

# *Persondataforordningen* ...den nye erklæringsstandard

September 2017

## *Persondataforordningen igen....*

Udkast til erklæring i høring hos revisorer, advokater, databehandlere, virksomheder mfl.:

- Dataansvarliges ansvar vs. Databehandlers ansvar
- Meget omfattende erklæring – hvad så med de små virksomheder
- Mange procedurer og krav om dokumentation
- Tekniske og organisatorisk sikringsforanstaltninger

**BREAKING NEWS! BREAKING NEWS!**

**Erklæringstemplaten kommer snart i endelig udgave!**

**.... og nu med en vejledning og eksempler på tekniske og organisatoriske sikringsforanstaltninger**

---

# *Agenda*

Kort om forordningen

Erklæringstemplaten og vejledningen

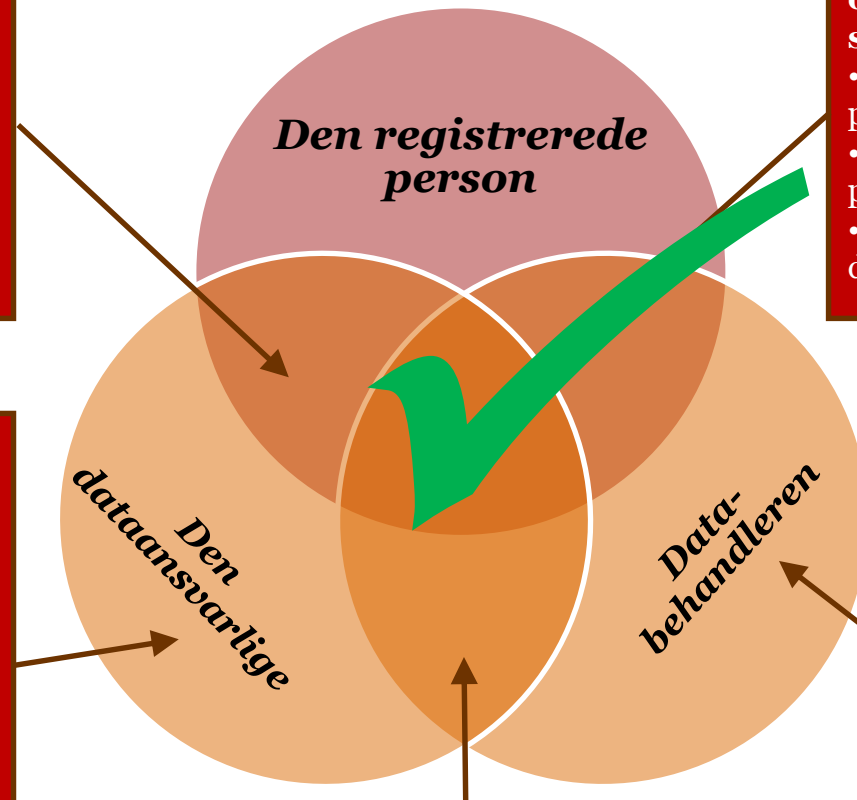
# Persondata – indhold af forordningen

## Den dataansvarlige skal overfor den registrerede sikre:

- Samtykke
- Oplysning om behandling
- Oplysning om rettigheder (indsigt, berigtigelse og sletning)
- Kontaktoplysninger til den dataansvarlige

## Databehandler skal overfor den registrerede sikre:

- Oversigt over registrerede personoplysninger
- Lovpligtig indsamling af personoplysninger
- Mulighed for dataportabilitet



## Den Dataansvarlige skal sikre:

- DPO funktion
- Konsekvensanalyser (Privacy Impact Analysis)
- Organisatoriske sikringsforanstaltninger
- Tekniske sikringsforanstaltninger
- "Privacy by default" og "Privacy by design"
- Uddannelse af egne medarbejdere
- Myndighedskontakt

## Databehandler skal sikre:

- DPO funktion
- Organisatoriske sikringsforanstaltninger
- Tekniske sikringsforanstaltninger
- Uddannelse af egne medarb.
- Aftaler med underleverandører

## Den dataansvarlige og databehandleren skal sikre:

- Databehandleraftale/-instruks
- Fortegnelse over behandlingsaktiviteter
- Aftale om overførsel af data til andre lande

# Persondataforordningen

## - Hvad er nyt!

### Den registreredes rettigheder

- *Den registreredes rettigheder styrkes* - retten til at blive glemt, samtykker, indsigt
- Forordningen stiller *krav om etablering af politikker om den registreredes rettigheder* og håndteringen af disse rettigheder

### Dokumentationskrav

- Anmeldelsesordningen under persondataloven afskaffes
- Både den dataansvarlige og databehandlere skal i stedet føre dokumentation for de behandlingsaktiviteter som de er ansvarlige for
- Dokumentation for at forordningens bestemmelser efterleves

### Risikoanalyse og krav til sikkerhed

- Forud for en persondatabehandling skal der gennemføres en risikoanalyse og udvidede konsekvensanalyser samt løbende opfølgning mv.
- Privacy by Design og Default indføres = sikkerhed skal være standard!

### Sikkerhedsbrud

- Nye krav til håndtering af sikkerhedsbrister introduceres, herunder bl.a. underretningskrav til tilsyn og den registrerede inden for 72 timer.

# *Særlige kategorier af personoplysninger*

- ny definition

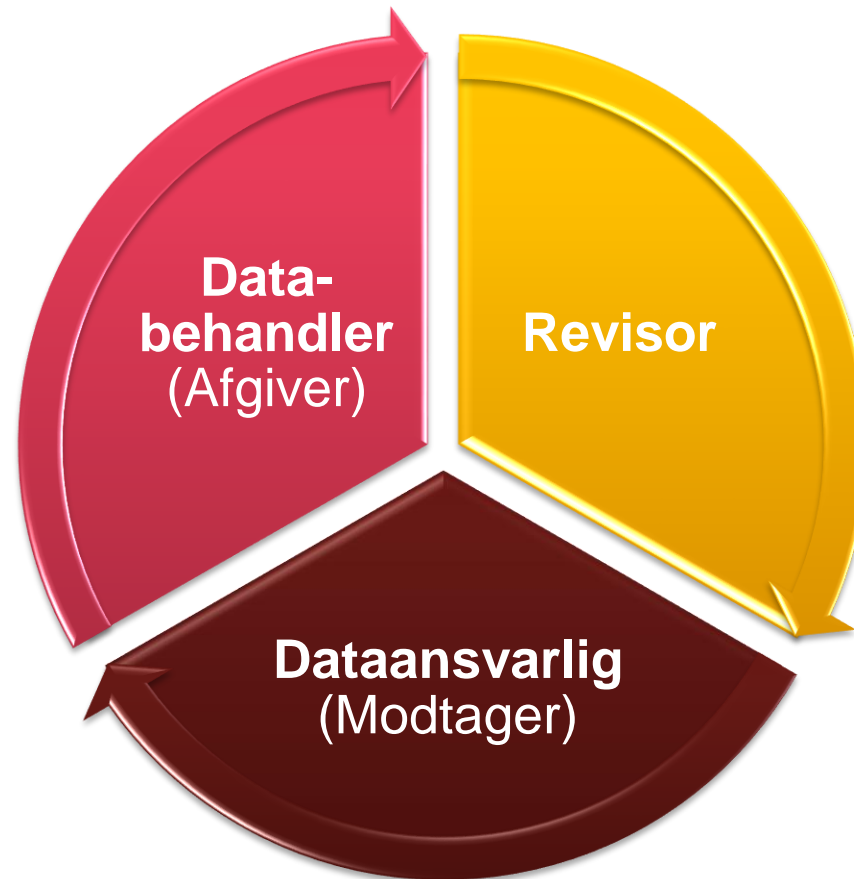
<b>Persondataloven</b>	<b>Indhold</b>	<b>Persondataforordningen</b>
Almindelig personoplysninger	Identifikationsoplysninger, såsom navn, adresse, fødselsdato og e-mail.	Almindelig personoplysninger
Fortrolige personoplysninger	Private forhold, såsom økonomiske og strafbare forhold, sociale problemer og lignende	Særlige kategorier af personoplysninger
Følsomme personoplysninger	Race, religiøs og politisk overbevisning, helbredsmæssige og seksuelle forhold	

---

# *Hvordan griber virksomhederne GDPR an?*

- Kortlæg omfang af persondata i organisationen – Det er processer og modenhed ift. eksisterende persondatalov (As-Is)
- Vurdering af compliance i forhold til de nye skærpede krav i forordningen (To-Be)
- Styrkelse af sikkerhedsniveauet ved at se på (eksempler):
  - Governance og evt. Data Protection Officer
  - Awareness i organisationen
  - Opdagelse og respons på hændelser (sikkerhedshændelser)
  - Teknisk sikkerhedsniveau (arkitektur og beskyttelse)
  - Aftaler med databehandlere – koncerninterne og -eksterne
  - Håndtering af databehandlere

# *Erklæringsforholdet*





# Erklæringens opbygning/indhold

	<i>ISAE 3000</i>	<i>ISAE 3000 - Persondata</i>	<i>ISAE 3402</i>
<b>Beskrivelse af leverandørens system</b>	Valgfrit	<b>Obligatorisk</b>	Obligatorisk
<b>Leverandørens udtalelse</b>	Valgfrit	<b>Obligatorisk</b>	Obligatorisk
<b>Beskrivelse af kontrolmål</b>	Valgfrit	<b>Obligatorisk</b>	Obligatorisk
<b>Beskrivelse af kontrolaktiviteter</b>	Valgfrit	<b>Obligatorisk</b>	Obligatorisk
<b>Beskrivelse af testhandlinger</b>	Obligatorisk	<b>Obligatorisk</b>	Obligatorisk
<b>Beskrivelse af resultat af de enkelte testhandlinger</b>	Valgfrit	<b>Obligatorisk</b>	Obligatorisk
<b>Samlet konklusion i revisors erklæring</b>	Obligatorisk	<b>Obligatorisk</b>	Obligatorisk
<b>Grad af sikkerhed</b>	Begrænset eller Høj	<b>Begrænset eller Høj</b>	Høj

## Erklæringens indhold

1. Ledelsens udtalelse .....	3
2. Uafhængig revisors erklæring .....	5
3. Systembeskrivelse .....	7
3.1 Beskrivelse af [navnet på system/ydelse] .....	7
3.2 Komplementerede kontroller hos de dataansvarlige .....	7
4. Kontrolmål, kontrolaktivitet, test og resultat heraf .....	8
Principper for behandling af personoplysninger (artikel 5) .....	8
Lovlig behandling (artikel 6) .....	9
Betingelser for samtykke (artikel 7 og artikel 8) .....	10
Behandling af særlige kategorier af personoplysninger (artikel 9 og artikel 10) .....	11
Behandling, der ikke kræver identifikation (artikel 11) .....	12
Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder (artikel 12) .....	13
Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 og artikel 14) .....	15
Den registreredes indsigtret (artikel 15) .....	17
Ret til berigtigelse (artikel 16 og artikel 19) .....	18
Ret til sletning ("retten til at blive glemt") (artikel 17 og artikel 19) .....	19
Ret til begrænsning af behandling (artikel 18 og artikel 19) .....	20
Ret til dataportabilitet (artikel 20) .....	21
Den dataansvarliges ansvar – implementering af passende databeskyttelse (artikel 24) .....	22
Databeskyttelse gennem design og standardindstillinger (artikel 25) .....	23
Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29) .....	25
Fortegnelse over behandlingsaktiviteter (artikel 30) .....	29
Behandlingssikkerhed (artikel 32) .....	30
Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33 og artikel 34) .....	32
Konsekvensanalyse vedrørende databeskyttelse (artikel 35) .....	33
Forudgående høring (artikel 36) .....	34
Databeskyttelsesrådgiver (artikel 37) .....	35
Databeskyttelsesrådgiverens stilling (artikel 38) .....	36
Databeskyttelsesrådgiverens opgaver (artikel 39) .....	37
Overførsel af personoplysninger (artikel 44, artikel 45, artikel 46, artikel 47, artikel 48, artikel 49 og artikel 50) .....	38

---

## *Hvordan bruges erklæringstemplaten*

- Fastlæg sammen med databehandler hvilke artikler som er relevante for erklæringsforholdet
  - Brug ”scopingoversigten” i vejledningen som inspiration
  - Få den dataansvarliges accept af omfanget
- Gennemgå databehandlers systembeskrivelse
- Få indsigt i de faktiske kontroller som er implementeret hos databehandler for de artikler som er i scope – de anførte kontroller og revisionshandlinger i templateen er alene til inspiration

# Erklæringens indhold og de faktiske forhold

Art.	Databehandler - Housing	Databehandler - Drift (OS/DB)	Databehandler - Applika-tions- ansvar	Databehandler - proces- ansvar
1 – Genstand og Formål				
2 – Materielt anvendelsesområde				
3 – Territorialt anvendelsesområde				
4 – Definitioner				
5 - Principper for behandling af personoplysninger	(X)	X	X	X
6 – Lovlig behandling		X	X	X
7 – Betingelser for samtykke			(X)	X
8 - Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester				
9 - Behandling af særlige kategorier af personoplysninger	(X)	X	X	X
10 - Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser				
11 - Behandling, der ikke kræver identifikation	(X)	X	X	X
12 - Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder			X	X
13 - Oplysningspligt ved indsamling af personoplysninger hos den registrerede			(X)	X
14 - Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede				
15 - Den registreredes indsigtret				X
16 – Ret til berigtigelse		(X)	X	X
19 - Underretningspligt i forbindelse med berigtigelse eller sletning				

# Kontrolmål og kontroller

## Ret til berigtigelse (artikel 16 og artikel 19)

### Kontrolmål:

Der efterleves procedurer og kontroller som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger er overholdt, herunder berigtigelse hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af Revisors test
1	<p>Der foreligger skriftlige procedurer, hvori håndtering af de registreredes ret til berigtigelse af personoplysninger er beskrevet eller hvordan databehandler kan bistå den dataansvarlige hermed.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til berigtigelse af personoplysninger.</p>	
2	<p>Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer at berigtigelse af personoplysninger kan gennemføres.</p>	<p>Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til berigtigelse af personoplysninger.</p> <p>Inspiceret dokumentation for at berigtigelse af personoplysninger alene sker ved anvendelse af de etableret tekniske foranstaltninger.</p>	
3	<p>Der foretages løbende – og mindst en gang årligt – vurdering af, at berigtigelse af personoplysninger er sket korrekt og uden unødigt forsinkelse.</p>	<p>Inspiceret dokumentation for kontrol af, at berigtigelse af personoplysninger er sket korrekt og uden unødigt forsinkelse.</p>	
4	<p>Ledelsen har behandlet og godkendt vurderingen af om berigtigelse af personoplysninger er sket korrekt og uden unødigt forsinkelse.</p>	<p>Inspiceret dokumentation for at ledelsen har sikret, at berigtigelse af personoplysninger er sket korrekt og uden unødigt forsinkelse.</p>	

# Hvad kan jeg gøre?



Den dataansvarlige:

- Drøft behandling af persondata – identificér behov for erklæring fra eksterne databehandlere

Databehandleren:

- Drøft kundernes behov for erklæring
  - Generel erklæring
  - Specifik erklæring – eks. særlige kategorier af persondata



---

# *Succes skaber vi sammen...*

Denne publikation er udarbejdet alene som en generel orientering om forhold, som måtte være af interesse, og gør det ikke ud for professionel rådgivning. Du bør ikke disponere på baggrund af de oplysninger, der er indeholdt i denne publikation, uden at indhente specifik professionel rådgivning. Vi afgiver ingen erklæringer eller garantier (udtrykkeligt eller underforstået) hvad angår nøjagtigheden og fuldstændigheden af de oplysninger, der findes i publikationen, og, i det omfang loven tillader, accepterer eller påtager PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, dets aktionærer, medarbejdere og repræsentanter sig ikke nogen forpligtelse, ansvar eller agtpågivenhedspflicht for eventuelle konsekvenser, som følger af, at du eller andre handler eller undlader at handle i tillid til de oplysninger, der findes i publikationen, eller for eventuelle beslutninger truffet på baggrund af publikationen.

© 2017 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. Alle rettigheder forbeholdes. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed.