Sikkerhed og Revision

Anvendelse af ny GDPR – revisionserklæring fra FSR

september 2019

pwc

Introduktion

Thomas Gi Scharf
thomas.gi.scharf@pwc.com
+45 2155 8918

Director PwC, Digital Trust

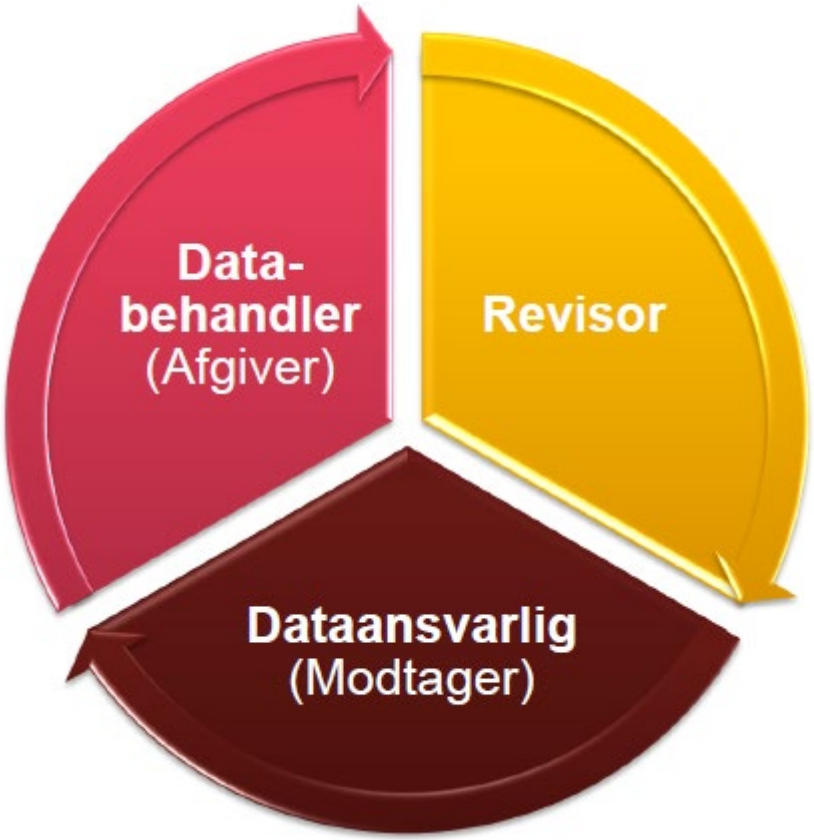
Thomas har mere end 15 års erfaring inden for it-revision og –sikkerhed og en uddannelsesmæssig baggrund som cand. Merc. aud. samt CISA og CISSP

Lars Jeppesen
lars.jeppesen@pwc.com
+45 2373 2139

Director PwC, Digital Trust

Lars har mere end 19 års erfaring inden for it-revision og –sikkerhed og en uddannelsesmæssig baggrund som Civil-Ingeniør.

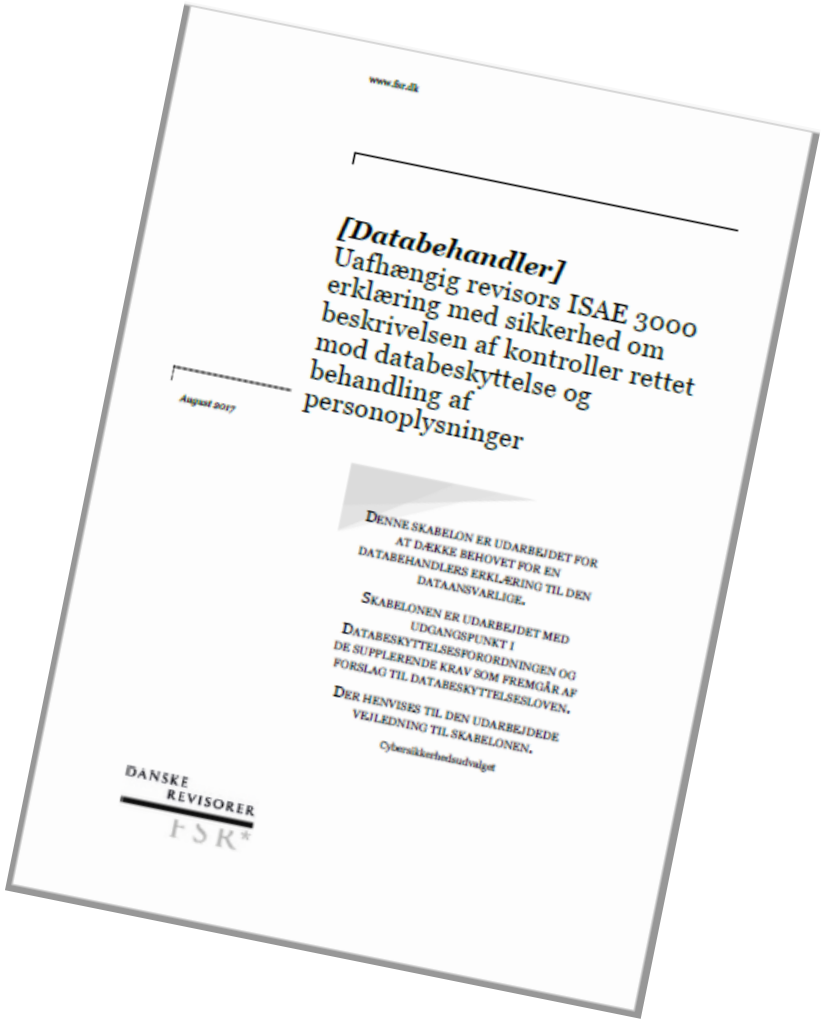
Erklæringsforholdet



GDPR – FSR's første forslag til erklæring august 2017

FSR's Cybersikkerhedsudvalg har udarbejdet et erklæringseksempel om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger.

For virksomheder (private og offentlige), som har outsourcet drift af systemer, der indeholder persondata, eller selve behandlingen af personoplysninger til en leverandør, vil det ofte være relevant at indhente en revisorerklæring fra denne leverandør for derved at kunne dokumentere og påvise overholdelse af den kommende persondataforordning.



GDPR – FSR's første forslag til erklæring august 2017

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.	

Svar på feedback - et nyt udgangspunkt

Databehandleraftale

Mellem

Den dataansvarlige:

[Navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og by]

[Land]

og

Databehandleren

[Navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og by]

[Land]

Med udgangspunkt i databehandleraftale og instruks uddrages:

- kontrolmål
- kontrolaktiviteter

og der udarbejdes en revisorerklæring herom.

GDPR – FSR's andet forslag til erklæring februar 2019

FSR – danske revisorer har i samarbejde med Datatilsynet udarbejdet en ny revisorerklæring, som giver sikkerhed for, at databehandlere lever op til kravene i GDPR, som de har forpligtet sig til i de indgåede databehandleraftaler.

Som reglerne er i dag, er det den dataansvarliges ansvar at sikre, at personoplysninger bliver behandlet korrekt, selvom behandling af oplysningerne er overladt til andre. Dette kan være en svær opgave for den dataansvarlige at løfte, men her hjælper den nye erklæring, der giver sikkerhed for, at procedurer og regler er overholdt som aftalt mellem parterne.

[Databehandler]

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]

Bemærk: Denne skabelon for erklæring indeholder en række eksempler på kontrolaktiviteter og revisionshandlinger. Disse er alene til inspiration og bør altid tilpasses til den konkrete risikovurdering, de foranstaltninger, der i øvrigt måtte være aftalt parterne imellem, og under hensyn til revisors professionelle vurdering.

1. februar 2019

GDPR – FSR's andet forslag til erklæring februar 2019

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på XX behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med	

Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er: [Her indsættes en kort beskrivelse af det/de underliggende aftaleforhold mellem parterne, der er baggrunden for behovet for en databehandleraftale, gerne med henvisning til "hovedaftalen", databehandleraftalen og øvrige relevante aftaler, formålet med behandlingen og karakteren af behandlingen].

- Karakteren af behandlingen
- Personoplysninger
- Praktiske tiltag
- Risikovurdering
- Kontrolforanstaltninger
- Komplementerende kontroller hos de dataansvarlige

Kontrolmål
Der efterleves procedurer og kontroller, som sikrer, at…

- instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.
- databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.
- databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.
- personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.
- databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.
- der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.
- databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.
- databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.
- eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Hvordan bruges erklæringstemplaten

- Fastlæg sammen med databehandler hvilke kontrolmål og kontroller som er relevante for erklæringsforholdet, og få den dataansvarliges accept af omfanget

- Gennemgå databehandleres systembeskrivelse

- Få indsigt i de faktiske kontroller som er implementeret hos databehandler for de kontrolmål som er i scope – de anførte kontroller og revisionshandlinger i templaten er alene til inspiration

Hvor har udfordringerne været i praksis?

- Hvad er scope for erklæringen? Skal interne persondata medtages?
- Mange kontroller i skabelon – svært at omsætte til praktik i virksomheden – og svært at lave GAP assessment?
- Mange virksomheder har været drevet af fokus på virksomhedens egne persondata samt at få styr på databehandleraftaler med kunderne.
- Hvordan håndteres kontroller på ledelsestilsyn og godkendelse af procedurer mv.?
- P.t. flest type 1 erklæringer – hvordan skal virksomheden forankre og dokumentere kontrollerne?
- Svært for virksomheden at lave risikovurderinger – andet fokus end klassiske risikovurderinger da den registreredes rettigheder er i fokus og ikke CIA
- Svært at lave systembeskrivelsen – hvad skal med og ikke med?
- Overlap til eksisterende erklæringer hos virksomhederne eller deres sikkerhedscertificeringer?
- Hvad er passende tekniske og organisatoriske kontroller?

Opmærksomhedspunkter

- Type 1 eller Type 2
- Høj eller begrænset grad af sikkerhed
- Carve-out eller inclusive
- Behandling/systemer i scope
- Kontrolaktiviteter/kontrolmål
- Generel eller kundespecifik
- Perioder og frister
- Komplementære kontroller
- Møder
- Straksrapportering
- Findings med detaljer
- Bridge letter
- Adgang til revisors arbejde
- Kompetencer hos revisor

og om ISAE 3000 er den rigtige erklæring

Spørgsmål

Succes skaber vi sammen…

www.pwc.dk

Succes skaber vi sammen …