www.pwc.dk

Persondataforordningen

...den nye erklæringsstandard

September 2017

pwc

Revision. Skat. Rådgivning.

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

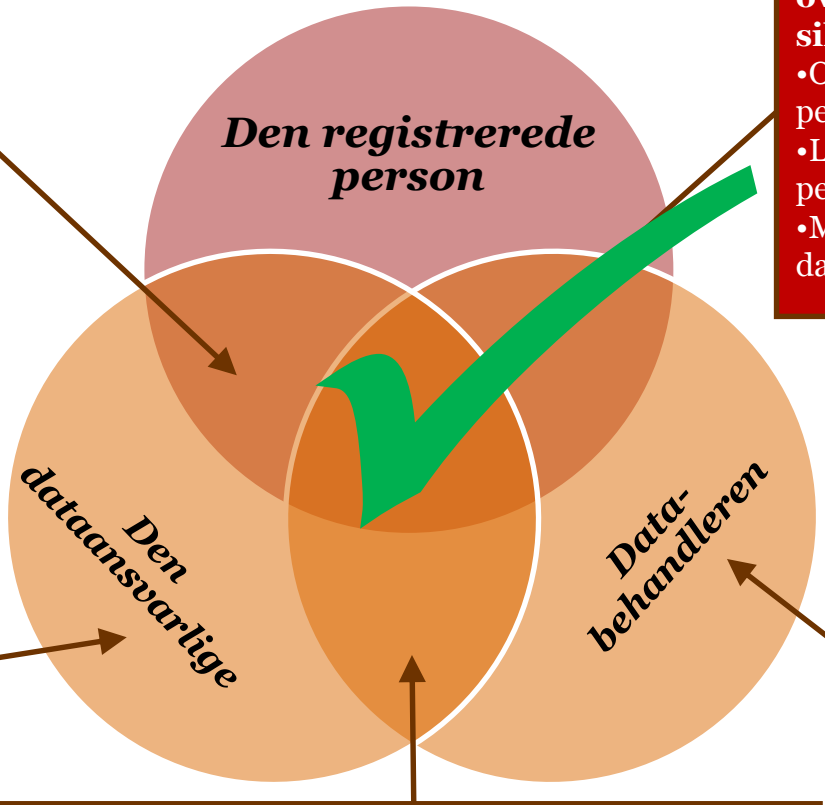
Persondata – indhold af forordningen

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
- Kommunikation om brud

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.

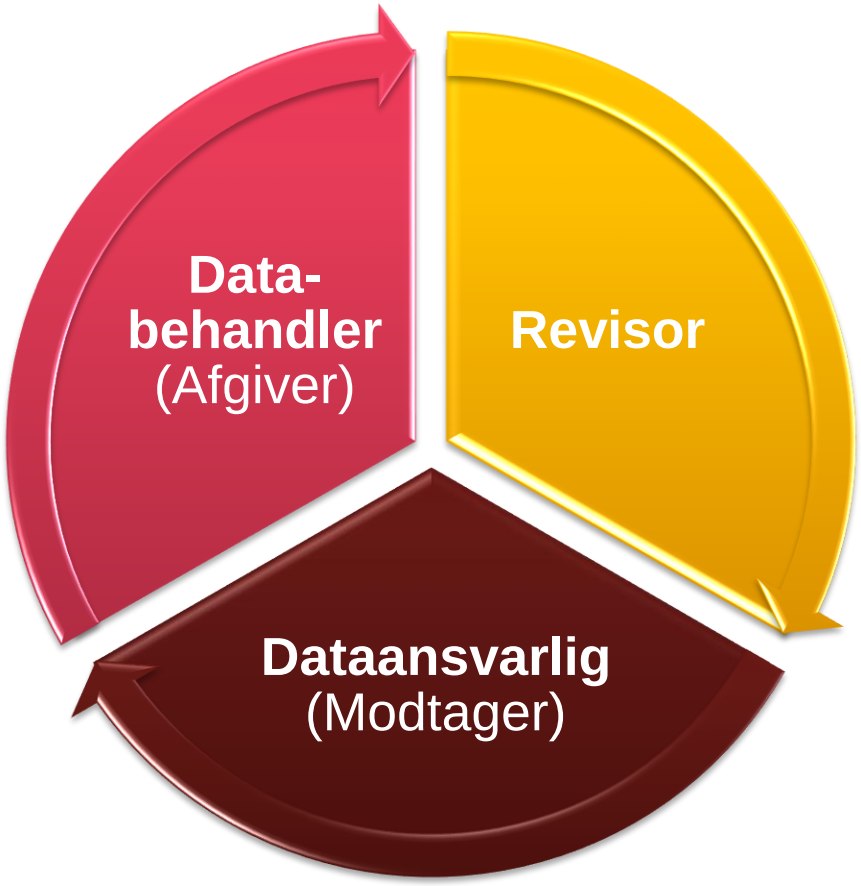
Særlige kategorier af personoplysninger
- ny definition

Persondataloven	Indhold	Persondata-forordningen
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. Date 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

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

Erklæringens indhold

Indholdsfortegnelse

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 templaten 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 8 - Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester			(X)	X
9 - Behandling af særlige kategorier af personoplysninger 10 - Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser	(X)	X	X	X
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 14 - Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede			(X)	X
15 - Den registreredes indsigtsret				X
16 – Ret til berigtigelse 19 - Underretningspligt i forbindelse med berigtigelse eller sletning		(X)	X	X

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

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...