

ITSikkerhedsGruppen´s

# Cloud Act

Hvad er Cloud Act?

---

januar 22, 2026

## Hvad er Cloud Act?

Den amerikanske Cloud Act (Clarifying Lawful Overseas Use of Data Act) blev vedtaget i 2018 og giver amerikanske myndigheder ret til at få adgang til data kontrolleret af amerikanske virksomheder, uanset *hvor i verden* dataene fysisk ligger. Dette gælder bl.a.:

- Amerikanske Cloud-udbydere som Microsoft, iCloud, Google og Amazon
- Softwaretjenester som Teams, Slack m.fl.
- Enhver platform ejet af en amerikansk virksomhed. Uanset om data ligger i Europa eller ej

Loven er ekstraterritorial, hvilket betyder, at den overtrumfer lokal datalovgivning, når amerikanske myndigheder udsteder en gyldig ordre eller warrant. Den kræver heller ikke en international aftale (som f.eks. en MLAT<sup>1</sup>) for at få adgang.

Det kan derfor skabe konflikter med EU´s databeskyttelsesforordning, GDPR, hvis europæiske virksomheder efterkommer en amerikansk Cloud Act-anmodning. Omvendt vil de bryde amerikansk lov, hvis de nægter.

## Risiko for konflikt med GDPR

GDPR kræver, at dataoverførsler til tredjelande som USA kun må ske på baggrund af en international aftale. Men Cloud Act omgår dette, hvilket skaber en juridisk gråzone for alle europæiske virksomheder, der bruger amerikanske Cloud-tjenester.

## Mangel på gennemsigtighed og retssikkerhed

Cloud Act tillader nemlig amerikanske myndigheder at få adgang til data uden at informere brugeren eller europæiske myndigheder og uden EU-retslig prøvelse. En væsentlig trussel mod den europæiske datasuverænit. Selv tjenester og løsninger, der markedsføres som “EU Sovereign Cloud”, kan være omfattet, hvis moderselskabet er amerikansk.

---

<sup>1</sup> En juridisk bindende aftale der gør det muligt for et land at anmode et andet land om f.eks. fremskaffe dokumenter og data, afhøre vidner, gennemføre ransagninger.

## Hvad så med EU's Data Act (Dataforordningen)?

EU's Data Act har et andet formål end Cloud Act. Den handler ikke om myndighedsadgang, men derimod om:

- at give virksomheder og brugere kontrol over egne data
- at sikre ret til datadeling og adgang, især IoT<sup>2</sup>- og Cloud-data
- at modvirke unødige vendor lock-in (leverandørbindinger) (f.eks. fra Cloud-udbydere)
- og at styrke konkurrence og datasuverænitet i EU

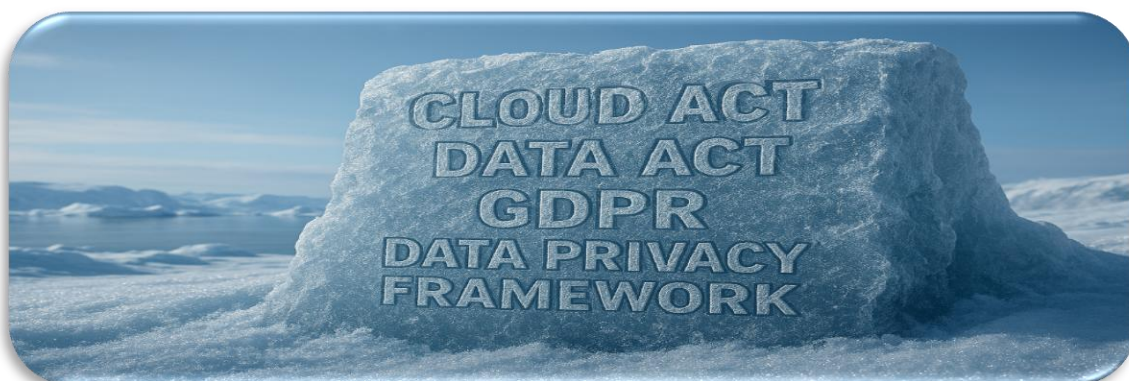
Data Act skal altså forhindre misbrug af kontraktbalancen i datadelingsaftaler, give myndigheder adgang til private data under ekstraordinære omstændigheder (f.eks. nødsituationer), og gøre det nemmere at flytte data mellem Cloududbydere. Det skal gerne fremme innovative tjenester og konkurrence.

Det vil altså sige, at producenter af produkter, der indsamler brugerdata fra f.eks. hårde hvidevarer eller elmålere, skal kunne give brugerne adgang til disse data uden omkostninger.

Data Act pålægger altså virksomheder der opererer i EU at:

- Tillade nem og billig dataportabilitet
- Fjerne switching fees (senest januar 2027)
- Give klare kontraktlige rettigheder til kunder
- Sikre interoperabilitet mellem Cloud-tjenester

**Der er altså fundamentalt forskellige formål med Cloud Act og EU's Data Act.  
De trækker i hver sin retning.**



---

<sup>2</sup> Internet of Things. Fysiske objekter med netværksforbindelse som f.eks. sensorer.

## Hvor Cloud Act kræver retten til dine data, giver Data Act dig rettigheder til at beskytte dem.

### Kan Cloud Act og Data Act fungere sammen i praksis?

Da Cloud Act kan pålægge en amerikansk udbyder at udlevere europæiske data *uden EU-godkendelse*, og vores europæiske forordninger kræver, at sådanne overførsler skal være lovlige under EU-regler, opstår der en uundgåelig konflikt.

Der kræves en gyldig hjemmel for dataoverførsler jf. GDPR. En Cloud Act-ordre er ikke en gyldig ordre.

### Hvad er forsøgt?

For at afbøde den grundlæggende konflikt mellem amerikansk adgang til data og EU's krav om databeskyttelse, har EU og USA gentagne gange forsøgt at etablere fælles aftaler for transatlantiske dataoverførsler. Det seneste forsøg er EU-US Data Privacy Framework (DPF).

DPF blev etableret i 2023 som erstatning for de to tidligere ordninger, Privacy Shield og Safe Harbor, der begge blev kendt ugyldige af EU-Domstolen (Schrems I og II).

Men tanken var god og formålet var at skabe:

- en mere juridisk holdbar ramme for dataoverførsler
- større gennemsigtighed og tilsyn med amerikansk overvågning
- bedre klagemekanismer for EU-borgere

### Men der er udfordringer med Data Privacy Framework

For trods ambitionerne viser udviklingen, at DPF står på usikker grund. Der er stadig tvivl om mekanismerne, der skal sikre uafhængig kontrol. Vi skal huske på, at der som udgangspunkt er tale om en årlig egenkontrol fra de amerikanske virksomheder. Det svarer lidt til, at danske skoleelever selv-evaluerer deres eksamensopgaver, og håber på, at de ikke bliver udtaget til en stikprøvekontrol.

Læg dertil at Cloud Act og FISA<sup>3</sup> fortsat sikrer USA ekstraterritorial adgang til europæiske data, selv når DPF er i kraft.

---

<sup>3</sup> FISA (Foreign Intelligence Surveillance Act) regulerer efterretningsovervågning til national sikkerhed, især rettet mod ikke-amerikanske borgere uden for USA. Section 702 bruges af efterretningstjenester

## Hvorfor DPF ikke løser konflikten fuldt ud

Selv om EU og USA politisk ønsker at bevare DPF, er den ikke en løsning på selve konflikten:

- Cloud Act forbliver amerikansk føderal lov og omgår MLAT-processen
- GDPR kræver stadig, at EU-persondata kun overføres til lande, der giver “tilstrækkelig beskyttelse”

DPF kan gøre det *lettere* at overføre data lovligt i det daglige, men den ændrer ikke på Cloud Act’s fundamentale konfliktelementer.

## Så hvad betyder det for europæiske virksomheder i praksis?

Man skal selvfølgelig ikke gå hen og blive paranoid. Men der skal tages stilling til om Cloud Act er et problem eller om det er et acceptabelt vilkår eller i konflikt med lovgivningen. Det kan f.eks. gøres når der udarbejdes risikovurderinger for ens leverandører. Man bør være opmærksom på leverandørens ejerstruktur, da selv EU-hostede tjenester kan være underlagt Cloud Act.

At der er tale om et “EU datacenter” kan altså ikke alene eliminere risikoen.

Alt tyder på at der fortsat kommer flere EU-leverandører der tilbyder løsninger, der er 100% europæiske i ejerskab og drift. Dette er i dag den eneste sikre vej til fuld Cloud Act-frihed.

---

til at kræve adgang til data hos udbydere for overvågning, ofte uden individuel dommerkendelse i klassisk strafferetslig forstand, og i høj grad hemmeligt