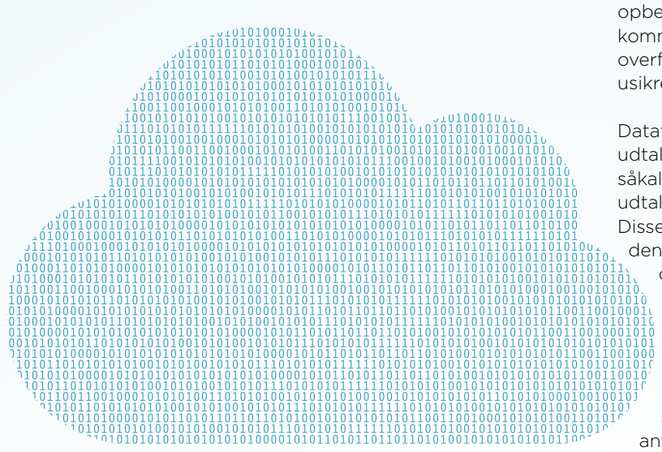

CLOUD-LØSNINGER I DET OFFENTLIGE – HVAD ER MULIGT?

Offentlige myndigheder ser i stigende grad på mulighederne for at anvende cloud-løsninger, som alternativ til traditionelle it-løsninger. Persondatalovens regler og praksis fra Datatilsynet sætter dog ofte begrænsninger for myndigheders brug af cloud-løsninger. Bl.a. afhængig af om en efterspurgt it-løsning vil skulle behandle persondata, vil det være muligt at anvende visse typer af cloud-løsninger i det offentlige. Denne artikel ser nærmere på disse muligheder.

FORSKELLIGE TYPER AF CLOUD-LØSNINGER

En cloud-løsning adskiller sig fra en mere traditionel it-systemanskaffelse, hvor en it-løsning anskaffes og installeres i myndighedens eget it-miljø, eller i et it-miljø, som driftes af en underleverandør, ved følgende kendetegn:

- Løsningen tilgås via internettet
- Løsningen giver mulighed for fleksibilitet i antallet af brugere (op- og nedskalering)
- En kort implementeringsperiode med fokus på at etablere adgang til it-løsningen samt at få migreret myndighedens data ind i it-løsningen
- Vedligeholdelse og support af løsningen ligger hos leverandøren

Der findes primært følgende typer af cloud-løsninger:

- Public cloud: Tjenesterne leveres fra en offentligt tilgængelig infrastruktur (åbent netværk) med fælles standardiseret platform og infrastruktur.
- Private cloud: Tjenesterne leveres fra en ikke-offentligt tilgængelig infrastruktur (lukket netværk) med platform og infrastruktur tilpasset den enkelte kunde.
- Community cloud: Tjenesterne leveres fra en infrastruktur, som er tilgængelig for en bestemt gruppe (community) med platform og infrastruktur tilpasset gruppen.
- Hybrid cloud: En kombination af ovennævnte cloudtyper.

Som offentlig myndighed vil udfordringen ofte være, at jo mere standardiseret en cloud-løsning er, jo mindre mulighed for kontrol med løsningen vil myndigheden have. Dette kan især give udfordringer i forhold til overholdelse af krav til håndtering af personoplysninger i løsningen.

KRAV TIL HÅNDTERING AF PERSONOPLYSNINGER

Persondataloven gælder alene for behandling af personoplysninger. Loven gælder derfor kun for it-løsninger, som indeholder personoplysninger. I praksis vil de fleste løsninger dog behandle personoplysninger. Dette skyldes blandt andet, at begrebet "personoplysninger" er meget bredt. Det dækker enhver form for information om en fysisk person, som indebærer, at personen kan identificeres, herunder IP-adresser og e-mailadresser.

Det er den dataansvarlige, der skal sikre, at persondatalovens og sikkerhedsbekendtgørelsens regler overholdes. Dette gælder også ved brug af cloud-løsninger.

Det er særligt cloud-løsninger, hvor den offentlige myndighed ikke ved, hvor dataene befinder sig, der giver udfordringer i forhold til overholdelse af persondatalovens og sikkerhedsbekendtgørelsens regler. Det skyldes, at det følger af disse regler, at den dataansvarlige skal vide, hvor persondata opbevares og behandles. Hertil kommer, at de særlige regler om overførsel af oplysninger til såkaldte usikre tredjelande skal overholdes.

Datatilsynets har afgivet tre vejledende udtalelser om cloud-løsninger. Den såkaldte artikel 29-gruppe har også udtalt sig om brugen af cloud-løsninger. Disse udtalelser kan opsummeres til, at den dataansvarlige skal være særligt opmærksom på følgende overordnede forhold:

- Den dataansvarlige skal indledningsvist foretage en grundig risikovurdering af samtlige aspekter af den påtænkte anvendelse af cloud-løsningen, herunder særligt af risici forårsaget af dels det kontroltab, som den pågældende løsning vil indebære, dels den uigennemsigtighed, som cloud-løsninger indebærer. Risikovurderingen skal foretages med henblik på at sikre, at persondatalovens og sikkerhedsbekendtgørelsens regler kan overholdes i sin helhed.
- Den dataansvarlige skal ved skriftlig databehandleraftale sikre, at databehandleren alene handler efter instruks fra den dataansvarlige, og at persondatalovens og sikkerhedsbekendtgørelsens krav til tekniske og organisatoriske sikkerhedsforanstaltninger opfyldes, herunder kravene om logning.
- Den dataansvarlige skal kontrollere, at ovenævnte sikkerhedsforanstaltninger iværksættes.
- Hvis dataene overføres til og behandles, herunder opbevares, uden for et EU/EØS-land eller et såkaldt sikkert tredjeland, skal der sikres et højt beskyttelsesniveau. Dette sker typisk ved at anvende EU-Kommissionens standardkontrakt for overførsel af personoplysninger til databehandlere.
- Såfremt databehandleren anvender underdatabehandlere, skal det også sikres, at disse overholder persondatalovens og sikkerhedsbekendtgørelsens regler, herunder reglerne om overførsel af oplysninger til usikre tredjelande.

Persondataretten giver således mulighed for at anvende de cloud-løsninger, hvor ovennævnte persondataretlige krav kan opfyldes. Dette må naturligvis sikres i udbudsmaterialet, herunder særligt i kontrakten.

KRAV I FORBINDELSE MED UDBUD AF EN CLOUD-LØSNING

Udbud af cloud-løsninger kan naturligvis alene ske, såfremt den udbudte løsning overholder persondatalovens krav. Cloud-løsninger, hvor kunden ikke ved, hvor dataene befinder sig, vil ikke kunne anvendes af offentlige myndigheder, medmindre it-løsningen ikke vil komme til at indeholde persondata.

Hvis den udbudte løsning vil indeholde persondata, skal der indarbejdes en række krav i udbudsmaterialet, så overholdelse af persondataloven og sikkerhedsbekendtgørelsen sikres, jf. ovenfor. Disse vil typisk fremgå af kontrakten, der er en del af udbudsmaterialet. Idet den offentlige myndighed i en cloud-løsning mister kontrol med data i forhold til at data opbevares i eget it-miljø, er det også relevant at stille krav til leverandørens egnethed til at kunne løfte opgaven og dermed kontrakten. I forbindelse med et udbud af en cloud-løsning vil det derfor være sagligt at opstille minimumskrav til eksempelvis størrelsen af leverandørens egenkapital og soliditet. Risikoen for bl.a. leverandørens konkurs, og dermed arbejde med at få data ud af et konkursbo i kontraktperioden, vil på denne måde kunne begrænses.

Endelig er det vigtigt, at offentlige myndigheder baserer sit udbud på et kontraktgrundlag, som tager højde for de særlige karakteristika, som gældende for en cloud-løsning, jf. nedenfor.

KONTRAKTVILKÅR

Cloud-løsninger adskiller sig fra traditionelle it-løsninger på en række områder. Derfor vil de kontraktvilkår, som regulerer anskaffelse og brug af en cloud-løsning, være væsentlig anderledes på en række punkter, end de kontrakter som anvendes til anskaffelse af mere traditionelle it-løsninger, dvs. bl.a. fra de statslige standard-it-kontrakter som K01 og K02.

Med andre ord er der en række andre risici forbundet med cloud-løsninger, som skal afdækkes med kontrakten, end tilfældet er ved mere traditionelle it-løsninger. En af disse risici, der skal afdækkes er blandt andet det ovenfor nævnte tab af kontrol over data.

Først og fremmest skal der indarbejdes kontraktkrav, således at persondataloven overholdes, herunder de deraf følgende krav til sikkerhed.

Herudover vil et helt centralt vilkår i kontrakten være krav til oppetid og tilgængelighed i den pågældende løsning. Idet kravene til oppetid og tilgængelighed til løsningen vil afspejle sig direkte i prisen for brug af løsningen, bør man afstemme disse krav med brugerne af løsningen.

Kontrakten skal desuden have fokus på håndtering af grænseflader til løsningen. I den forbindelse skal det afklares, om der i løsningen tilbydes standard integrationsmuligheder til øvrige it-systemer, om der tilbydes API'er til udvikling af kundespecifikke løsninger, eller om løsningen understøtter eksempelvis NemID, hvis dette er nødvendigt, for at myndigheden rent sikkerhedsmæssigt kan anvende løsningen.

Andre opmærksomhedspunkter i kontrakten vil være spørgsmålet om "lock-in" til leverandøren, såvel juridisk, teknisk og/eller økonomisk. Et helt centralt vilkår vil i den forbindelse være krav om mulighed for udlæsning af data i et bestemt format, således at disse er anvendelige i en ny løsning efter kontraktophør, eller at den offentlige myndighed har mulighed for at opsige kontrakten efter en begrænset bindingsperiode ■

Hans Abildstrøm
Advokat
ha@horten.dk

Charlotte Kunckel
Advokat
cku@horten.dk

Thomas Grønkær
Advokat
tgr@horten.dk