

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Databehandlersaftale

Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold, tilsynspligt og faldgruber

Version 1 · Opdateret 21. jul. 2026 · 19 afgørelser · 2019-2026

[Læs online](#)

INTRODUKTION

En **databehandlersaftale** er den skriftlige kontrakt, der skal regulere forholdet, når en virksomhed eller myndighed (den *dataansvarlige*) lader en anden part (*databehandleren*) behandle personoplysninger på sine vegne – typisk hosting, cloud, lønsystem, CRM, IT-supportydelser, backup, nyhedsbrevsværktøj eller ekstern IT-drift. Kravet følger direkte af [databeskyttelsesforordningen artikel 28, stk. 3](#), som er umiddelbart gældende i Danmark, og aftalen skal foreligge skriftligt, herunder elektronisk, jf. [artikel 28, stk. 9](#).

Parterne er altid to (eller flere) selvstændige juridiske enheder: den dataansvarlige, der efter [artikel 4, nr. 7](#) afgør formål og hjælpemidler, og databehandleren, der efter [artikel 4, nr. 8](#) alene behandler oplysningerne på den dataansvarliges vegne. Rollefordelingen afgøres af de faktiske forhold – ikke af hvad parterne kalder hinanden i kontrakten. Ligger der reelt et selvstændigt skøn hos leverandøren, er vedkommende selvstændigt dataansvarlig, og en databehandlersaftale er da både overflødig og direkte vildledende.

Oversigten er ordnet efter dokumentets naturlige forløb: først *hvornår* pligten udløses, dernæst *hvad* aftalen som minimum skal indeholde (checklisten følger art. 28, stk. 3, litra a-h), og til sidst de fejl der i Datatilsynets praksis faktisk udløser kritik, påbud og bødeindstillinger. Undervejs uddybes rollefordelingen, instruksens betydning, underdatabehandlerkæden, tredjelandsoverførsler og den løbende tilsynspligt, der ikke ophører med aftalens underskrift.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Databehandlersaftalen er **lovpligtig** efter [databeskyttelsesforordningen artikel 28, stk. 3](#), når en leverandør behandler personoplysninger på dine vegne – og den skal foreligge skriftligt (herunder elektronisk), inden behandlingen begynder.
- 02** Rollefordelingen afgøres af de **faktiske forhold**, ikke af kontraktens overskrift: har leverandøren eget skøn over formål og væsentlige midler, er vedkommende selvstændigt dataansvarlig, og en databehandlersaftale er da forkert.
- 03** Aftalen skal som minimum indeholde alle otte elementer i art. 28, stk. 3, litra a-h – mangler ét af dem, er aftalen mangelfuld, uanset hvor omfangsrig den ellers er.
- 04** En databehandler, der behandler oplysninger til egne formål eller uden for instruksen, anses efter [artikel 28, stk. 10](#) selv for dataansvarlig for den behandling – med fuldt selvstændigt ansvar til følge.

- 05** Aftalen er ikke nok i sig selv: ansvarlighedsprincippet i [artikel 5, stk. 2](#) og [artikel 24, stk. 1](#) kræver, at du **fører løbende, dokumenteret tilsyn** med at aftalen faktisk overholdes.
-
- 06** Standardkontraktbestemmelser om tredjelandsoverførsel (SCC'er) kan **ikke stå alene** som databehandleraftale – de dækker overførselsgrundlaget, ikke minimumskravene i art. 28, stk. 3.
-
- 07** Overtrædelse af art. 28 er omfattet af det høje bødeloft i [artikel 83, stk. 4](#) (op til 10 mio. EUR eller 2 % af global omsætning) og straffes i Danmark med bøde eller fængsel indtil 6 måneder efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#).
-
- 08** Både dataansvarlig og databehandler kan gøres erstatningsansvarlige over for den registrerede efter [artikel 82](#) – og de hæfter solidarisk, når begge er involveret i samme behandling.
-

§ 1 Hvornår er dokumentet påkrævet?

Lovpligtig – uden undtagelse og uden bagatelgrænse. Så snart en fysisk eller juridisk person behandler personoplysninger på den dataansvarliges vegne, *skal* behandlingen være reguleret af en kontrakt eller et andet retligt bindende dokument, jf. [artikel 28, stk. 3](#). Der er ingen undtagelse for små virksomheder, for få registrerede, for koncernforbundne selskaber eller for kortvarige forløb. Aftalen skal foreligge, **inden** behandlingen påbegyndes – en aftale indgået efterfølgende reparerer ikke den mellemliggende periode, hvor overladelsen var uhjemlet. Bemærk desuden, at kravet ikke kun rammer den dataansvarlige: databehandleren må efter [artikel 28, stk. 2](#) og [stk. 4](#) heller ikke selv anvende en underdatabehandler uden både godkendelse og en tilsvarende aftale i næste led.

Betinget – pligten udløses af rollen, ikke af kontrakttypen. Det afgørende er, om leverandøren behandler oplysninger *på vegne af* dig og efter din instruks. Er svaret ja – også selv om ydelsen primært er noget andet end databehandling – udløses aftalekravet. Typiske udløsende omstændigheder: leverandøren hoster, drifter, supporterer eller har fjernadgang til et system med personoplysninger; leverandøren opbevarer backup; leverandøren udfører opgaven efter en detaljeret og bindende instruks uden eget skøn. Omvendt udløses pligten *ikke*, når modparten fastlægger sit eget formål og selv bærer et fagligt eller retligt ansvar – revisor, advokat, ekstern rådgiver og typisk også rekrutteringsbureauer og eksterne whistleblower-administratorer med selvstændige vurderingsbeføjelser er som udgangspunkt selvstændigt dataansvarlige. Rene faciliteter uden adgang til data – fx colocation, hvor leverandøren alene leverer plads, strøm, køling og netværk – udløser heller ikke aftalekravet, men gør det, så snart der leveres tillægsydelser som backup, firewall eller hardwarehåndtering med indblik i data.

Særregel for retshåndhævelse. For politiet, anklagemyndigheden, kriminalforsorgen m.fl. gælder GDPR ikke, men et tilsvarende og lige så bindende krav i [retshåndhævelsesloven § 22, stk. 2](#), der oplister kravene til den skriftlige aftale, herunder at overladelse til en anden databehandler efter en generel aftale skal varsles senest 14 dage forud, jf. [§ 22, stk. 3](#).

Frivilligt, men retssikrende. Selve databehandleraftalen er aldrig frivillig, men det *er* frivilligt at gå videre end minimumskravene: fastsætte konkrete slettefrister, krav om kryptering, responstider ved indsigtsanmodninger, ISAE 3000-revisionserklæringer, bod ved misligholdelse og en egentlig exitplan. Uden sådanne vilkår står du med en aftale, der formelt opfylder art. 28, men som i praksis er svær at håndhæve. Er modparten

derimod selvstændigt dataansvarlig, findes ingen aftalepligt efter art. 28 – her kan et fælles dataansvar efter [artikel 26](#) være påkrævet, og ellers er en fortrolighedsaftale eller en datadelingsaftale den frivillige, men anbefalelsesværdige løsning.

§ 2 Det skal dokumentet indeholde

1. Aftalen skal foreligge skriftligt, herunder elektronisk, og være et retligt dokument der er bindende for databehandleren i forhold til den dataansvarlige. Den kan udformes som selvstændig aftale eller som et afsnit/bilag i hovedkontrakten. (*Databeskyttelsesforordningen § 28, stk. 9*)
2. Aftalen skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger, kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Rammen skal være konkret nok til, at man kan se præcis hvilke oplysninger leverandøren behandler og hvorfor. (*Databeskyttelsesforordningen § 28, stk. 3*)
3. Det skal fremgå, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige – herunder for så vidt angår overførsel til tredjelande. Aftalen skal desuden pålægge databehandleren omgående at underrette den dataansvarlige, hvis en instruks efter databehandlerens opfattelse strider mod databeskyttelsesreglerne. (*Databeskyttelsesforordningen § 28, stk. 3*)
4. Databehandleren skal sikre, at de personer, der er autoriseret til at behandle oplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. (*Databeskyttelsesforordningen § 28, stk. 3*)
5. Databehandleren skal iværksætte alle sikkerhedsforanstaltninger, som kræves efter artikel 32 – pseudonymisering/kryptering, fortrolighed, integritet, tilgængelighed, robusthed samt regelmæssig afprøvning. Foranstaltningerne bør konkretiseres i et bilag, så de kan kontrolleres. (*Databeskyttelsesforordningen § 32, stk. 1*)
6. Aftalen skal fastsætte betingelserne for brug af underdatabehandlere: forudgående specifik eller generel skriftlig godkendelse, underretning om planlagte tilføjelser eller udskiftninger, og en reel mulighed for den dataansvarlige at gøre indsigelse. En "flydende" underdatabehandlerliste, som leverandøren ensidigt kan ændre, opfylder ikke kravet. (*Databeskyttelsesforordningen § 28, stk. 2*)
7. Databehandleren skal pålægge enhver underdatabehandler de samme databeskyttelsesforpligtelser via en tilsvarende aftale og forbliver fuldt ansvarlig over for den dataansvarlige for underdatabehandlerens opfyldelse. Beskyttelsesniveauet må ikke sænkes ned gennem leverandørkæden. (*Databeskyttelsesforordningen § 28, stk. 4*)
8. Databehandleren skal – under hensyn til behandlingens karakter og så vidt muligt ved passende tekniske og organisatoriske foranstaltninger – bistå den dataansvarlige med at besvare de registreredes anmodninger om indsigt, sletning, berigtigelse, dataportabilitet mv. efter forordningens kapitel III. (*Databeskyttelsesforordningen § 28, stk. 3*)
9. Databehandleren skal bistå den dataansvarlige med at overholde artikel 32-36, dvs. behandlingssikkerhed, anmeldelse og underretning ved brud på persondatasikkerheden samt konsekvensanalyser og forudgående høring. Aftalen bør fastsætte konkrete frister for underretning ved brud, så den dataansvarliges 72-timers frist kan overholdes. (*Databeskyttelsesforordningen § 28, stk. 3*)
10. Det skal fremgå, at databehandleren efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger, når tjenesterne ophører, og sletter eksisterende kopier – medmindre EU-ret

eller national ret kræver fortsat opbevaring. Format og frist for tilbagelevering bør aftales konkret.

(*Databeskyttelsesforordningen § 28, stk. 3*)

11. Databehandleren skal stille alle oplysninger til rådighed, der er nødvendige for at påvise overholdelse af artikel 28, og give mulighed for og bidrage til revisioner og inspektioner udført af den dataansvarlige eller en bemyndiget revisor. Aftalen bør fastlægge tilsynsform og -frekvens (fx årlig ISAE 3000-erklæring) ud fra en risikovurdering. (*Databeskyttelsesforordningen § 28, stk. 3*)
12. Sker der overførsel til tredjelande – også som følge af underdatabehandlere eller en klausul om efterlevelse af udenlandske myndighedskrav – skal aftalen både indeholde instruksen herom og et gyldigt overførselsgrundlag efter forordningens kapitel V, typisk Kommissionens standardkontraktbestemmelser eller en tilstrækkelighedsafgørelse. (*Databeskyttelsesforordningen § 46, stk. 2*)
13. Aftalen bør herudover regulere de kommercielle og praktiske forhold, som forordningen ikke kræver: kontaktpunkter hos begge parter, vederlag for bistand og audits, ikrafttræden og ophør sammen med hovedkontrakten, misligholdelsesbeføjelser samt ansvars- og regresfordeling mellem parterne.

LOV

[Databeskyttelsesforordningen § 28, stk. 2, 3, 4, 9](#)[Databeskyttelsesforordningen § 32, stk. 1](#)[Databeskyttelsesforordningen § 46, stk. 2](#)

§ 3 Dataansvarlig, databehandler eller fælles dataansvarlig?

Alt afhænger af rollefordelingen, og den afgøres ikke af kontraktens overskrift, men af hvem der reelt bestemmer **formålet** med og de væsentligste **hjælpemidler** til behandlingen. Efter [databeskyttelsesforordningen artikel 4, nr. 7](#) er den dataansvarlige den, der alene eller sammen med andre afgør formål og hjælpemidler, mens databehandleren efter [artikel 4, nr. 8](#) alene behandler oplysningerne på den dataansvarliges vegne.

Datatilsynet har trukket grænsen skarpt op i en række vejledende udtalelser. I sagen om outsourcing af interne whistleblowerordninger (j.nr. 2021-211-6947) opstillede tilsynet tre scenarier: leverer tredjeparten alene en it-plattform, som arbejdsgiverens egne medarbejdere bruger, foreligger der utvivlsomt en databehandlerkonstruktion. Har leverandøren derimod skønsmæssige beføjelser til selv at vurdere, sortere eller afvise indberetninger, agerer parterne som udgangspunkt som **selvstændige dataansvarlige** – og det er ikke afgørende, at arbejdsgiveren har "igangsat" behandlingen ved at tilkøbe en ydelse. Samme logik forklarer, hvorfor revisor, advokat og eksterne rådgivere med eget fagligt ansvar normalt ikke er databehandlere.

Grænsen kan også gå den anden vej: i j.nr. 2022-212-3470 fastslog Datatilsynet, at en leverandør af ren colocation – plads i et serverskab, strøm, køling og netværk – **ikke** er databehandler, fordi ydelsen ikke består i behandling af personoplysninger. Databehandlerstatus indtræder først, hvis leverandøren får adgang til oplysningerne, håndterer hardware med indblik i data, eller leverer tillægsydelser som backup, firewall eller redundans. For netop de tillægsydelser skal der så indgås en databehandleraftale.

Er rollen derimod delt – to parter fastlægger i fællesskab formål og hjælpemidler – gælder [artikel 26](#) om fælles dataansvar. Så skal der laves en *ordning* mellem parterne, der gennemsigtigt fastlægger deres respektive ansvar, navnlig for de registreredes rettigheder og oplysningspligten, og ordningens væsentligste indhold skal gøres tilgængeligt for de registrerede. Det er en anden aftaletype end databehandleraftalen og kan ikke erstatte den. Datatilsynet påpegede i tilsynet med Varde Kommune (j.nr. 2018-423-0018), at begrebet fælles dataansvar retter sig mod eksterne juridiske enheder – interne ansvarsdelegeringer i egen organisation er ikke

fælles dataansvar, og at kunne skelne mellem databehandlere og selvstændige dataansvarlige er samtidig en forudsætning for en korrekt artikel 30-fortegnelse.

LOV

Databeskyttelsesforordningen § 4

Databeskyttelsesforordningen § 26, stk. 1

Databeskyttelsesforordningen § 28, stk. 1

Databeskyttelsesforordningen § 30, stk. 1

PRAKSIS

Datatilsynet · Vurdering af databehandlerstatus for leverandører af colocation-ydelser

17.03.2023

Datatilsynet · Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning?

13.10.2021

Datatilsynet · Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter

10.08.2020

§ 4 Instruksen er aftalens kerne – og databehandlerens grænse

Alle otte krav i art. 28, stk. 3, litra a-h kredser om samme grundtanke: databehandleren behandler aldrig oplysninger til egne formål. Det udtrykkes både i [artikel 28, stk. 3, litra a](#) om dokumenteret instruks og i [artikel 29](#), hvorefter databehandleren og enhver, der udfører arbejde for parterne, kun må behandle oplysningerne efter instruks fra den dataansvarlige.

En instruks, der blot henviser til sig selv, er ubrugelig. Den skal beskrive, hvilke behandlinger leverandøren må foretage, i hvilke systemer, hvilke oplysningstyper der er omfattet, hvor længe, og hvad der udtrykkeligt ikke er tilladt. Modstykket er databehandlerens pligt efter art. 28, stk. 3, sidste afsnit til **omgående** at underrette den dataansvarlige, hvis en instruks efter databehandlerens opfattelse strider mod forordningen – en sikkerhedsventil, der kun virker, hvis instruksen er tilstrækkelig konkret til, at den kan vurderes.

Sanktionen for at gå uden for instruksen er indbygget i forordningen selv: overtræder databehandleren reglerne ved at fastlægge formålene med og hjælpemidlerne til behandlingen, anses vedkommende efter [artikel 28, stk. 10](#) for dataansvarlig for den pågældende behandling – med krav om selvstændigt behandlingsgrundlag, oplysningspligt og fuldt ansvar. Datatilsynet udtalte i j.nr. 2019-442-3996 alvorlig kritik af netop en databehandler, der behandlede personoplysninger uden for instruksen.

Instruksen dækker også sikkerheden. I Schultz-sagen (j.nr. 2019-431-0048) blev en sikkerhedskomponent i et kommunalt fagsystem deaktiveret under en opdatering og aldrig genaktiveret, hvorved medarbejdere i flere kommuner fik adgang til oplysninger om ca. 1,5 mio. borgere. Datatilsynet udtalte kritik direkte efter [artikel 28, stk. 3, litra f](#), jf. [artikel 32](#), fordi databehandleren ikke havde procedurer for at kontrollere ændringer. Tilsvarende fik KMD alvorlig kritik i j.nr. 2021-431-0126 for manglende end-to-end-test af en snitflade, hvor kommunerne netop havde en berettiget forventning baseret på databehandleraftalen. Bistandsforpligtelsen efter litra f rækker desuden ind i brudhåndteringen: databehandleren skal efter [artikel 33, stk. 2](#) underrette den dataansvarlige uden unødigt forsinkelse, og aftalen bør derfor sætte en konkret frist, så den dataansvarliges 72-timers frist kan overholdes.

LOV

Databeskyttelsesforordningen § 28, stk. 3, 10

Databeskyttelsesforordningen § 29

Databeskyttelsesforordningen § 32, stk. 1

Databeskyttelsesforordningen § 33, stk. 2

PRAKSIS

Datatilsynet · Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger

25.08.2022

Datatilsynet · Kritik af Schultz efter sikkerhedshul i fagsystemet Expose

22.09.2020

Datatilsynet · Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks

19.12.2019

§ 5 Underdatabehandlere: kæden af aftaler må ikke sænke beskyttelsen

Næsten alle moderne it-leverancer hviler på underleverandører, og forordningen følger kæden hele vejen ned. Efter [artikel 28, stk. 2](#) må databehandleren ikke anvende en anden databehandler uden forudgående **specifik eller generel skriftlig godkendelse**, og ved generel godkendelse skal databehandleren underrette om planlagte tilføjelser eller udskiftninger, så den dataansvarlige kan gøre indsigelse. Efter [artikel 28, stk. 4](#) skal underdatabehandleren pålægges de samme forpligtelser, og den oprindelige databehandler forbliver fuldt ansvarlig over for den dataansvarlige, hvis underleddet svigter.

Datatilsynet har udtalt, at forordningen ikke kræver, at samtlige underdatabehandlere står i selve aftaledokumentet – listen kan ligge i et tillæg – men at listen skal være retvisende, vedvarende tilgængelig og løbende ajourført. En "flydende" liste, som leverandøren ændrer uden at inddrage den dataansvarlige, vil normalt ikke være i overensstemmelse med reglerne, netop fordi den udhuler godkendelses- og indsigelsesretten. Grundtanken er, at de registreredes beskyttelse ikke må sænkes, blot fordi behandlingen overlades videre i kæden, og at resultaterne af leverandørens screening af underdatabehandlere skal kunne udleveres til den dataansvarlige.

Hvad der sker, når kæden ikke fungerer, illustreres af j.nr. 2022-431-0167, hvor Datatilsynet udtalte alvorlig kritik af en underdatabehandler, der nægtede at udlevere oplysninger til den dataansvarlige. Uden en aftale, der viderefører oplysnings- og auditforpligtelserne, står den dataansvarlige uden reel adgang til at kontrollere, hvordan oplysningerne behandles i sidste led – og kan dermed ikke løfte sin ansvarlighedsforpligtelse.

En ofte overset detalje: også databehandleren har selvstændige forpligtelser, som aftalen ikke kan fritage for. Databehandleren skal efter [artikel 30, stk. 2](#) føre sin egen fortegnelse over de kategorier af behandlinger, der foretages på vegne af hver enkelt dataansvarlig, herunder over tredjelandsoverførsler og de generelle sikkerhedsforanstaltninger.

LOV	Databeskyttelsesforordningen § 28, stk. 2, 4	Databeskyttelsesforordningen § 30, stk. 2
PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	23.01.2026
	Datatilsynet · Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	07.02.2022

§ 6 Tredjelandsoverførsler – databehandleraftalen er ikke i sig selv et overførselsgrundlag

Ligger databehandleren eller en underdatabehandler uden for EU/EØS, eller kan data tilgås derfra, gælder forordningens kapitel V oveni art. 28. Efter [artikel 44](#) må overførsel kun ske, hvis kapitlets betingelser er opfyldt, og beskyttelsesniveauet ikke undermineres. Grundlaget kan være en tilstrækkelighedsafgørelse efter [artikel 45](#) eller fornødne garantier efter [artikel 46, stk. 2, litra c](#) – Kommissionens standardkontraktbestemmelser (SCC'er).

De to regelsæt må ikke forveksles. I sagen om Aarhus Universitet (j.nr. 2023-421-0001) havde universitetet anvendt SCC'er over for en australsk databehandler uden en særskilt databehandleraftale. Datatilsynet fastslog, at det ikke er tilstrækkeligt alene at etablere et overførselsgrundlag: der skal også foreligge et retligt bindende dokument, der indholdsmæssigt opfylder minimumskravene i art. 28, stk. 3. Tilsynet accepterede udtrykkeligt, at man samler det i **ét** dokument – men så skal dokumentet dække begge sæt krav, og standardbestemmelserne

må ikke ændres i strid med deres indhold, da de derved bliver en ad hoc-aftale, der kræver Datatilsynets godkendelse.

Den praktisk farligste bestemmelse er den lille klausul om efterlevelse af udenlandsk lovgivning. I KOMBIT/AWS-sagen (j.nr. 2022-212-3529) indeholdt databehandleraftalen et vilkår om, at leverandøren kunne flytte data ud af den valgte region, hvis det var nødvendigt for at overholde "the law or binding order of a governmental body". Datatilsynet fandt, at der var tale om en **tilsigtet** overførsel for kommunernes vedkommende, netop fordi instruksen ikke var geografisk afgrænset – og at en tredjelandsmyndigheds anmodning ikke i sig selv udgør et overførselsgrundlag, medmindre den hviler på en international aftale, jf. [artikel 48](#). Datatilsynet har senest i j.nr. 2025-211-3556 taget stilling til rækkevidden af sådanne generelle tilladelser til tredjelandsoverførsler i databehandleraftaler.

Endelig kan cloudleverandørens egen brug af data give problemer, som databehandleraftalen ikke løser. I vurderingen af Region Syddanmarks påtænkte migrering til Microsoft 365 (j.nr. 2023-431-0012) understregede Datatilsynet, at en standardløsning eller markedsposition ikke fritager den dataansvarlige for at påvise lovlighed efter [artikel 5, stk. 2](#), og at der skal kortlægges, om leverandøren behandler oplysninger til **egne** formål – for i så fald er der tale om videregivelse, der kræver selvstændigt behandlingsgrundlag, og ikke om databehandling.

LOV	Databeskyttelsesforordningen § 28, stk. 3	Databeskyttelsesforordningen § 44
	Databeskyttelsesforordningen § 45, stk. 1	Databeskyttelsesforordningen § 46, stk. 2
PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler 23.01.2026	
	Datatilsynet · Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter 22.05.2024	
	Datatilsynet · Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger 15.02.2024	
	Datatilsynet · Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande 29.03.2022	

Aftalen er ikke nok – tilsynsplikten, sanktioner og erstatningsansvaret

Den enkeltstående mest gentagne udtalelse i Datatilsynets praksis er, at den dataansvarlige **ikke** kan løfte ansvarlighedsprincippet ved blot at indgå en databehandleraftale. Kravet følger af [artikel 5, stk. 2](#) og [artikel 24, stk. 1](#) sammenholdt med [artikel 28, stk. 1](#), hvorefter man udelukkende må benytte databehandlere, der kan stille de fornødne garantier. Den dataansvarlige må derfor føre et større eller mindre tilsyn med, at aftalen faktisk overholdes, og – som Datatilsynet formulerede det i tilsynet med Hjemrejsestyrelsen (j.nr. 2021-421-0101) – jo større risici for de registrerede, jo større krav til tilsynets form og hyppighed.

Praksis viser en tydelig linje. Randers Kommune fik alvorlig kritik for mangelfuld styring af databehandlere (j.nr. 2018-423-0021). Region Hovedstaden (j.nr. 2020-422-0025) og Region Syddanmark (j.nr. 2020-422-0026) fik kritik for slet ikke at have taget stilling til tilsynsniveauet eller for ikke at gennemføre det årlige tilsyn, deres egne retningslinjer krævede. Aarhus Universitet (j.nr. 2023-421-0001) og Styrelsen for International Rekruttering og Integration (j.nr. 2021-421-0102) fik kritik for manglende tilsyn. Omvendt slap Beskæftigelsesministeriet (j.nr. 2021-421-0097), Skatteforvaltningen (j.nr. 2021-421-0099), Sundhedsdatastyrelsen (j.nr. 2021-421-0100) og Hjemrejsestyrelsen (j.nr. 2021-421-0101) for kritik, fordi de kunne dokumentere en risikobaseret og faktisk

gennemført tilsynsmodel. Konklusionen er praktisk: fastsæt tilsynsniveauet i selve aftalen, vælg et koncept (fx årlig ISAE 3000-revisionserklæring, certificering eller egen kontrol), og gem dokumentationen.

Sanktionsmæssigt hører overtrædelse af art. 28 til det lavere bødeloft i [artikel 83, stk. 4](#) – op til 10 mio. EUR eller 2 % af den samlede globale årlige omsætning, alt efter hvad der er højest. Danmark har ikke administrative bøder: Datatilsynet politianmelder og indstiller til bøde, og overtrædelse af den dataansvarliges og databehandlers forpligtelser efter forordningens artikel 25-39 – herunder art. 28 – straffes efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#) med bøde eller fængsel indtil 6 måneder. Kriterierne i art. 83, stk. 2 skal følges ved strafudmålingen, jf. [§ 41, stk. 3](#), sager kan afgøres med bødeforelæg efter [§ 42](#), juridiske personer kan straffes, og offentlige myndigheder er efter [§ 41, stk. 6](#) undtaget fra straffelovens § 27, stk. 2. Forældelsesfristen er 5 år. Praksis for bødeniveauet og de øvrige overtrædelsestyper er samlet i [oversigten over Datatilsynets bødesager](#), og tilsynets afgørelsespraksis i bredere forstand i [oversigten over Datatilsynets afgørelser](#). Anvendes leverandørens løsning til automatiserede eller AI-baserede behandlinger, er der supplerende krav beskrevet i [oversigten om AI-systemer og GDPR](#).

Oven i straffen kommer det civilretlige: efter [artikel 82](#) har enhver, der har lidt materiel eller immateriel skade, ret til erstatning fra den dataansvarlige eller databehandleren, og er begge involveret i samme behandling, hæfter de **solidarisk** for hele skaden. Databehandleren hæfter navnlig, hvis vedkommende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser – endnu en grund til, at instruksen skal være skrevet ned og præcis.

LOV	Databeskyttelsesforordningen § 5, stk. 2	Databeskyttelsesforordningen § 24, stk. 1
	Databeskyttelsesforordningen § 82, stk. 2	Databeskyttelsesforordningen § 83, stk. 4
	Databeskyttelsesloven § 41, stk. 1	Databeskyttelsesloven § 42
PRAKSIS	Datatilsynet · Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter	22.05.2024
	Datatilsynet · Kritik af Styrelsen for International Rekruttering og Integrations manglende tilsyn med databehandlere	16.12.2022
	Datatilsynet · Datatilsynets kontrol med Sundhedsdatastyrelsens tilsyn med databehandlere	16.12.2022
	Datatilsynet · Datatilsynets tilsyn med Hjemrejsestyrelsens kontrol af databehandlere resulterer i ingen kritik	15.12.2022
	Datatilsynet · Beskæftigelsesministeriets tilsyn med databehandler: Datatilsynet udtaler ingen kritik	15.12.2022
	Datatilsynet · Skatteforvaltningens tilsyn med databehandlere i overensstemmelse med reglerne	15.12.2022
	Datatilsynet · Kritik af Region Syddanmark for mangelfuld kontrol med personoplysninger til forskning	20.07.2022
	Datatilsynet · Kritik af Region Hovedstaden for manglende databehandleraftale og kontrol med underdatabehandlere i forskningsprojekt	16.02.2022
	Datatilsynet · Alvorlig kritik af Randers Kommunes mangelfulde styring af databehandlere	05.08.2019

§ 8 Typiske faldgruber

Databehandleraftale med en, der slet ikke er databehandler. Revisor, advokat, ekstern rådgiver og typisk også rekrutteringsbureauer og whistleblower-administratorer med selvstændige vurderingsbeføjelser er som hovedregel **selvstændigt dataansvarlige** – de fastlægger selv formålet med deres behandling og bærer eget fagligt ansvar. Datatilsynet fastslog i j.nr. 2021-211-6947 om outsourcing af whistleblowerordninger, at parterne som udgangspunkt hver især agerer som selvstændige dataansvarlige, når leverandøren har

skønsmæssige beføjelser. En databehandleraftale i den situation giver falsk tryghed: den dokumenterer en instruksbeføjelse, du ikke har, og skjuler at der reelt sker en videregivelse, som kræver selvstændig hjemmel.

Aftalen indgås først efter, at behandlingen er gået i gang. Kravet i art. 28, stk. 3 er en forudsætning for overhovedet at måtte overlade oplysningerne – ikke en efterfølgende dokumentationsøvelse. I Datatilsynets tilsyn med Region Hovedstadens forskningsprojekter (j.nr. 2020-422-0025) blev det konstateret, at databehandleraftalen med et udenlandsk center først blev indgået længe efter, at centret var inkluderet i projektet. Perioden uden aftale kan ikke repareres bagudrettet og udgør en selvstændig overtrædelse.

Leverandørens standardaftale accepteres ukritisk. Store cloud- og SaaS-leverandører leverer standardvilkår med ensidig ændringsret, brede formålsbeskrivelser og "flydende" underdatabehandlerlister. Datatilsynet har udtalt, at en liste over underdatabehandlere, som leverandøren kan ændre uden løbende inddragelse af den dataansvarlige, normalt **ikke** vil være i overensstemmelse med reglerne, fordi det udhuler godkendelses- og indsigelsesretten i [artikel 28, stk. 2](#). Ansvar for at aftalen lever op til kravene ligger hos dig som dataansvarlig – også når leverandøren er markedsdominerende.

SCC'er bruges som erstatning for databehandleraftalen. Kommissionens standardkontraktbestemmelser er et *overførselsgrundlag* efter kapitel V – ikke en databehandleraftale. I Datatilsynets afgørelse om Aarhus Universitet (j.nr. 2023-421-0001) havde universitetet anvendt SCC'er over for en australsk databehandler uden at indgå en databehandleraftale, og tilsynet fastslog, at det ikke er tilstrækkeligt alene at etablere et overførselsgrundlag. De to sæt krav må gerne samles i ét dokument, men så skal dokumentet dække både overførselsgrundlaget og alle minimumskrav i art. 28, stk. 3 – og standardbestemmelserne må ikke ændres i strid med deres indhold, da de ellers bliver en ad hoc-aftale, der kræver Datatilsynets godkendelse.

Aftalen indgås – men der føres aldrig tilsyn. Dette er den hyppigste overtrædelse i Datatilsynets praksis. Tilsynet har gentagne gange udtalt, at den dataansvarlige **ikke** kan leve op til ansvarlighedsprincippet blot ved at indgå en databehandleraftale, men også må føre et større eller mindre tilsyn med, at aftalen faktisk overholdes. Randers Kommune fik alvorlig kritik (j.nr. 2018-423-0021) for mangelfuld styring af databehandlere, og både Region Hovedstaden, Region Syddanmark, Aarhus Universitet og Styrelsen for International Rekruttering og Integration har fået kritik for enten slet ikke at have fastsat et tilsynsniveau eller for ikke at have gennemført det tilsyn, de selv havde besluttet.

Instruksen er tom – og databehandleren bliver dataansvarlig. Skriver aftalen kun, at "databehandleren behandler oplysninger efter den dataansvarliges instruks", uden at instruksen nogensinde konkretiseres, er der ingen ramme at måle leverandøren imod. Behandler databehandleren derefter oplysninger til egne formål – analyse, produktudvikling, statistik, videresalg – anses vedkommende efter [artikel 28, stk. 10](#) selv for dataansvarlig for den behandling. Datatilsynet udtalte alvorlig kritik i j.nr. 2019-442-3996 netop af en databehandler, der behandlede personoplysninger uden for instruksen.

Tredjelandsklausulen i det små overses. Mange cloudaftaler indeholder en klausul om, at leverandøren kan flytte eller udlevere data uden for den valgte region, hvis det er nødvendigt for at overholde lovgivning eller bindende myndighedsafgørelser. Datatilsynet fastslog i KOMBIT/AWS-sagen (j.nr. 2022-212-3529), at en sådan geografisk ubegrænset instruks gør en eventuel udlevering til en **tilsigtet** overførsel, som udløser kapitel V-kravene for den dataansvarlige – og at en tredjelandsmyndigheds anmodning ikke i sig selv er et overførselsgrundlag. Overses klausulen, mangler der et overførselsgrundlag, og det rammer det høje bøde loft i [artikel 83, stk. 5](#).

Ingen exitplan – data efterlades hos leverandøren. Art. 28, stk. 3, litra g kræver, at databehandleren efter dit valg sletter eller tilbageleverer alle oplysninger og sletter kopier ved ophør. Er format, frist og dokumentation for sletningen ikke aftalt på forhånd, står man ved leverandørskifte typisk uden reel mulighed for at få data ud i brugbar form – og uden dokumentation for, at backup og testmiljøer er ryddet. Fortsat opbevaring uden formål er samtidig en selvstændig overtrædelse af opbevaringsbegrænsningen i [artikel 5, stk. 1, litra e](#).

§ 9 Relaterede dokumenter

- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn
- [Konsekvensanalyse \(DPIA\)](#) – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet
- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Samtykkeerklæring \(GDPR\)](#) – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)
- [IT-kontrakt \(systemleverance/SaaS\)](#) – Kontrakten om softwareleverancer og cloud-drift – K-standarderne, agile leverancer, SLA'er og exit
- [Fortrolighedsaftale \(NDA\)](#) – Hemmeligholdelsesaftalen før forhandlinger og samarbejder – og dens samspil med forretningshemmelighedsloven
- [Whistleblowerpolitik og -ordning](#) – Den lovpligtige interne indberetningsordning for arbejdsgivere med 50+ ansatte – etablering, procedurer og fortrolighed

REFERENCE Lovgrundlag

7 paragraffer

Databeskyttelsesforordningen § 5	stk. 2	Databeskyttelsesforordningen § 26	stk. 1
Databeskyttelsesforordningen § 28	stk. 2, 3	Databeskyttelsesforordningen § 32	stk. 1
Databeskyttelsesforordningen § 46	stk. 2	Databeskyttelsesloven § 41	stk. 1
Retshåndhævelsesloven § 22	stk. 2		

MATERIALE Citerede afgørelser

19 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS

19

23.01.2026	Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	2025-211-3556
22.05.2024	Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter	2023-421-0001

15.02.2024	Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger	2023-431-0012
17.03.2023	Vurdering af databehandlerstatus for leverandører af colocation-ydelser	2022-212-3470
16.12.2022	Datatilsynets kontrol med Sundhedsdatastyrelsens tilsyn med databehandlere	2021-421-0100
16.12.2022	Kritik af Styrelsen for International Rekruttering og Integrations manglende tilsyn med databehandlere	2021-421-0102
15.12.2022	Beskæftigelsesministeriets tilsyn med databehandler: Datatilsynet udtaler ingen kritik	2021-421-0097
15.12.2022	Skatteforvaltningens tilsyn med databehandlere i overensstemmelse med reglerne	2021-421-0099
15.12.2022	Datatilsynets tilsyn med Hjemrejsestyrelsens kontrol af databehandlere resulterer i ingen kritik	2021-421-0101
25.08.2022	Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	2021-431-0126
20.07.2022	Kritik af Region Syddanmark for mangelfuld kontrol med personoplysninger til forskning	2020-422-0026
29.03.2022	Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	2022-212-3529
16.02.2022	Kritik af Region Hovedstaden for manglende databehandleraftale og kontrol med underdatabehandlere i forskningsprojekt	2020-422-0025
07.02.2022	Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	2022-431-0167
13.10.2021	Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning?	2021-211-6947
22.09.2020	Kritik af Schultz efter sikkerhedshul i fagsystemet Expose	2019-431-0048
10.08.2020	Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter	2018-423-0018
19.12.2019	Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	2019-442-3996
05.08.2019	Alvorlig kritik af Randers Kommunes mangelfulde styring af databehandlere	2018-423-0021