

PRAKSISOVERSIGT · ERHVERVSKONTRAKTER

IT-kontrakt (systemleverance/SaaS)

Kontrakten om softwareleverancer og cloud-drift – kravspecifikation, prøver, SLA, ansvarsbegrænsning og exit

Version 1 · Opdateret 21. jul. 2026 · 17 afgørelser · 2009-2026

[Læs online](#)

INTRODUKTION

En IT-kontrakt regulerer forholdet mellem en **kunde** og en **IT-leverandør** om levering, tilpasning, drift og vedligeholdelse af software – fra den klassiske systemleverance (leverandøren udvikler og idriftsætter et system efter kundens kravspecifikation) over abonnementsbaseret SaaS/cloud (kunden får brugsret til en standardtjeneste, der driftes hos leverandøren) til rene drifts-, support- og vedligeholdelsesaftaler. I praksis er de fleste kontrakter blandinger: en systemleverance med efterfølgende drift, eller en SaaS-aftale med tilkøbt konfiguration og integrationer.

Kontraktypen har **ingen egen lovregulering** i dansk ret. Købeloven er deklaratorisk og skrevet om løsøre, ikke om software, og obligationsrettens almindelige regler om misligholdelse giver kun grovkornede svar på, hvornår et IT-system er "mangelfuldt". Derfor bærer aftalen alt: leverancens indhold, hvornår den er godkendt, hvad forsinkelse koster, hvem der ejer koden og dataene, og hvordan kunden kommer ud igen. Samtidig er en række **enkeltvilkår** blevet lovbundne af EU-regulering – databehandleraftalen efter GDPR, exit- og porteringsvilkår efter dataforordningen, minimumsindhold i finansielle enheders IKT-kontrakter efter DORA og sikkerhedskrav i leverandørkæden efter NIS 2.

Oversigten er ordnet sådan: først hvornår kontrakten (og de lovbundne enkeltvilkår) kræves, dernæst en checkliste over det indhold, kontrakten bør og skal have i sin naturlige rækkefølge, så de typiske faldgruber med deres konsekvenser, og til sidst uddybende afsnit om kontrakttyperne, vandfald kontra agile forløb, ansvarsbegrænsningens grænser, exit og leverandørafhængighed, persondata- og sikkerhedskrav samt de særlige regler, når kunden er forbruger.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Ingen lov kræver en IT-kontrakt, og købelovens regler er deklaratoriske, jf. [Købeloven § 1](#) – det, kontrakten ikke regulerer, afgøres af obligationsrettens almindelige regler og af bevisbyrden.
- 02** Kravspecifikationen er den altdominerende tvistkilde: uklare krav bliver til leverandørens fortolkningsret, og krav, der ikke står i bilaget, kan som udgangspunkt ikke kræves opfyldt bagefter.
- 03** Behandler leverandøren personoplysninger på kundens vegne, er en databehandleraftale med indholdet i [GDPR artikel 28, stk. 3](#) ufravigelig – og ansvaret for den ligger hos kunden som dataansvarlig.

- 04** Ansvarsbegrænsninger er som udgangspunkt gyldige mellem erhvervsdrivende, men kan tilsidesættes efter [aftaleloven § 36](#), og en fraskrivelse af ansvar for forsæt eller grov uagtsomhed i datarelaterede vilkår er direkte ikke-bindende efter [dataforordningen artikel 13, stk. 4](#).
- 05** Exit er ikke længere kun et forhandlingsspørgsmål for cloud- og SaaS-aftaler: dataforordningen fastsætter obligatoriske frister, dataformater og gebyrgrænser for skift af leverandør.
- 06** Rettigheder til specialudviklet kode overgår ikke automatisk til kunden – [ophavsretsloven § 53](#) hviler på en specialitetsgrundsætning, hvorefter en overdragelse kun rækker så langt, som den udtrykkeligt er aftalt.
- 07** Agile og vandfaldsbaserede kontrakter har forskellige misligholdelsesankere: uden aftalte delleverancer, målbare acceptkriterier og en prioriteringsmekanisme har kunden i et agilt forløb ingen konkret leverance at reklamere over eller hæve på.
- 08** Reklamations- og forældelsesfrister løber, uanset hvad kontrakten siger: den almindelige 3-årige frist i [forældelsesloven § 3](#) rammer også krav mod IT-leverandører.

§ 1 Hvornår er dokumentet påkrævet?

Ingen generel lovpligt. Der findes ingen dansk lov, der kræver, at en aftale om levering af IT skal være skriftlig eller have et bestemt indhold. Dansk aftaleret bygger på formfrihed, og [Købeloven § 1](#) fastslår udtrykkeligt, at lovens bestemmelser "kun kommer til anvendelse, for så vidt ikke andet er udtrykkelig aftalt, eller må anses for indeholdt i aftalen eller følger af handelsbrug eller anden sædvane". Baggrundsretten er altså fravigelig – og den er så dårligt tilpasset software, at fraværet af en kontrakt i praksis betyder, at ingen ved, hvad der var aftalt. Kontrakten er derfor **frivillig, men reelt uundværlig**.

Betinget pligt til bestemte kontraktvilkår. En række situationer udløser lovkrav til, hvad kontrakten *skal* indeholde:

- **Personoplysninger.** Behandler leverandøren personoplysninger på kundens vegne – hvad næsten enhver SaaS-, drifts- og supportleverandør gør – skal behandlingen reguleres af en skriftlig kontrakt med det indhold, der er opregnet i [GDPR artikel 28, stk. 3](#), jf. artiklens stk. 9 om skriftlighedskravet. Databehandlaftalen indgår typisk som bilag til IT-kontrakten.
- **Cloud- og databehandlingstjenester.** Aftaler om databehandlingstjenester (cloud, SaaS, edge, hosting) skal efter [dataforordningen artikel 25, stk. 2](#) indeholde en række obligatoriske exit-vilkår: maksimal opsigelsesfrist på to måneder, overgangsperiode på højst 30 kalenderdage, udtømmende specifikation af eksporterbare data, mindst 30 dages udtræksperiode og sletning derefter. Skiftegebyrer skal udfases og må fra den 12. januar 2027 slet ikke opkræves, jf. [artikel 29](#). Digitaliseringsstyrelsen fører tilsyn og kan udstede påbud, jf. [datadelingsloven § 9](#).
- **Finansielle enheder.** Er kunden en finansiell enhed omfattet af DORA, er kontraktens minimumsindhold direkte lovbestemt i [DORA artikel 30, stk. 2](#) – og skærpet i stk. 3 for IKT-tjenester, der understøtter kritiske eller vigtige funktioner (fuldstændige serviceniveauer med kvantitative mål, revisionsret, beredskabstest, exitstrategier med obligatorisk overgangsperiode).

- **Væsentlige og vigtige enheder efter NIS 2.** Enheder omfattet af [NIS 2-loven § 6, stk. 1, nr. 4](#) skal håndtere forsyningskædesikkerhed, herunder de sikkerhedsrelaterede aspekter af forholdet til direkte leverandører og tjenesteudbydere. I praksis opfyldes pligten ved sikkerheds-, underretnings- og revisionsvilkår i leverandørkontrakten.
- **Offentlige ordregivere.** Er kontrakten udbudspligtig, er indholdet i vidt omfang låst af udbudsmaterialet, og efterfølgende ændringer er begrænset af [udbudsloven § 178](#) om ændring af grundlæggende elementer. Offentlige myndigheders IT-systemer med personoplysninger kan desuden være omfattet af lokationskravet i [databeskyttelsesloven § 3, stk. 9](#).
- **Forbrugerkunder.** Leveres digitalt indhold eller en digital tjeneste til en forbruger – herunder mod betaling i form af personoplysninger – gælder købelovens præceptive mangelsregler, jf. [købeloven § 4 a, stk. 3](#), sammenholdt med lovens § 1, stk. 2. Vilkår, der stiller forbrugeren ringere, er ugyldige.

Frivilligt, men retssikrende. Alt det øvrige – kravspecifikation, tidsplan, overtagelsesprøve, dagbod, mangelsbeføjelser, ansvarsloft, SLA-bod, rettighedsfordeling, escrow og transitionsbistand – er ren aftalefrihed. Uden disse vilkår afgøres tvisten af obligationsrettens almindelige regler, hvor kunden typisk har bevisbyrden for, hvad der var aftalt om funktionalitet, og hvor der hverken er dagbod, ansvarsloft eller pligt til at udlevere data i et brugbart format.

§ 2 Det skal dokumentet indeholde

1. Parter, kontraktgenstand og en udtømmende bilagsfortegnelse med klar fortolkningsrangorden mellem kontrakt, kravspecifikation, tilbud og SLA. Kontrakten bør udtrykkeligt angive, at vilkår i udbudsmateriale og tilbud, som ikke er gentaget i kontrakten eller dens bilag, ikke er bindende.
2. Leverancebeskrivelse og kravspecifikation, hvor krav er adskilt fra ønsker og optioner, og hvor funktions-, kapacitets- og integrationskrav er formuleret målbart. Ved agile forløb bør kontrakten i stedet beskrive den aftalte prioriterings- og styringsmekanisme, backlog-governance og hvad der udgør "færdig" leverance.
3. Tidsplan med bindende milepæle samt kundens medvirkenspligter (data, testressourcer, beslutningsfrister, adgang til testmiljøer) – og retsvirkningen af, at kunden ikke medvirker rettidigt.
4. Afprøvning: hvilke prøver der gennemføres (installations-, overtagelses- og driftsprøve), hvem der udfører dem, hvilke godkendelseskriterier og fejl kategorier der gælder, og hvad godkendelse retligt betyder for kundens senere mangelsbeføjelser.
5. Misligholdelse ved forsinkelse: dagbodens beregningsgrundlag og loft, hvilke milepæle den knytter sig til, om dagbod er eneste beføjelse, og hvornår kunden kan hæve – samt pligt til at reklamere over forsinkelse uden ugrundet ophold.
6. Mangelsbegreb, leverandørens afhjælpningspligt, svarfrister og de tidsmæssige yderrammer for at gøre krav gældende. Kontraktens reklationsfrister bør holdes inden for den almindelige 3-årige forældelsesfrist, som ikke kan aftales væk til skade for kravets rettidige indbringelse. (*Forældelsesloven § 3*)
7. Ansvarsbegrænsning: beløbsloft (typisk 12 måneders vederlag), undtagelse af indirekte tab og driftstab samt en udtrykkelig stillingtagen til datatab og databrud. Loftet skal fravige forsæt og grov uagtsomhed, da et ubetinget loft ellers risikerer tilsidesættelse som urimeligt. (*Aftaleloven § 36*)
8. Serviceniveauaftale (SLA) med målbare servicemål for opetid, svartider og reaktions-/løsningstider, en aftalt målemetode, rapportering, bod og eskalation. For finansielle enheders IKT-kontrakter, der

understøtter kritiske eller vigtige funktioner, skal SLA'en indeholde præcise kvantitative og kvalitative præstationsmål. (*DORA-forordningen om digital modstandsdygtighed i finanssektoren § 30, stk. 3*)

9. Immaterialrettigheder: hvem der har rettigheder til specialudviklet kode, hvilken brugsret kunden får til leverandørens standardkomponenter og tredjepartslicenser, håndtering af open source, og at kunden bevarer rettighederne til sine egne data. Overdragelsen skal beskrives udtrykkeligt, da en rettighedsoverdragelse ikke rækker videre end aftalt. (*Ophavsretsloven § 53*)
10. Fortrolighed om begge parterets forretningshemmeligheder – herunder kildekode, systemdokumentation, sikkerhedsopsætning og kundens forretningsdata – med angivelse af varighed og af, hvilke medarbejdere og underleverandører der må få adgang. (*Erhvervshemmelighedsloven § 4*)
11. Databehandlersaftale som bilag, når leverandøren behandler personoplysninger på kundens vegne: dokumenteret instruks, fortrolighed, sikkerhedsforanstaltninger, godkendelse af underdatabehandlere, bistand med de registreredes rettigheder, sletning eller tilbagelevering ved ophør samt revisions- og inspektionsret. (*Databeskyttelsesforordningen § 28, stk. 3*)
12. Sikkerhedskrav, underretning om hændelser uden unødigt forsinkelse samt kundens ret til audit eller til at modtage revisionserklæringer. For væsentlige og vigtige enheder skal forsyningskædesikkerheden håndteres, hvilket i praksis kræver, at kravene står i kontrakten. (*NIS 2-loven § 6, stk. 1*)
13. Exit: opsigelsesvarsler, udlevering af kundens data i et almindeligt anvendt og maskinlæsbart format, transitionsbistand til ny leverandør, sletning efter udtræksperioden og prisen for bistanden. For cloud- og SaaS-aftaler er frister og formatkrav lovbounde, og kontrakten bør desuden regulere escrow af kildekode og adgang til systemdokumentation. (*Dataforordningen om harmoniserede regler for adgang og brug af data § 25, stk. 2*)

LOV

Aftaleloven § 36

Databeskyttelsesforordningen § 28, stk. 3

Dataforordningen om harmoniserede regler for adgang og brug af data § 25, stk. 2

DORA-forordningen om digital modstandsdygtighed i finanssektoren § 30, stk. 3

Erhvervshemmelighedsloven § 4

Forældelsesloven § 3

NIS 2-loven § 6, stk. 1

Ophavsretsloven § 53

Systemleverance, SaaS eller drift – og hvorfor baggrundsretten ikke rækker

IT-kontrakter dækker retligt set flere forskellige aftaletyper, og valget af type afgør, hvilke beføjelser der overhovedet giver mening. **Systemleverancen** ligner en værksleverance: leverandøren skal frembringe et resultat, der opfylder en kravspecifikation, og leveringen afsluttes med en prøve og en overtagelsesdag. **SaaS og cloud** er derimod en løbende tjenesteydelse med brugsret til en standardløsning – her er der ingen "levering" at hæve på, men til gengæld en løbende tilgængelighedsforpligtelse, som SLA'en måler. **Drifts-, support- og vedligeholdelsesaftaler** er rene løbende ydelser, hvor det afgørende er servicemål, prisregulering og opsigelsesvarsler. De fleste større kontrakter kombinerer typerne, og det er netop i overgangene – fra projekt til drift, fra standard til tilpasning – at tvisterne opstår.

Den deklaratoriske baggrundsret hjælper kun lidt. Købelovens mangels- og forsinkelsesregler er skrevet om løsøre og anvendes i bedste fald analogt på software, og de kan under alle omstændigheder fraviges ved aftale mellem erhvervsdrivende. Ophavsretsloven giver kunden nogle ufravigelige minimumsrettigheder som bruger – retten til at fremstille et sikkerhedseksempel og til at undersøge programmet kan ikke fraviges ved

aftale, jf. [ophavsretsloven § 36, stk. 3](#) – men den regulerer ikke, hvem der ejer det, leverandøren udvikler. Er koden frembragt af leverandørens ansatte under udførelsen af deres arbejde, tilfalder ophavsretten som udgangspunkt leverandøren som arbejdsgiver, jf. [ophavsretsloven § 59](#); skal kunden have rettigheder, skal det aftales udtrykkeligt.

Markedets svar på tomrummet er standardkontrakter. Staten har siden begyndelsen af 1990'erne udgivet standardkontrakter til IT-anskaffelser – den ældre generation findes stadig som [Vejledning om Statens standardkontrakt for standardiserede edb-systemer](#), der bl.a. indeholder de klassiske vilkår om driftsprøve, hæftelse for underleverandører og indeståelse for tredjemands rettigheder. Den er i dag i praksis afløst af Finansministeriets og Digitaliseringsstyrelsens K-standarder: **K01** til kortvarige IT-projekter, **K02** til længerevarende leverancer efter en vandfaldsmodel og **K03** til længerevarende projekter baseret på iterativ og agil metode. K-standarderne er ikke bindende ret, men fungerer som markedsreference og forhandlingsudgangspunkt også i rent private aftaler – og den ældre vejlednings pointe gælder stadig: når man tilpasser i kontraktteksten, skal man passe på ikke at bryde sammenhængen mellem parternes beføjelser.

LOV

[KøbeLoVen § 1](#)[Ophavsretsloven § 36, stk. 3](#)[Ophavsretsloven § 59](#)

§ 4 Vandfald eller agilt – to helt forskellige misligholdelsesanker

I den vandfaldsbaserede kontrakt er alt hængt op på **kravspecifikationen og overtagelsesprøven**. Kravene beskrives detaljeret på forhånd, leverandøren udvikler mod dem, og prøven afgør, om leverancen er kontraktmæssig. Beføjelserne følger naturligt: består prøven ikke inden for en aftalt frist, løber dagbod, og efter et vist antal mislykkede forsøg opstår ophævelsesretten. Prisen for modellen er, at kunden skal kunne beskrive sit behov præcist på et tidspunkt, hvor det ofte endnu ikke er kendt – og at enhver senere erkendelse bliver til en betalbar ændringsanmodning.

I det agile forløb er kravene indledningsvis kun beskrevet overordnet og konkretiseres løbende. Rigsrevisionen har i sine undersøgelser af statslige IT-projekter beskrevet netop den forskel og noteret, at ministerierne i stigende grad anvender agil eller delvist agil metode – men også, at valget af metode ikke i sig selv får projekterne bedre i mål. Kontraktilt er udfordringen, at når tid og økonomi låses, og kun scope kan flytte sig, forsvinder den faste leverance, som misligholdelsesbeføjelserne normalt knytter sig til. Den agile kontrakt må derfor bygge sine anker andre steder: på **aftalte delleverancer og releases** med egne acceptkriterier, på en **prioriteringsmekanisme**, hvor kunden har den reelle beslutningsret over backloggen, på **krav til teamets sammensætning og kontinuitet**, og på en **ophørs- og afregningsmodel**, der gør det muligt at stoppe et forløb, som ikke skaber værdi, uden at kunden har betalt for et resultat, der aldrig kom.

Uanset model bør reklimations- og påmindelsesdisciplinen stå i kontrakten. Reklamerer kunden ikke rettidigt over forsinkelse eller mangler, risikerer kunden at fortabe beføjelserne, og den yderste ramme sætter forældelsesreglerne. Skal leverandøren betale renter af tilbagebetalings- eller erstatningskrav, følger forfaldstidspunktet af aftalen – ellers af [renteloven § 3](#). Retspraksis om, hvornår en IT-leverance er så mangelfuld eller forsinket, at kontrakten kan hæves, er samlet i praksisoversigten om [IT-systemleverancer, forsinkelse og mangler](#), og de almindelige rammer for ophævelse og erstatning i [misligholdelse, ophævelse og erstatning i kontrakt](#).

LOV

[Forældelsesloven § 3](#)[Renteloven § 3](#)

§ 5 Ansvarsbegrænsning, SLA og grænserne for aftalefriheden

Ansvarsbegrænsningen er kontraktens dyreste enkeltvilkår. Markedsstandarden er et beløbsloft svarende til 12 måneders vederlag kombineret med en undtagelse af indirekte tab. Problemet er, at netop de tab, en fejlslagen IT-leverance forvolder – **driftstab, tabte data, omkostninger til reetablering og til en erstatningsleverandør** – ofte kvalificeres som indirekte. En kunde, der accepterer klausulen uden at trække datatab, databrud og krænkelse af tredjemands rettigheder ud af undtagelsen, har reelt accepteret at bære risikoen selv.

Aftalefriheden har dog grænser. [Aftaleloven § 36](#) giver adgang til at ændre eller tilsidesætte et vilkår helt eller delvist, hvis det vil være urimeligt eller i strid med redelig handlemåde at gøre det gældende, og der tages ved vurderingen hensyn både til forholdene ved aftalens indgåelse, til aftalens indhold og til senere indtrufne omstændigheder. Et ubetinget ansvarsloft, der også dækker forsæt og grov uagtsomhed, er den klassiske kandidat til tilsidesættelse. For datarelaterede vilkår mellem virksomheder er retstilstanden skærpet: et **ensidigt pålagt** vilkår om adgang til og anvendelse af data eller om ansvar og retsmidler er slet ikke bindende, hvis det er urimeligt, og det anses navnlig for urimeligt, hvis det udelukker eller begrænser ansvaret for forsætlige handlinger eller grov uagtsomhed, udelukker modpartens retsmidler eller giver den, der har pålagt vilkåret, eneret til at afgøre, om det leverede opfylder aftalen. Bevisbyrden for, at et vilkår *ikke* er ensidigt pålagt, ligger hos den, der har fremsat det.

SLA'en er ansvarsbegrænsningens praktiske modstykke: den omsætter driftsforpligtelsen til målbare tal og knytter en bod til afvigelser. Uden en aftalt målemetode, et defineret nedetidsbegreb og en rapporteringsforpligtelse er servicemålene reelt uden indhold. For finansielle enheder er kravene lovbundne: [DORA artikel 30, stk. 2](#) kræver bl.a. en klar og fuldstændig beskrivelse af de leverede funktioner og tjenester, angivelse af behandlings- og lagringssteder, bestemmelser om adgang, genopretning og tilbagesendelse af data ved insolvens eller ophør, beskrivelser af serviceniveauet og opsigelsesrettigheder – og for IKT-tjenester, der understøtter kritiske eller vigtige funktioner, tillige præcise kvantitative præstationsmål, uindskrænket revisions- og inspektionsret samt exitstrategier med en obligatorisk overgangsperiode.

LOV

[Aftaleloven § 36](#)[Dataforordningen om harmoniserede regler for adgang og brug af data § 13, stk. 4](#)[DORA-forordningen om digital modstandsdygtighed i finanssektoren § 30, stk. 2](#)

§ 6 Exit, escrow og leverandørafhængighed

Exit-vilkårene afgør, om kunden nogensinde kan komme videre. Kontrakten bør regulere fire ting: **hvornår** aftalen kan bringes til ophør, **hvilke data** kunden får med og i hvilket format, **hvilken bistand** leverandøren skal yde under overgangen og til hvilken pris, og **hvad der sker med kopier** hos leverandøren bagefter. Hertil kommer adgang til systemdokumentationen – uden den kan kunden hverken kravspecifilere en ny anskaffelse eller konkurrenceudsætte driften.

For cloud- og SaaS-aftaler er dette ikke længere forhandlingsstof alene. [Dataforordningen artikel 23](#) pålægger udbydere af databehandlingstjenester at fjerne prækommercielle, kommercielle, tekniske, kontraktmæssige og organisatoriske hindringer for, at kunden kan skifte, og artikel 25 fastsætter det obligatoriske aftaleindhold:

højst to måneders opsigelsesfrist for at indlede skiftet, en obligatorisk overgangsperiode på maksimalt 30 kalenderdage (i særlige tilfælde op til syv måneder mod behørig begrundelse), en udtømmende specifikation af eksporterbare data, en udtræksperiode på mindst 30 dage og fuldstændig sletning derefter. Skiftegebyrer er under udfasning og må ikke opkræves fra den 12. januar 2027. Rent skræddersyede tjenester, der ikke udbydes i stor kommerciel målestok, er dog undtaget fra dele af regelsættet. Digitaliseringsstyrelsen er tilsynsmyndighed, og styrelsens afgørelser kan ikke indbringes for anden administrativ myndighed, jf. [datadelingsloven § 4, stk. 2](#).

Escrow – deponering af kildekode og byggeinstruktioner hos tredjemand med udleveringsret ved leverandørens konkurs eller væsentlige misligholdelse – er fortsat ren aftalefrihed, men bør ses i sammenhæng med konkursretten: konkursboet kan vælge at indtræde i gensidigt bebyrdende aftaler, jf. [konkursloven § 55](#), og kan ved løbende ydelser altid opsiges med en måneds varsel. Uden en escrow-ordning og uden dokumenterede rettigheder til systemdokumentationen kan kunden stå uden både kode og drift.

For offentlige kunder er leverandørafhængighed også et udbudsretligt problem. Rigsrevisionen konstaterede i beretning nr. 8/2016 om statens udbud af IT-drift og -vedligeholdelse, at otte større kontrakter aldrig havde været udbudt – bl.a. med henvisning til manglende systemdokumentation, uklare rettigheder og for store omkostninger ved leverandørskift – og Statsrevisorerne fulgte så sent som i november 2025 op på, at flere legacy-kontrakter fortsat ikke er konkurrenceudsat. Ændringer i en igangværende kontrakt kan kun ske inden for rammerne af klare, præcise og entydige ændringsklausuler, jf. [udbudsloven § 179](#), og ordregiveren har efter [udbudsloven § 185](#) adgang – og i visse tilfælde pligt – til at bringe kontrakten til ophør. De udbudsretlige rammer er uddybet i praksisoversigten om [udbudsret](#).

LOV

[Dataforordningen om harmoniserede regler for adgang og brug af data § 23](#)[Konkursloven § 55](#)[Udbudsloven § 179](#)[Udbudsloven § 185](#)

Persondata, sikkerhed og tilsynspraksis – hvor kontrakten faktisk § 7 håndhæves

Den del af IT-kontrakten, der oftest bliver prøvet af en myndighed, er ikke dagboden – det er databehandlerbilaget. Datatilsynet har i en lang række tilsynssager konkretiseret, hvad der kræves, og kritikken rammer **kunden som dataansvarlig**, ikke kun leverandøren.

I tilsynet med Randers Kommune udtalte Datatilsynet alvorlig kritik, fordi kommunen manglede aftaler med 68 databehandlere, og fordi instruksens ikke var tilstrækkeligt præcis – i ét tilfælde fremgik det af et bilag, at leverandøren brugte brugeradfærdsdata til markedsførings- og produktformål, uden at kommunen havde forholdt sig til hjemlen. I tilsynet med Viborg Kommune fandt tilsynet det utilstrækkeligt, at en aftale gav leverandøren ret til selv at ændre ydelsesbeskrivelsen, hvor kommunens tavshed blev fortolket som accept: en dataansvarlig kan ikke overlade det til leverandøren at definere formålene. Konsekvensen af at gå uden om instruksens kan være dramatisk – i sagen om økonomisystemet ØS Indsigt tog leverandøren en SaaS-underleverandør i brug, som ikke var opført på listen over godkendte underdatabehandlere, og Datatilsynet fandt, at leverandøren derved selv blev **dataansvarlig** for videregivelsen og manglede behandlingsgrundlag, ligesom overførslen til tredjelande blev uhjemlet. En underdatabehandlers nægtelse af at udlevere oplysninger til den dataansvarlige har ligeledes udløst alvorlig kritik – hvilket viser, hvorfor revisions- og oplysningsretten skal stå i kontrakten og gælde hele kæden.

Cloud-specifikke spørgsmål går igen: tilsynet med Region Syddanmarks brug af Microsoft 365 satte rammerne for offentlige myndigheders cloud-anvendelse, og Datatilsynet har taget stilling både til utilsigtede overførsler ved teknisk routing og til, hvor langt generelle tilladelser til tredjelandsoverførsler i databehandleraftaler kan gå. Tilsyn, der er ført korrekt – som hos Beskæftigelsesministeriet og Skatteforvaltningen – er endt uden kritik, mens manglende opfølgning hos Styrelsen for International Rekruttering og Integration udløste kritik. Pointen er den samme hver gang: kontrakten skal ikke bare indgås, den skal følges op.

Selve **udviklingen** kan også blive sanktioneret. I sagen om mit.dk indstillede Datatilsynet Netcompany til en bøde på 15 mio. kr. og politianmeldte virksomheden, fordi kritiske risikoscenarier ikke var identificeret og testet inden idriftsættelsen, og fordi der ikke var udarbejdet en konsekvensanalyse. Tilsvarende fik Sundhedsdatastyrelsen kritik for ikke at kontrollere, om personoplysninger utilsigtet lå i et agilt DevOps-miljø, mens et tilsyn med Salling Groups login- og rettighedsstyring endte uden kritik. Det taler for, at IT-kontrakten indeholder konkrete krav til testregime, testdata, privacy by design og adskillelse af udviklings- og produktionsmiljøer – ikke blot en henvisning til "passende sikkerhed". Er kunden en væsentlig eller vigtig enhed efter NIS 2, skal forsyningskædesikkerheden desuden håndteres aktivt, og for visse digitale udbydere præciserer Kommissionens gennemførelsesforordning (EU) 2024/2690, at kontrakterne bl.a. skal angive cybersikkerhedskrav, baggrundskontrol af leverandørens ansatte, pligt til at underrette om hændelser uden unødigt forsinkelse og retten til audit eller til at modtage auditrapporter.

LOV

Databeskyttelsesforordningen § 28, stk. 3

Databeskyttelsesloven § 3, stk. 9

NIS 2-loven § 6, stk. 1

PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	23.01.2026
	Datatilsynet · Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger	15.02.2024
	Datatilsynet · Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	12.01.2024
	Datatilsynet · Kritik af Styrelsen for International Rekruttering og Integrations manglende tilsyn med databehandlere	16.12.2022
	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 · Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelände	29.03.2022
	Datatilsynet · Sundhedsdatastyrelsen får kritik for manglende kontrol med personoplysninger i it-miljø	16.03.2022
	Datatilsynet · Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	07.02.2022
	Datatilsynet · Datatilsynets tilsyn med Salling Group A/S vedrørende it-sikkerhed og rettighedsstyring	15.01.2021
	Datatilsynet · Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	19.12.2019
	Datatilsynet · Alvorlig kritik af Randers Kommunes mangelfulde styring af databehandlere	05.08.2019
	Datatilsynet · Alvorlig kritik og påbud til Viborg Kommune i sag om Google Workspace	05.08.2019

§ 8 Når kunden er forbruger – SaaS-vilkår under præceptiv beskyttelse

Sælges softwaren eller tjenesten til en forbruger, forsvinder aftalefriheden i vidt omfang. Aftaler om levering af **digitalt indhold eller en digital tjeneste** er forbrugerkøb, når leveringen sker mod betaling af et pengebeløb,

et digitalt udtryk for værdi eller mod personoplysninger, jf. [købeloven § 4 a, stk. 3](#). Dermed gælder købelovens mangelsbeføjelser – afhjælpning, omlevering, forholdsmæssigt afslag og ophævelse, jf. [købeloven § 78](#) – og de kan ikke fraviges til skade for forbrugeren. Free and open source-licenser uden betaling samt visse finansielle, sundhedsfaglige og spilrelaterede tjenester er undtaget.

Selve vilkårene skal desuden være gennemsigtige. En skriftlig aftale, der tilbydes forbrugeren, skal være udarbejdet på en klar og forståelig måde, jf. [aftaleloven § 38 b](#), og tvivl fortolkes mod den erhvervsdrivende, når vilkåret ikke har været individuelt forhandlet. Er et vilkår i strid med hæderlig forretningsskik og skaber en betydelig skævhed til skade for forbrugeren, kan det tilsidesættes efter [aftaleloven § 38 c](#).

Forbrugerombudsmandens praksis er retningsgivende for tre vilkårstyper, der er standard i SaaS-abonnementer. For det første **ensidige ændringer**: forbeholder udbyderen sig ret til at ændre ydelsen eller prisen, skal begrundelsen og retningslinjerne for ændringen fremgå af aftalen, forbrugeren skal varsles direkte og individuelt, og varslet skal være tydeligt fremhævet og oplyse om konsekvenserne – ellers er vilkåret urimeligt. For det andet **gebyrer**: det skal fremgå klart af vilkårene, efter hvilke kriterier gebyrer kan ændres eller indføres, og kriterierne må ikke være usaglige. For det tredje **bindings- og udtrædelsesvilkår**: gebyrer, der reelt gør opsigelsesretten illusorisk, er blevet krævet fjernet. Endelig har Forbrugerombudsmanden anset **generelle ansvarsfraskrivelser** i rådgivningsforhold for at stride mod god skik – en påmindelse om, at den B2B-standardklausul, der fraskriver alt ansvar, ikke uden videre kan genbruges i forbrugerforhold.

LOV	Aftaleloven § 38b	Aftaleloven § 38c	Købeloven § 4a, stk. 3	Købeloven § 78
PRAKSIS	Forbrugerombudsmanden · Elselskabs opkrævning af urimelige gebyrer ved opsigelse af varmepumpeabonnement 26.06.2025 Forbrugerombudsmanden · Forbrugerombudsmandens udtalelse om varsling af ændringer i programpakker og priser 18.12.2014 Forbrugerombudsmanden · Juridisk rådgiver tilsidesatte formelle krav og anvendte ansvarsfraskrivelse 03.07.2013 Forbrugerombudsmanden · Teleselskab pålagt at præcisere kriterier for gebyrændringer i abonnementsvilkår 07.04.2009			

§ 9 Typiske faldgruber

Kravspezifikationen er en ønseseddel, ikke en specifikation. Behovsopgørelser, der blander bindende krav med "ønsker", "forventninger" og hensigtserklæringer, gør leverandøren til fortolker af sin egen leveranceforpligtelse. Krav, der ikke fremgår af bilaget ved kontraktindgåelsen, kan som udgangspunkt ikke kræves opfyldt bagefter – og bliver i stedet til betalbare ændringsanmodninger. Konsekvensen er budgetoverskridelse hos kunden og en tvist, hvor kunden bærer bevisbyrden for, hvad der var aftalt.

Overtagelsesprøven godkendes uden dokumenteret fejlliste. En godkendelse afgivet under pres for at komme i drift – uden en registreret liste over udestående fejl, deres kategori og afhjælpningsfrist – svækker kundens position markant. Leverandøren vil efterfølgende anføre, at systemet blev accepteret som kontraktmæssigt, og at senere reklamationer er for sene. Godkendelse bør derfor altid ske med forbehold og bilagt en fejlliste med aftalte frister.

Dagbod uden ophævelsesanker. En dagbodsklausul med loft, der samtidig er kundens eneste misligholdelsesbeføjelse ved forsinkelse, betyder, at kunden efter loftets udløb hverken kan hæve eller kræve

erstatning – men blot kan vente. I forliste projekter er det netop ophævelsesadgangen, der har værdi. Kontrakten bør derfor knytte en udtrykkelig ophævelsesret til bestemte milepæle eller til, at dagbodsloftet nås.

Ansvarsbegrænsningen rammer også databas og databrud. Standardklausulen "leverandøren er ikke ansvarlig for indirekte tab, herunder driftstab og tab af data" flytter hele risikoen for et databrud eller en mislykket migrering over på kunden – også når kunden hæfter over for tilsynsmyndigheder og registrerede. Fraskrivelse for forsæt og grov uagtsomhed holder desuden ikke: for ensidigt pålagte datarelaterede vilkår mellem virksomheder er de direkte ikke-bindende, og generelt kan de tilsidesættes efter [aftaleloven § 36](#).

Ingen exit-plan – og dermed lock-in. Uden aftalte krav til dataformat, transitionsbistand og pris kan kunden reelt ikke skifte leverandør: data udleveres i leverandørens eget format, systemdokumentationen ejes af leverandøren, og migreringen bliver dyrere end at blive. For cloud- og SaaS-aftaler er lock-in-vilkår nu tillige retsstridige efter dataforordningens skifteregler, og for offentlige kunder har manglende exit ført til, at kontrakter reelt aldrig er blevet konkurrenceudsat.

Databehandleraftalen kopieres ind som ureflekteret standardbilag. Bilaget underskrives, uden at kunden forholder sig til, hvilke oplysninger leverandøren behandler, om leverandøren også bruger data til egne formål som produktforbedring, og hvilke underdatabehandlere der er godkendt. Datatilsynet har i flere sager udtalt alvorlig kritik af netop dette – bl.a. hvor en leverandør ensidigt kunne ændre ydelsesbeskrivelsen med kundens stiltiende accept, og hvor en SaaS-underleverandør blev taget i brug uden godkendelse, med den følge at databehandleren blev anset for selvstændig dataansvarlig uden behandlingsgrundlag.

Agile forløb uden misligholdelsesanket. Når tid og økonomi låses, og kun scope kan flytte sig, forsvinder den målbare leverance, som misligholdelsesbeføjelserne normalt knytter sig til. Uden aftalte delleverancer, acceptkriterier pr. iteration og en prioriteringsmekanisme med kundens beslutningsret står kunden uden reklamationsobjekt – og risikerer at betale for et forløb frem for et resultat.

Offentlige kunder ændrer kontrakten ud over det tilladte. Udvidelser, forlængelser og tilkøb i et længerevarende IT-projekt kan udgøre en ændring af grundlæggende elementer, som kræver nyt udbud, jf. [udbudsloven § 178](#). Ordregiveren kan blive mødt med krav om, at kontrakten bringes til ophør, og risikerer erstatningsansvar og sanktionen "uden virkning". Klare, præcise og entydige ændringsklausuler i udbudsmaterialet er den lovlige vej til fleksibilitet.

§ 10 Relaterede dokumenter

- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Fortrolighedsaftale \(NDA\)](#) – Hemmeligholdelsesaftalen før forhandlinger og samarbejder – og dens samspil med forretningshemmelighedsloven
- [Konsekvensanalyse \(DPIA\)](#) – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet
- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og Datatilsynets første anmodning ved tilsyn
- [Entreprisekontrakt \(AB 18\)](#) – Byggeriets aftalegrundlag – vedtagelse af AB 18, fravigelser, dagbod, aflevering og 5-års-ansvaret

- [Handelsbetingelser \(webshop/B2C\)](#) – Vilkårene bag købsknappen – forbrugeraftalelovens oplysningskrav, fortrydelsesret og de vilkår der ikke binder

REFERENCE Lovgrundlag

8 paragraffer

Aftaleloven § 36	Databeskyttelsesforordningen § 28 stk. 3
Dataforordningen om harmoniserede regler for adgang og brug af data § 25 stk. 2	Forældelsesloven § 3
Købeloven § 1	NIS 2-loven § 6 stk. 1
Ophavsretsloven § 53	Udbudsloven § 178

MATERIALE Citerede afgørelser

17 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS

13

23.01.2026	Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandlaftaler	2025-211-3556
15.02.2024	Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger	2023-431-0012
12.01.2024	Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	
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
29.03.2022	Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	2022-212-3529
16.03.2022	Sundhedsdatastyrelsen får kritik for manglende kontrol med personoplysninger i it-miljø	2021-442-12991
07.02.2022	Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	2022-431-0167
15.01.2021	Datatilsynets tilsyn med Salling Group A/S vedrørende it-sikkerhed og rettighedsstyring	2020-41-0064
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
05.08.2019	Alvorlig kritik og påbud til Viborg Kommune i sag om Google Workspace	2018-423-0022

FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS

4

26.06.2025	Elselskabs opkrævning af urimelige gebyrer ved opsigelse af varmepumpeabonnement
18.12.2014	Forbrugerombudsmandens udtalelse om varsling af ændringer i programpakker og priser
03.07.2013	Juridisk rådgiver tilsidesatte formelle krav og anvendte ansvarsfraskrivelse
07.04.2009	Teleselskab pålagt at præcisere kriterier for gebyrændringer i abonnementsvilkår