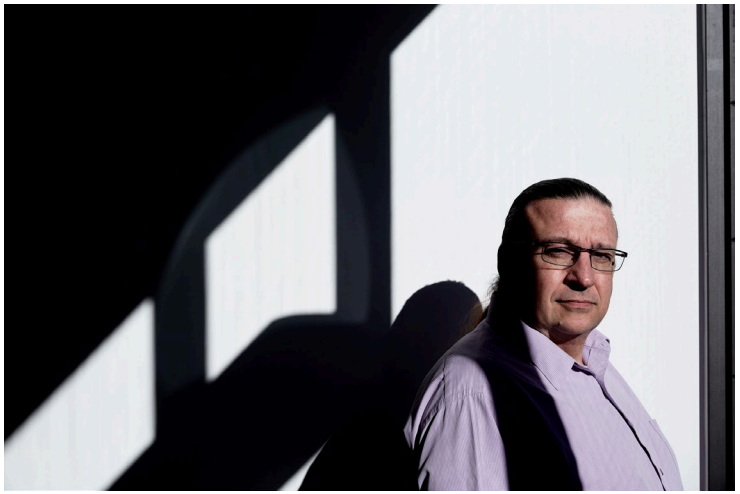
Thanks for your time

E bo@sixtus-compliance.dk

T +45 30 65 45 65

SIXTUS

COMPLIANCE



SPEAKER
BO PYSKOW
CEO & Founder

SIXTUS
COMPLIANCE