



ADVOKATGRUPPEN



RET LIGETIL. SIDEN 1987.



ADVOKATGRUPPEN

# PERSONDATARET

Eva Kaya & Bjarke G. Jochumsen



RETSPLEJELOV · STRAFFELOV

RET LIGETIL. SIDEN 1987.

# LIDT OM MIG



EVA KAYA

Advokat (L) / LL.M.

---

**Direkte:** 87 32 81 24

**E-mail:** [ek@advokatgruppen.dk](mailto:ek@advokatgruppen.dk)

## MINE SPECIALER

PERSONDATARET

SELSKABSRET

ANSÆTTELSESR

HANDELSAGENTER OG MELLEMMÆND

RET LIGETIL. SIDEN 1987.

# LIDT OM MIG



**BJARKE G. JOCHUMSEN**

Advokat

---

**Direkte:** 87 32 81 80

**E-mail:** [bj@advokatgruppen.dk](mailto:bj@advokatgruppen.dk)

## MINE SPECIALER

PERSONDATARET

---

IMMATERIALRET

---

PROCES

---

INKASSO

---

**RET LIGETIL. SIDEN 1987.**



## PERSONDATA – KUN EN OVERSIGT

Dette minikursus er beregnet for DMs/Gafsams/MLs/SHPs medlemmer, dvs. mindre og mellemstore virksomheder, hvis erhvervsaktiviteter primært består i salg og service af landbrugs-, entreprenør og have/park-maskiner.

Kurset giver alene et **overblik** over persondataforordningen.

En del områder indenfor persondata er stadig uafklarede; pt. afventer vi en del vejledninger og en ny persondatalov, se fx.

[http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan\\_for\\_vejledninger\\_om\\_forordningen.pdf](http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan_for_vejledninger_om_forordningen.pdf)

# PERSONDATA – HVAD ER DET?

## Eksempel: Facebook

Hvad med dine persondata?

Mod at bruge Facebook har du **accepteret**, at en hvilken som helst virksomhed i verden får lov til at bruge oplysninger om, hvem du er, hvem du kender, hvem du taler med, hvad du foretager dig, hvor du færdes, og hvad du interesserer dig for, i reklameøjemed.





## PERSONDATA – HVAD ER DET?

### Eksempel : Facebook

Har den viden om dig så nogen værdi?

Ja - i 2016 var Facebooks indtægter fra salg af annoncer til brugerne 179 milliarder kroner.

Kilde: Artikel i Zetland fra 15. juni 2017, "Snart har Facebook to milliarder brugere. Her er, hvad vi siger ja til (hint: ikke småting)".

RET LIGETIL. SIDEN 1987.





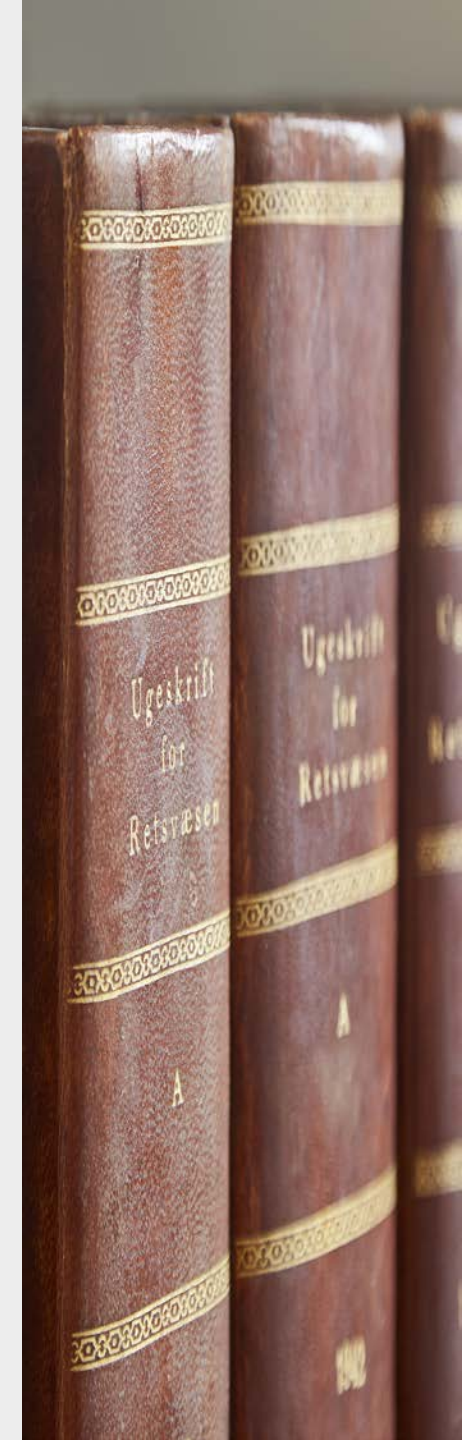
# PERSONDATAFORORDNINGEN

**Anvendelsesområde:** Erhvervsmæssig brug af persondata

**Ikrafttræden:** Den 25. maj 2018

Medfører persondataforordningen nye **pligter**?

Ja, men bygger videre på allerede gældende persondatalov.





# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Hvilke persondata har din virksomhed?

### A. Følsomme data:

Race eller etnisk oprindelse

Seksuelle forhold

Politisk, religiøs eller filosofisk overbevisning

Fagforeningsmæssigt tilhørsforhold

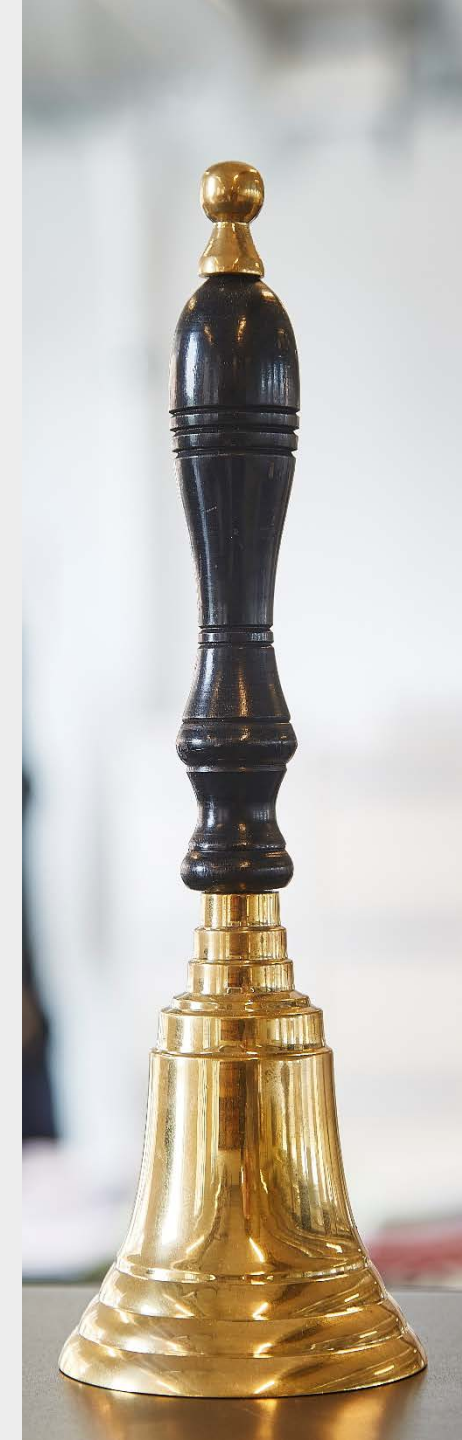
Biometrisk data med formål om identifikation

Helbredsoplysninger \*

Oplysninger om børne- eller straffeattest \*

\* Persondata som ofte er registreret i en virksomhed i forbindelse med ansatte og udbud, og som oftest bør være anmeldt til Datatilsynet.

RET LIGETIL. SIDEN 1987.



# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Hvilke persondata har din virksomhed?

### B. Ikke-følsomme data:

Oplysninger om fysiske leverandørers og kunders identitet, adresse, køb, salg

Persondata om medarbejdere, som er ikke-følsomme data

Bemærk afgrænsningen: Kundekartoteket i en virksomhed er en erhvervshemmelighed, men er ikke en følsom oplysning efter persondataloven eller persondataforordningen.

Hvad med markedsandele og prispolitik, som er ret følsomt?  
Kunders kreditkortoplysninger?

Personnumre – må man registrere: Kunders? Ansattes? Er det følsomme data?



# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Hvor er virksomhedens persondata?

### Server

Egen server eller andres?

Hvor er den **fysisk** beliggende?

Hvad med data i printer/scanner/fax/kopimaskine?

### Cloud-løsning

Hvor er data **fysisk**, hvis de lagres i skyen?



# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Bliver virksomhedens persondata overført?

Til andre virksomheder (hosting eller cloud-løsning)?

Til udlandet?

Hvis data ikke ligger på virksomhedens **egen** server i EU, kan databehandleraftale og samtykke være nødvendigt...



# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Persondataforordningen og persondataloven

Den nuværende persondatalov fra år 2000 fastlægger allerede en del forpligtelser for de virksomheder, som har eller indsamler persondata.

Persondataforordningen, som træder i kraft i maj 2018, bygger i vid udstrækning videre på indholdet i [persondataloven](#).

Man får en bedre forståelse af persondataregulering, hvis man læser Datatilsynets gennemgang af 12 spørgsmål om persondata, se:

[https://www.datatilsynet.dk/fileadmin/user\\_upload/dokumenter/12\\_spoergsmaal\\_-\\_GDPR.pdf](https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf)

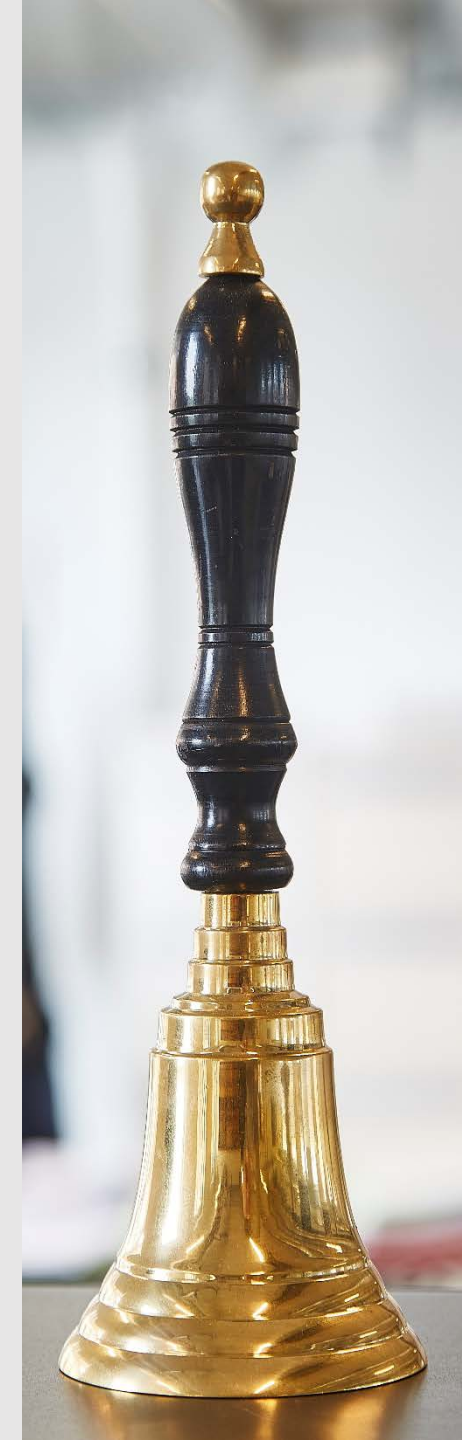


# STYR PÅ VIRKSOMHEDENS PERSONDATA

## Hvilke forpligtelser har virksomheden

Når man har fået styr på, hvilke persondata, virksomheden har liggende, er det relevant at finde ud af, hvad virksomheden skal **overholde** i forbindelse med sine persondata.

Den vigtigste bestemmelse er **persondataforordningens artikel 5**.





# HOVEDFORPLIGTELSENE I FORORDNINGEN

## Artikel 5, stk. 1.

*Personoplysninger skal:*

- a) *behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede ("lovlighed, rimelighed og gennemsigtighed").*
- b) *indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål ("formålsbegrænsning").*
- c) *være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles ("dataminimering").*
- d) *være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges ("rigtighed").*
- e) *opbevares op en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder ("opbevaringsbegrænsning").*
- f) *Behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger ("integritet og fortrolighed").*

Artikel 5, stk . 2.

Den dataansvarlige er **ansvarlig** for og skal kunne **påvise**, at stk. 1 overholdes (ansvarlighed).

## ARTIKEL 5, STK. 1, LITRA A

### a) Lovlighed, rimelighed og gennemsigtighed

#### Samtykke

Frivilligt, specifikt, informeret, utvetydigt ja.

Ugyldigt, hvis ikke ved indhentelse af samtykke er oplyst, at et samtykke kan **tilbagetrækkes**.

Samtykket skal kunne **bevises** (skriftlighed).

Samtykke **anerkendes** muligvis ikke i ansættelsesforhold

*OBS nuværende følsomme persondata : anmeldelse og samtykke!*

#### Kontrakt

Hvis persondata indsamlet som led i **kontrakt**-(indgåelse).







## ARTIKEL 5, STK. 1, LITRA B-C

### b) Formål

Der skal altid være et **legitimt** formål for at have persondata

Formålet skal **oplyses** til den registrerede.

Data må kun anvendes/opbevares til det angivne **formål**.

### c) Dataminimering

Kun persondata **relevante** for formålet.

Kun i relevant **tidsrum**.

F.eks. makulering og sletning af ansøgning fra ikke-ansat ansøger til stilling





## ARTIKEL 5, STK. 1, LITRA D-E

### d) Korrekte data

Pligt til at sørge for at registrerede persondata er **korrekte**.

Pligten modsvarer af den registreredes rettigheder til **indsigt**, ændringer af ukorrekte data, sletning af data mv.

### e) Opbevaringstid

Persondata skal ikke **opbevares** længere end formålet tilsiger.

Husk dog også andre forpligtelser, fx. opbevaring i min 5 år iht. bogføringslov





## ARTIKEL 5, STK. 1, LITRA F

### f) Behandling af persondata

Beskyttelse af data mod **uautoriseret** adgang.

Beskyttelse af data mod **ulovlig** brug.

Begge er både internt (adgangsbegrænsning mv) og eksternt (hacking mv.)

Beskyttelse mod **tab**, **tilintetgørelse** eller **skade** på data.





## ARTIKEL 5, STK. 1, LITRA A-F

En virksomhed skal altså sørge for, at dens persondata indsamles og behandles i overensstemmelse med principperne i artikel 5.

Dette søges opretholdt ved:

at kræve at virksomheden kan påvise **overholdelse**, og  
at tildele de personer, hvis data er registreret, **rettigheder**.





## REGISTREREDES RETTIGHEDER

Først gennemgås kort de **rettigheder**, som forordningen (art. 13-23) tildeler de personer, hvis data er registeret (*de registrerede*).

Langt de fleste af de registreredes rettigheder i persondataforordningen er allerede fastlagt i den nuværende persondatalov.





## REGISTREREDES RETTIGHEDER

Retten til at modtage **oplysning** om en behandling af sine personoplysninger (oplysningspligt).

Retten til at få **indsigt** i sine personoplysninger.

Retten til at få urigtige personoplysninger **berigtiget**.

Retten til at få sine personoplysninger **slettet** \*

Retten til at gøre **indsigelse** mod at personoplysninger anvendes til direkte markedsføring.

Retten til at **flytte** sine personoplysninger (dataportabilitet)\*





## REGISTREREDES RETTIGHEDER

Retten til at **modtage** oplysning om en behandling af sine personoplysninger (oplysningspligt)

At der skal gives oplysninger om den dataansvarliges identitet og kontaktoplysninger, formålene med behandlingen mv. er ikke nyt; findes oftest i "persondatapolitik" afsnit på hjemmeside.

Der er inspiration at hente i Erhvervsstyrelsens værktøj:  
<https://privacykompasset.erhvervsstyrelsen.dk/vaerktoejer>

Retten til **indsigt** i sine personoplysninger

Information om den registreredes rettigheder på anmodning.





## REGISTREREDES RETTIGHEDER

Retten til at få urigtige personoplysninger **berigtiget**

Bemærk at underretning om berigtigelse skal ske til modtagere af persondata.

Ved uenighed om indhold / behandling af persondata kan den registrerede forlange, at data kun opbevares, medmindre der er givet samtykke til andet.

Retten til at få sine personoplysninger **slettet** \*

Ret til sletning er nyt – og noget uafklaret.

Sletning bør ikke ske, før reklamationsperiode, og evt. garantiperiode er udløbet og heller ikke før bogføringsreglerne overholdt!

Hovedregel: Sletning efter 6 år af kundedata og personaledata.







## REGISTREREDES RETTIGHEDER

Retten til at gøre **indsigelse** mod at personoplysninger anvendes, bl.a. til direkte markedsføring

Reglerne i Markedsføringsloven om forbud mod spam, mod uanmodet henvendelse, robinson-listen mv. gælder stadig.

Før anvendelse skal den registrerede oplyses om sin ret til at gøre indsigelse mod anvendelse af data til direkte, lovlig markedsføring.

Bemærk at indirekte markedsføring ikke er omhandlet.

Retten til at **flytte** sine personoplysninger(dataportabilitet) \*

Denne ret til at få udskrift af sine egne persondata er ny.

Ret til at få flyttet sine data over til en anden dataansvarlig, hvis muligt.



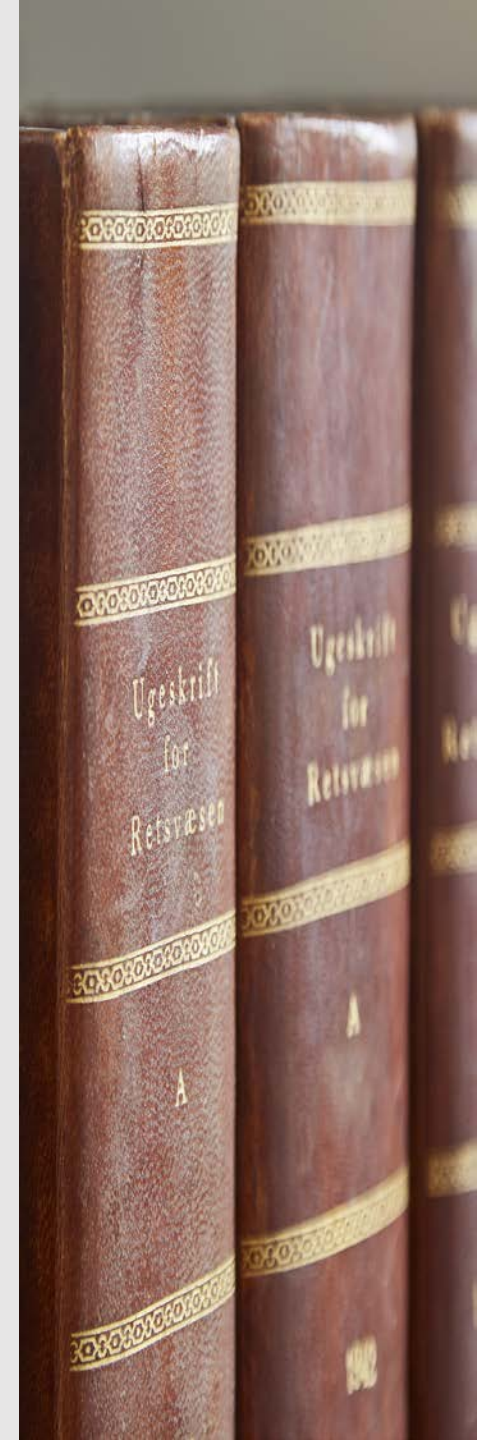


## OVERHOLDELSE AF FORORDNINGEN

Udover tildeling af rettigheder kræver forordningen, at en virksomhed kan påvise, at forordningen **overholdes**.

Dette kan påvises på forskellige måder, med en kombination af tiltag. Der er ikke – slet ikke endnu – nogen enkelt måde, der 100% sikkert opfylder alle kravene.

I det følgende gennemgås kort de tiltag, som forordningen **foreslår** og i nogle tilfælde **kræver**.





## OVERHOLDELSE AF FORORDNINGEN

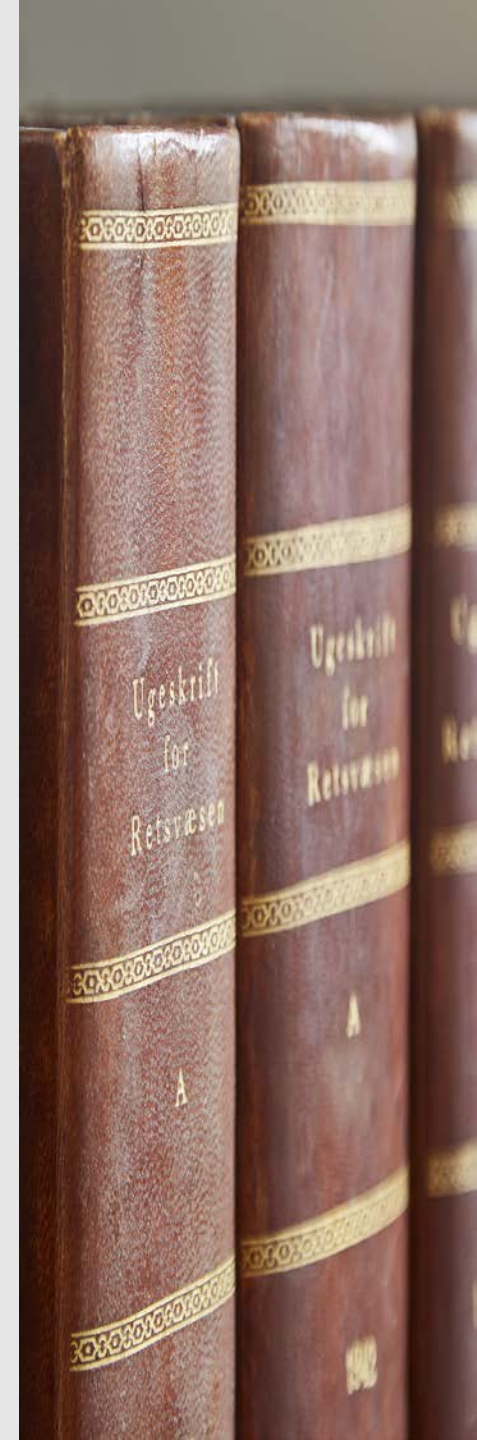
### Standardindstillinger i virksomhedens IT (art. 25)

Der er ikke krav om ny IT efter de ny regler, men måske efter de gamle.

Hvis det nuværende IT kan **ændre** standardindstillinger, bør virksomheden sørge for dataminimering, kun at indsamle og gemme data iht. formål, slette efter fx. 6 år efter seneste databehandling og indstille så registreredes rettigheder kan overholdes (ændring af ukorrekte data, udskrift af data mv.).

Hvis virksomhedens nuværende IT ikke kan ændre standardindstillinger, må virksomheden bruge andre tiltag for at opfylde forordningen.

Ved nyanskaffelse af IT bør IT-leverandøren afkræves, at persondataregulering i Danmark bliver overholdt.





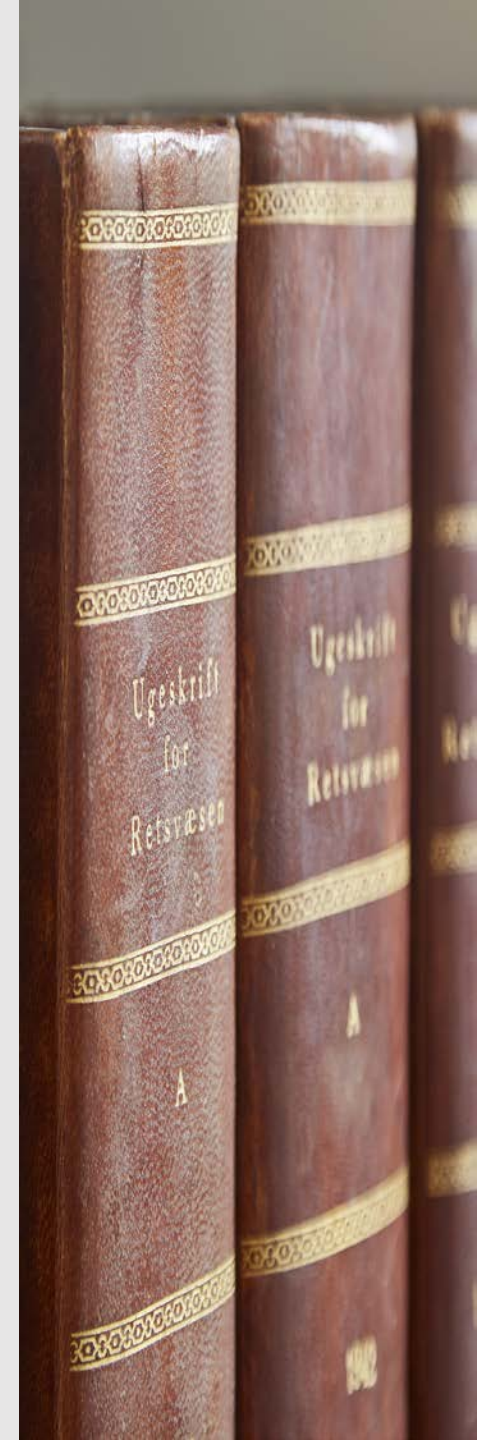
## OVERHOLDELSE AF FORORDNINGEN

### Fortegnelse over behandlingsaktiviteter (art. 30)

Hver virksomhed skal føre en intern **fortegnelse** – som Datatilsynet kan bede om en udskrift af ved eftersyn.

Fortegnelsen over virksomhedens databehandling virker enormt omfattende, men se venligst Justitsministeriets forslag til fortegnelse for personaledata på de næste sider (fra betænkningens side 461 ff).

Der er tale om en fortegnelse, der deles op i kategorier (personale, kunder, leverandører, (ejere, hvis straffeattester v. udbud)) og som laves en gang og herefter kan justeres årligt, hvis der er ændringer.





EKSEMPEL PÅ EN FORTEGNELSE OVER BEHANDLINGSAKTIVITETER VED HR

<b>Dataansvarlig</b>	<b>Myndighedens/virksomhedens navn, CVR-nr. og kontaktoplysninger</b> <i>(adresse, hjemmeside, telefonnummer og e-mail)</i>	Københavns Kommune Økonomiforvaltningen Rådhuset 1599 København V CVR:
	<b>Den fælles dataansvarlige samt dennes kontaktoplysninger</b> <i>(adresse, hjemmeside, telefonnummer og e-mail)</i>	-
	<b>Den dataansvarliges repræsentant samt dennes kontaktoplysninger</b> <i>(adresse, hjemmeside, telefonnummer og e-mail)</i> <i>(Offentlige myndigheder er ikke omfattet, jf. artikel 27, stk. 2, litra b)</i>	-
	<b>Myndighedens/virksomhedens databeskyttelsesrådgiver samt dennes kontaktoplysninger</b> <i>(adresse, hjemmeside, telefonnummer og e-mail)</i>	DPO, Anders Andersen Kongestien XXX, 1111 Kongsted <a href="http://www.hjemmeside.dk">www.hjemmeside.dk</a> + 45 88 88 88 88 dpo@andersandersen.dk

<p><b>Formål (-ene)</b></p>	<p><b>Behandlingens eller behandlingernes formål</b>  <i>(et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige)</i></p>	<p>Personleadministration</p>
<p><b>Kategorierne af registrerede og kategorierne af personoplysningerne</b></p>	<p><b>Kategori af registrerede personer</b>  <i>(eksempelvis borger/kunder, partsrepræsentanter nuværende eller tidligere ansatte, andre virksomheder, andre myndigheder mv.)</i></p>	<p>Der behandles oplysninger om følgende kategorier af registrerede personer:</p> <ul style="list-style-type: none"> <li>a) Ansøgere</li> <li>b) Ansatte</li> <li>c) Tidligere ansatte</li> <li>d) Pårørende</li> <li>e) Borger der henvender sig til Københavns Kommune</li> <li>f) Politikere</li> </ul>

	<p><b>Oplysninger, som behandles om de registrerede personer</b>  <i>(afkryds og beskriv de typer af oplysninger, som er omfattet af behandlingsaktiviteterne)</i></p>	<p>Oplysninger, som indgår i den specifikke behandling.  Beskriv:</p> <p>Identifikationsoplysninger <span style="float: right;">X</span></p> <p>Oplysninger vedrørende ansættelsesforholdet til brug for administration, herunder stilling og tjenestested, lønforhold, oplysninger af relevans for lønindeholdelse, personalepapirer, uddannelse og sygefravær. <span style="float: right;">X</span></p> <p>Race, eller etnisk oprindelse</p> <p>Politisk, religiøs eller filosofisk overbevisning</p> <p>Fagforeningsmæssigt tilhørsforhold <span style="float: right;">X</span></p>
		<p>Helbredsoplysninger herunder genetisk data <span style="float: right;">X</span></p> <p>Biometrisk data med henblik på identifikation <span style="float: right;">X</span></p> <p>Seksuelle forhold</p> <p>Strafbare forhold <span style="float: right;">X</span></p>



<p><b>Modtagerne af personoplysningerne</b></p>	<p><b>Kategorier af modtagere som oplysninger er eller vil blive videregivet til herunder modtagere i tredjelande og internationale organisationer (eksempelvis andre myndigheder, virksomheder, borger/ kunder mv.)</b></p>	<p><b>1. Offentlige myndigheder (så vidt muligt myndighedens navn, f.eks. SKAT)</b></p> <p><b>2. Banker</b></p> <p><b>3. Kreditbureauer</b></p>
<p>Tredjelande og internationale organisationer</p>	<p>Oplysninger om overførelse af personoplysninger til tredjelande eller internationale organisationer (eksempelvis databehandlers placering i tredjelande, databehandlers brug af cloudløsninger placeret i tredjelande)</p>	<p>Nej (Angivelse af virksomhed/ samarbejdspartner, hvis denne er placeret i tredjeland)</p>
<p>Sletning</p>	<p>Tidspunkt for sletning af oplysninger (de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger)</p>	<p>Oplysninger om tidligere ansatte slettes senest X år efter afslutningen af den journalperiode, hvor personalesagen er afsluttet.</p> <p>Oplysninger om ansøgere slettes senest X måneder efter afslutningen af den journalperiode, hvor sagen er afsluttet.</p> <p>Oplysninger overføres løbende til Rigsarkivet efter arkivlovens regler og Statens Arkivers bestemmelser herom.</p>

**Tekniske og organisatoriske sikkerhedsforanstaltninger**

**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger**

*(hvis muligt skal der gives en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, jf. artikel 32, stk. 1)*

Behandling af personoplysninger i forbindelse med HR-arbejde sker i overensstemmelse med interne retningslinjer, som bl.a. fastsætter rammerne for autorisation- og adgangsstyring og logning.

Personoplysninger opbevares i pseudonymiseret og i krypteret form og transmitteres krypteret.

Fysisk materiale opbevares aflåst.

Der anvendes følgende sikkerhedsstandarder: ISOXXXXX.

BACK UP??

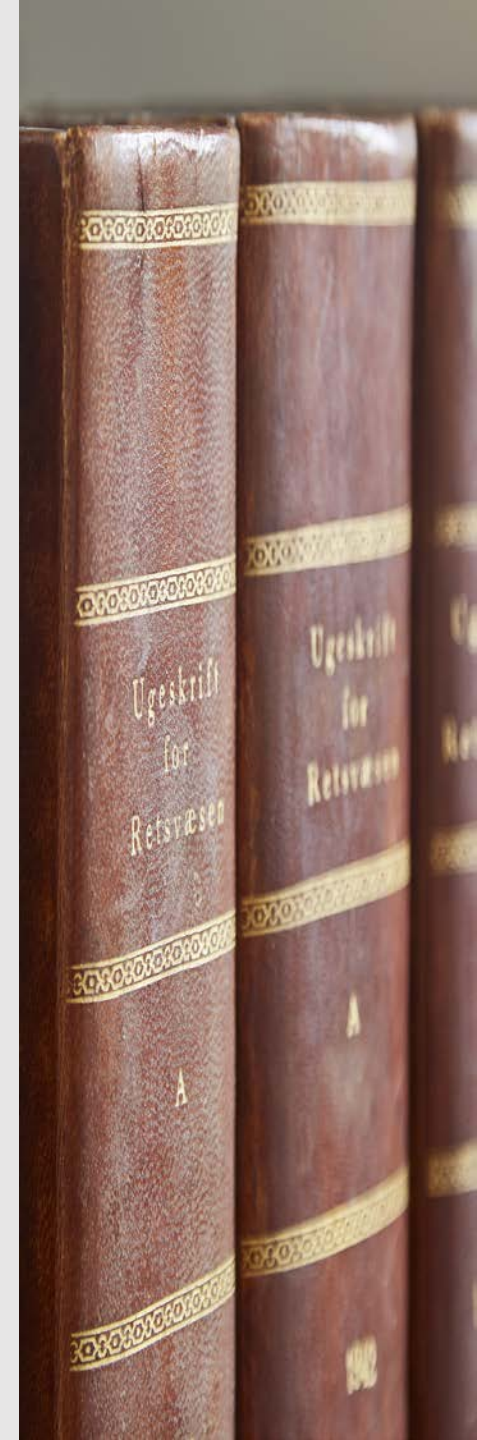


# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

Nugældende regler:

Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt **tilintetgøres**, **fortabes** eller **foringes**, samt mod, at de kommer til uvedkommendes **kendskab**, **misbruges** eller i øvrigt behandles i strid med loven.





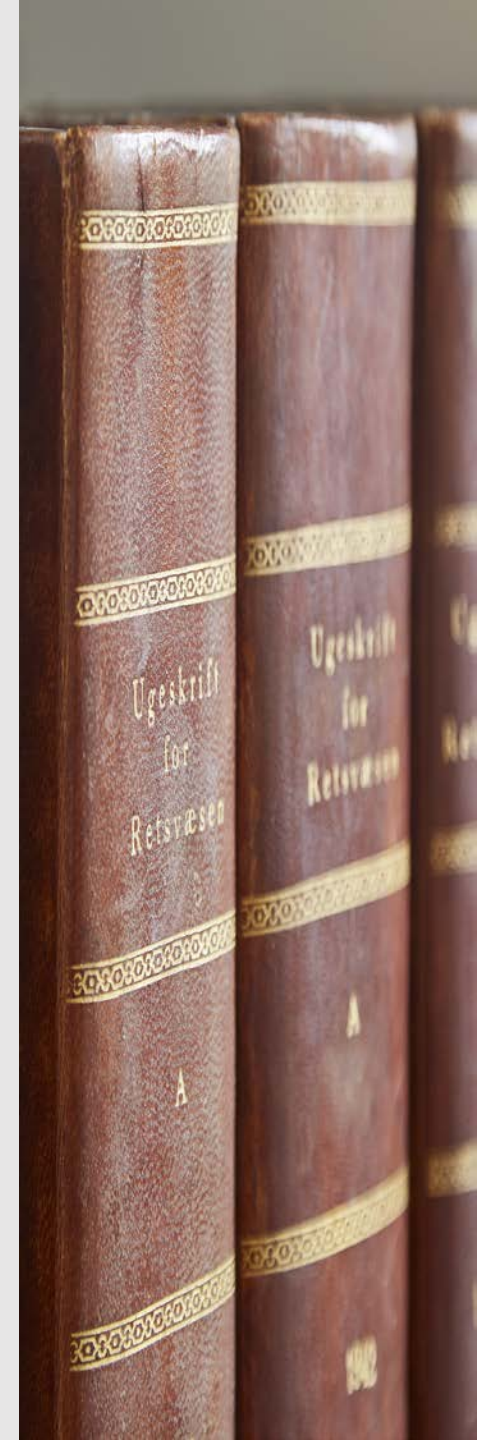
# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

Nye regler:

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansværlige og databehandleren **passende tekniske og organisatoriske foranstaltninger** for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

- a) pseudonymisering og kryptering af personoplysninger
- b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
- d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.



# OVERHOLDELSE AF FORORDNINGEN

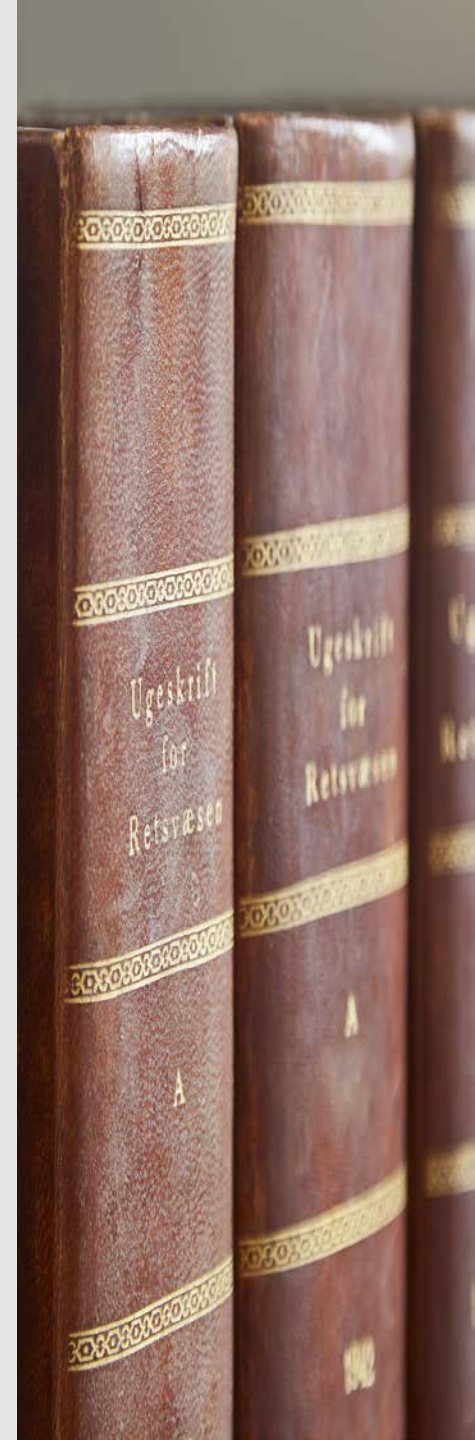
## Behandlingssikkerhed (art. 32)

....”passende tekniske og organisatoriske foranstaltninger”

... Hvad betyder så det??

Følgende lille film viser et kontor uden passende foranstaltninger:

<https://www.youtube.com/watch?v=U3QXMMV-Srs>





# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

Hvad ligger i behandlingssikkerhed?

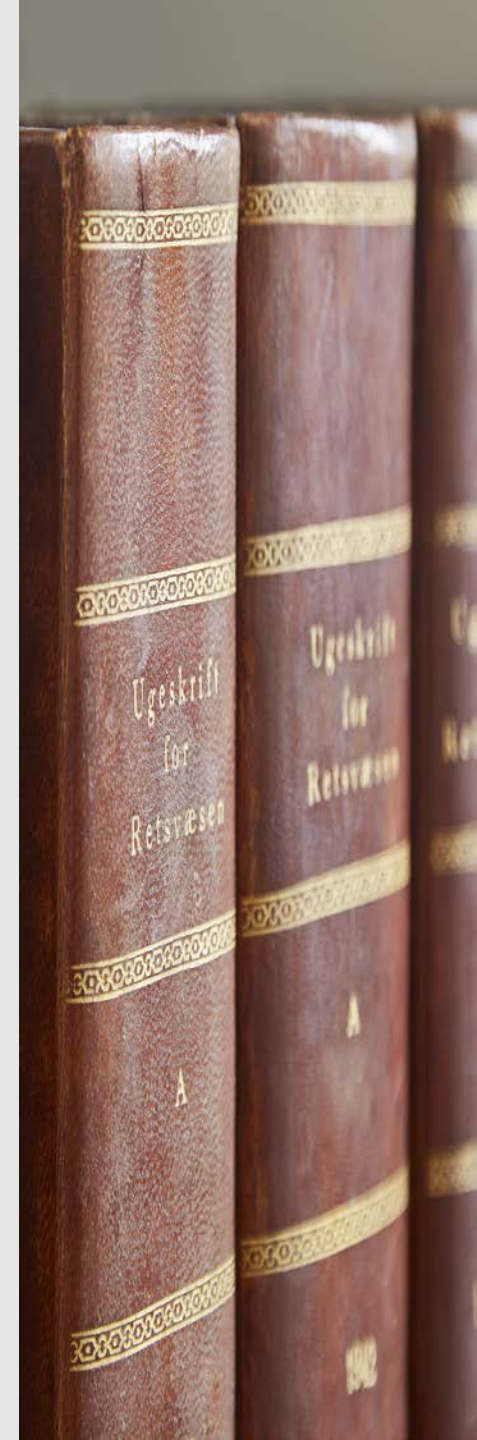
Der må ikke komme nogle **uautoriserede** ind til virksomhedens persondata (internt eller udefra via hacking).

Data må ikke slippe ud.

Indsamling og anvendelse af data skal ske på en sikker måde.

Data må ikke mistes/tilintetgøres/skades.

Anmeldelse af sikkerhedsnedbrud (hacking m.v).





# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

### Organisatorisk

**Informere** medarbejdere om håndtering af persondata,

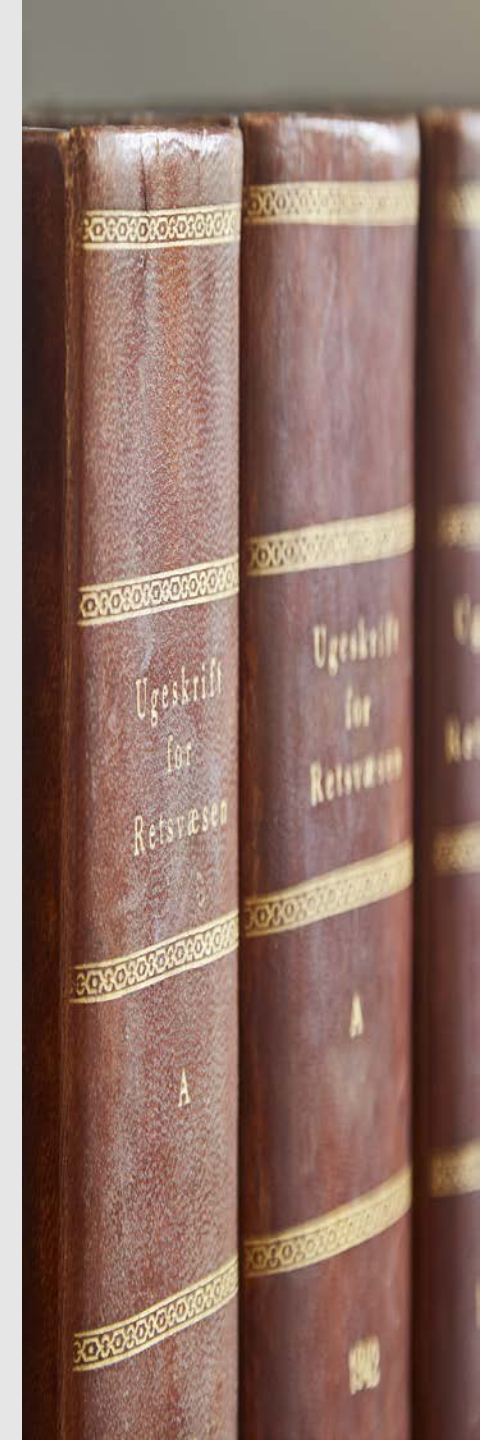
F.eks. gennemgang af og adgang til intern politik/adfærdskodeksom persondata.

Hver medarbejder bør kun få **adgang** til relevante persondata,

F.eks. bør print hentes straks fra kopimaskinen, hvis det indeholder følsomme data.

Fysiske, følsomme persondata skal opbevares **aflåst**, når de ikke er i brug.

Informere jævnligt om aldrig at trykke på ukendte **links**, uanset lokkemaden!





# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

### IT - Adgang til virksomhedens IT-system:

Hver medarbejder bør bruge **hemmeligt** password.

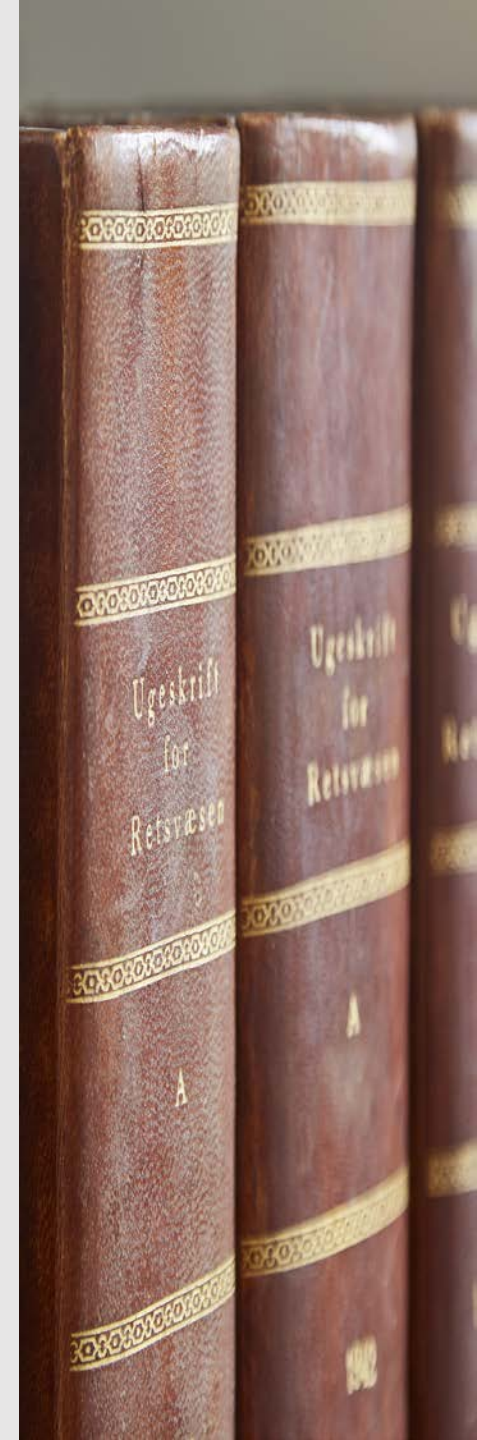
Ved mobile enheder med adgang til virksomhedens data bør anvendes **dobbelt id**.

Ingen medarbejder bør have adgang til alt, kun til **relevante** data.

Andre skal **holdes ude** via firewalls, virustjek, jævnlig opdatering af programmer.

**Gæster** bør ikke kunne koble op på virksomhedens internet.

Evt. kan man have dobbelte netværk (et til virksomhedens data, et til alm. kontorfunktioner som fx labelprinter, alarm, gæstewifi, ventilation)







# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

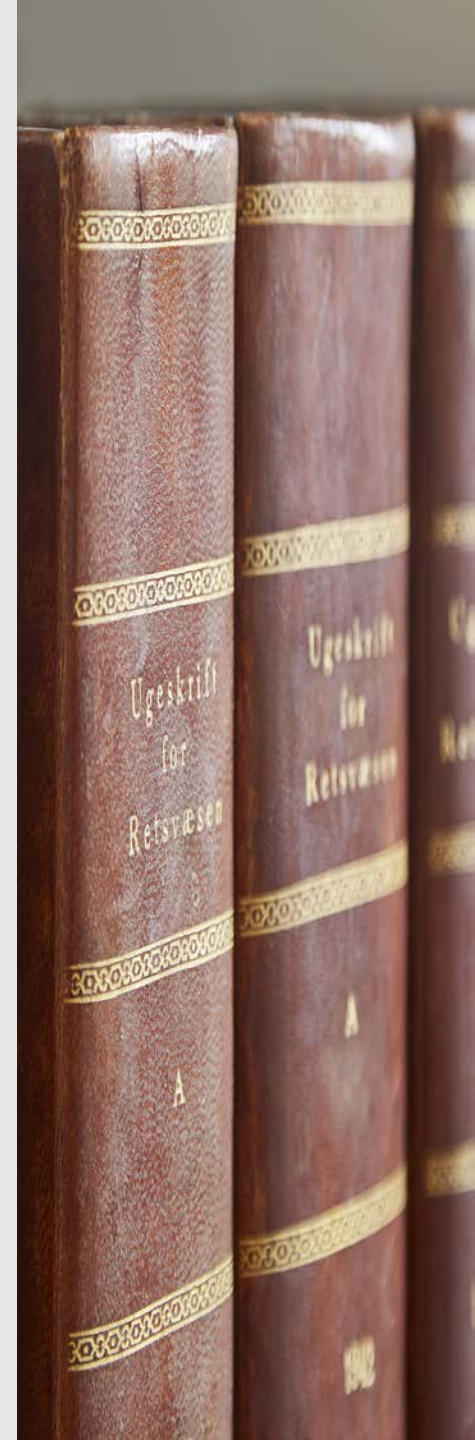
Praktisk i tilfælde af

Sletning

Anmodning om indsigt

Fremvisning af dokumentation for samtykke

**Undtagelse** fra reglerne gennem anonymisering





## OVERHOLDELSE AF FORORDNINGEN

Behandlingssikkerhed (art. 32)

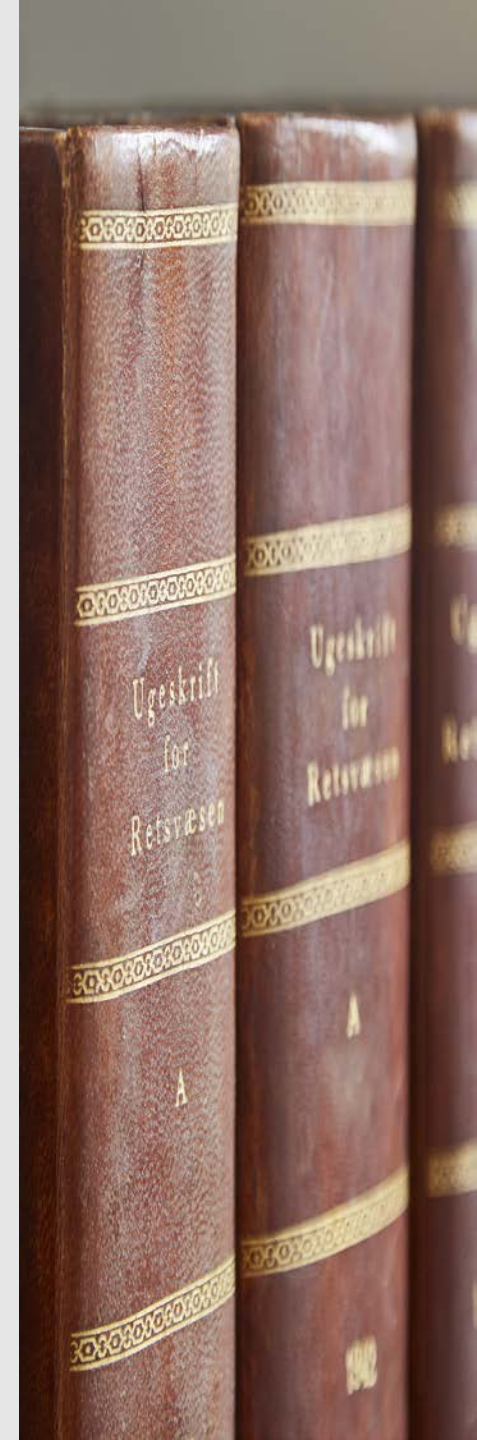
IT - Behandling af persondata:

Virksomhedens back up skal fysisk befinde sig et **andet sted** end serveren.

Hemmeligholdelse; der er ikke nødvendigvis et krav om kryptering af følsomme oplysninger ved **personleadministration**.

Få styr på om persondata også gemmes i printer/scanner/kopimaskine

Virksomhedens (person)data bør jævnligt gemmes i **back up**.





# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

### IT - Overladelse eller videregivelse af persondata:

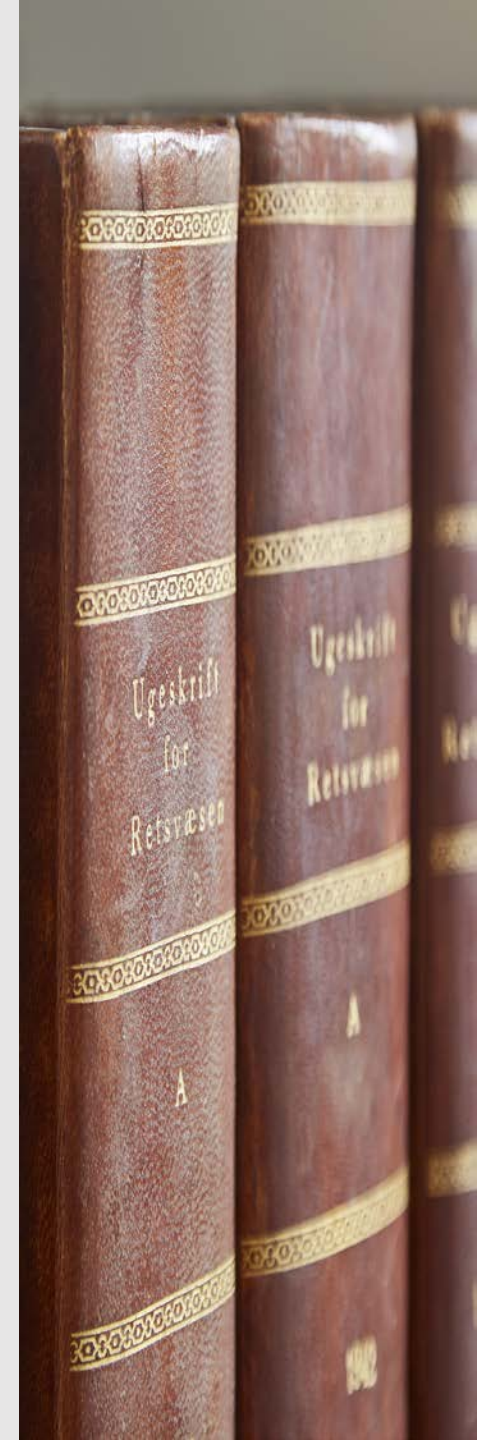
Overladelse til databehandler kræver databehandleraftale

Ved fremsendelse af følsomme oplysninger el. cpr.nr på mail anbefales **kryptering eller anvendelse af adgangskode på vedhæftede filer**

Ingen brug af **personlig** email til arbejdsformål

Ingen brug af **ukendt** wifi på arbejdstelefon/-tablet/-computer

Evt. **kontrol** af hvad der udsendes digitalt fra virksomheden





## OVERHOLDELSE AF FORORDNINGEN

### Behandlingssikkerhed (art. 32)

IT – Kort om CEO-fraud (mere end 200 mill. kr. mistet i DK i 2016-17):

Fast procedure ved overførselsanmodninger bør indføres  
ex. overførsel kræver kodeord både fra bogholder og direktør  
ex. ved tvivl bør ringes/tales, aldrig mailes  
plus sikring

ex programmet DMARC (Domain-based Message Authentication, Reporting and Conformance (DMARC) kan sikre at mail fra virksomhedens domænenavn kommer fra virksomheden, og ikke fra andre

Hvis det sker overførsel alligevel – kontakt straks banken





# OVERHOLDELSE AF FORORDNINGEN

## Behandlingssikkerhed (art. 32)

Se mere om behandling af ansattes data i Datatilsynets vejledning:

<https://www.datatilsynet.dk/erhverv/personaleadministration/krav-om-datasikkerhed-i-forbindelse-med-personaleadministration/>

Anmeldelse af hacking m.v.

**Inden** 72 timer til Datatilsynet (eller tilsvarende myndighed).

Hvis **kritisk** sikkerhedsbrud skal virksomheden informere de registrerede...





## OVERHOLDELSE AF FORORDNINGEN

### Konsekvensanalyse (art. 35)

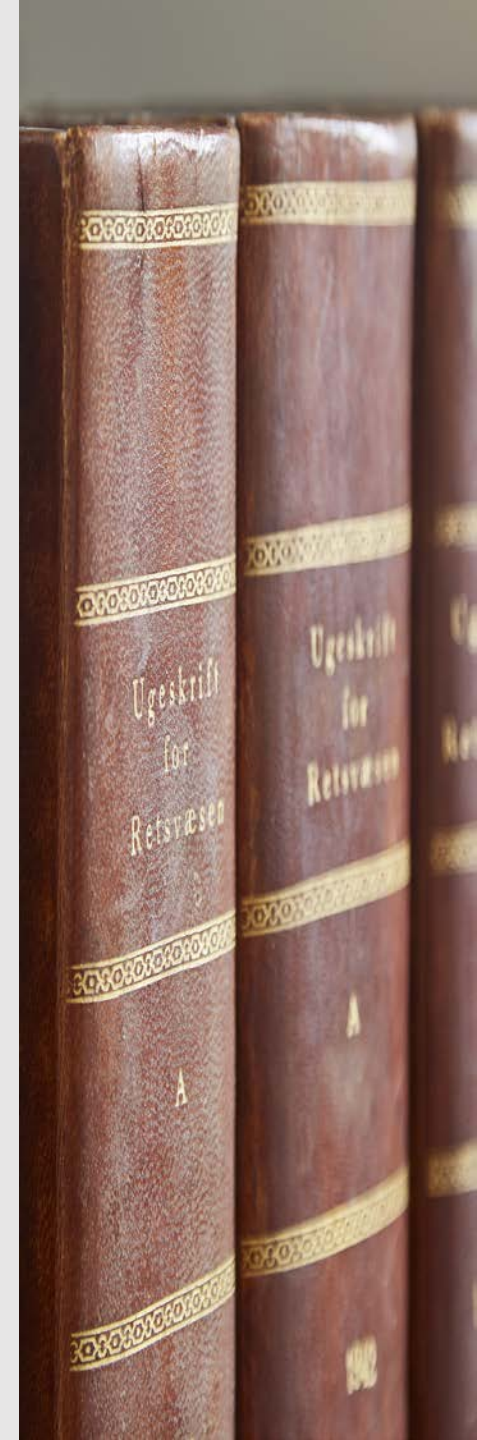
Gælder for virksomheder, som behandler høj-risiko persondata, **særligt:**

En systematisk, omfattende og automatisk vurdering af personlige forhold, der har betydelig indvirkning på den pågældende person.

Behandling i et stort omfang af følsomme oplysninger.

Systematisk overvågning af et offentligt tilgængeligt område i et stort omfang.

Sekretariatets medlemmer pålægges pt. **ikke** at udføre en konsekvensanalyse.





## OVERHOLDELSE AF FORORDNINGEN

### Databeskyttelsesrådgiver (art. 37)

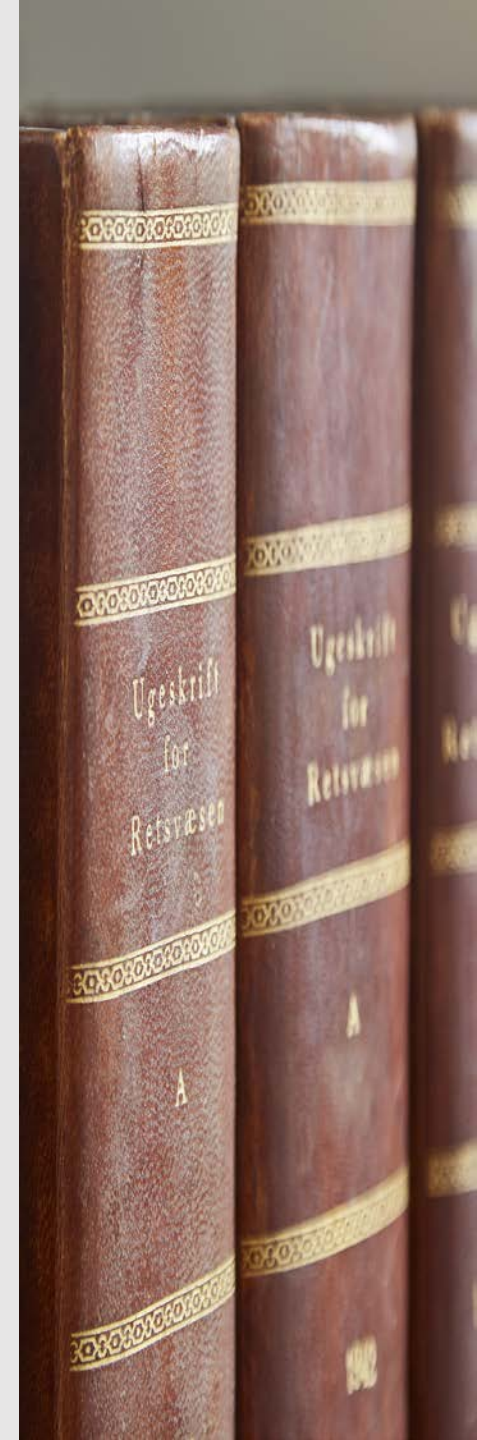
Kræves i virksomheder, som har følgende tre karakteristika:

Behandling af personoplysninger er virksomhedens **kerneaktivitet**

Personoplysninger behandles i et **stort** omfang, og

Behandlingsaktiviteten består i regelmæssig og systematisk overvågning af personer eller behandlingen vedrører følsomme oplysninger.

Sekretariatets medlemmer skal pt. **ikke** have en databeskyttelsesrådgiver.





# OVERHOLDELSE AF FORORDNINGEN

## Adfærdskodeks (art. 40)

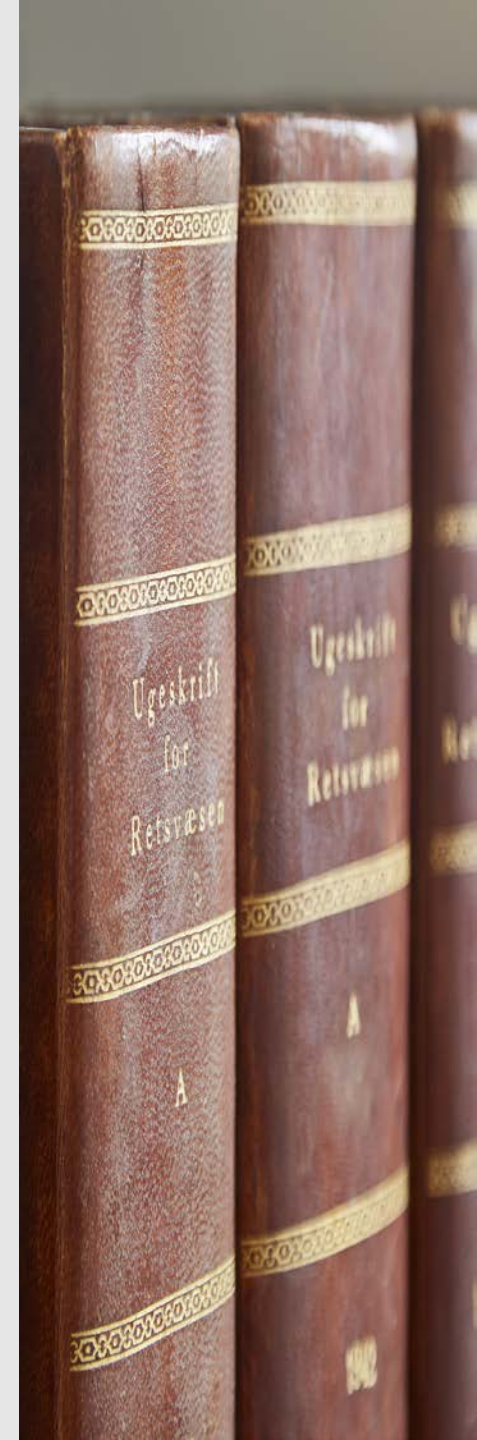
Udarbejdelse og overholdelse af et kodeks om persondata er ikke en pligt, MEN..

Det ville være en god ide at få de persondataregler, som skal overholdes af DMS medlemmer, skrevet ned.

Det ville være med til at øge medarbejderes opmærksomhed, forståelse og overholdelse af persondatareglerne.

Og ikke mindst skal virksomheden kunne påvise overholdelse af persondatareglerne: et kodeks, som medarbejderne er blevet informeret om og overholder, er et meget velegnet element til at påvise overholdelse af virksomhedens forpligtelser i henhold til forordningen.

Sekretariatet vil udarbejde et **kodeks**, tilpasset medlemmernes virksomhedstyper, som medlemmerne kan anvende. Datatilsynet vil blive bedt om at godkende kodekset i maj 2018.







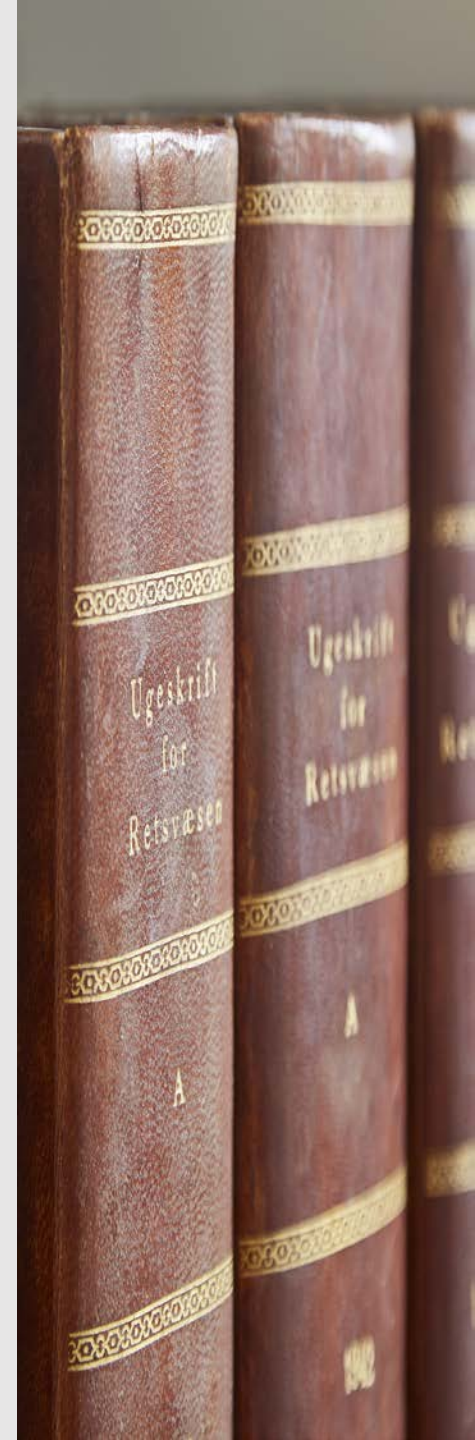
## OVERHOLDELSE AF FORORDNINGEN

### **Certificering (art. 43)**

Certificering er også et velegnet element til at påvise overholdelse af virksomhedens forpligtelser i henhold til forordningen.

Der er endnu ikke nogen certificeringsordninger på plads.

Certificering af persondatabehandling er **ikke** et krav.

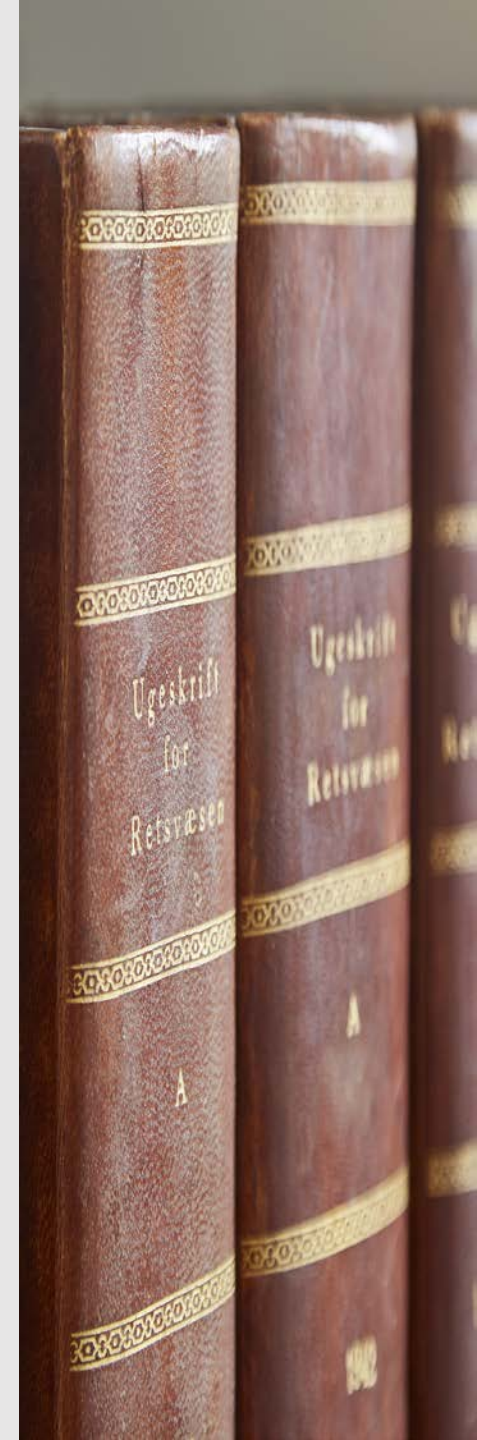




## OVERHOLDELSE AF FORORDNINGEN

Som nævnt er der endnu **uafklarede** områder i forordningen, og vejledninger til forordningen og en ny persondatalov afventes.

Alligevel er der en del, som en virksomhed allerede kan gøre nu for at kunne overholde – og kunne påvise overholdelse af – persondataforordningen fra 25. maj 2018.





## HVAD GØR MAN I PRAKSIS?

### Få styr på:

1. Hvilke **data** virksomheden har, herunder

Hvilke ikke-følsomme data for hhv. ansatte, kunder og samarbejdspartnere,

Hvilke følsomme data for hhv. ansatte, kunder og samarbejdspartnere,

Få slettet forældede data – og unødvendige data.

2. Lav herefter en **fortegnelse** over persondata (se side 30-34).





## HVAD GØR MAN I PRAKSIS?

### Få styr på:

#### 3. Hvilke data virksomheden **indsamler**:

Indsamles kun data til brug for kontrakt / som del af gennemførelse af aftale?

Hvis dette ikke er tilfældet, får virksomheden indhentet et skriftligt samtykke før indsamling?

Følsomme data kræver samtykke – indhent samtykkeerklæringer og gem dem.

#### 4. Sørg herefter for at virksomhedens IT-indstillinger **begrænser** indsamling af persondata ifht. hvad der er brug efter aftalens formål eller samtykke samt at indstillingerne giver adgang til korrektion, sletning og udprintning af data og lav en oversigt over de forskellige indstillinger.





## HVAD GØR MAN I PRAKSIS?

Få styr på:

5. Hvor virksomhedens data er og hvordan de **sikres**

Er IT-systemet forsvarligt sikret, både udefra og indefra? (se s. 8)

Er adgang til data forsvarligt sikret, både udefra og indefra?

Der bør tages jævnlig back up, som gemmes, indtil næste back up er taget.

6. Sørg for at få lavet en **oversigt** over virksomhedens tiltag for at sikre sine persondata (IT-sikkerhed og organisatorisk).





## HVAD GØR MAN I PRAKSIS?

**Få styr på:**

7. Bliver virksomhedens persondata **overført**?

Hvor sker overførslen til? Cloudløsning?

Hvis andre end virksomheden selv skal behandle (evt. bare gemme!) virksomhedens persondata, kræves en skriftlig aftale med databehandleren allerede efter nuværende lov.

Overførsel indenfor EU er typisk OK, men udenfor er ikke uden specifikt samtykke.

Er der givet samtykke til overførslen?





## HVAD GØR MAN I PRAKSIS?

### Få lavet eller gennemgået:

8. Persondatainformation (hvorfor indsamles data, hvad bruges det til, overføres data, registreres rettigheder osv.) til kunder og samarbejdspartnere og få lavet en **offentlig** persondatapolitik med informationen til virksomhedens hjemmeside.

9. Virksomhedens **interne** persondatapolitik (inklusive persondatainformation til medarbejdere), gerne med afsæt i det adfærdskodeks, som DM får udarbejdet og gennemgå det med medarbejderne og gem det et internt tilgængeligt sted.





## HVAD GØR MAN I PRAKSIS?

### Få samlet og gemt:

10. Informationen om gennemgang af punkterne 2)-9) og dokumenterne iht. punkt 2), 3), 6), 8), 9) og evt. 7) for at kunne dokumentere virksomhedens bestræbelser på at opfylde kravene

skal gemmes samlet og tilgængeligt,

hvis nu Datatilsynet skulle spørge om noget.







## HVAD GØR MAN I PRAKSIS?

### Gennemførelse af punkt 1)-10) kan bruges til:

En grundig **oprydning** i gamle data, det kan øge IT-kapaciteten,

Gennemførelse af ny, mindre datatunge arbejdsgange,

Sikre mod hacking og tab af data, og

Overholdelse af persondataskyttelsesforordningen.





ADVOKATGRUPPEN

RET LIGETIL SIDEN 1957