# It-avtal –

## en vägledning om it-tjänsternas avtal

April 2020

eSam

# Innehåll


1. Inledning ..... 4
   - 1.1 Målgrupp ..... 4
   - 1.2 Omfattning och avgränsning ..... 5
   - 1.3 Koppling till eSams övriga vägledningar ..... 5
2. Allmänt för it-avtal ..... 7
   - 2.1 Tillämpliga rättsregler ..... 7
   - 2.2 It-avtalens utveckling över tid ..... 8
   - 2.3 Olika kategorier av it-avtal ..... 10
   - 2.4 Utvalda kategorier av it-avtal ..... 12
3. Avtal för it-konsulttjänster ..... 14
   - 3.1 Allmänt ..... 14
   - 3.2 Nyckelregleringar ..... 15
   - 3.3 Fallgropar ..... 18
   - 3.4 Avtalens form och allmänna standardvillkor ..... 19
4. Avtal för it-projektuppdrag ..... 21
   - 4.1 Allmänt ..... 21
   - 4.2 Nyckelregleringar ..... 21
   - 4.3 Fallgropar ..... 24
   - 4.4 Agila projekt ..... 25
   - 4.5 Avtalens form och allmänna standardvillkor ..... 25
5. Programvarulicensiering ..... 27
   - 5.1 Allmänt ..... 27
   - 5.2 Nyckelregleringar ..... 27
   - 5.3 Fallgropar ..... 31
6. Avtal för it-underhållstjänster ..... 34
   - 6.1 Allmänt om it-underhållstjänster ..... 34

6.2 Nyckelregleringar ..... 34
6.3 Fallgropar ..... 36
6.4 Avtalens form och allmänna standardvillkor ..... 37
7. Avtal för it-drifttjänster och andra it-infrastrukturtjänster ..... 38
7.1 Allmänt om it-infrastrukturtjänster ..... 38
7.2 Allmänt om avtal för it-drifttjänster och andra it-infrastrukturtjänster ..... 38
7.3 Nyckelregleringar ..... 39
7.4 Fallgropar ..... 41
7.5 Avtalens form och allmänna standardvillkor ..... 43
8. Avtal för it-supporttjänster ..... 44
8.1 Allmänt ..... 44
8.2 Nyckelregleringar ..... 44
8.3 Fallgropar ..... 45
8.4 Avtalens form och allmänna standardvillkor ..... 46
9. Avtal för molntjänster ..... 47
9.1 Allmänt ..... 47
9.2 Nyckelregleringar ..... 50
9.3 Fallgropar ..... 52
9.4 Avtalens form och allmänna standardvillkor ..... 54
10. It-avtalens likheter ..... 55
10.1 Avtalsstruktur och prioritetsordning ..... 55
10.2 Personuppgiftsbiträdesavtal ..... 55
10.3 Säkerhetsskyddsavtal ..... 56
10.4 Lagval och forum för tvist ..... 57
11. Trender inom it-avtal ..... 59
11.1 Standardisering & ”Molnifiering” ..... 59
11.2 Förenklad struktur ..... 59
11.3 Mer balanserade avtalsvillkor ..... 59
11.4 Avtalsförvaltning och revision ..... 60

# 1. Inledning

Digitalisering av offentlig sektor innebär att olika typer av it-resurser behöver införskaffas genom upphandling eller avrop från ramavtal. För att formalisera inköpen träffas it-avtal med leverantörer om olika tjänster och produkter. Under informationssamhällets framväxt har olika kategorier av it-avtal utvecklats vilket innebär att det idag finns en rik flora av it-avtal som reglerar it-branschens tjänster och produkter. Då offentlig förvaltning digitaliseras i allt större omfattning och allt snabbare takt, ökar behovet av it-avtal med externa leverantörer. Den utvecklingen ställer i sin tur stora krav på myndigheterna att hantera it-avtal på ett juridiskt hållbart och affärsmässigt gynnsamt sätt.

Digitaliseringsrättsutredningen konstaterade att myndigheters behov av avtalsstöd för it-avtal har ökat med växande utkontraktering och mer komplexa it-avtal. Utredningen föreslår därför att myndigheterna i den offentliga förvaltningen bör tillhandahållas stöd i arbetet med att formulera juridiskt hållbara och affärsmässigt gynnsamma villkor i it-avtal.[1] Mot denna bakgrund ser eSam ett behov av en vägledning om it-avtal som erbjuder en orientering på området anpassad för offentlig förvaltning.

Syftet med denna vägledning är därför att ge en överblick över it-avtalsområdet och en orientering kring de it-avtal som är vanligt förekommande. Genom att beskriva hur inköp av olika it-resurser regleras i avtal vill vi med vägledningen skapa en övergripande förståelse för it-avtalens särdrag och likheter. It-avtalsområdet är omfattande och komplext med ett antal huvudkategorier och ett mycket stort antal specialområden där avtalspraxis varierar beroende vilken part som författar avtalet. Ambitionen med vägledningen är att göra detta avtalsrättsliga specialistområde tillgängligt för en vidare krets inom offentlig förvaltning med en översiktlig beskrivning av it-avtalsområdet inom det begränsade utrymme som denna vägledning erbjuder.

## 1.1 Målgrupp

Vägledningen är skriven för läsare som vill få en introduktion till it-avtal och en inblick i den praxis som utvecklats kring olika typer av it-avtal. Vi fokuserar på it-avtalstyper som är relevanta för offentlig förvaltning och utgår från de förhållanden som normalt råder för en myndighet då it-tjänster ska upphandlas. Vägledningen kan därför vara av intresse för verksjurister, it-chefer, upphandlare, projektledare, kontraktsansvariga och

[1] SOU 2018:25 s 426

andra som i vardagen kommer i kontakt med affärsjuridiska avtal på it-området. Vägledningen kan i viss omfattning vara intressant även för privat sektor och då särskilt i roller där man arbetar mot offentlig förvaltning.

## 1.2 Omfattning och avgränsning

Vägledningen beskriver övergripande vanligt förekommande typer av it-avtal och rymmer således *ingen uttömmande uppräkning av it-branschens avtal. För de it-avtalstyper vi valt att belysa beskrivs* inledningsvis it-tjänstens särdrag tillsammans med it-avtalstypens generella drag. Därefter behandlas nyckelregleringar och fallgropar som kan förekomma i den aktuella it-avtalstypen. Eftersom utrymmet är begränsat nämns enbart några exempel på nyckelregleringarna för varje kategori. För att skapa viss bredd i orienteringen har vi valt en variation i de nyckelregleringar som lyfts fram under respektive it-avtalskategori. Vi vill dock göra läsaren uppmärksam på att en viss typ av reglering kan utgöra nyckelreglering i många olika kategorier av it-avtal. Som exempel på kan regleringar om ansvarsbegränsning, sekretess, personuppgiftsbehandling, avtalets upphörande, rättighetsupplåtelse, avtalade servicenivåer nämnas.

Upphandlingsrättsliga frågeställningar behandlas inte i vägledningen, men är inte desto mindre viktiga för utformningen av it-avtal. Exempelvis finns betydelsefulla regler om ändringar av avtal. Utgångspunkten i vägledningen är att myndigheten agerar som köpare, men frågeställningar som behandlas här kan också bli relevanta då myndigheten tillhandahåller it-tjänster till enskilda eller till annan myndighet. Frågor om överenskommelser om it-tjänster mellan myndigheter behandlas inte heller särskilt i denna vägledning, men utesluter inte att vägledningen berör it-avtalsfrågor som kan bli relevanta i sådana överenskommelser. Referenser till Kammarkollegiets ramavtal och IT&Telekomföretagens standardavtalsvillkor är exempel på referensavtal, aktuella vid tiden för vägledningens publicering.

Författande av it-avtal är ett komplext specialistområde som kräver kunskap och erfarenhet samt ingående förståelse för förutsättningarna i det enskilda fallet för ett gott resultat. Innehållet i denna vägledning ska inte uppfattas som råd i det enskilda fallet utan som en allmän orientering inom it-avtalsområdet som syftar till att skapa större förståelse för och möjlighet att identifiera it-avtalets möjligheter och risker.

## 1.3 Koppling till eSams övriga vägledningar

Inför förändring eller utveckling av en myndighets verksamhet, där utkontraktering övervägs, måste myndigheten normalt gå igenom ett antal steg för att genomföra förändringen genom utkontraktering. De olika stegen kan sammanfattats på följande sätt, se bild nedan.

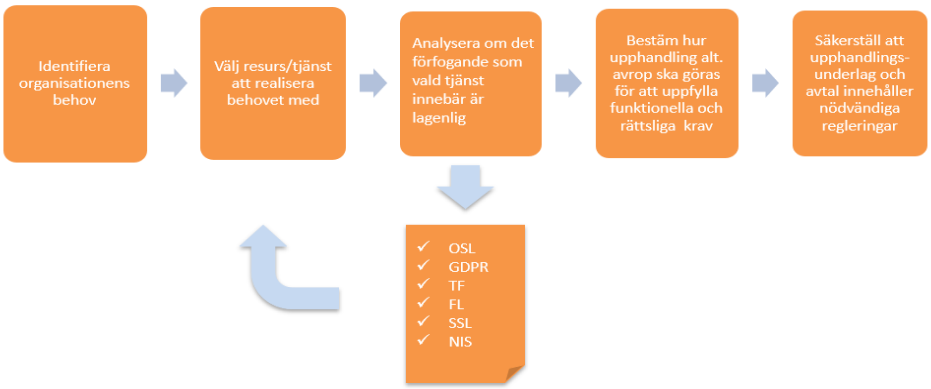


Bild 1. Realisera digitalisering med beaktande av rättsliga krav

De steg som behöver tas för att realisera digitalisering med beaktande av rättsliga krav beskrivs närmare i ”Outsourcing 2.0 – en vägledning om sekretess och dataskydd” utgiven december 2019. eSam har också tagit fram följande publikationer som kan vara till hjälp då rättsliga krav ska identifieras och avtal ska författas;

- Checklista för jurister (Version 2.0, juni 2019)
- Juridisk vägledning för verksamhetsutveckling inom e-förvaltning (Version 3.0, april 2018)
- Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form (maj 2016)
- Digitalisera rätt – En praktisk juridisk vägledning (juni 2019)

Samtliga eSam vägledningar finns att finna på esamverka.se.

## 1.4 Medverkande

Arbetet med att ta fram denna uppdaterade vägledning har genomförts av eSams juridiska expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Eva Maria Broberg Lennartsson, Malgorzata Drewniak, Per Furberg, Erik Janzon, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson, Mikael Westberg och Christina Wikström. Adjungerade ledamöter i expertgruppen är Veronica Eckerby, Nils Fjelkegård, Linn Kempe och Maria Sertcanli. Adjungerade ledamöter står inte formellt bakom ställningstaganden i vägledningen. I arbetet har även eSams juridiska sakområdesgrupp samt en referensgrupp med särskilt kompetens inom området deltagit.

# 2. Allmänt för it-avtal

## 2.1 Tillämpliga rättsregler

Inom avtalsrätten förekommer den klassiska uppdelningen av avtalstyper i överlåtelse, upplåtelse och tjänster. It-avtal avser i många fall tillhandahållande av en tjänst. Men it-avtal kan också avse köp av lös egendom såsom köp av hårdvara eller upplåtelse av en immateriell rättighet som licensiering av programvara. Det är dessutom vanligt att samma it-avtal innehåller flera olika avtalstyper, till exempel då en programvarulicens anskaffas tillsammans med en supporttjänst. Många it-avtal är därför rättsliga hybrider omfattande flera olika avtalstyper.

Uppdelningen i olika avtalstyper kan vara av betydelse av flera skäl. För vissa avtalstyper finns tvingande bestämmelser i lag som parterna inte med bindande verkan kan frångå i avtal. Lagstiftning som rör förhållanden mellan näringsidkare är dock normalt dispositiv, men även här kan uppdelningen i avtalstyp ha betydelse för vilken dispositiv lag som ska fylla ut parternas avtal när en fråga lämnats oreglerad.

Inom svensk rätt finns ingen särskild lagstiftning om it-avtal utan istället tillämpas allmänna lagar på avtalsrättens område. Köplagens (1990:931) dispositiva bestämmelser är till exempel direkt tillämplig avseende inköp av hårdvara, som datorer, nätverksutrustning och skrivare, om parterna inte avtalat annat. I avsaknad av direkt tillämplig lag kan det istället bli aktuellt att tillämpa en för avtalstypen närliggande lag analogt. De har exempelvis i doktrin ansetts att köplagens principer om felansvar, som överensstämmer med grundläggande kontraktsrättsliga principer, bör kunna tillämpas i förhållande till licensgivaren för att göra gällande fel i ett datorprogram då specifik reglering i avtalet saknas.[2] Vid tolkning av it-avtal kan det också bli aktuellt att tillämpa allmänna rättsgrundsatser som utvecklats inom rättspraxis och doktrin. Handelsbruk och sedvänja inom it-branschen kan också vara av betydelse vid tolkning av it-avtal.

Normalt har dock parterna i ett it-avtal ambitionen att reglera samtliga relevanta omständigheter och villkor i avtalet. Den ambitionen leder vanligtvis till att it-avtalen innehåller ett antal sedvanliga allmänjuridiska regleringar om till exempel avtalstid, felansvar, force majeure, tvistlösning. Därutöver innehåller it-avtalen ett relativt stort antal specifika it-regleringar. Dessa specifika it-regleringar är ofta av teknisk karaktär och varierar beroende på vilken typ av tjänst eller produkt som avtalet avser. It-specifika regleringar kan avse avtalade servicenivåer av olika slag, regler om ansvar för data, garantier avseende teknisk funktionalitet eller ansvar för åtaganden vid avtalets upphörande.

[2] Lindberg Westman, Praktisk IT-rätt, 3:e uppl. Stockholm 2001, s 375.

Den tekniska terminologin kan anses vara typisk för it-avtalen och uppfattas ofta som komplex för den oinvigde. Men att förstå den tekniska terminologin och vad it-avtalet faktiskt avser är många gånger avgörande för att kunna reglera parternas förhållande avseende ansvar, riskfördelning och kommersiella villkor på rätt sätt.

## 2.2 It-avtalens utveckling över tid

Bild 2. It-avtalens utveckling över tid

I många sammanhang beskrivs it-avtalsområdet som komplext och svårtillgängligt. För att underlätta förståelsen för ämnet följer här en översiktlig beskrivning av hur it-avtalen vuxit fram i nära anslutning till it-branschens utveckling. Detta avsnitt är inte avgörande för förståelsen av vägledningen i övrigt, varför läsaren kan fortsätta till nästa avsnitt om historiebeskrivningen inte är av intresse. I stora drag kan it-avtalens utveckling beskrivas på följande sätt.

Under 1960-talet började större organisationer som myndigheter och företag köpa in egna datorer. Först stordatorer och därefter minidatorer och mikrodatorer (eller persondatorer/PC som vi kallar dem idag). Datorerna införskaffades genom att traditionella köpeavtal ingicks. Datorprogramvaran ansågs som en integrerad del av hårdvaran och ingick till en början som en del av köpet. Först mot slutet av 70-talet började datorprogramvara licensieras i någon större omfattning. Microsoft var företaget som bidrog till den nya utvecklingen genom att licensiera operativsystemen PC-DOS och MS-DOS till sina kunder på privat- och företagsmarknaden. Microsoft behöll därmed upphovsrätten till datorprogramvaran till skillnad från andra tidigare programvarubolag som vanligen överlåtit upphovsrätten till hårdvaruproducenterna.

När organisationernas användning av datorer och ADB (automatisk databehandling) ökade så växte också behovet av personal med kunskap och erfarenhet av att hantera

datorer och programvara. Mot bakgrund av detta behov utvecklades och växte it-konsultbranschen under slutet av 1960- och i början av 70-talet. För att reglera tillhandahållandet av it-konsultkompetens tecknades it-konsultavtal.

Inom många större organisationer skapades it-avdelningar vars personal kom att hantera organisationens löpande it-frågor. Men för större projekt där system skulle integreras eller utvecklas behövdes externa experter. It-projekt skapades där parterna kom överens om att konsulten skulle skapa ett visst resultat, under en viss tid till ett överenskommet pris. Behovet av att reglera parternas överenskommelse om it-projekten innebar att it-projektavtalen växte fram.

I takt med att olika system, datorutrustning och infrastruktur bredde ut sig i organisationerna ökade behovet av olika typer av support- och underhållstjänster. Tjänsterna kunde vara av olika karaktär, till exempel på-platsen-support för it-infrastruktur eller telefonsupport för ett lönesystem. Support- och underhållstjänsterna reglerades vanligtvis i support- och underhållsavtal, ibland tillsammans i ett avtal och i andra fall i var sitt avtal.

Organisationer efterfrågade i allt större utsträckning hjälp med att hantera de servrar som organisationens system var beroende av. Leverantörer började därför erbjuda serverdrifttjänster där organisationerna kunde ställa sina servrar i leverantörens lokaler och få hjälp med driften. Den här typen av företag, så kallade servicebyråer, erbjöd även möjligheten för organisationerna att dela på hårdvaran och på så sätt undgå inköp av en dyr hårdvara. Åtaganden av detta slag reglerades mellan parterna i ett it-driftavtal. Drifttjänsterna har succesivt utvecklats och standardiserats och idag erbjuder it-leverantörer av olika slag ett brett utbud av drifttjänster som till exempel webbhosting för webbsidor, samlokaliseringstjänster (co-location) och molnbaserade servertjänster.

Traditionell outsourcing har förekommit sedan 90-talet där utvecklingen drivits av internationella it-koncerner som IBM, Cap Gemini och HP, men också av nordiska företag som WM-data och TietoEnator. Omfattande outsourcingavtal skapades för att reglera den typ av affärsuppgörelse som, förutom tillhandahållande av olika it-tjänster, ofta reglerade övertagande av viss del av kundens verksamhet (medarbetare, utrustning och programvara) och transformation till, för organisationen, nya it-tjänster.

Olika typer av kundanpassade och standardiserade it-tjänster växte således fram på bred front hos leverantörerna. Samordningsfördelar och kostnadsbesparingar blev styrande då kunderna valde att köpa in tjänster istället för att producera inom den egna organisationen. Särskilt möjligheten till finansiering av i it-tjänsten ingående investeringar (till exempel datorhallar, datorer och nätverkskomponenter), vilket innebar att kunden

kunde betala en fast avgift, ledde till att externa it-tjänster blev attraktiva - inte minst inom offentlig förvaltning.

Den tekniska utvecklingen där priset på datorkraft ständigt minskat har inneburit att stora mängder data numera kan behandlas vilket möjliggjort en digital transformation inom ett växande antal områden. Digital innovation har också inneburit att produktionstekniken har utvecklats. Till exempel har virtualiseringsteknik och utvecklingen av internet inneburit att en ny typ av it-tjänster växte fram under början av 2000-talet, så kallade molntjänster. Molntjänsterna har tagit standardisering, samutnyttjande och finansiering inom it-tjänsteområdet till en högre nivå. Med molntjänsternas framväxt utvecklades de standardiserade molntjänstavtalen av leverantörerna. I vissa fall genom så kallade ”click”-avtal som måste accepteras innan den webbaserade molntjänsten tillhandahölls. Mer om molntjänster under avsnitt 8 nedan.

Utvecklingen har inneburit att det idag finns en stor variation i utbudet av it-avtal och it-avtalsvillkor. Variationen beror bland annat på vilken eller vilka it-resurser som avtalet avser vilken part som skrivit avtalet, värdet av de tjänster och produkter som avtalet avser och om avtalet är kundanpassat eller standardiserat.

## 2.3 Olika kategorier av it-avtal

It-avtal kan på olika sätt delas upp i olika grupperingar. För att förstå it-avtalets innehåll underlättar det att förstå dessa uppdelningar. Nedan följer en uppräkning av vanligt förekommande grupperingar med förklaring av vad som avses.

### 2.3.1 IM och AM

Med IM avses det engelska begreppet ”Infrastructure Management” som syftar på olika it-infrastrukturtjänster som exempelvis serverdrift, lagringstjänster (storage), övervakning och kommunikationstjänster.

AM hänvisar till det engelska begreppet ”Application Management” och avser olika typer av applikationstjänster, det vill säga programvarurelaterade tjänster, som exempelvis applikationsunderhåll, applikationsförvaltning och applikationsutveckling.

### 2.3.2 It-avtal med paketerade tjänster

Ett it-avtal kan innehålla flera olika it-tjänster och produkter, till exempel en programvarulicens, underhåll, support och it-drift som regleras i olika avsnitt och bilagor av av-

talet, men där de olika delarna ändå definieras som olika tjänster och produkter. Ett annat alternativ är att leverantören paketerar flera tjänster till en tjänst (vanligen definierad som ”Tjänsten” i avtalet) och att avtalet enbart innehåller avtalsvillkor och bilagor avseende den paketerade tjänsten[3]. Systemleveransavtalen är ett vanligt exempel på en paketerad tjänst med sådana avtalsvillkor. I det paketerade avtalet tar leverantören inte sällan betalt per användare för samtliga ingående delar i den paketerade tjänsten, till skillnad från avtalet där flera tjänster ingår och leverantören tar betalt för respektive del.

### 2.3.3 Fristående avtal, ramavtal, avropsavtal och tilläggsavtal

Efterfrågan på stora mängder it-tjänster och it-produkter har inneburit initiativ för att förenkla upphandling och inköp. Det är därför vanligt att upphandling inom privat och offentlig sektor görs genom ramavtal för olika typer av it-resurser som kunden har ett återkommande behov av. Vanligast är ramavtal för konsulttjänster och olika standardtjänster där behovet varierar över tid. Ramavtal skiljer sig från vanliga kontrakt genom att ramavtal fastställer villkoren för framtida avrop under ramavtalets giltighetstid medan ett vanligt kontrakt avser en faktisk anskaffning och innehåller en fullständig reglering av leverantörens åtagande.[4] Tilläggsavtal tecknas inte sällan för att komplettera ett redan ingånget it-avtal då händelseutvecklingen inneburit att parterna behöver komplettera eller förtydliga det tidigare ingångna avtalet. Det bör dock noteras att det finns särskilda upphandlingsrättsliga bestämmelser om ändringar av avtal under avtalstiden, som klargör i vilka fall en upphandlande myndighet eller enhet kan ändra i ett upphandlat avtal utan att den behöver genomföra en ny upphandling.[5]

### 2.3.4 Standardavtal

För att underlätta hantering av stora mängder it-avtal har olika slags standardavtal och standardavtalsvillkor vuxit fram. Inledningsvis tog leverantörer fram konsultavtalsvillkor och allmänna it-tjänstevillkor. Branschorganisationen IT&Telekomföretagen har sedan 90-talet tagit fram allmänna avtalsvillkor för it-tjänster tillsammans med andra dokument som SLA-bilagor med mera.[6] Många större organisationer har också tagit fram egna konsultavtalsvillkor på vilka man upphandlar it-konsulttjänster. Eftersom it idag till stor del är kärnverksamhet för organisationer inom både offentlig och privat sektor

[3] Bilagor, till exempel en säkerhetsbilaga, blir då tillämpliga på samtliga ingående delar i tjänsten.
[4] Det finns ju olika typer av ramavtal och mer information finns på Upphandlingsmyndighetens hemsida - www.upphandlingsmyndigheten.se/upphandla/om-upphandlingsreglerna/om-lagstiftningen/ramavtal/
[5] Se mer vidare - www.upphandlingsmyndigheten.se/upphandla/om-upphandlingsreglerna/om-lagstiftningen/vasentiga-andringar/
[6] Se närmare IT&Telekomföretagens webbsida om standardvillkor https://www.itot.se/om-oss/var-verksamhet/standardavtal/

och it-resurser införskaffas för stora belopp varje år förekommer det i allt större omfattning att även kunderna tar fram sina egna standardvillkor för olika vanligt förekommande it-tjänster, till exempel allmänna villkor för it-drift och it-support.

I sammanhanget kan också de offentligt upphandlade ramavtalen genom Statens inköpscentral (Kammarkollegiet), Ekonomistyrningsverket och SKL Kommentus nämnas eftersom regleringarna i dessa avtal ofta får spridning till andra avtalsdokument och utgör referensmaterial när man önskar vägledning i mer kundvänliga avtalsformuleringar. Läsaren bör också notera att IT&Telekomföretagens allmänna avtalsvillkor är framtagna av it-leverantörernas branschorganisation och på motsvarande sätt är viktade till leverantörens fördel.

## 2.4 Utvalda kategorier av it-avtal

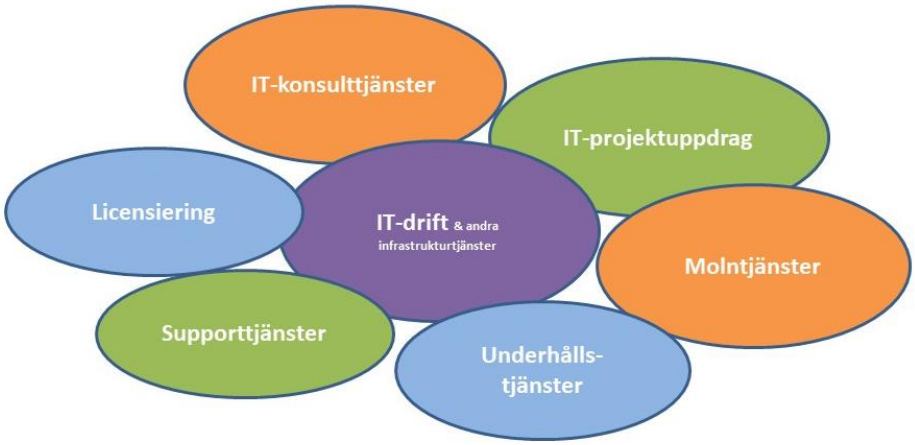


Bild 3. Översiktlig bild av olika kategorier av It-avtal

I denna framställning som syftar till att vara en orientering på it-avtalsområdet har vi valt att lyfta fram ett antal olika kategorier av it-avtal. Vi har valt att lyfta fram de huvudkategorier som vi tror på ett bra sätt speglar den stora bredd som finns i floran av it-avtal. Här ska man hålla i minnet att det inte finns någon fastslagen nomenklatur på it-avtalsområdet. Beteckningarna på de olika kategorierna av it-avtal varierar och en enhetlig praxis saknas. Men utifrån våra erfarenheter, av vad som idag är relevant för offentlig förvaltning, har vi i denna vägledning valt att lyfta fram följande kategorier:

1) Avtal om it-konsulttjänster
2) Avtal om it-projektuppdrag
3) Programvarulicensiering
4) Avtal om it-underhållstjänster
5) Avtal om it-drifttjänster och andra it-infrastrukturtjänster

6) Avtal om it-supporttjänster
7) Avtal om molntjänster

Motivet till att vi valt just dessa kategorier är att vi anser att de är vanligt förekommande i allmänhet, men särskilt relevanta för inköp inom offentlig förvaltning. Tillsamman representerar dessa it-avtalstyper en stor andel av de it-avtal som idag träffas mellan arter på it-området.

# 3. Avtal för it-konsulttjänster

## 3.1 Allmänt

Inköp av konsulttjänster är ofta ett användbart verktyg för att snabbt erhålla ytterligare resurser och utökad kompetens för arbetsområden som normalt inte ingår i organisationens dagliga verksamhet. It-konsulttjänster omfattar vanligtvis olika specialistkompetenser inom it-området och kan bestå av kompetens för systemutveckling, it-infrastruktur, applikationsförvaltning eller it-säkerhet.

Mot bakgrund av att det saknas tvingande eller direkt tillämpbar dispositiv rätt är det ofta avgörande för tjänstens utförande att parterna på förhand har överenskommit hur it-konsulten ska utföra sitt arbete samt tydligt reglerat parternas skyldigheter och rättigheter.

En viktig gränsdragning mellan it-konsulttjänster och it-projektuppdrag (vilket beskrivs närmare under avsnitt 4 nedan) är att leverantören i regel inte åtar sig att leverera något på förhand angivet resultat under en viss tidsperiod till ett överenskommet pris, vid tillhandhållandet av it-konsulttjänster. It-konsulttjänster kan översiktligt delas upp i två kategorier:

Den ena kategorin är resurskonsult där it-konsulten utgör en förstärkning av organisationens befintliga personalstyrka och där it-konsulten normalt arbetar under uppdragsgivarens ledning och kontroll. Den andra kategorin är uppdragskonsult som typiskt arbetar mer självständigt med ett visst uppdrag, till exempel med en it-säkerhetsstrategi.

Uppdragskonsulten arbetar ofta utanför myndighetens organisation, vanligen i egna lokaler och med egen utrustning. Väsentligt för både resurskonsulter och uppdragskonsulter är it-konsultens kompetens och kompetensområde samt att it-konsulten utför sitt arbete på ett fackmannamässigt och noggrant sätt. Valet av formell form för att anlita konsulten är av stor betydelse från offentlighetssynpunkt.

Tillhandahållande av it-konsulter görs ofta på löpande räkning, det vill säga uppdragsgivaren betalar för de timmar som it-konsulten lägger ner och tidsredovisar. Men det förekommer även överenskommelser om fast ersättning exempelvis genom viss bestämd ersättning per månad eller fast pris för en viss uppgift, som till exempel för uppgiften att ta fram en it-säkerhetspolicy.

## 3.2 Nyckelregleringar

### 3.2.1 Uppdragsbeskrivning

Uppdragsbeskrivningen är av central betydelse eftersom den beskriver för vilka ändamål som it-konsulterna anlitas och vilka uppgifter som denne ska utföra. Det är uppdragsbeskrivningen som på förhand anger grunden för leverantörens skyldighet att tillhandahålla it-konsulter med erforderlig och avtalad kompetens. Det är därför avgörande för båda parter att det av uppdragsbeskrivningen framgår de arbetsuppgifter som respektive it-konsult anlitas för att utföra, den kompetensnivå som efterfrågas samt i vilken omfattning som it-konsulten ska vara tillgänglig för uppdragsgivaren.

Det kan i vissa fall vara praktiskt att endast på hög nivå exemplifiera de uppgifter som it-konsulten ska anlitas för. Anledningen till detta är att it-konsulten i rena resursuppdrag ofta ska jobba under uppdragsgivarens ledning och kontroll, vilket innebär att uppdragsgivaren efter ingånget avtal på egen hand kan styra it-konsultens arbetsuppgifter enligt önskemål. Denna möjlighet riskerar att begränsas om uppdragsbeskrivningen är alltför snäv, då ytterligare arbetsuppgifter kan komma att betraktas som tilläggsuppdrag som berättigar leverantören ytterligare ersättning. Detta måste dock balanseras av det upphandlingsrättsliga kravet på transparens. Det måste med andra ord tydligt framgå vilka krav som ställs och vad uppdraget innebär.

Det måste vidare framgå av antingen avtalet eller uppdragsbeskrivningen var arbetet ska bedrivas och vem som ska tillhandahålla för it-konsulten nödvändig information, material, licenser och datorutrustning. I det fall parterna överenskommer om namngivna it-konsulter bör dessa personer uttryckligen anges i uppdragsbeskrivningen.

Då uppdragsbeskrivningen inte sällan blir förhållandevis omfattande rekommenderas det att den utgör en bilaga till huvudavtalet. Detta tillåter även att på ett enkelt sätt dokumentera förändring av tjänstens innehåll. Att formulera en uppdragsbeskrivning är inte sällan tidskrävande. Det är därför viktigt att avsätta gott om tid till förberedelsefasen inför en upphandling. Att avsätta ordentligt med tid för planering, kartläggning och analys av det aktuella behovet skapar goda förutsättningar för att upphandlingsfasen går smidigt och att målet, ett bra avtal som ger ändamålsenliga leveranser, kan uppnås.

### 3.2.2 Rätten till resultat

En mycket central reglering är bestämmelsen om att uppdragsgivaren erhåller fullständiga rättigheter till it-konsultens arbete. Denna berättigade förväntan har uppdragsgiva-

ren oavsett om resultatet omfattar utveckling av datorprogramvara, en it-säkerhetspolicy eller databasstruktur. Definitionen av upphovsrättsskyddade verk är bred, och innefattar enligt 1 § lag (1960:729) om upphovsrätt till litterära och konstnärliga verk (”URL”) bland annat litterära verk, datorprogram, förberedande designmaterial för datorprogram och andra verk som kommit till uttryck på något annat sätt. Enligt 49 § URL är även databaser och kataloger skyddade av upphovsrätt, förutsatt att det är ett resultat av att ett stort antal uppgifter har sammanställts eller om databasen eller katalogen är ett resultat av en betydande investering.

Enligt 1, 5 och 6 §§ URL tillkommer upphovsrätten till upprättat resultat som huvudregel den eller de fysiska personer som skapat, sammanställt eller bearbetat det upphovsskyddade verket. Enligt den så kallade tumregeln erhåller arbetsgivarens en begränsad nyttjanderätt för sådana verk som tillkommer vid utförande av arbetstagarens normala arbetsuppgifter eller särskilda åtaganden gentemot arbetsgivaren. Normalt har leverantören i anställningsavtalet med it-konsulterna avtalat om att leverantören erhåller samtliga rättigheter till det resultat som it-konsulterna skapar i sin anställning.[7] Därför ligger således i normalfallet rätten till resultatet i första skedet hos leverantören varför frågan måste regleras i it-konsultavtalet för att äganderätt eller viss nyttjanderätt ska överföras till uppdragsgivaren.

Vid anlitande av it-konsulter som arbetar under uppdragsgivarens ledning och kontroll är det normala utfallet att uppdragsgivaren erhåller samtliga rättigheter till resultatet. Det är därför av betydande vikt att parterna uttryckligen reglerar detta i avtalet. I många sammanhang vill leverantören inte överlåta upphovsrätten (äganderätt) till datorprogramvara till uppdragsgivaren eftersom man innehar upphovsrätt till den underliggande datorprogramvaran och vill kunna upplåta en begränsad nyttjanderätt till samma programvarukod till flera uppdragsgivare. Den typen av begränsning innebär ofta att uppdragsgivaren erhåller ett betydligt förmånligare pris, vilket ofta resulterar i att uppdragsgivaren accepterar den mer begränsade nyttjanderätten.

[7] Det bör här även nämnas att enligt 40 § a i URL presumeras arbetsgivaren erhålla upphovsrätten till datorprogram om inget annat avtalats.

Exempel på reglering där uppdragsgivaren erhåller samtliga rättigheter till resultatet;
*Kunden erhåller full äganderätt till resultatet inkluderande upphovsrätt och övriga immateriella rättigheter med rätten att ändra och korrigera i resultatet och överlåta det vidare. Leverantören har inte rätt, utan Kundens skriftliga medgivande, att utnyttja resultatet i sin fortsatta verksamhet. Leverantören ska gentemot anlitad underleverantör göra förbehåll för Kundens här föreskrivna rätt till resultatet.*

### 3.2.3 Uppdragsgivarens rätt att avbryta tjänsten inklusive byte av it-konsult

En vanlig anledning till att använda sig av it-konsulter är att uppdragsgivaren önskar skapa tillgång till tjänster med den flexibilitet som organisationen från tid till annan efterfrågar. Det innebär att det ofta är viktigt för uppdragsgivaren att ha flexibilitet och möjlighet att säga upp hela eller delar av avtalet om uppdragsgivarens behov förändras. Avtalet ska om så är fallet innehålla en rätt för uppdragsgivaren att säga upp avtalet i förtid om behovet av it-konsulttjänster förändras. Det är därför vanligt förkommande att uppdragsgivaren ges en rätt att när som helst under avtalstiden säga upp avtalet med trettio dagars uppsägningstid.

Utöver möjlighet att säga upp hela eller delar av avtalet bör avtalet också innehålla en möjlighet för uppdragsgivaren att byta ut enskilda it-konsulter i det fall uppdragsgivaren anser att it-konsulten saknar erforderlig kompetens eller om det föreligger samarbetssvårigheter.

### 3.2.4 Sekretess

I de fall konsulttjänsten består av att utföra arbete nära eller direkt i uppdragsgivarens verksamhet kommer den enskilde it-konsulten inte sällan i kontakt med information som kan vara att anse som känslig eller som omfattas av sekretess. Det därför viktigt att leverantören, antingen i avtalet eller genom ett särskilt sekretessavtal, åtar sig att inte behandla eller röja information erhållen i samband med tjänsten i strid med sekretessbestämmelsen. Utöver ett sekretessavtal eller i avtalet angiven sekretessbestämmelse bör den enskilde it-konsulten även ingå personliga sekretessförbindelser. Det kan i sammanhanget nämnas att det i vissa fall kan krävas en säkerhetsprövning av konsulten enligt säkerhetsskyddslagen (2018:585).[8]

[8] Se Säkerhetspolisens vägledning https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2019-06-17-vagledningar-inom-sakerhetsskydd.html

Det är också vanligt att uppdragstagaren och de konsulter som utför tjänsterna förbinder sig att följa interna sekretess- och säkerhetsföreskrifter hos uppdragsgivaren. Eftersom efterlevnad av sekretess är av stor betydelse, samtidigt som det kan vara svårt att visa en ersättningsgill skada vid brott mot sekretess, innehåller sekretessregleringen inte sällan en reglering om att avtalsbrott i denna del innebär att uppdragstagaren ska erlägga ett visst på förhand angivet vitesbelopp.

Vid en utkontraktering som medför att information hos myndigheten blir tillgänglig även för uppdragstagaren måste offentlighet- och sekretesslagens (2009:400; OSL) begränsningar beaktas. En utförlig beskrivning av de sekretessöverväganden en myndighet har att beakta återfinns i eSams vägledning ”Outsourcing 2.0 – en vägledning om sekretess och dataskydd”[9] . I detta sammanhang kan dock nämnas att sekretess inte behöver beaktas vid överlämnande av uppgifter till en fysisk person som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet och därför själv omfattas av samma lagstadgade tystnadsplikt som myndighetens anställda.[10]

### 3.2.5 Interna föreskrifter

För it-konsultens arbete och uppdrag kan även regler för uppdragsgivarens organisation i övrigt bli relevanta, till exempel interna föreskrifter, policys och riktlinjer. Regelverken kan få betydelse både för konsultens dagliga arbete och för utförandet av uppdraget. Exempelvis kan regler om it-säkerhet, behörighetshantering och regler för användande av öppen källkod vara av betydelse. För att säkerställa en skyldighet för it-konsulterna att efterleva sådana föreskrifter är det viktigt att frågan adresseras i avtalet.

## 3.3 Fallgropar

### 3.3.1 Bristande kompetens hos it-konsulten

Vid anlitande av enskilda it-konsulter är det avgörande att it-konsulten är kapabel att utföra de uppgifter som uppdragsgivaren avser och att personen fungerar i uppdragsgivarens organisation. Problem kan dock uppstå om it-konsulten enbart på pappret innehar de kvalifikationer som parterna har avtalat om och inte i praktiken kan omsätta sina meriter. Uppdragstagaren har i en sådan situation uppfyllt sina skyldigheter enligt avtalet och har normalt ingen skyldighet att utan ersättning ersätta den enskilda it-konsulten.

Mot bakgrund av ovanstående är det viktigt att uppdragsgivaren har rätt att ersätta enskild it-konsult i det fall att it-konsulten inte klarar av att utföra de uppgifter för vilka

[9] Se närmare kapitel 4, Sekretessöverväganden
[10] 2 kap. 1 § 2 st. OSL

denne har anlitats eller vid den situationen att it-konsulten har samarbetssvårigheter som påverkar uppdraget och uppdragsgivaren negativt. En sådan lydelse brukar normalt innehålla ett krav på att uppdragsgivaren ska visa att det föreligger sakliga skäl för byte av it-konsult.

### 3.3.2 Effekten på uppdragsavtal vid upphörande av ramavtal

Ett vanligt upplägg vid anlitande av konsulttjänster är att uppdragsgivare och uppdragstagare träffar ett ramavtal från vilket uppdragsgivaren tillerkänns rätten att genom uppdragsavtal avropa enskilda konsulttjänster. I vissa fall kan ett sådant avrop ske mot slutet av ramavtalets giltighetstid, vilket innebär att uppdragsavtalets tid överstiger ramavtalets.

I denna situation bör uppdragsavtalet ange att ramavtalets bestämmelser är tillämpliga på avropsavtalet. Vidare bör det tydliggöras att uppdragsavtalets giltighet inte är beroende av ramavtalets löptid, utan att uppdragsavtalet ska fortsätta gälla även efter ramavtalets upphörande.

### 3.3.3 Om personuppgiftsansvar

I de fall en uppdragstagare får åtkomst till och behandlar personuppgifter som del av konsulttjänsten uppkommer ofta frågan om parternas roller och ansvar enligt dataskyddsförordningen. Man kan inte utgå ifrån att personuppgiftsansvaret och rollfördelning alltid är detsamma vid tillhandahållande av konsulttjänster. Omständigheterna i det enskilda fallet blir avgörande för bedömningen av personuppgiftsansvaret. En resurskonsult som utför arbete under uppdragsgivarens överinseende är typiskt sett en s.k. ”medhjälpare”, och som inte får ett eget ansvar varken som personuppgiftsansvarig eller personuppgiftsbiträde. Om resurskonsulten däremot behandlar personuppgifter i samband med sitt uppdrag, men inte under uppdragsgivarens ledning och ansvar, talar sådant förhållande mer för att konsulten har rollen som personuppgiftsbiträde. Notera att det även kan vara fråga om ett gemensamt ansvar. Parterna bör alltså i förväg söka identifiera vilken roll uppdragstagaren får enligt dataskyddsförordningen och därefter tydliggöra detta förhållande i avtalet och om tillämpligt ingå personuppgiftsbiträdesavtal eller datadelningsavtal.

## 3.4 Avtalens form och allmänna standardvillkor

För it-konsulttjänster finns det en bred skara allmänna villkor tillgängliga på leverantörers hemsidor. Uppmärksamma att dessa i sina regleringar många gånger är leverantörsvänliga till sin karaktär och att vissa för uppdragsgivarens intressen väsentliga regleringar kan saknas. Även större köpande organisationer inom offentlig och privat sektor

tar fram egna allmänna villkor för it-konsulttjänster. Utöver leverantörernas allmänna villkor finns det framförallt två allmänna standardavtal som kan användas som referens vid framtagande av villkor för konsulttjänster:

- IT&Telekomföretagens Allmänna bestämmelser It–tjänster version 2014
- Kammarkollegiet – Allmänna villkor it-konsulttjänster Resurskonsulter 2018-01-08, diarienummer 23.3-7067-17

# 4. Avtal för it-projektuppdrag

## 4.1 Allmänt

It-projekt har historiskt vanligen omfattat ett större åtagande där ett visst resultat ska presteras, under viss angiven tidsrymd till ett överenskommet pris. Olika typer av utvecklings- och integrationsprojekt där uppdragsgivaren vill koppla samman olika system eller anpassa befintliga system med ny funktionalitet är vanligt förkommande it-projekt. Skillnaden i förhållande till konsultuppdrag är att förutsättningarna för vad som ska åstadkommas specificeras tydligt inledningsvis och att uppdragstagaren tar risken för att åstadkomma resultatet inom överenskomna tidsramar. Det bör dock redan nu uppmärksammas att det finns olika modeller för it-projekt som utgör en blandform där vissa parametrar överenskommes medan det finns flexibilitet i andra, se nedan under avsnitt 4.4 om agila it-projekt.

Förutsättningarna för it-projekt gör att avtalen ofta rymmer en stor operativ risk för parterna. Uppdragstagaren ska tolka uppdragsgivarens kravspecifikation och estimera insatsen i tid och resurser. Uppdragsgivaren ska fånga verksamhetens behov i en kravspecifikation och är ofta höggradigt beroende av att resultatet av it-projektet levereras i tid. Det är mot denna bakgrund det kan noteras att it-projekt ofta avviker från parternas ursprungliga planer och blir föremål för oenighet och tvist. För att minska risken och skapa förutsättningar för ett väl fungerande it-projekt bör parterna överenskomma om en för it-projektet lämplig samverkansmodell.

## 4.2 Nyckelregleringar

### 4.2.1 Kravspecifikation

Avgörande för ett väl genomfört it-projekt är att uppdragstagaren har en förståelse för vad uppdragsgivaren eftersträvar med uppdraget. Det är också viktigt att uppdragsgivaren inför en upphandling skaffar sig kunskap om vilken typ av lösningar marknaden kan erbjuda eller utveckla. Detta kan exempelvis göras genom tidig dialog.[11] När detta förberedelsearbete är gjort kan en kravspecifikation formuleras där beskrivning av art, omfattning och kvalitet på resultatet framgår. Genom att komma överens om en högre detaljeringsgrad innan uppdraget påbörjas blir det normalt lättare för uppdragstagaren att tillhandahålla önskat resultat. Detta i sig minskar risken för att ändringar behöver göras under arbetets gång och kommer därför att innebära att den uppskattade tidsåtgången lättare kan hållas. Kravspecifikationen kan exempelvis innehålla funktionella[12]

[11] Mer om tidig dialog finns att läsa på www.upphandlingsmyndigheten.se/omraden/dialog-och-innovation/dialog/
[12] Mer om funktionskrav finns att läsa på www.upphandlingsmyndigheten.se/omraden/dialog-och-innovation/funktion/

och icke-funktionella krav på resultatet, särskilda säkerhetskrav, resultatets kompatibilitet med andra produkter eller krav på dokumentation.

### 4.2.2 Leveranskontroll och försening

För att säkerställa att det levererade resultatet uppfyller de i avtalet uppställda kraven vid överenskommen tidpunkt, är det avgörande att uppdragsgivaren ges möjlighet att utföra kontroller. Normalt innehåller it-projektavtalet en reglering om viss avtalad leveransdag. Ett av syftena med leveranskontrollen är att säkerställa att faktisk leveransdag överensstämmer med avtalad leveransdag. Avtalet behöver därför innehålla en reglering om hur uppdragsgivarens acceptanskontroll av resultatet ska genomföras, där det rekommenderas att faktisk leveransdag inte ska inträda förrän uppdragsgivaren har kunnat konstatera att resultatet uppfyller de i avtalet uppställda kraven.

Resultatet leverans-testas normalt av uppdragstagaren innan det överlämnas till uppdragsgivaren för acceptanstest. Syftet med detta är att uppdragstagaren ska kontrollera att resultatet är avtalsenligt innan man besvärar uppdragsgivaren med ett acceptanstest. Uppdragsgivaren, å sin sida, vill heller inte bli lämnad med hela ansvaret att upptäcka eventuella brister. Såväl leveranstestet som acceptanstestet bör omfatta samtliga delar av leveransen, inklusive funktionella och icke-funktionella krav samt säkerhet. I det fall resultatet ska vara kompatibelt med andra produkter eller programvaror bör testen även avse detta.

I det fall uppdragsgivaren efter genomfört acceptanstest inte godkänner leveransen av resultatet bör det även i avtalet tydliggöras vilka skyldigheter uppdragstagaren har för att åtgärda brister och svara för kostnader som uppkommer vid åtgärdandet. Eventuella brister måste normalt skyndsamt kommuniceras till uppdragstagaren för att säkerställa att uppdragsgivaren bibehåller sina rättigheter under avtalet.

Om faktisk leveransdag på grund av omständigheter som uppdragstagaren ansvarar för inträder senare än avtalad leveransdag anses leveransen försenad. Projektavtalet ska i sådant fall ge uppdragsgivaren rätt till avtalade sanktioner med anledning av förseningen. Vanligt förekommande är ett leveransförseningsvite som utgår per vecka med viss procentsats av ersättningen för projektet under den period förseningen föreligger. Normalt har uppdragsgivaren också rätt till ersättning för direkt skada som uppkommit med anledning av förseningen, möjligen med avdrag för det leveransförseningsvite som erhållits för den aktuella förseningen. Det är av stor vikt att bestämmelserna om leveransförsening utformas på ett genomtänkt sätt så att uppdragstagaren har rätt incitament att tillhandahålla resultatet på avtalad leveransdag och inte frestas att allokera sina resurser till annat projekt där sanktionerna för en försening är mer kraftfulla.

Exempel på reglering avseende försening och leveransförseningsvite:

*Om faktisk startdag inträder efter avtalad startdag, föreligger försening. Vid försening, som inte beror på kunden eller något förhållande på kundens sida, har kunden rätt till vite för varje påbörjad förseningsvecka med två (2) procent av ersättningen för tjänsten, dock sammanlagt med högst tjugo (20) procent av nämnda belopp.*

### 4.2.3 Felansvar och avhjälpande

Det är viktigt att avtalet reglerar det felansvar som uppdragstagaren har för det resultat som levereras. Som huvudregel ska fel anses föreligga om resultatet inte uppfyller de i kravspecifikationen uppställda kraven. Det är dock i många fall svårt att vid utformandet av kravspecifikationen förutse samtliga brister som kan uppkomma vid framtagandet av resultatet, varför uppdragstagarens felansvar normalt utvidgas ytterligare. Krav kan exempelvis ställas på att uppdragstagaren ska ha ett ansvar för att resultatet kan användas för det syfte som framtagandet av resultatet avsåg. Vidare bör krav ställas på att uppdragstagaren ansvarar för att resultatet ska vara fackmannamässigt utfört och i enlighet med god yrkessed.

Uppdragstagarens ansvar kan också förstärkas genom att i avtalet ange att uppdragstagaren garanterar att resultatet ska ha viss funktion och kapacitet, där det rekommenderas att ett garantiåtagande knyts till tydligt beskrivna krav i kravspecifikationen.

I det fall resultatet inte uppfyller kravspecifikationen, inte är fackmannamässigt utfört eller i enlighet med god yrkessed ska uppdragstagaren ha en skyldighet att avhjälpa bristerna inom en viss utsatt tid. Denna tid kan variera beroende på komplexiteten och karaktären av uppdraget, men en tidsfrist om trettio dagar är vanligt förekommande.

### 4.2.4 Rätt till resultatet

I de fall resultatet är unikt framtaget för uppdragsgivaren, det vill säga när det slutliga resultatet inte innebär en påbyggnad av uppdragstagarens sedan tidigare framtagna basprodukt eller tredjepartsprodukt, är det ofta oproblematiskt såvitt gäller att uppdragsgivaren ska erhålla samtliga rättigheter till resultatet.

Mer problematiskt är det om resultatet endast är en vidareutveckling av tidigare framtaget material, vilket gör att uppdragstagaren eller annan tredje part kan inneha rättigheter till delar av resultatet.

Mot bakgrund av detta måste parterna på förhand komma överens om uppdragsgivarens rätt till resultatet. I det fall uppdragsgivaren inte kan erhålla en fullständig rätt till samtliga immateriella rättigheter måste det i avtalet säkerställas att uppdragsgivaren erhåller en rätt att nyttja (licens) uppdragstagarens eller tredje parts immateriella rättigheter.

### 4.2.5 Löpande uppföljning av arbetet

Avtalet bör reglera hur parterna ska samverka under projektets fortlöpande. Syftet med detta bör vara att parterna aktivt ska samverka för att proaktivt förebygga problem och förseningar i projektet. Detta uppnås bäst genom att parterna överenskommer om en tydlig samverkansmodell där forum, ansvar och roller i samverkan kring projektet beskrivs tillsammans med en eskaleringsrutin.

## 4.3 Fallgropar

### 4.3.1 Otydligt definierat uppdrag

En vanlig orsak till tvist mellan uppdragsgivaren och uppdragstagaren är att det levererade resultatet inte uppfyller uppdragsgivarens förväntningar. Detta är oproblematiskt för uppdragsgivaren om bristen tydligt kan härledas till ett icke uppfyllt krav angivet i kravspecifikationen. Det blir däremot mer komplicerat om bristen endast är hänförlig till uppdragsgivarens uppfattning om vad resultatet borde innebära. Tidig dialog i förberedelsefasen kan bidra till att anpassa förväntningar om vad som är möjligt inom ramen för uppdraget.

Brister som inte är hänförliga till kravspecifikationens angivna krav riskerar att mynna ut i komplicerade tvister där uppdragsgivaren har bevisbördan för att den enligt uppdragsgivaren förkommande bristen faktiskt är en brist enligt avtalet.

För att undvika att denna typ av situationer uppstår måste parterna på förhand ta fram en tydlig kravspecifikation innan uppdraget påbörjas enligt vad som angetts i avsnitt 4.2.1 ovan. I de fall parterna identifierar brister eller otydligheter i kravspecifikationen under arbetets gång bör kravspecifikationen kompletteras och undertecknas av båda parter, i den mån det är upphandlingsrättsligt möjligt. I det fall detta skulle föranleda ytterligare arbete för uppdragstagaren bör parterna på förhand komma överens om kostnad och tid för det tillkommande arbetet innan arbetet påbörjas.

### 4.3.2 Intrång

Vid utveckling av olika typer av resultat kommer i regel vissa typer av immateriella rättigheter att aktualiseras. Detta kan röra sig om exempelvis patent, designskydd och upphovsrätt. Mot bakgrund av att uppdragsgivaren är den part som ska nyttja det resultat som uppdragstagaren tagit fram är det viktigt att det i avtalet regleras vilka skyldigheter som uppdragstagaren har mot uppdragsgivaren och tredje part i det fall resultatet utgör eller misstänks utgöra ett intrång i tredje parts rätt.

Utgångspunkten är här att uppdragstagaren ska ta ett långgående ansvar och hålla uppdragsgivaren skadeslös samt på ett ansvarsfullt sätt hantera situationen om tredje part gör gällande ett upphovsrättsligt intrång på grund av till exempel en datorprogramvara som uppdragstagaren tillhandahåller.

## 4.4 Agila projekt

Någonstans mitt emellan konsulttjänster och it-projekt hittar vi en typ av projekt som brukar benämnas ”agila projekt”. Konceptet kan i stort liknas med it-projekt med skillnaden att ett agilt projekt normalt inte har ett på förhand definierat resultat som leverantören ska tillhandahålla. Istället ska uppdragstagaren eller parterna tillsammans utveckla ett resultat som ska uppfylla ett på förhand angivet ändamål eller funktionellt mål. Denna typ av projekt lämpar sig främst för olika typer av utvecklingsavtal, då det i sådana fall kan vara svårt att på förhand ange vad resultatet ska innehålla. Den agila projektmetoden har vuxit fram som ett svar mot det formaliserade klassiska it-projektet. Metodiken syftar till att främja flexibilitet, där parterna löpande utvärderar arbetet och det som produceras. En fördel med detta arbetssätt är att parterna under projektet har möjlighet att tillföra och reducera de resurser som är allokerade och därmed vara mer effektiva. Den agila projektformen kan dock innebära vissa upphandlingsrättsliga utmaningar.

Det centrala i agila projekt avseende projektmetodik är parternas arbetssätt och samverkan. Parterna arbetar med delleveranser och arbetsperioder (så kallade ”sprintar”). Varje arbetsperiod föregås av en avstämning och planering av nästkommande arbetsperiod. På detta vis säkerställer parterna att projektet fortskrider i rätt riktning och uppnår funktionella mål.

## 4.5 Avtalens form och allmänna standardvillkor

För it-projekt finns det en bred skara villkor tillgängliga på olika uppdragstagares hemsidor. Utöver detta är det framförallt tre standardavtal som kan användas som referens vid framtagande av egna avtalsvillkor:

- IT&Telekomföretagens Allmänna bestämmelser IT-Projekt version 2014
- IT&Telekomföretagens Allmänna bestämmelser AGILA PROJEKT version 2014
- Kammarkollegiet – Särskilda villkor för Konsulttjänst Programvaror & tjänster 2017-11-15, diarienummer 23.3-5559-17 tillsammans med avsnitt 6 om leverans Allmänna villkor Programvaror & tjänster 2017-12-15, diarienummer 23.3-5559-17

# 5. Programvarulicensiering

## 5.1 Allmänt

Alla verksamheter är idag beroende av datorprogram. Datorprogram finns i kontorets skrivare, i det automatiska inpasseringssystemet och självklart i medarbetarnas datorer i olika former. Datorprogram är upphovsrättsligt skyddade enligt URL. Att ett datorprogram är upphovsrättsligt skyddat innebär att upphovsmannen ensamt förfogar över programmet genom att framställa exemplar av det och genom att göra det tillgängligt för allmänheten, med vissa inskränkningar. Det finns många företag vars affärsidé är att skapa datorprogram och därefter upplåta en rätt till andra att nyttja datorprogrammet. En sådan upplåtelse av nyttjanderätt kallas vanligtvis för licensavtal.

Licensiering av datorprogram innebär att licensgivaren upplåter en rätt till licenstagaren att nyttja datorprogrammet i utbyte mot betalning. Licensavtalet innebär inte att licenstagaren köper samtliga rättigheter till datorprogrammet, utan endast att licenstagaren får rätt att nyttja datorprogrammet enligt vissa förutsättningar. Som för de flesta områden inom civilrätten har lagstiftaren lämnat upp till parterna att själva bestämma över avtalsinnehållet i licensavtalet. Det finns dock ett antal tvingande regler i URL som blir tillämpliga vid upplåtelse av nyttjanderätt till datorprogram, till exempel avseende de kompilering, se 26 h § URL.[13]

## 5.2 Nyckelregleringar

### 5.2.1 Licensupplåtelse

Den centrala regleringen i ett avtal om programvarulicensiering är vilken förfoganderätt som licenstagaren ges över datorprogrammet. Licensupplåtelsen innebär att licensgivaren upplåter en viss nyttjanderätt till licenstagaren att använda licensobjektet, vilket normalt är ett visst datorprogram. Upplåtelsen brukar innehålla tydliga regler om hur licenstagaren får nyttja datorprogrammet. Vid upphandling av programvarulicens bör licenstagaren identifiera på vilket sätt datorprogrammet är avsett att användas, exempelvis om det ska göras tillgängligt för tredje man eller endast användas internt inom den egna verksamheten. Av intresse för licenstagaren är även om rättighetsupplåtelsen är exklusiv eller icke-exklusiv för licenstagaren. En icke-exklusiv upplåtelse innebär att licensgivaren får upplåta motsvarande programvarulicens till andra. Det är inte helt ovanligt att licenstagare som varit med och bekostat utvecklingen av ett visst datorprogram

[13] En licenstagares rätt att göra säkerhetsexemplar, observationsrätten samt rätten att utföra dekompilering är tvingande lagstiftning, och kan inte avtals bort i enlighet med 26 g § sjätte stycket och 26 h § tredje stycket URL. Med dekompilering avses ett förfarande där licenstagaren översätter objektkoden tillbaka till källkod för att kunna läsa och förstå källkoden.

kräver en exklusiv rätt till datorprogrammet. Vidare brukar licensupplåtelsen innehålla begränsningar för licenstagarens rätt att nyttja datorprogrammet. Sådana begränsningar kan vara under vilken tid och inom vilken geografi licenstagaren har rätt att nyttja datorprogrammet.

Den rätt som inte blir föremål för upplåtelsen blir kvar hos upphovsrättsinnehavaren, något som inom upphovsrätten kallas för specifikationsprincipen. Rätten anses från början tillhöra den som skapat datorprogrammet och övergår endast till någon annan om så uttryckligen eller underförstått avtalas[14]. Av detta följer att själva licensupplåtelsen behöver vara detaljerad avseende vilken rätt licenstagaren erhåller och vilka rättigheter som är knutna till licensobjektet.

Det är viktigt att parterna definierar vilka komponenter som ingår i licensen, det vill säga vad som är licensobjektet. Givetvis ingår själva datorprogrammet, men för licenstagaren är det ofta viktigt att dokumentation och manualer också omfattas av upplåtelsen. Även frågan om framtida uppdateringar och utveckling av datorprogrammet bör adresseras i avtalet. Att så görs är även viktigt av upphandlingsrättsliga skäl, för att undvika otillåtna ändringar av avtalet. Ska kunden ha rätt till uppdateringar under viss tidsperiod regleras frågan vanligen i ett underhållsavtal. Vidare är det viktigt att reglera om licenstagaren ska få utföra egna ändringar i datorprogrammet. Saknas sådan reglering får licenstagaren inte utföra ändringar, utöver vad som gäller enligt 26 g § URL. Enligt 26 g § första stycket URL får licenstagaren göra nödvändiga ändringar och rättelser av fel i datorprogrammet så att licenstagaren kan använda datorprogrammet för dess avsedda ändamål. Den rätten är dispositiv, vilket innebär att den gäller endast om parterna inte avtalat om annat.

### 5.2.2 Licensmodell

En programvarulicens kan upplåtas och begränsas på flera olika sätt. Vanligt förekommande typer är:

- Användarlicens – en användarlicens innebär att licensen gäller för endast en viss användare eller persondator.
- Verksamhetslicens – en verksamhetslicens innebär typiskt sett att licensen är upplåten till en hel verksamhet (oftast en utpekad juridisk person) och att alla inom den verksamheten får installera och nyttja licensen.
- Nätverkslicens – en nätverkslicens innebär att licensen är upplåten till viss hårdvara eller visst nätverk.

[14] Olsson, Copyright, 10:e upplagan, Stockholm 2018, s 261

- Kapacitetslicens - en kapacitetslicens innebär att rätten upplåts för en viss kapacitet. Det kan exempelvis handla om viss beräkningskapacitet eller avse bearbetning av en viss mängd data per tidsenhet.

Till vald licensmodell knyts ofta ersättningsfrågan på sätt att licenstagaren till exempel erlägger ersättning för licensen per användare. Det är således viktigt att licensavtalet klargör om en viss licensmodell ska tillämpas eller om upplåtelsen är av mer allmän karaktär.

### 5.2.3 Underhåll och uppdateringar

Licenstagare har i regel ett intresse av att få underhållstjänster och standarduppdateringar av programvaran under avtalstiden. Vanligtvis tecknar parterna ett separat underhållsavtal rörande detta. Innebörden av begrepp som underhåll, uppdateringar, version, patchar och liknande varierar vilket licenstagaren bör vara uppmärksam på. Med ”underhåll” i programvarusammanhang avses i regel sådan tjänst som gör att programvaran fungerar som den ska, till exempel bug-fixar och mindre uppdateringar. Med ”standarduppdateringar” avses i regel större uppdateringar som nya versioner eller releaser.

Parterna bör i förekommande fall särskilt reglera omfattningen av åtagandet att tillhandahålla programvaruunderhåll och standarduppdateringar samt ersättningen därför (såvida det inte ingår i licensavgiften). Särskilt i längre avtalsrelationer är det viktigt att säkerställa ett åtagande från licensgivaren att underhålla programvaran och rätta fel under avtalsperioden. För licenstagaren finns även ett intresse att ha möjlighet att själv bestämma om denne ska ligga kvar och nyttja tidigare versioner av programvaran och inte tvingas uppdatera med nya releaser från licensgivaren för att få tillgång till underhålls- och support.

### 5.2.4 Intrång

Licenstagaren utgår från att denne har rätt att nyttja programvaran i enlighet med avtalet. En grundförutsättning för detta är att licensgivaren har haft rätt att upplåta nyttjanderätten till datorprogrammet. Om det visar sig att licenstagarens nyttjande av programvaran inkräktar på annans rättighet är det således av största vikt att licensgivaren håller licenstagaren skadeslös. Avtalspraxis torde vara att om tredje man som anser att intrång föreligger inleder talan mot licenstagaren och gör gällande ett intrång i dennes upphovsrätt så ska licensgivaren bekosta försvaret, tillhandahålla alternativ datorprogramvara och i övrigt hålla licenstagaren skadeslös. Mot bakgrund av det omfattande ansvar denna utfästelse innebär är det vanligt att skador och kostnader som licenstagaren lider på grund av intrång undantas från den generella ansvarsbegränsning som ofta finns i av-

tal om programvarulicensiering. Vidare är det som licenstagare önskvärt att det ska finnas en förpliktelse för licensgivaren att göra sådana ändringar som krävs för att licenstagaren ska kunna nyttja programvaran fullt ut, eller att licensgivaren ersätter programvaran mot annan programvara med motsvarande funktionalitet.

### 5.2.5 Revision

Licensgivaren har i regel ett intresse att kontrollera att den upplåtna programvarulicensen nyttjas i enlighet med avtalet. Därför vill licensgivaren vanligen ha möjlighet att utöva kontroll av licenstagarens nyttjande. I flera licensgivares avtalsvillkor förekommer därför regleringar rörande dennes rätt att genomföra revision av licenstagaren och dennes nyttjande. Det ligger i båda parters intresse att avtala om formerna för detta, bland annat vad avser antal tillfällen, vilka resurser som ska avsättas, hur ingripande revisionen får vara och kostnaderna för revision. Det har blivit vanligare med mer aggressiva revisioner från större programvarubolag, inte sällan med syfte att forcera fram merförsäljning av licenser. Mot denna bakgrund är det av viktigt att revisionsreglering blir balanserad och att rätten till revision inte kan göras gällande allt för frekvent. För det fall en revision visar eventuell underlicensiering bör licenstagaren säkerställa att underlicensieringen inte innebär att denne går miste om all rätt att nyttja den övriga licensen i enlighet med licensavtalet.

Exempel på leverantörsvänlig reglering avseende licensgivarens rätt att genomföra revision;

*Licensgivaren äger rätt att med hjälp av oberoende tredje part, inom skälig tid, dock senast fjorton (14) dagar, efter skriftligt meddelande till Licenstagaren, under Licenstagarens normala arbetstider kontrollera att Licensobjektet används i enlighet med de villkor och begränsningar som fastställs i Licensavtalet.*

*Licensgivarens granskning skall utföras på ett sådant sätt att den i minsta möjliga mån påverkar Licenstagarens verksamhet. Licenstagaren förbinder sig att omedelbart vidta rättelse avseende de brister och brott mot Licensavtalet, innefattande men inte begränsat bristande betalning för användarlicenser, som uppdagas vid en kontroll.*

*För det fall granskningen avslöjar att Licenstagaren betalat licensavgift avseende för att få användarlicenser, motsvarande ett belopp om minst fem (5) procent av den överenskomna licensavgiften för avtalsperioden, skall Licenstagaren dessutom vara skyldig att betala samtliga Licensgivarens kostnader för granskningen.*

## 5.3 Fallgropar

### 5.3.1 Uppdragsgivarens behov under avtalstiden

Vid upphandling av programvarulicens är det viktigt att specificera den funktionalitet som behövs för att programvaran ska fylla sitt syfte hos licenstagaren. Datorprogramvarans funktionalitet beskrivs vanligen i någon form av specifikation eller licensbeskrivning och i den bör den önskade funktionaliteten gå att utläsa. Många gånger när programvaran avser ett system finns olika ”moduler” eller ”enheter” för specifik systemfunktionalitet. Eftersom licensgivaren vanligen förbehåller sig rätten att förändra programvarans funktionalitet över tid är det viktigt att licenstagaren säkerställer att den efterfrågade funktionaliteten finns att tillgå under avtalstiden och att licensgivaren tillhandahåller underhålls- och supporttjänster för densamma. Det rekommenderas att licenstagaren även inventerar och tar hänsyn till framtida behov, både avseende funktion och omfattningen, då licensavtalet träffas, så att möjlighet ges att avropa tillkommande funktionalitet och omfattning om behov uppkommer.

### 5.3.2 Dokumentation ska omfattas av licensiering

Som licenstagare är det i regel viktigt att dokumentation till programvaran omfattas av programvarulicensen, till exempel i form av en manual. Dokumentationen ska vara av sådan innehållsmässig omfattning och vara tillgänglig på sätt att den uppfyller organisationens behov när datorprogramvaran ska användas av organisationens medarbetare. Det rekommenderas att avtalet reglerar på vilket sätt dokumentationen tillhandahålls samt att uppdateringar löpande tillgängliggörs i takt med datorprogrammets utveckling. Det kan också vara bra att särskilt reglera på vilket språk dokumentationen ska tillhandahållas.

### 5.3.3 Deponering av källkod

Licenstagaren har ofta önskemål om att själv kunna göra egna ändringar i programvaran. Sådana ändringar görs i källkoden. Licenstagaren har i sådant fall intresse av att få tillgång till källkoden. Licensgivaren har i regel ett motstående intresse och vill skydda källkoden. En kompromiss som är vanligt förekommande är att parterna avtalar om att källkoden ska deponeras hos en tredje part. Om källkoden deponeras hos en tredje part ingås ett trepartsavtal. Det finns flera institut i Sverige som erbjuder deponeringstjänst, till exempel Stockholms Handelskammare och Västsvenska Handelskammaren. Parterna avtalar då om förutsättningarna för och i vilka situationer licenstagaren har rätt att få tillgång till källkoden. Typiskt sett är bland annat licensgivarens obestånd ett sådant villkor. Därutöver avtalas även vilken av parterna som ska stå kostnaden för deponeringen och hur ofta uppdateringar av den deponerade programvaran ska genomföras.

Källkodsdeponeringsavtal är särskilt värt att beakta om licensen gäller en programvara som är verksamhetskritisk för licenstagaren eller om det finns risk att licensgivaren i framtiden upphör att tillhandahålla den efterfrågade programvaran.

### 5.3.4 Öppen källkod

Så kallad ”öppen källkod” är ett samlingsbegrepp för programvara som inte är proprietär[15]. Eftersom utvecklaren bestämmer reglerna för nyttjandet av den öppna källkoden, varierar regelverk och övriga förutsättningar stort för olika typer av öppen källkod. Det är därför viktigt att närmare undersöka vilka regelverk som följer med den öppna källkod som myndigheten överväger att använda.

I många fall är det oklart varifrån den öppna källkoden kommer då den utvecklats i gemensamma initiativ under olika regelverk. Det finns en osäkerhet kring möjligheterna att göra gällande fel eller utkräva ansvar vad gäller öppen källkod. För licenstagare som upphandlar utvecklingsarbete och it-projekt kopplade till en viss programvara är det lämpligt att överväga om öppen källkod ska få förekomma i programvaran. Särskilt då licensgivaren sällan har rätt att överlåta rättigheterna i öppen källkod eftersom den inte ägs av licensgivaren.

För det fall öppen källkod ska få förekomma är det lämpligt att dessa listas i en förteckning tillsammans med respektive licensvillkor så att det möjliggör för licenstagaren att granska dessa och vad dessa innebär för det utvecklade datorprogrammet. Det kan också framhållas att användande av öppen källkod kan ha fördelar som att skapa oberoende i förhållande till den ursprungliga utvecklaren av programvaran och motverka inlåsningseffekter[16].

### 5.3.5 Tredjepartsapplikationer

Om upplåtelsen också omfattar tillhandahållande av datorprogramvara från tredje part, till exempel större programvarubolag, så omfattas tredjepartsprogramvaran vanligen av standardavtalsvillkor från dessa programvarubolag och inte licensgivarens licensvillkor. Det är för licenstagaren viktigt att noggrant granska dessa villkor eftersom de kan avvika väsentligt från de i det förhandlade licensavtalet och i de flesta fall är mycket licensgivarvänliga.

---

[15] Att en programvara är *proprietär* innebär att den tillhör och ägs av viss person som inte har tillgängliggjort densamma under en öppen licens.

[16] Se vidare avsnitt 2.4.1. om öppen källkod i Konkurrensverkets rapport IT-standarder, inlåsning och konkurrens, se www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/forsk_rapport_2016-2.pdf

### 5.3.6 Avtalens form och allmänna standardvillkor

Licensavtalet kan ha många olika former. De flesta programvarubolag tar fram standardiserade allmänna villkor för licensiering av sina programvaruprodukter. Sådana villkor är vanligtvis licensgivarvänliga och de större kunderna kräver därför normalt anpassningar av de allmänna villkoren genom kravställning i upphandlingar eller i förhandling. De flesta programvarubolagen accepterar justeringar av sina allmänna licensvillkor i förhållande till storleken och betydelsen av den affär som ska ingås. Notera att det för vissa typer av datorprogramvara som avser verksamhetssystem eller applikationer som nyttjas av många användare, finns särskilda användarvillkor som licensgivaren vill att licenstagarens användare ska tillämpa när programvaran nyttjas. Användarvillkoren blir också vanligen en del av licensavtalet och bör granskas på samma sätt som övriga delar av licensavtalet.

Följande exempel finns på standardavtal för programvarulicens:

- EDEL 2019. EDEL 2019 har tagits fram av föreningen Swedish Software (SweS), tidigare Föreningen Svensk Programvaruindustri. Det är alltså en förening för licensgivare. EDEL 2019 kommer i två olika versioner, EDEL 2019 A och EDEL 2019 I. A-versionen ingås genom skriftligt undertecknat avtal och kan även kompletteras med tilläggstjänster. I-versionen är avsett som ett icke-skriftligt avtal som ingås till exempel genom bekräftelse vid nedladdning från internet av datorprogrammet (så kallade clickwrap-avtal).
- Kammarkollegiets ramavtal för ”Programvarulösningar”. I ramavtalet finns allmänna villkor som täcker licensiering av programvaror, men också molntjänster med mera. För licensiering av programvara gäller villkoret ”Särskilda villkor för proprietär programvara” 2017-11-15, diarienummer 23.3-5562-17.

# 6. Avtal för it-underhållstjänster

## 6.1 Allmänt om it-underhållstjänster

Begreppet ”it-underhåll” har inte en specifik innebörd vilket innebär att olika aktörer lägger olika innebörd i begreppet och att underhållstjänstens innehåll kan variera. Det finns två huvudkategorier av it-underhåll; underhåll för hårdvara och underhåll för programvara. Programvaruunderhåll behandlas närmare under avsnitt 5 ovan. Detta avsnitt kommer att belysa avtal om underhåll av hårdvara, det vill säga utrustning av olika slag som till exempel datorer, skrivare och nätverkskomponenter.

Kundens underhållsbehov handlar ofta om att man önskar hjälp med att löpande ”ta hand om” viss utrustning som organisationen är beroende av, till exempel ett lokalt nätverk eller kontorets skrivare. Leverantören specialiserar sig ofta på vissa produkter eller tekniker och har tekniker som på plats eller på distans kan säkerställa att utrustningen fungerar som den ska. Det är också vanligt att leverantören tillhandahåller underhåll på sina egna hårdvaruprodukter.

Underhållsavtalet innebär således att leverantören ska se till att utrustningen eller hårdvaran fungerar och utför de åtgärder som krävs, för felfri funktionalitet. Underhållsåtgärder som kan vara aktuella är övervakning, uppdatering av ingående programvara, utbyte av reservdelar och andra tekniska åtgärder på plats för att utrustningen ska fungera utan avbrott.

## 6.2 Nyckelregleringar

### 6.2.1 Underhållsobjekt

I underhållsavtalet ska det finnas ett åtagande från leverantören att tillhandahålla underhåll på underhållsobjekten i enlighet med avtalet och bilagorna. Vanligtvis brukar det i själva avtalsdokumentet eller villkoret inte anges på vilka specifika underhållsobjekt som underhållstjänsten ska tillhandahållas. Underhållsobjekten anges vanligen genom en uppräkning i en särskild bilaga. I bilagan anges också underhållsobjektens identitet, antal, modell och var det geografiskt befinner sig. Sammanställningen kan också ange servicenivåer och avtalad servicetid för olika underhållsobjekt. Bilagan med sammanställningen över underhållsobjekten uppdateras vanligen många gånger under underhållsavtalets löptid då underhållsobjekt tillkommer och avgår samtidigt som andra variabler som servicenivåer förändras.

### 6.2.2 Tjänstebeskrivning

Underhållstjänstens omfattning, innehåll och avgränsning framgår vanligen av en tjänstebeskrivning. Inte sällan är tjänstebeskrivningen allmänt hållen för att vara tillämplig på flera olika typer av it-underhållstjänster. Här är det viktigt för kunden att säkerställa att underhållstjänsten omfattar de åtgärder som kunden är i behov av samt att underhållsorganisationen är bemannad med tekniker som har rätt kunskap och erfarenhet. Om underhållstjänsten ska utföras på plats bör tjänstebeskrivningen också beskriva leverantörens geografiska etablering och bemanning. Underhållstjänsterna kan delas upp i proaktiva och reaktiva tjänster. Proaktiva underhållstjänster syftar till att fel och störning inte ska uppstå, till exempel regelbunden kontroll och utbyte av reservdelar. Reaktiva underhållstjänster gränsar till supporttjänster och innebär vanligen att kunden kan ringa leverantörens tekniker som på plats eller på distans (”remote”) åtgärdar felet.

Tjänstebeskrivningens omfattning är utgångspunkten för de krav kunden kan ställa på underhållstjänsten och vilka servicenivåer som avtalet kan omfatta.

### 6.2.3 Servicenivåer och servicenivåviten

Underhållstjänsten omfattas vanligen av vissa angivna servicenivåer (SLA)[17]. Syftet med servicenivåer är att parterna redan då avtalet ingås ska vara överens om vilken servicenivå som underhållstjänsten ska omfatta. Exempel på servicenivåer kan vara underhållsobjektets tillgänglighet (hur stor del av tiden utrustningen fungerar felfritt), hur långt tid det tar för leverantören att åtgärda ett fel eller hur lång tid det tar för leverantören att påbörja felavhjälpningen. Servicenivåerna ska vara mätbara och i regel behöver det finnas ett åtagande från leverantören att rapportera dessa servicenivåer till kunden med viss periodicitet. Om leverantören avviker från avtalade servicenivåer utgår vanligen ett så kallat SLA-vite som ökar i takt med avvikelsen från vad parterna har avtalat.

Parterna bör också komma överens om förutsättningar för servicenivåerna, exempelvis om hur felanmälan ska göras, gällande servicetider och sättet för beräkningen av servicenivåerna.

[17] Förkortningen SLA härrör från den engelska definitionen Service Level Agreement och översätts vanligen till Överenskomna servicenivåer

Exempel på reglering avseende servicenivå för felavhjälpning samt vite;

*Felklass 1 – Under Produktionsperiod ska Fel som på verkar produktionen vara åtgärdat inom tre (3) timmar från det att Leverantören upptäckte Felet eller Kunden anmält Felet till Leverantören. Under övrig Servicetid (som inte utgör Produktionsperiod) ska Fel åtgärdas inom tio (10) timmar.*

*Vite utgår med en halv (0,5) procent av Vitesgrundande Belopp för varje påbörjad timme som felavhjälpningen överstiger avtalad felavhjälpningstid.*

## 6.3 Fallgropar

### 6.3.1 Avtalets omfattning

Många gånger omfattas ett stort antal underhållsobjekt av ett underhållsavtal. Ständiga förändringar i kundens organisation gör att underhållsobjekten ändras till omfattning, geografi och tjänsteinnehåll. Utmaningen för parterna är ofta att på ett effektivt sätt hantera dessa förändringar så att tjänsteinnehåll och fakturerad ersättning blir korrekt. Ur ett kundperspektiv kan brister i denna hantering innebära oklarhet om vilka underhållsobjekt som underhållsavtalet omfattar och problem med fakturering och betalning av underhållstjänsten. Nya underhållsobjekt brukar vanligen hanteras korrekt men problem brukar kretsa kring de underhållsobjekt som ska utgå, på så sätt att de inte avförs från avtalet utan fortsatt faktureras kunden. Många leverantörer har idag olika typer av webbaserade kundportaler för denna ändringshantering. I denna del bör kunden ställa krav på att leverantören har implementerade processer och relevant systemstöd för ändringshanteringen.

### 6.3.2 Säkerhet och personuppgifter

It-underhållstjänster tillhandahålls på kundens utrustning och många gånger i kundens lokaler. Det är därför viktigt att leverantören åtar sig att följa de säkerhetsföreskrifter som kunden har för sin verksamhet. På motsvarande sätt är det viktigt att leverantörens personal som ges tillgång till kundens nätverk och system följer gällande säkerhetsföreskrifter och övriga anvisningar. Föreskrifterna kan avse begränsningar i behörighet eller att installation av viss programvara endast får göras under uppsikt av kunden. Överväg om ett personligt åtagande krävs från leverantörens personal i form av ett sekretess- och säkerhetsåtagande.

Därutöver är det inte ovanligt att leverantören inom ramen för tillhandahållandet av it-underhållstjänsten behandlar personuppgifter för kundens räkning. Det kan till exempel avse ansvar för att upprätthålla en förteckning över den utrustning som omfattas av underhållsavtalet, tillsammans med uppgifter om kundens kontaktpersoner i olika berörda delar av organisationen. I sådant fall behöver parterna även ingå ett personuppgiftsbiträdesavtal som reglerar behandlingen av personuppgifterna, och parternas ansvar kopplat till detta.

## 6.4 Avtalens form och allmänna standardvillkor

It-underhållsavtalet kan vara ett fristående avtal om it-underhållstjänst, men även vara en del i ett större avtal om it-tjänster. Oftast är it-underhållsavtalet av den senare typen, det vill säga del i ett annat avtal där kunden köper en hårdvara som denne behöver en it-underhållstjänst för. Många leverantörer av hårdvara och andra objekt har med ett visst underhållsåtagande i sina standardvillkor. I regel är åtagandet begränsat avseende kvaliteten på it-underhållstjänsten (till exempel i servicenivåer) och kan sakna sanktioner vid bristande underhåll. Kvaliteten på it-underhållstjänsten och servicenivåerna är givetvis beroende av de krav som ställts, men många leverantörer tillämpar standardvillkor med olika modeller för servicenivåer och servicenivåviten.

Följande standardvillkor finns för it-underhållstjänster:

- IT&Telekomföretagens Allmänna bestämmelser It-Underhåll version 2014
- IT&Telekomföretagens Villkor Servicenivåer för underhåll (SLA-bilaga – underhåll)
- Kammarkollegiets tillägg till It-Underhåll

# 7. Avtal för it-drifttjänster och andra it-infrastrukturtjänster

## 7.1 Allmänt om it-infrastrukturtjänster

I detta avsnitt kommer avtal för it-drifttjänster och andra it-infrastrukturtjänster behandlas. It-infrastrukturtjänster är en typ av bastjänst som andra it-tjänster ofta är beroende av och bygger vanligen på en underliggande hårdvara. Exempel på it-infrastrukturtjänster är serverdrift, lagringstjänster och kommunikationstjänster. När man talar om it-drift menar man vanligen löpande tillhandahållande av drifttjänster för att upprätthålla funktionen i ett system, applikationer och databaser. Även så kallade output-services som avser skanning och print räknas normalt till it-infrastrukturtjänster.

Det bör uppmärksammas att it-infrastrukturtjänster kan tillhandahållas på många olika sätt beroende på ansvarsfördelning och ägarförhållanden för den hanterade utrustningen. It-drift kan avse situationen när leverantören i sin datorhall och med egna tekniker upprätthåller funktionalitet och tillgänglighet för en server som kunden äger. En annan typ av it-infrastrukturtjänst kan utgöra den webbaserade lagringstjänsten där kundens data lagras i molnet på leverantörens servrar tillsammans med andra kunders data. It-infrastrukturtjänster kan således tillhandahållas under konsultliknande förhållanden, men också som molntjänst varför det är avgörande att förstå de bakomliggande förutsättningarna för leverantörens tillhandahållande, för att på rätt sätt hantera avtalsrättsliga frågeställningar och risker.

## 7.2 Allmänt om avtal för it-drifttjänster och andra it-infrastrukturtjänster

De flesta it-infrastrukturtjänster bygger på någon form av standardisering och samnyttjande av den underliggande hårdvaran, även om det förekommer kundunika it-infrastrukturtjänster. Om leverantören har ett standarderbjudande avseende it-infrastrukturtjänsten har leverantören vanligtvis tjänstebeskrivning, servicenivåer, prislistor och standardavtal med allmänna villkor för tjänsten. Om myndigheten i upphandling inte ställer särskilda krav i dessa delar offererar vanligen leverantören på dessa förutsättningar. De av leverantören framtagna standardförutsättningarna är vanligen leverantörsvänliga varför upphandlande organisationer både på offentlig och privat sida vanligen anger de särskilda villkor som man vill att leverantörerna ska offerera sina tjänster på.

Avtal för it-infrastrukturtjänster kan således ha olika utformning, omfattning och struktur beroende på omständigheterna bakom avtalets tillkomst. Vanligen är avtal för it-infrastrukturtjänster ett under viss tid löpande avtal där leverantören ska tillhandahålla

tjänsten med innehåll enligt tjänstebeskrivning till vissa särskilt avtalade servicenivåer. Till avtalet hör också allmänjuridiska regleringar anpassade för it-tjänster som till exempel regler om leverantörens ansvar, ansvarsbegräsning, förtida upphörande. Ersättningsmodellen kan vara individuellt anpassad till visst belopp per månad, men många gånger är ersättningen baserad på volym eller antal objekt.

Notera att frågor kring säkerhet, sekretess och informationssäkerhet även är av stor vikt i avtal för it-drifttjänster och andra it-infrastrukturtjänster varför avsnitt 8.3.3., 9.2.2 och 9.2.4 är av betydelse även i avseende nämnda it-tjänster.

## 7.3 Nyckelregleringar

### 7.3.1 Tjänstebeskrivning och leverantörens ansvar för tjänster

De flesta organisationer är idag höggradigt beroende av sina it-tjänster och särskilt de it-infrastrukturtjänster som upprätthåller organisationens verksamhets- och kontorsstödsystem. Det är därför av avgörande betydelse att avtalet tydliggör tjänstens innehåll och avgränsning samt leverantörens ansvar för it-drifttjänstens tillhandahållande. Tjänstens omfattning, innehåll och avgränsning regleras vanligen i en tjänstebeskrivning som utgör bilaga till avtalet. Här är det viktigt att den kravspecifikation som kunden tar fram i samband med upphandlingen omvandlas till en tjänstebeskrivning som uppfyller ställda krav. Därutöver bör det i huvudavtalet finnas en text som tydliggör att leverantören ska tillhandahålla tjänsten enligt tjänstebeskrivningen med avtalade servicenivåer (SLA) samt att leverantören ska ansvara för och bekosta samtliga åtgärder som krävs för tillhandahållandet. Det är viktigt att säkerställa att tjänstebeskrivningen verkligen motsvarar myndighetens behov och krav eftersom ett mer långtgående ansvar normalt inte kan utkrävas efter att avtal har ingåtts.

Exempel på reglering avseende felansvar som är till leverantörs fördel och som inte utan ändring bör accepteras;

*Leverantören ska skyndsamt avhjälpa Fel om så är möjligt. För det fall Felet innebär att Kunden inte kan nyttja Tjänsten har Kunden även rätt till en prisreduktion motsvarande tiden mellan tidpunkten från att Felet anmäls till att Kunden kan nyttja Tjänsten igen.*

*Leverantören ansvarar inte för Fel som orsakas av (i) omständigheter som Kunden ansvarar för, (ii) omständigheter utanför Leverantörens ansvarsområde, och (iii) omständigheter som Leverantören inte rimligen kunnat förutse, t.ex. eldsvåda eller strejk.*

### 7.3.2 Servicenivåer (SLA) och vite

Normalt förekommer allmänna regleringar om felansvar i it-driftavtal, men eftersom åtagandet vanligen utförs hos leverantören och kunden normalt enbart kan kontrollera om viss funktionalitet finns på plats har branschen funnit andra vägar att hålla leverantören ansvarig för att fullgöra sitt tjänsteansvar. Parterna avtalar därför om att vissa specifika servicenivåer ska vara uppfyllda under avtalstiden. Vanligast för en drifttjänst som avser serverdrift är att tjänsten ska ha en viss tillgänglighet angiven i procent.

Uppfyllnad av servicenivån mäts därefter löpande och rapporteras av leverantören till kunden. Om leverantören understiger den avtalade servicenivån utgår normalt ett vite angivet i visst belopp eller som del av ersättningen för tjänsten. Det är vanligt med en trappa för vitet på sätt att vitet succesivt höjs i takt med att servicenivån sjunker. En högsta vitesavgift brukar avtalas och kunden bör ha rätt att säga upp hela eller delar av avtalet till förtida upphörande om leverantören upprepade gånger slår i taket för maximal vitesavgift.

### 7.3.3 Skadestånd och ansvarsbegränsning

Det är viktigt att en kund verkligen kan ställa leverantören till ansvar om denne inte fullgör sina åtaganden när en för kunden central It-infrastrukturtjänst tillhandahålls. Många gånger gör leverantören viktiga åtaganden och utfästelser avseende bland annat säkerhet, tillgänglighet, funktionalitet och sekretess som kunden måste kunna förlita sig på. Det är därför avgörande att leverantören tar ett rimligt ansvar om dessa åtaganden och utfästelser inte infrias och ersätter kunden för den skada ett sådant avtalsbrott innebär. Det är inte ovanligt att leverantören försöker att begränsa sin skada inte enbart till direkt skada utan också exkludera tredjeparts skada, skada på grund av förlust av data och skada över visst angivet belopp. Vad som är en rimlig begränsning får avgöras från fall till fall, men det är angeläget att avtalet rymmer en för leverantören kännbar skadeståndssanktion om avtalade utfästelser inte infrias, som står i skälig relation till den ersättning som leverantören erhåller för tillhandahållandet.

### 7.3.4 Förtida upphörande

Avtal om it-drift och andra it-infrastrukturtjänster löper många gånger över längre tid som 2 - 3 år, och i vissa fall upp emot tio år. Om leverantören inte tillhandahåller tjänsten enligt tjänstebeskrivningen, avtalade servicenivåer och övriga åtaganden önskar kunden normalt att säga upp tjänsten i förtid. Vanligen innehåller avtalen därför en reglering om rätt att säga upp avtalet till förtida upphörande. Regleringen görs normalt ömsesidig i fall av obestånd och väsentligt avtalsbrott i allmänhet, men anges ibland också

som en särskild rätt för kunden att säga upp avtalet till förtida upphörande om leverantören brustit i något specifikt åtagande som till exempel vid upprepade tillfällen avsevärt avvikit från avtalade servicenivåer, behandlat personuppgifter i strid med personuppgiftsavtalet eller brutit mot säkerhetsåtaganden.

Det är viktigt att minnas att it-infrastrukturtjänsterna har en viss inlåsningseffekt[18] och att det vanligen krävs en viss period för att upphandla och migrera över till en annan leverantörs it-infarstrukturtjänst.

## 7.4 Fallgropar

### 7.4.1 Ändringshantering

Många gånger tecknas it-driftavtal och andra it-kommunikationsavtal på relativt långa avtalstider. Med den förändringstakt vi idag har i många organisationer innebär det att it-driftavtalet behöver anpassas till förändringarna under avtalstiden. Det är inte relevant att avtala om ett visst tjänsteinnehåll, till exempel drift av ett givet antal servrar, lagring av vissa datamängder eller kommunikation med viss kapacitet eftersom verksamhetens behov förändras.

En utmaning är därför att i avtalet komma överens om ett tjänsteinnehåll ur vilket kunden under avtalstiden kan välja de deltjänster, den kvantitet och de servicenivåer som vid varje tillfälle svarar mot kundens behov. I sammanhanget ska också beaktas att leverantören många gånger önskar utveckla och förändra en standardiserad tjänst och därför önskar att kunna anpassa avtalet i enlighet härmed.

Mot denna bakgrund behöver man vid avtalsskrivningen överväga parternas intresse av förändring av tjänstens innehåll och omfattning, samt identifiera regleringar som på ett rimligt sätt avväger parternas intressen.

### 7.4.2 Avveckling av tjänsten

För de flesta större organisationer innebär ett byte av leverantör av drifts- eller kommunikationstjänst ett större arbete. Förutom att en upphandling behöver företas ska ett avvecklings- respektive införandeprojekt genomföras. I de flesta fall behöver kunden någon form av assistans från den befintliga leverantören. Insatserna kan avse migrering av data eller andra insatser i relation till den nya tjänsten. Avtalet bör därför innehålla en

[18] Mer om inlåsningseffekter och hur man motverkar dem finns att läsa i Konkurrensverkets rapport IT-standarder, inlåsning och konkurrens, se www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/forsk_rapport_2016-2.pdf

skyldighet för leverantören att tillhandahålla dessa avvecklingstjänster enligt kundens instruktioner.

Vanligen är det svårt att uppskatta omfattningen av dessa avvecklingstjänster vid avtalets ingående och överenskomma om rimlig ersättning varför parterna ibland överenskommer om att tjänsterna tillhandahålls på löpande räkning. Detta kan skapa en inlåsningseffekt när den befintliga leverantören ska utvärderas i förhållande till en ny leverantör. Vanligen går det att i samband med upphandlingen identifiera och ställa krav på vissa av de insatser som myndigheten har behov av vid en avveckling.

Ett allmänt ospecificerat åtagande från leverantören att tillhandahålla avvecklingstjänster leder ofta till diskussioner i samband med avvecklingen och kan medföra risk för störningar i myndighetens verksamhet vid migrering till en ny it-tjänst.

Exempel på reglering avseende avveckling av drifttjänst och leverantörens åtagande;

*Vid Avtalets upphörande ska Leverantören återlämna Kundens Programvara och Kundens Data till Kunden eller den Kunden anvisar. Leverantören ska överföra Kundens Data i överenskommet format och vidta de avvecklingsåtgärder avseende Driftstjänsten som närmare beskrivs i punkt 5, Bilaga 1 – Tjänstebeskrivning, inom ramen för ersättningen för Driftstjänsten.*

*Leverantören åtar sig vidare att bistå Kunden med tillkommande avvecklingstjänster för överföring av Driftstjänsten från Leverantören till annan organisation, på det sätt som Kunden närmare anvisar, för att tillse att sådan överföring kan ske med så liten störning som möjligt för Kunden. Leverantören har rätt till ersättning tillkommande avvecklingstjänster i enlighet med avtalade timpriser i Bilaga 2 – Prisbilaga.*

### 7.4.3 Samverkan

Eftersom it-driftavtal och andra it-kommunikationsavtal vanligen löper över längre tid så bör avtalet innehålla en lämplig samverkansmodell där operativa och övergripande frågor hanteras på olika nivåer och i olika forum för samverkan. Formerna för rapportering och ändringshantering behöver också klaras ut. En eskaleringsrutin kan också vara lämplig för situationer då parterna är oeniga och inte på operativ nivå lyckas lösa tvistigheter. Vid forum för samverkan bör protokoll föras och justeras av parterna.

## 7.5 Avtalens form och allmänna standardvillkor

It-infrastrukturtjänsternas avtal kan ha varierande form. Leverantörerna tar fram standardavtal med allmänna villkor för den här typen av standardtjänster. I upphandlingar är det regel att den upphandlande organisationen tar fram ett mer omfattande affärsunikt avtal där samtliga juridiska regleringar står i samma avtalsdokument. Större upphandlande organisationer tar idag också fram standardvillkor för de typer av it-avtal som i stor omfattning upphandlas och kontakteras.

För it-infrastrukturtjänster finns det ett antal publika allmänna villkor, där vissa är allmänna för it-infrastrukturtjänster i stort och andra mer specifika för till exempel it-drifttjänster. Två exempel på allmänna villkor inom dessa områden är:

- IT&Telekomföretagens Allmänna bestämmelser It–infrastrukturtjänster version 2014
- Kammarkollegiet – Allmänna villkor It-drift 2016, diarienummer 96-40-2015

# 8. Avtal för it-supporttjänster

## 8.1 Allmänt

Kännetecknande för it-supporttjänster är att det är löpande tjänsteuppdrag. Inte sällan har it-supporttjänsten anknytning till en annan ”affär” mellan parterna, till exempel en systemleverans, programvarulicens eller hårdvara. Supporttjänsten kan omfatta många typer av tjänster där det gemensamma kan sägas vara att leverantören ska bistå med felavhjälpning eller på annat sätt säkerställa att kunden kan använda viss tjänst eller produkt på ändamålsenligt sätt. Tjänsten kan utföras på distans via telefon, mejl eller över internet, alternativt på plats hos kunden. Ersättningsmodellen för it-supporttjänster varierar. Ersättningen kan utgå per användare, per ärende eller enligt löpande räkning. Centralt för supporttjänsten är att leverantörens organisation besitter specialistkompetens inom det område som support ska tillhandahållas.

## 8.2 Nyckelregleringar

### 8.2.1 Tjänstebeskrivning

Eftersom leverantörens kunskap och erfarenhet inom det område som it-support ska tillhandahållas är central blir tjänstebeskrivningen en nyckelkomponent i avtalet. Av tjänstebeskrivningen bör bland annat supporttjänstens bemanning, kompetenser och tekniska hjälpmedel framgå. Vanligen beskrivs leverantörens organisation som en ”helpdesk” och på vilka sätt den kan kontaktas. För ”på platsen”- support är det väsentligt att supportpersonalens geografiska spridning beskrivs. Här bör särskilt uppmärksammas hur eskalering av mer komplexa problem löses.

Många gånger använder leverantörer underleverantörer eller dotterbolag i andra delar av världen för att lösa de svåraste uppgifterna. Det tillvägagångssättet kan var ändamålsenligt utifrån ett problemlösningsperspektiv, men kan innebära ett rättsligt problem avseende sekretess och/eller persondataskydd då sekretessreglerade uppgifter röjs eller personuppgifter behandlas på ett otillåtet sätt.

### 8.2.2 Specifikation av supportobjekt

Viktigt är också att parterna tydligt definierat supportobjektet (det vill säga vilken applikation, system eller produkt som ska supporteras). När det gäller datorprogramvara till system eller applikationer som verksamheten använder under längre perioder är det viktigt att säkerställa att support tillhandahålls för programvaran i enlighet med myndighet-

ens behov. De supportobjekt som typiskt omfattas av avtalet framgår vanligen av tjänstebeskrivningen. Därutöver behöver parterna i vissa sammanhang mer i detalj specificera hur många supportobjekt som föreligger av ett visst slag. Avtalet bör därför på lämpligt sätt reglera hur parterna under avtalstiden ska hålla räkning på hur många användare som erhåller support eller/och vilka produkter som omfattas av supportavtalet.

### 8.2.3 Servicenivåer och vite

Eftersom supporttjänsten avser stöd till verksamheten och vanligen omfattar kritiska funktioner och system är det väsentligt att parterna klargör vilket ansvar leverantören har för att tillhandahålla supporttjänsten med viss servicenivå. I detta sammanhang kan servicenivå avse helpdeskens svarstid, det vill säga den tid inom vilken leverantörens personal svarar i helpdesk då kundens medarbetare ringer. En typ av servicenivå är åtgärdstid, det vill säga tiden inom vilken det anmälda felet ska vara åtgärdat.

Det är vanligt att leverantören tar på sig att löpande mäta och rapportera de avtalade servicenivåerna. Om avvikelser från avtalade servicenivåer föreligger erbjuder leverantören ett servicenivåvite. Servicenivåvite är ett på förhand bestämt vite vars storlek ofta står i relation till graden av avvikelse från den avtalade servicenivån.

## 8.3 Fallgropar

### 8.3.1 Personuppgiftsbiträdesavtal

I många it-supporttjänster behandlar leverantören personuppgifter för kundens, eller kundens kunds, räkning. Så är fallet i it-supporttjänster som tillhandahålls över telefon eller internet. I regel har leverantören ett ärendehanteringssystem där olika ärenden loggas, exempelvis med information om den support som tillhandahållits. Om leverantören behandlar personuppgifter för kundens räkning ska ett personuppgiftsbiträdesavtal ingås mellan parterna. Parterna bör identifiera de behandlingar som utförs samt för vilka ändamål behandlingar görs, exempelvis felrättning och beställning. Vanligt förekommande är att sådana specifikationer av behandlingar som utförs hanteras i en underbilaga till personuppgiftsbiträdesavtalet, ofta benämnd instruktion.

### 8.3.2 Sanktioner

Kopplat till servicenivåerna är det lämpligt att parterna avtalar om konsekvenserna av att leverantören inte uppfyller avtalade servicenivåer. Exempel på sådana konsekvenser kan vara prisavdrag eller vite. Parterna bör exempelvis ställa sig frågan om grunden för

prisavdraget eller vitet ska vara en viss procentsats av ersättningen för it-supporttjänsten eller en fast summa. Vidare bör även regleras om det finns en maxgräns för prisavdrag eller vitet. Det får anses vara sedvanligt att erlagda viten avräknas från ett eventuellt skadeståndskrav – det står dock parterna fritt att avtala om annat.

### 8.3.3 Säkerhet och sekretess

Vid tillhandahållande av supporttjänster kommer leverantörens anställda många gånger nära den organisation som supporteras. Supporttjänsten innebär ofta att leverantörens personal behöver ta del av uppgifter av olika slag, inte minst personuppgifter, och även röra sig i kundens lokaler med tillgång till utrustning och nätverk. Det är därför angeläget att formerna för tillhandahållandet regleras i avtalet och att de föreskrifter för säkerhet och tillgång till kundens uppgifter tydligt regleras. I denna del är spårbarhet, kontroll och rapportering viktigt samt kundens möjlighet att företa revision och kontrollera att avtalade säkerhets- och sekretessföreskrifter efterlevs.

Exempel på reglering avseende säkerhet vid supporttjänst;

*Leverantören ska vid fullgörande av detta avtal uppfylla de säkerhetskrav som närmare anges i Bilaga [X]: Säkerhet. Leverantören ska vidare i sin verksamhet bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Ledningssystemet ska till utformning och innehåll vara i enlighet med standarderna [Infoga relevant standard] eller motsvarande. Leverantören ska vid tillhandahållande av Tjänsten dessutom uppfylla de säkerhetskrav, inklusive krav på behörighetshantering och loggning som närmare anges i Bilaga [Y]: Tjänstebeskrivning.*

## 8.4 Avtalens form och allmänna standardvillkor

It-supporttjänsteavtalet kan vara ett fristående avtal, men ingår i regel som del av ett annat avtal rörande viss tjänst eller system. Leverantörerna har i regel egna framtagna supportvillkor, eftersom de ofta vill samordna resurser för flera kunder och därför tillhandahålla samma supporttjänst till sina olika kunder. Notera att dessa kan vara leverantörsvänliga och att de inte nödvändigtvis tar höjd för kundens särskilda krav.

IT&Telekomföretagens *Allmänna bestämmelser IT-Underhåll version 2014*, är standardvillkor för it-support-tjänster.

# 9. Avtal för molntjänster

## 9.1 Allmänt

Den tekniska utvecklingen har möjliggjort framväxten av molntjänster. Den kommersiella framgången för molntjänsterna beror på att kunder samnyttjar utvecklad funktionalitet som därmed kan erbjudas till en låg kostnad. Molntjänsten kan enkelt beskrivas som en standardiserad paketering av olika it-resurser (inklusive finansiering), som produceras i leverantörens produktionsmiljö, ofta med hjälp av underleverantören.

Det finns två allmänna definitioner av molntjänster som brukar lyftas fram. IASA (Sveriges it-arkitekter) har publicerat en definition från 2009 som är: ”Termen Cloud Computing relaterar både till applikationer som levereras som tjänster över Internet och till den hårdvara och systemmjukvara som tillhandahåller dessa tjänster”.

En annan definition har publicerats av NIST (National Institute of Standards and Technology), som är del av U.S. Department of Commerce. Enligt NIST:s definition har en molntjänst fem väsentliga särdrag, tre tjänstemodeller och fyra leveransmodeller. Dessa fem väsentliga särdrag är:

1) Självbetjäning efter behov (en. ”On-demand self-service”),
2) Bred tillgänglighet via nätverk (en. ”Broad network access”),
3) Resurspooling (en. ”Resource pooling”),
4) Snabb elasticitet (en. ”Rapid elasticity”), och
5) Mätbar tjänst (en. ”Measured service”).

Sammantaget innebär ovan definition att molntjänsten är en tjänst där leverantören nyttjar sina resurser för flera kunder (resurspooling), vilket på flera sätt blir både billigare och effektivare än produktionen av traditionella it-tjänster. För kunden innebär molntjänsten enligt ovan definition att denne har möjlighet att själv reglera hur mycket av molntjänsten som nyttjas (självbetjäning efter behov) och att nyttjandet kan skruvas upp eller ned beroende på behov (snabb elasticitet).

Vidare tillhandahålls molntjänster över internet på ett sätt som gör det enkelt och effektivt för kunden att koppla upp sig och använda systemet (bred tillgänglighet via nätverk). Eftersom molntjänsten tillhandahålls via internet ligger det både i leverantörens och kundens intresse att mäta och kontrollera leveransen för att skapa transparens med mera (mätbar tjänst).

De tre tjänstemodellerna av en molntjänst, enligt NIST:s definition, är:

1) Infrastructure as a Service (IaaS),
2) Platform as a Service (PaaS) och
3) Software as a Service (SaaS).

**IaaS** är en typisk bastjänst inom it-infrastruktur som till exempel drift, lagring, nätverk. Kunden har inte kontroll över den underliggande infrastrukturen, men kan själv styra operativsystem och applikationer som implementeras ovanpå infrastrukturen.

**PaaS** är tjänster som typiskt sett möjliggör för kunden att implementera och köra sina egna, eller licensierade, applikationer ovanpå en plattformstjänst. Kunden får tillgång till en plattformstjänst där underliggande infrastruktur, operativsystem och lagring typiskt ingår som standard.

**SaaS** innebär att leverantören tillhandahåller hela kedjan från infrastruktur till applikation och tillhandahåller detta till kunden som en standardtjänst. Kunden har typiskt sett inte möjlighet att styra någon del av infrastrukturen eller själva applikationen, bortsett från val av olika tilläggstjänster eller särskilda kundanpassningar i vissa fall.

De fyra leveransmodellerna, enligt NIST:s definition, är:

1) Privat moln (en. ”Private cloud”),
2) Gemensamt moln (en. ”Community cloud”),
3) Publikt moln (en. ”Public cloud”) och
4) Hybrid moln (en. ”Hybrid cloud”).

”Privata moln” innebär att själva infrastrukturen för molntjänsten tillhandahålls en enskild organisation. Infrastrukturen kan ägas, underhållas och driftas av den enskilda organisationen eller av leverantör och befinner sig antingen i organisationens egen datorhall (*on-prem*) eller hos annans datorhall (*off-prem*).

Leveransmodellen ”Gemensamt moln” innebär att molnets infrastruktur tillhandahålls särskilt till en viss avgränsad grupp av organisationer som har gemensamma mål, säkerhetskrav, policies eller på annat sätt delar gemenskap som möjliggör delad molntjänst. Infrastrukturen ägs, driftas och underhålls av någon eller flera av organisationerna alternativt av leverantör. Infrastrukturen kan befinna sig ”on-prem” eller ”off-prem”.

Leveransmodellen ”Publikt moln” är det mest kända och sannolikt mest vanligt förekommande av de fyra leveransmodellerna. Molntjänsten tillhandahålls öppet till alla kunder och tillhandahålls via ett webbgränssnitt över internet. Infrastrukturen befinner sig i leverantörens datorhall. ”Hybrid moln” är en blandning av två eller flera av de andra leveransmodellerna, men som binds samman med någon form av teknik.

Denna översiktliga genomgång av avtal om molntjänster behandlar i huvudsak molntjänster som levereras enligt leveransmodellen publikt moln. Molntjänsten är i regel en standardprodukt med begränsade möjligheter för den enskilda kunden att ställa krav på kundanpassning av molntjänsten. Dock tillhandahålls många molntjänster med olika moduler eller tillvalstjänster som gör att kunden kan uppnå viss flexibilitet. Fördelen med en molntjänst för kunden är normalt lägre kostnader jämfört med att köpa, installera och drifta en programvarulicens på en server som kunden själv bekostar. Även för leverantören innebär leverans av molntjänster normalt lägre kostnader då leverantören får stordriftsfördelar när samma systemuppsättning kan tillhandahållas till flera olika kunder och som delar på leverantörens infrastruktur.

Det finns idag många olika leverantörer av olika molntjänster, både stora och små. Ett kännetecken för molntjänsterna är att leverantören helt kontrollerar produktionsmiljön och att kundens kunskap om hur leverantören mer i detalj tillhandahåller molntjänsten är begränsad. Branschfolk talar ibland om att molntjänsten tillhandahålls ”bakom ett skynke” och att det är leverantörens ”know how” hur man valt att sätt upp sin leveransmiljö. Leverantörens utfästelse avser primärt den funktionalitet som tillhandahålls genom molntjänsten och vanligtvis sekundärt de krav som avser kunden ställer på leverantörens produktionsmiljö.

Det är alltså ett ojämlikt förhållande mellan parterna i ett molntjänstavtal om själva tillhandahållandet där leverantören har ett stort informationsövertag. Till detta tillkommer att många leverantörer endast tillhandahåller sin molntjänst på sitt eget allmänna standardvillkor med begränsade möjligheter för presumtiva kunder att förhandla villkoren.

Ovan har angetts vissa fördelar med molntjänster, kanske främst de ekonomiska. De nackdelar som många kunder upplever med molntjänster är ofta kopplade till säkerhet. Kunden är osäker var dess data lagras, vem som har åtkomst till kundens data och om kundens data överförs till annan part. Dessa frågor har fått särskild uppmärksamhet kopplat till rättsregler om dataskydd och lagstadgad sekretess vilket belysts av bland annat eSam.[19]

[19] Se eSam ”Rättsligt uttalande om röjande och molntjänster” från 23 oktober 2018, Försäkringskassan ”Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt” från november 2019, se eSam ”Outsourcing 2.0 – en vägledning om sekretess och dataskydd” utgiven december 2019. [ANM. Överväg om ytterligare hänvisningar bör införas]

## 9.2 Nyckelregleringar

### 9.2.1 Specifikation

Molntjänster är, som ovan nämnt, i regel en standardiserad tjänst som leverantören tillhandahåller. Leverantören paketerar programvara, uppdateringar, drift, lagring och support tillsammans med finansiering till en sammansatt tjänst för alla sina kunder. I molntjänstavtalet bör därför ingå en specifikation om vilken funktionalitet tjänsten har och dess tekniska specifikationer. Kundens begränsade insyn i molntjänstens tillhandahållande gör att specifikationen blir särskilt viktig. Kunden bör därför noggrant kontrollera att specifikationen, för att säkerställa att molntjänsten med tillhörande moduler eller tilläggstjänster, erbjuder den funktionalitet som motsvarar myndighetens behov.

Till detta hör även att leverantören normalt har rätt att löpande göra uppdateringar och förändringar av molntjänsten. Här bör kunden kontrollera att leverantörens rätt inte är för långtgående och omfattande. En vanligt förekommande reglering innebär att leverantören har rätt att ensidigt göra mindre uppdateringar som inte påverkar funktionalitet eller dylikt, men att mer omfattande ändringar i molntjänsten behöver accepteras i förväg av kunden.

Exempel på reglering avseende ändring av molntjänsten som leverantörer tillämpar;

*Inom de yttre ramarna för Molntjänst, vilka framgår av Kravspecifikation, har Leverantören rätt att ändra innehållet i Molntjänsten enligt den ändringsprocess som Parterna avtalat om. Skulle ändringarna av Molntjänsten, enligt Kundens bedömning, innebära en väsentlig försämring eller annan väsentlig olägenhet för Kunden, har Kunden rätt att inom två (2) månader från det att ändringen genomförts, skriftligen säga upp Avtalet.*

### 9.2.2 Sekretess

För myndigheter och andra offentliga verksamheter som hanterar uppgifter som är sekretessreglerade är det viktigt att säkerställa att dessa inte röjs. I enlighet med eSams uttalande ”Röjandebegreppet enligt offentlighets- och sekretesslagen” från 17 december 2015, ska uppgifter som görs tekniskt tillgängliga för en tjänsteleverantör och som enligt avtalet inte får ta del av eller vidarebefordra uppgifterna, samt att omständigheterna i övrigt medför att det är osannolikt att detta ändå sker, inte anses som röjda i OSL:s mening.

Ovan angivet uttalande från 2015 tog dock inte sikte *på sådana molntjänster som erbjuds av företag som har servrar i olika länder så att informationen kan finnas sparad (speglad) i flera länder och snabbt kan flyttas mellan olika jurisdiktioner samt vara åtkomlig via nät.*[20]

eSam har i ”Rättsligt uttalande om röjande och molntjänster” från 23 oktober 2018 uttalat särskilt om röjandebegreppet och molntjänster. I det senare uttalandet framgår att:

*Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda. Detsamma får anses gälla om redan ägarförhållanden eller geografisk placering av tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.*

Det är således av yttersta vikt för offentliga verksamheter att en rättslig analys genomförs tidigt i upphandlingsprocessen, för att identifiera de krav som myndigheten behöver ställa på molntjänsten och att säkerställa att sekretessreglerade uppgifter som görs tillgängliga för leverantören inte genom molntjänsten senare anses såsom röjda.

### 9.2.3 Personuppgifter

De flesta molntjänsterna innebär att leverantören och dess underleverantörer behandlar personuppgifter vars behandling kunden är personuppgiftsansvarig för, eller som kunden behandlar för annans räkning. Således behövs det i regel ett personuppgiftsbiträdesavtal eller ett underbiträdesavtal för den behandling som leverantören utför för kundens räkning. Det är inte heller ovanligt att för en del behandlingar av personuppgifterna i tjänsten är leverantören att anse som personuppgiftsansvarig. I sådant fall är det lämpligt att parterna ingår ett avtal för att reglera dess ansvar för respektive behandlingar särskilt.

I och med GDPR:s ikraftträdande, samt uppmärksammade rättsfall som mål C-362/14 Maximilian Schrems mot Data Protection Commissioner, har detta inneburit tuffare krav på överföringar till tredjeland. Det är därför viktigt i molntjänster att kunden säkerställer vilka överföringar som görs, till vilket land och enligt vilka förutsättningar.

[20] Se eSam ”Rättsligt uttalande om röjande och molntjänster” från 23 oktober 2018

### 9.2.4 Säkerhet

Kopplat till avsnitten 9.2.2 och 9.2.3 rörande sekretess och personuppgifter är det givetvis viktigt att kunden identifierar vilka säkerhetskrav som behöver uppfyllas av molntjänsten för att vara i enlighet med gällande lagstiftning och kundens egna policies och riktlinjer. Sådana säkerhetskrav som bör kontrolleras och föras in i avtalet är både organisatoriska och tekniska. Som utgångspunkt bör det finnas ett åtagande från leverantören att åtminstone vidta och bekosta sådana säkerhetsåtgärder som krävs av tillämplig lagstiftning. Vidare är det även lämpligt att revision av säkerhetsåtgärderna sker löpande under avtalstiden.

### 9.2.5 Servicenivåer

Molntjänsten innefattar drift och tillhandahållande via internet och oftast support och underhåll till tjänsten. För mer prioriterade molntjänster bör således finnas med ett åtagande från leverantören om servicenivåer kopplade till nämnda tjänster. Särskilt viktigt är det med servicenivåer kopplade till tillgänglighet, men även support och underhåll vid olika problem. Till servicenivåerna kopplas lämpligen någon form av sanktion för det fall leverantören inte uppfyller dessa. Vite eller prisavdrag är vanliga exempel på sådana sanktioner. Servicenivåer kan avtalas antingen i huvudavtalet eller i separat bilaga. Till servicenivåerna bör det även avtalas om mätning och rapportering av dessa.

## 9.3 Fallgropar

### 9.3.1 Underbiträden och underleverantörer

Molntjänsten är en paketering av olika tjänster vilket innebär att det finns en stor sannolikhet att leverantören själv har underleverantörer för att tillhandahålla delar av molntjänsten, till exempel lagring eller support. Med hänvisning till avsnittet ovan om personuppgifter är det därför viktigt att kunden har vetskap om samtliga underbiträden och var dessa behandlar personuppgifter för kundens räkning. Därutöver bör det i personuppgiftsbiträdesavtalet finnas med en reglering om att underbiträden åtminstone ska åläggas samma skyldigheter som leverantören vad avser dataskydd.

Även ur ett allmänt ansvarsperspektiv är det viktigt att ha överblick över vilka underleverantörer som leverantören anlitar. Särskilt i de fall underleverantören bedriver sin verksamhet i annat land och detta lands lagar kan påverka tillhandahållandet av molntjänsten och uppfyllandet av avtalsförpliktelser.

### 9.3.2 Leverantörens ansvar

I regel har leverantörer av molntjänster ett begränsat ansvar för skador, om ens något, i sina egna standarddokument. Molntjänster är förvisso i regel en standardtjänst och det kan därför tyckas rimligt med en mer långtgående ansvarsbegränsning, men det måste givetvis vara inom rimliga gränser. Ofta begränsar leverantören inte bara sitt ansvar för ersättning av skada till visst belopp och till direkt skada utan inte sällan exkluderas andra typer av skada till exempel för förlust av data.

Exempel på reglering avseende en leverantörs mycket begränsade ansvar för en molntjänst;

*Leverantören kan inte göras ansvarigt för fel eller brister i Molntjänsten. Leverantören ansvarar ej för skador eller förluster (varken direkta eller indirekta) hänförliga till användandet av Molntjänsten, eller till förhållandet att Molntjänsten inte kunnat användas. Leverantören ansvarar endast för direkta skador om Leverantören varit vårdslös, och i så fall är Leverantörens ansvar begränsat till ett belopp motsvarande tolv (12) månaders avgift för Molntjänsten.*

### 9.3.3 Backup och tillgång till data

Normalt ansvarar leverantören för att löpande hantera och lagra backup av kundens data i molntjänsten. Detta åtagande bör tydligt framgå av molntjänstavtalet tillsammans med sanktioner som kunden kan göra gällande om leverantören inte fullgör skyldigheterna i denna del. Kunden bör i sammanhanget säkerställa att det back-up-åtagande som molntjänsten omfattar motsvarar kundens behov avseende frekvens, lagringstid och säkerhetsrutiner så att det vid ett eventuellt misstag är möjligt att återskapa nödvändiga data.

Avtalet bör säkerställa att kunden har full tillgång till kundens data i molntjänsten och att leverantören inte ges rätt att begränsa denna tillgång. Sanktionerade regleringar om avtalade servicenivåer och begränsade möjligheter till stillestånd i molntjänsten på grund av serviceåtgärder bör vanligen eftersträvas av kunden.

### 9.3.4 Avtalets upphörande

Att molntjänsten är en standardtjänst som är enkel att ingå avtal om, respektive säga upp, innebär inte att regleringar om åtgärder vid avtalets upphörande ska negligeras – tvärtom. Leverantören hanterar data och personuppgifter åt kunden och det är viktigt att dessa återförs till kunden, alternativt raderas, skyndsamt efter avtalets upphörande.

Leverantören bör således åläggas en skyldighet att samarbeta vid avtalets upphörande och vara behjälplig med att överföra kundens data till den nya leverantören.

## 9.4 Avtalens form och allmänna standardvillkor

Då molntjänsten ofta är en standardtjänst domineras avtalsområdet av standardavtal och allmänna villkor. För många webbaserade molntjänster finns inget alternativ till att klicka i leverantörens standardvillkor. Men det förekommer mer balanserade upphandlade och förhandlade molntjänstavtal, särskilt med lite mindre svenska eller nordiska molntjänstleverantörer intresserade av större affärer.

Följande exempel på standardavtal finns för molntjänster:

- IT&Telekomföretagens Allmänna bestämmelser Molntjänster version 2014
- Kammarkollegiet – Särskilda villkor för Publik molntjänst 2017-11-15, diarienummer 23.3-5562-17
- Kammarkollegiet – Särskilda villkor för Privat molntjänst 2017-11-15, diarienummer 23.3-5562-17

# 10. It-avtalens likheter

## 10.1 Avtalsstruktur och prioritetsordning

It-avtal kan variera till omfattning, struktur och innehåll beroende på omständigheterna i det enskilda fallet. Men vanligen finner vi de centrala avtalsregleringarna som parter, allmän beskrivning av åtagandet, avtalstid, bilageförteckning med mera i ett huvudavtalsdokument. De allmänjuridiska regleringarna om felansvar, ansvarsbegräsning, förtida upphörande, lagval och tvistlösning finner vi vanligen i huvudavtalsdokumentet eller i ett allmänt villkor för tjänsten. Många organisationer, både bland leverantörer och kunder, försöker förenkla och standardisera avtalshanteringen vilket inneburit att olika standarddokument har tagits fram som avtalsbilagor. Detta har sin tur inneburit att många organisationer idag arbetar med relativt förenklade huvudavtalsdokument där stora delen av avtalsinnehållet ligger i de underliggande bilagorna.

Exempel på avtalsstruktur för ett it-driftavtal kan se ut på följande sätt;

1) Huvudavtalsdokument
2) Bilaga 1 - Tjänstebeskrivning It-drift
3) Bilaga 2 - Ersättning och betalningsvillkor
4) Bilaga 3 - Avtalad servicenivå (SLA) för it-drift
5) Bilaga 4 - Personuppgiftsbiträdesavtal
6) Bilaga 5 - Allmänna villkor för it-drift

Vanligen äger avtalsdokumenten företräde i den ordning de anges i avtalet om inte omständigheterna tydligt anger annat. Dock ges personuppgiftsbiträdesavtalet företräde i frågor som avser behandling av personuppgifter.

I frågan om vilken ordning it-avtalets bilagor anges kan it-avtalen variera beroende på omständigheter i det enskilda fallet. Dock brukar vanligen ett allmänt avtalsvillkor för den aktuella tjänsten eller produkten avsluta uppräkningen av avtalsbilagor. Det är inte helt ovanligt att flera allmänna avtalsvillkor anges då it-avtalet omfattar flera tjänster och/eller produkter. Så kan också vara fallet med tjänstebeskrivning och SLA. I sådant fall regleras att dessa bilagor avser viss angiven tjänst eller produkt.

## 10.2 Personuppgiftsbiträdesavtal

I de flesta it-tjänster som vi redogör för i denna vägledning behandlar antingen kunden, leverantören eller båda parterna, personuppgifter vid tillhandahållandet och tillgodogörandet av it-tjänsten. När personuppgifter behandlas inom ramen för en it-tjänst blir dataskyddsförordningen och kompletterande dataskyddslagstiftning tillämplig. Den som

bestämmer ändamål och medel för respektive behandling blir personuppgiftsansvarig för behandlingen. Om det är flera parter som bestämmer ändamål och medel för behandlingen kan situationen ge upphov till ett gemensamt personuppgiftsansvar. Det är den personuppgiftsansvarige som ansvarar för att behandlingen av personuppgifter är laglig och korrekt. Den personuppgiftsansvarige har även det huvudsakliga ansvaret för att registrerades integritet inte kränks och att deras rättigheter uppfylls.

Om annan behandlar personuppgifter för den personuppgiftsansvariges räkning är denne personuppgiftsbiträde. Personuppgiftsansvarig och personuppgiftsbiträdet ska enligt artikel 28 i dataskyddsförordningen ingå ett skriftligt personuppgiftsbiträdesavtal. Personuppgiftsbiträdesavtal brukar ingå i it-avtalet som en bilaga till huvudavtalsdokumentet. Många större organisationer har upprättat en avtalsmall för personuppgiftsbiträdesavtal som används oberoende av vilken it-tjänst som personuppgiftsbiträdesavtalet är avsett att reglera. Ett sådant tillvägagångsätt kan fungera, men det är viktigt att tjänstespecifika frågor och situationsanpassade regleringar fångas upp. Ofta lämpar sig sådana it-tjänstespecifika regleringar att hamna i en underbilaga till personuppgiftsbiträdesavtalet, benämnt ”instruktion” eller ”specifikation”.

För myndigheter torde ofta regleringar avseende överföringar av personuppgifter till tredjeland, kontroll av underbiträden och leverantörens ansvar vara sådana som är av särskild vikt. Särskilt frågan om överföring om personuppgifter till tredjeland har blivit än mer viktig i ljuset av till exempel Cloud Act och liknande lagstiftningar i andra länder.

För både den personuppgiftsansvarige och personuppgiftsbiträdet är det viktigt att överväga personuppgiftsbiträdesavtalets hierarki i förhållande till övriga avtalsdokument och regleringar i it-avtalet. Att det är viktigt blir tydligt i frågan om ansvar för skador kopplade till behandlingen av personuppgifter (häri avser bland annat skadestånd till registrerade). För myndigheter torde det lämpligaste vara att personuppgiftsbiträdesavtalet ska äga företräde i alla frågor avseende behandling av personuppgifter och att reglering om ansvar för eventuellt skadestånd till registrerade äger företräde före it-avtalets generella reglering om ansvar och ansvarsbegränsning.

## 10.3 Säkerhetsskyddsavtal

Myndigheter som gör vissa typer av upphandlingar med koppling till säkerhetskänslig verksamhet ska teckna säkerhetsskyddsavtal med leverantören där det framgår vilka

krav om säkerhetsskydd som gäller för upphandlingen. Även företag ska i vissa fall teckna säkerhetsskyddsavtal med utomstående leverantörer.[21]

Säkerhetsskyddsavtal ska tecknas om det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller om leverantören genom upphandlingen får tillgång till i övrigt säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Statliga myndigheter, regioner och kommuner som har för avsikt att göra en upphandling av varor, tjänster eller byggentreprenader ska teckna ett avtal där det anges hur anbudsgivaren eller leverantören ska uppfylla kraven på säkerhetsskydd. Säkerhetsskyddsavtalet utgör också en grund för att besluta om vilka anställningar och annat deltagande hos leverantören som ska placeras i säkerhetsklass.

När en myndighet eller ett företag tecknar ett säkerhetsskyddsavtal med en leverantör ska Säkerhetspolisen underrättas. Detsamma gäller när ett säkerhetsskyddsavtal upphör, eller om avtalet förlängs utöver den sluttid som tidigare meddelats. Inför vissa upphandlingar måste också samråd ske med berörd tillsynsmyndighet, Säkerhetspolisen eller Försvarsmakten innan upphandlingsprocessen inleds.

## 10.4 Lagval och forum för tvist

Frågan om lagval och forum för tvist brukar vanligen avsluta it-avtalet som avtalsdokumentets sista reglering. Inom offentlig förvaltning har i avtalsvillkor historiskt vanligen angivits svensk lag och svensk allmän domstol vid upphandling. I vissa fall kan regleringar förekomma där myndigheten förbehåller sig rätten att välja om tvisten ska avgöras i allmän domstol eller genom skiljeförfarande.

Vid ett skiljeförfarande avgörs tvisten av en privat skiljedomstol som parterna bekostar. Förfarandet omfattas normalt av sekretess och har fördelen att handläggningstiden vanligen är kortare än vid allmän domstol. De finns en rad svenska och internationella organisationer som erbjuder skiljeförfarande[22]

Svenska it-leverantörer föredrar ofta skiljeförfarande framför allmän domstol, på grund att förfarandet omgärdas av sekretess och på grund av tidsaspekter, men har vanligen inget problem med att tillämpa svensk rätt. Internationella it-leverantörer föredrar dock i vissa sammanhang att utländsk rätt ska tillämpas på it-avtalet. Det kravet tillbakavisas regelmässigt av kunder inom offentlig förvaltning. Skälen är flera, bland annat krävs särskild juridisk kompetens för att tolka it-avtalet enligt utländsk rätt, något som gör att de

[21] Mer om säkerskyddad upphandling går att läsa i Säkerhetspolisens vägledning Säkerhetsskyddad upphandling, https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c671/1560847344410/Vagledning-Sakerhetsskyddad-upphandling.pdf
[22] Se till exempel Stockholms Handelskammares skiljedomsinstitut, https://sccinstitute.se/

flesta svenska köpande organisationerna föredrar svensk rätt. För en svensk myndighet vars uppdrag och verksamhet styrs av svensk författning blir det ofta ett oeftergivligt krav att it-avtalets regleringar avseende parternas skyldigheter, tjänstens innehåll, sekretessåtagande ska tolkas enligt svensk rätt.

# 11. Trender inom it-avtal

Utvecklingen på it-avtalsområdet följer i stort utvecklingen inom it-branschen. De trender som vi ser inom it-tjänstesektorn får ett naturligt genomslag då de nya tjänsterna ska regleras i avtal. Vid en utblick kan de trender vi ser inom it-avtalsområdet sammanfattas på följande sätt:

## 11.1 Standardisering & ”Molnifiering”

**I**t-tjänster och it-produkter standardiseras, paketeras och finansieras i allt större omfattning. Kunderna önskar flexibilitet och vill kunna reglera kostnaden för it när organisationen förändras. Detta har inneburit att många it-avtal idag har en kommersiell modell som innebär att kunden betalar för en paketerad tjänst per användare. Till exempel en arbetsplatstjänst där laptop, operativsystem, affärsstödapplikationer, support och underhåll ingår i den paketerade tjänsten. I tjänstebeskrivningen beskrivs de funktioner som tillhandahålls, SLA-bilagan de servicenivåer som överenskommits, men avtalen innehåller ingen detaljerad beskrivning av hur leverantören producerar tjänsten.

## 11.2 Förenklad struktur

En ökad digitaliseringstakt och ett större behov av it-tjänster innebär att organisationerna behöver teckna fler it-avtal. I början av it-avtalens utveckling skrev många dessa i ett dokument med alla regleringarna samlade. Detta har som beskrivits ovan förändrats och i dag återfinner vi mycket av avtalsinnehållet i avtalsbilagor. Detta har inneburit att huvudavtalsdokumentet succesivt har minskat i omfattning och idag i många fall bara utgör några sidor. I en önskan att förenkla avtalsarbetet har de olika frågorna kommit att behandlas i standarddokument som utgör bilagor till it-avtalet. Exempel på standarddokument är säkerhetsbilaga, personuppgiftsbrädesavtal och samverkansbilaga. Med en förenklad struktur där bilagor innehåller avtalsregleringar av olika slag som kan återanvändas i många olika sammanhang skapas en större effektivitet i avtalsarbetet.

## 11.3 Mer balanserade avtalsvillkor

Mot bakgrund av att många större organisationer varje år konsumerar it-resurser för miljardbelopp har kunderna sedan en tid börjat ta fram egna standardavtal och allmänna avtalsvillkor för olika typer it-inköp. Detta har blivit ett sätt för kunderna att på förhand bedöma den risk som organisationen önskar ta i olika it-avtal men också ett sätt att skapa snabbhet och effektivitet i tidskrävande och brådskande avtalsarbete. Även leverantörerna har insett värdet av att ha tydliga och enkla avtalsmallar som underlättar försäljningsprocessen. I samband med att avtalsmallar och villkor tagits fram

har organisationerna fått överväga hur kundvänliga respektive leverantörsvänliga avtalsdokumenten bör vara. Här har många organisationer valt att röra sig mot mitten och skriva relativt balanserade avtal för att underlätta och skynda på avtalsprocessen. Ur ett kundperspektiv kan denna hållning också innebära att långgående kostnadsdrivande regleringar, som inte skapar motsvarande värde, kan undvikas.

## 11.4 Avtalsförvaltning och revision

När digitaliseringsprojekten realiseras genom upphandling och inköp skapas stora mängder it-avtal som ska förvaltas av myndigheten. Betydelsen av avtalsförvaltning har ökat när allt större del av myndighetens verksamhet är beroende av att en extern leverantör fullgör sitt åtagande. It-avtalen innebär att myndigheten behöver hantera relationen till leverantören och utse en intern kontaktperson med rätt kompetens samt bemanna forum för samverkan på olika nivåer. Dessutom behöver it-avtal som löper över tid bevakas på olika sätt avseende tidsfrister, för att ta tillvara myndighetens rätt till exempelvis uppsägning eller avrop av optioner.

Ofta uppstår diskussioner med leverantören om enskilda regleringar i avtalet, som inte sällan behöver hanteras av en jurist med erfarenhet av it-avtalsrätt, för att myndigheten ska kunna tillvarata sina rättigheter i förhållande till leverantören.

Det interna ansvaret inom myndigheten för it-avtalet behöver tydliggöras och resurser allokeras för att myndigheten ska kunna tillgodogöra sig den formella rätt som it-avtalet ger. Inte minst uppföljning av leverantörens tjänsteinnehåll i förhållande till tjänstebeskrivning och servicenivåer kräver uppmärksamhet. Särskilt angeläget är att myndigheten följer upp leverantörens fullgörande enligt personuppgiftsbiträdesavtalet, genom kontroll av bland annat underbiträden, incidenthantering och tredjelandsöverföring. Även revision på it-säkerhetsområdet är av yttersta vikt där myndigheten på olika sätt bör säkerställa att upphandlade krav efterlevs avseende exempelvis fysisk säkerhet, behörighetshantering, it-säkerhet och hantering av säkerhetsskyddansvar.

eSam