# Persondataforordningen fra Dansk Energis perspektiv

Xellent inspirationsdag, 1. juni 2017

DANSK ENERGI

# Brancheorganisationen

DANSK ENERGI

DANSK ENERGI

Mathilde Øelund Jensen
**Konsulent**
cand. Jur.

Direkte: 35 300 422
msj@danskenergi.dk

# Agenda

- Hvad er databeskyttelse? – i store træk!
- Hvilke nye tiltag bringer persondataforordningen med sig?
- Hvad har Dansk Energi fokus på?

# Hvad er databeskyttelse – i store træk?

DANSK ENERGI

# Datasikkerhed er og har altid været vigtigt!
## - store bøder er én ting…..
## …..noget andet er mediernes ”gabestok”

Berlingske Tidende

BT

Ekstra Bladet

Stiftstidende

POLITIKEN
den levende avis

Her ligger hver sjette danskers CPR-nummer frit fremme

# Hvad er en personoplysning?

En personhenførbar oplysning. Dvs. enhver form for information om en identificeret eller identificerbar fysisk person.

- Oplysninger, som forefindes i form af billeder, personers stemmer, fingeraftryk eller genetiske kendetegn, hvis det i praksis er muligt at henføre oplysningerne til en bestemt fysisk person.

- Ved afgørelsen af, om en person er identificerbar, skal samtlige de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende, tages i betragtning.

Rigtig meget er omfattet: Personaledata, kundedata, leverandørdata…

# Kundernes personoplysninger, fx…

*Personoplysninger* og *særlige kategorier af personoplysninger*

- navn
- adresse
- Målernumre
- installationsnumre
- forbrug og lign
- CPR-nr.

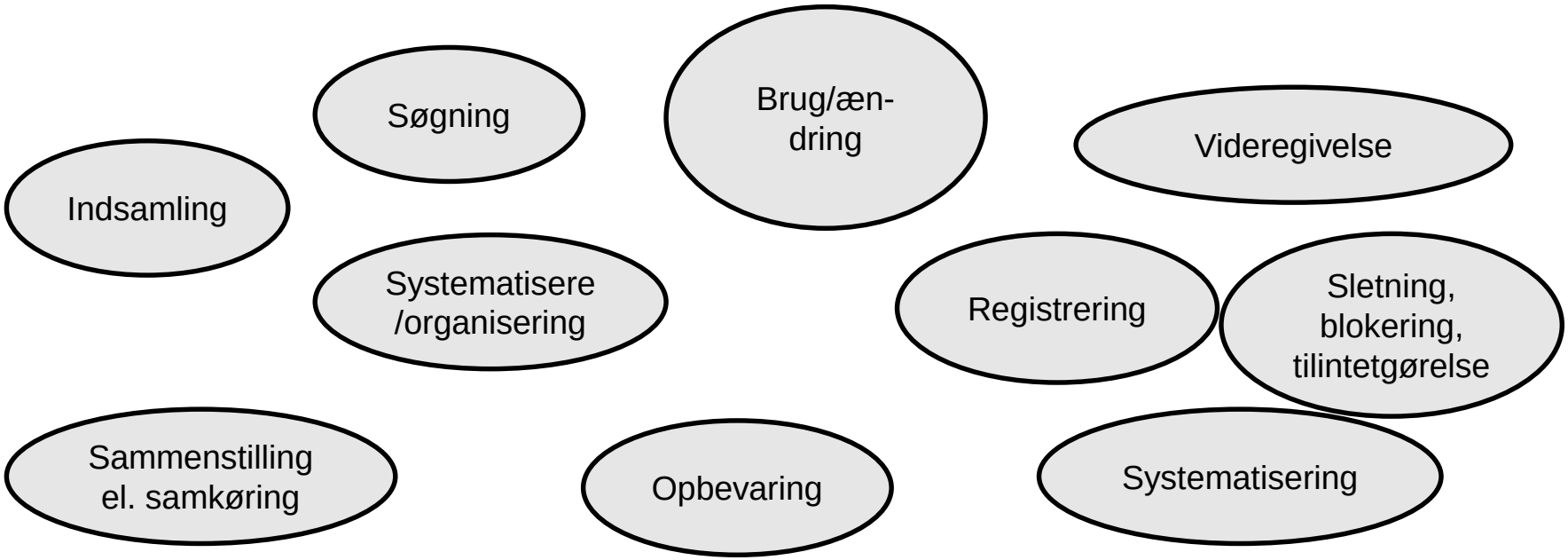
Personoplysninger

- Helbredsoplysninger?

Særlige kategorier af personoplysninger

- Intern (dårlig) omtale af kunder?
- Unødvendige/ikke-relevante oplysninger?

# Hvad er en behandling af en personoplysning?



# Har vi en hjemmel til behandling af en personoplysning?

- En behandling af personoplysninger er **ulovlig** med mindre man har hjemmel hertil – fremadrettet i persondataforordningen

# Hvilke hjemler har vi?

Hjemmelsgrundlag for behandling af almindelige oplysninger (art. 6):

1. Samtykke
2. Nødvendigt for at opfylde en kontrakt med den registrerede
3. Nødvendigt for at overholde en retlig forpligtelse
4. Nødvendigt for at beskytte personers vitale interesser
5. Nødvendigt i samfundets interesse/offentlig myndighedsudøvelse
6. Interesseafvejning: Nødvendig for at forfølge en legitim interesse

Hvad med cpr-nummer?

Helbredsoplysninger?

# Grundprincipper – skal altid overholdes!

- Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål (***formålsbestemthed***)
- Behandlede oplysninger skal være relevante og tilstrækkelige og ikke omfatte mere end påkrævet til opfyldelse af formålet (***proportionalitet***)
- Der skal ske fornøden ajourføring og kontrol (***datakvalitet***)
  - Urigtige/vildledende oplysninger slettes/berigtiges
- Oplysninger må ikke opbevares længere end nødvendigt (***sletning***)

# Datasikkerhed

- Teknisk og organisatorisk
- Passe på, at personoplysningerne ikke ”falder i de forkerte hænder” mens man har ansvaret for dem

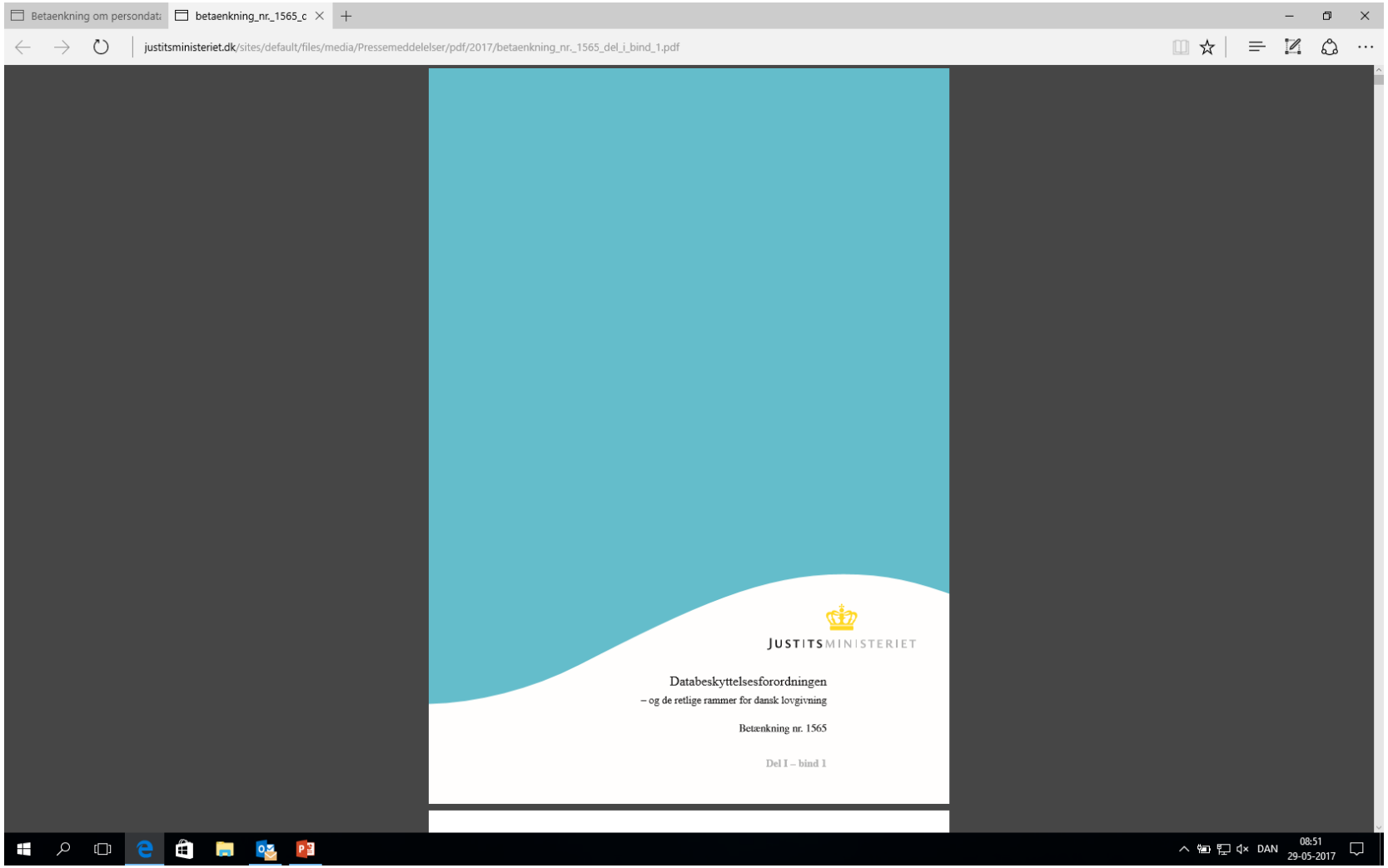
Hvilke nye tiltag bringer

persondataforordningen med sig?

DANSK ENERGI

# Gammel vin på nye flasker…

# Justitsministeriets betænkning er kommet!



# Vigtige pointer fra betænkningen…

- *"Forordningen svarer i et vidt omfang til gældende ret…"*
- *"Nyskabelserne er:* ***DPO, DPIA, fortegnelse over behandlingsaktiviteter, dataprotection by design"***
- *"Hvis man i forvejen lever op til gældende ret, vil der ikke være tale om omfattende ændringer…"*
- *"Med forordningen skabes større "awareness" om betydningen af beskyttelse af persondata…"*

# Noget af det nye…

1. Dokumentation og påvisning af ansvarlighed
2. Konkrete forslag til behandlingssikkerhed
3. Krav om ”Privacy by design”
4. Krav om dataportabilitet
5. Krav om DPO – for nogle!
6. Øget krav til databehandleraftaler
7. Krav om konsekvensanalyser – for nogle!

# 1.Dokumentationskrav/påvisningsforpligtelsen/ansvarlighed/accountability

- **Ansvarlighed** er et gennemgående tema i forordningen (art. 5)

- Dataansvarlig skal kunne **påvise** ( og dokumentere) ansvarlighed og kunne påvise, at vedkommende overholder alle principper for behandling af personoplysninger
  - Passende tekniske og organisatoriske sikkerhedsforanstaltninger
  - Behandlingssikkerhed (art. 32)
    - Pseudonymisering
    - Kryptering

- **Instruks** til medarbejdere – skabelon udarbejdet af DE (art. 32)
- **Fortegnelse** over behandlingsaktiviteter (art. 30) – skal bidrage til dokumentation

# 2. Behandlingssikkerhed – hvad siger forordningen?

- Pseudonymisering/kryptering
- Sikre vedvarende fortrolighed og integritet
- Procedure for regelmæssig afprøvning/vurdering af foranstaltninger til sikring af behandlingssikkerhed

- JM konkluderer:
  - Forordningen giver forslag (art. 32)
  - Men op til den enkelte databehandler at vælge foranstaltninger
  - Mere risikobaseret tilgang – risikoanalyse
    - Måske højere sikkerhedsniveau end sikkerhedsbekg.
    - Måske lavere sikkerhedsniveau end sikkerhedsbekg.

- Krav om logning hos private?

# Behandlingssikkerhed – hvad siger forordningen?

Justitsministeriet:

Ved identifikation af, hvilke foranstaltninger det kan være relevant at gennemføre, kan der f.eks. søges vejledning i ISO 27001-standardens anneks A, som indeholder en omfattende liste af kontrolmål og kontroller. Disse kontrolmål og kontroller modsvarer foranstaltninger, der kan træffes.

Ved udfoldelse af mulighederne for at træffe foranstaltninger, kan andre skriftsteder også være relevante at inddrage, alt afhængig af omstændighederne og situationen ved den aktuelle behandling. I denne forbindelse kan der igen peges på muligheden for at søge vejledning i publicerede udtalelser fra Artikel 29-gruppen og Datatilsynets IT-sikkerhedstekster. Endvidere kan der peges på publikationer fra Center fra Cybersikkerhed og Digitaliseringsstyrelsen, f.eks. *Cyberforsvar der virker.*[579]

# 3. Databeskyttelse by design (privacy by design)

Begrebet "databeskyttelse gennem design" må efter ordlyden forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Design må derfor antages at omfatte både et middel, eksempelvis et IT-systems tekniske indretning og brugergrænse-flade, samt den måde den dataansvarlige organisatorisk er indrettet på.

I modsætning til efter gældende ret er der med forordningens artikel 25, stk. 1, et eksplicit krav om databeskyttelse gennem design.

- Væsentligt råderum
- Fx Dataminimering/pseudonymisering
- Design af et IT-system skal fx kunne imødekomme dataportabilitet eller retten til indsigt
- Ikke krav om re-design af ældre systemer

# 4. Dataportabilitet

- Betyder, at kunden har ret til at modtage persondata om sig selv, som vedkommende har givet til den dataansvarlige, og den registrerede har ret til at overføre disse oplysninger til en anden dataansvarlig.

- Den registrerede har ret til at modtage oplysningerne i et struktureret, almindelig anvendt og maskinlæsbart format.

- Kunden har ret til at overføre personoplysningerne direkte fra den dataansvarlige til en anden dataansvarlig, hvis det er teknisk muligt.

- Den enkelte virksomheds it-systemer skal kunne understøtte retten til dataportabilitet.

# 5. Databeskyttelsesrådgiver (DPO) – måske ikke!

- Alle offentlige myndigheder eller offentlige organer!

- Dataansvarlige, *hvis kerneaktivitet består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang*

- Er behandling af persondata energibranchens kerneaktivitet?

- Justitsministeriets betænkning:

*[samme gør sig gældende for]forsyningsselskaber, idet disse ikke kan anses for at behandle personoplysninger som kerneaktivitet på en sådan måde, der er uløseligt forbundet med selve det at sælge eller distribuere f.eks. fjernvarme eller vandforsyning, selvom forsyningsselskaber i den forbindelse naturligvis behandler kundeoplysninger i et vist omfang.[…]*

# 6. Databehandleraftaler

I forhold til gældende ret, stilles der i forordningen flere og mere detaljerede krav til databehandleraftalen.

- Databehandler = Fysisk/juridisk person, der behandler persondata på den dataansvarliges vegne (”efter instruks”)
- Kun anvende databehandlere, der kan give fornødne garantier for sikkerhed

- Underdatabehandlere må ikke anvendes uden samtykke fra dataansvarlig

- Skal fremgå, at databehandler alene må handle efter instruks. Instruksen skal være dokumenteret!
- Databehandler skal være behjælpelig ved indsigtsanmodninger!

side

- DE har udarbejdet skabelon – 15 sider…

# 7. Konsekvensanalyser – et krav for de få…

Det følger af artikel 35, stk. 1, at der alene skal foretages en konsekvensanalyse, når der sandsynligvis vil være *høj risiko* for fysiske personers rettigheder og frihedsrettigheder. Dette må antageligvis indebære, at artikel 35 vil have et forholdsvis begrænset anvendelsesområde. Den dataansvarlige vil således i de fleste tilfælde ikke skulle foretage en konsekvensanalyse. Dette skal ses i lyset af, at det formentlig kun vil være i få tilfælde, at der konstateres en høj risiko, jf. også nedenfor om artikel 35, stk. 3.

Det kan ud fra karakteren af de eksempler, der nævnes i artikel 35, stk. 3, og i præambelbetragtning nr. 91 – med henvisningen til "meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan" – samt ud fra ordlyden af artikel 35, stk. 1, konstateres, at området for, hvornår en konsekvensanalyse er påkrævet er snævert. Dataansvarlige må således i de fleste tilfælde antages ikke at skulle udarbejde en konsekvensanalyse.

# Behandling af personoplysninger med henblik på markedsføring

- Hvis fx navn/adresse er indhentet af virksomhed X og denne ønsker at videregive navn/adresse til virksomhed y til brug for markedsføring?
  - Videregivelsen kan være ok (generelle kundeoplysninger)
  - Husk dog markedsføringslovens § 6 om krav om indhentelse af samtykke forud for en henvendelse fx pr. e-mail

- Persondataforordningens artikel 21 om indsigelsesretten:

*Hvis personoplysninger behandles med henblik på direkte markedsføring, har den registrerede til enhver tid ret til at gøre indsigelse mod behandling af sine personoplysninger til sådan markedsføring[…]*

Hvad har Dansk Energi fokus på?

DANSK ENERGI

# Beskyttelse af persondata er ikke noget nyt!

- Stort fokus på gældende ret!
- Efterleves gældende ret – så er vi langt!
- Også i tråd med JM's budskab i betænkningen

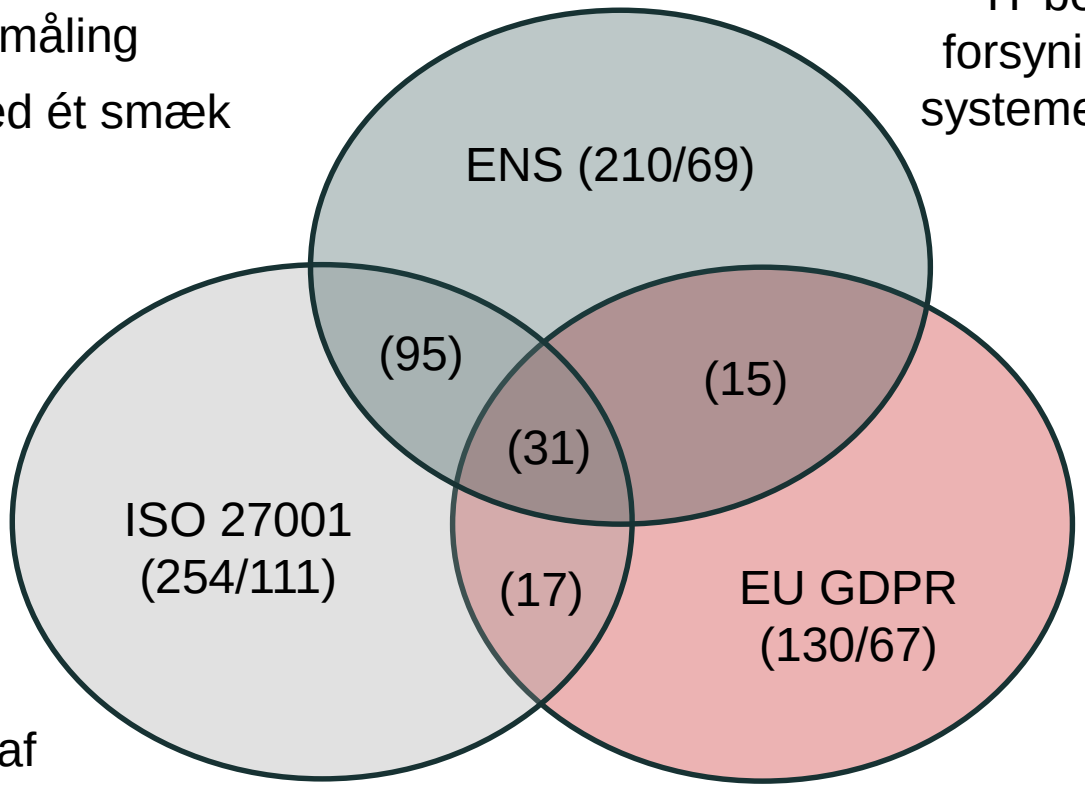
# Dansk Energis øvrige tiltag

- Skabelon til databehandleraftale
- Instruks til medarbejdere, der har adgang til persondata
- Fortegnelse over behandlingsaktiviteter
- Gratis Hotline for persondataretlige spørgsmål
- Mapning over krav (ISO, IT-beredskabskrav, persondataforordningen)

# Fokus på forsyningskritisk it-systemer - nye krav på vej. Synergier?

- Modenhedsmåling
- Tre fluer med ét smæk

IT-beredskab for forsyningskritiske IT-systemer (net og prod)




Ledelse af informationssikkerhed

Persondataforordning og beskyttelse af persondata

# Compliance-skridt

- Overblik over persondata i organisationen
- Oprydning i unødvendig data
- Anvendes databehandlere?
- Er der ”interne databehandlere”?
- Styr på dokumentation
  - Fortegnelse
    - Typer af data, behandling, formål, hjemmel?
  - It-politikker/fortegnelser/instrukser
  - Risikoanalyser?
- Uddannelse af medarbejdere (som vi også kender det inden for IO)

# Hvilke andre konsekvenser har forordningen for energibranchen?

- Skaber mere awareness
- Måske flere indsigtsanmodninger fra kunder?
- Konkurrenceparameter – godt for ry og rygte?

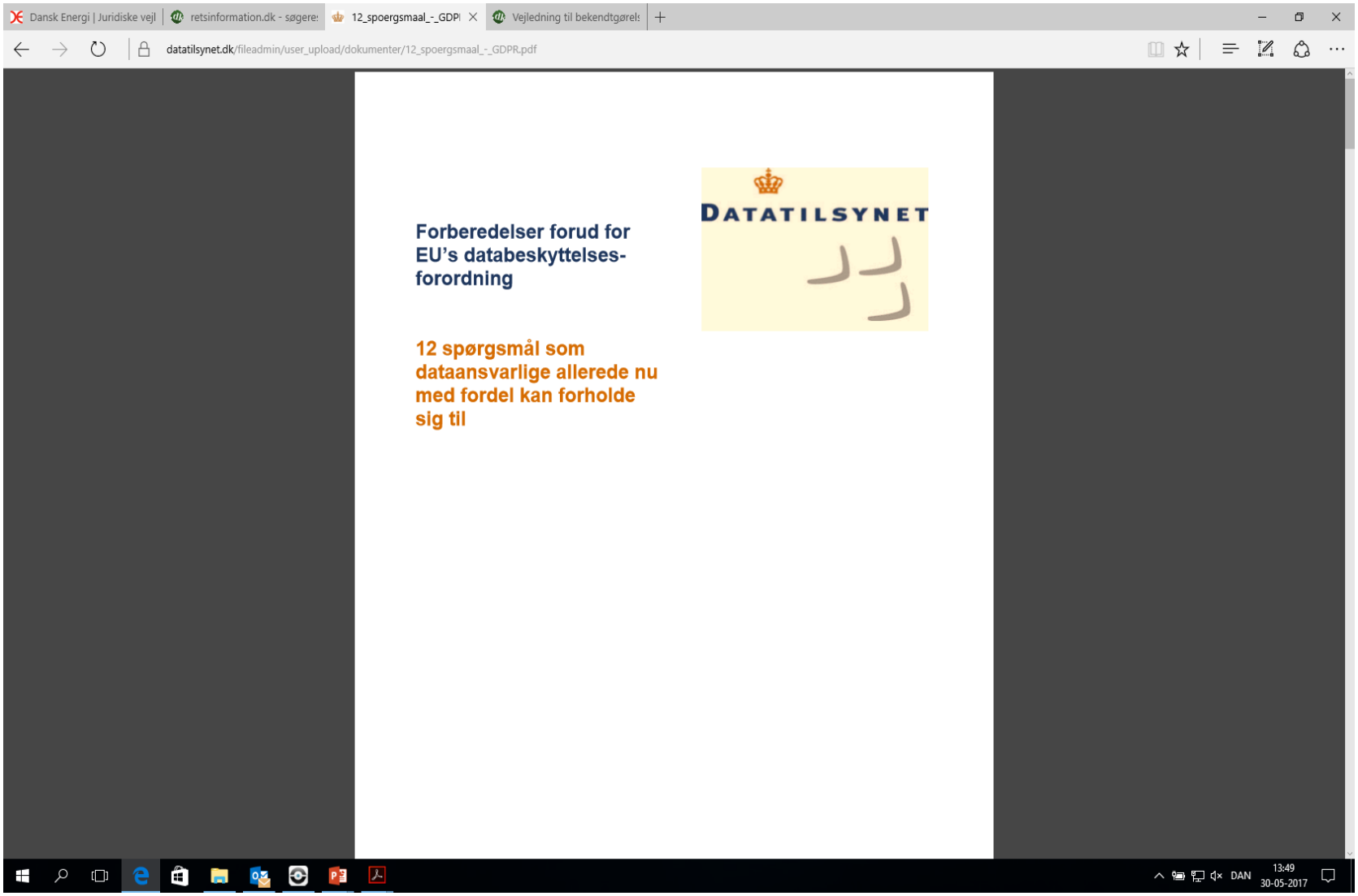
- Logning?

- Testmiljøer?
  - Datatilsynet har udtalt sig i 2011

- Fjernaflæste målere og hyppig indhentelse af data
  - Lovkrav inden 2020 på elområdet – hvad med andre energiarter?

- Energispareområdet? – Samkøring af data?

# Datatilsynets 12 spørgsmål – brug dem!



Tak for ordet☺