Datainspektionen informerar

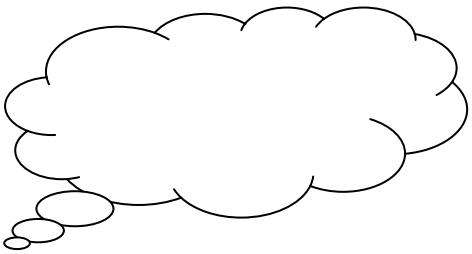
Nr 2/2014

Allmänna råd

om användning av molntjänster (Cloud Computing) i den offentliga sektorn.

Vid användningen av molntjänster aktualiseras en del problem och frågeställningar som den registeransvariga myndigheten behöver ta ställning till.

Verksamheter som tar i bruk molntjänster är juridiskt ansvariga och skyldiga att behandla personuppgifter i enlighet med personuppgiftslagen.



Datainspektionen

den 28 november 2014

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Innehåll

1 Molntjänster och personuppgiftslagen

Datormoln eller molntjänster är tekniker baserade på användingen av datorer över internet. Det är tekniker där stora skalbara resurser, såsom till exempel processorkraft, lagring och funktioner tillhandahålls som tjänster på internet till användare som inte behöver ha den tekniska kunskapen eller kontrollen över infrastrukturen.

Vid användningen av molntjänster aktualiseras en del problem och frågeställningar som den registeransvariga myndigheten behöver ta ställning till.

2 Vad är molntjänster?

Molntjänster (Cloud Computing) är ett samlingsbegrepp på allt från dataprocessning och datalagring till programvara på servrar som är tillgänglig från externa serverparker kopplade till internet. I korthet kan molnet sägas vara en benämning på de servrar, applikationer, data och tjänster som finns att tillgå via internet.

National Institute of Standards and Technology (NIST) http://csrs.nist.gov/publications/nistpubs/800-145/SP800-145.pdf delar upp defintionen på molntjänster enligt följande:

1. Essential Characteristics (bl.a. självbetjäning är ett viktigt kriterium)
2. Service Models (tjänste- och affärsmodeller såsom SaaS[1], PaaS, Iaas m.fl.)
3. Deployment Models (Installationssätt: Privat, publikt, gemensamt för olika organisationer, hybrid som kombinerar flera användare så att de förblir unika med gemensam data och applikationer)

Molntjänster täcker åtminstone nedanstående tre olika servicemodeller[2]:

1. Software as a Service (SaaS) enligt vilken en applikation används utan att kunna kontrollera operativsystemet, hårdvaran eller det nätverk som applikationen är uppbyggt kring
2. Platform as a Service(PaaS) genom att använda applikationsmiljön utan att kontrollera operativsystemet, hårdvaran eller den infrastruktur på vilken applikationen är uppbyggd.
3. Infrastructure as a Service (IaaS) genom att använda datorresurser på en virtuell maskin, såsom styrkan att processa, lagring och nätverk utan att kontrollera molninfrastrukturen.

Molntjänster är indelade i driftsorienterade molntjänster såsom för masshantering av ekonomiska transaktioner och applikationsorienterade molntjänster såsom kontorsrelaterad kommunikation.

[1] Exempel på sådana konsumentorienterade applikationer är Facebook, Linkedin, Twiter, Hotmail, Gmail och GoogleApps

[2] Nordic Public Sector Cloud Computing – a discussion paper (TemaNord 2011:566)

Fördelen med molntjänster kan vara att de är utbyggbara utan allvarlig försämring av prestanda, att betalningen gäller enbart förbrukningen, ingen onödig resursförbrukning och att energikonsumtionen kan vara lägre. Nackdelen kan vara att standarder saknas, att det finns en låsning till leverantören, säkerheten kan vara öppen, rättsliga komplikationer samt kostnaderna för dataöverföring kan vara höga.

Några exempel på avtalsreglering:
Kundens kontroll och tillgång till sina data

- För återskapande av data
- Reglering av exit (det vill säga möjlighet att avsluta arbetet med ett program eller en fil på ett ordnat sätt)

Krav på säkerhet

- Tas backup i traditionell mening?
- Hur ofta?
- Var lagras den?
- Är den krypterad?
- Multipla kopior?
- Återläsningstester?

Datormolnmodellen upplevs som lämplig då den möjliggör utbyggnad av datakapacitet utan krav på inledande investering.

3 Verksamheten har behandlingsansvaret

Molnleverantörer kan använda sig av leverantörer som i sin tur använder sig av leverantörer i flera led. Användaren har svårt att skaffa sig kännedom om vilka underleverantörer som anlitas. Det kan bero på olika orsaker såsom att moln-leverantörerna inte vill dela med sig av informationen eller av kunskapsbrist hos användaren.

Det kan även förekomma att molnleverantörerna använder sig av utrustning som är fysiskt utspridd till olika platser och även över nationsgränser. En molnleverantör kan även utan användarens vetskap flytta data inte bara mellan olika underleverantörer men också mellan olika länder, vilket kan resultera i att olika lagstiftning blir tillämplig för hantering av de personuppgifter som lagras.

En del molnleverantörer är stora aktörer och har standardiserade avtalsvillkor som kan vara svåra för den enskilda användaren att påverka och anpassa efter sin specifika situation. En del leverantörer har även villkor som säger att de kan ändras ensidigt utan att kunden förvarnas.

Personuppgiftslagen innehåller bestämmelser som är nödvändiga att känna till för den registeransvariga myndighet som använder sig av eller överväger att börja använda molntjänster för behandling av personuppgifter. Här kommer några viktiga punkter att tänka på:

Skyldighet att teckna avtal
Personuppgiftslagen ställer krav på att den registeransvariga myndigheten har kontroll över behandlingen av personuppgifter. Myndigheten ska ha kontroll över för vilka ändamål uppgifterna behandlas men också över att uppgifterna hanteras på ett säkert sätt.

För att personuppgifter ska få föras in i en molntjänst som innebär att data kan komma att lagras eller bearbetas utanför EES-området (d.v.s. EU- och EFTA-länderna) gäller särskilda rättsliga krav. Den som vill använda en molntjänst för lagring av personuppgifter måste alltså antingen försäkra sig om att lagring endast sker inom EES eller aktivt se till att uppfylla kraven för överföring till tredje land.

Den som anlitar en molnleverantör för sin behandling av personuppgifter ska därför enligt 19 § personuppgiftslagen upprätta ett skriftligt avtal med instruktioner till molnleverantören. I avtalet ska det särskilt föreskrivas att leverantören får behandla personuppgifterna bara i enlighet med instruktioner från den registeransvariga myndigheten och att leverantören är skyldig att vidta sådana lämpliga tekniska och organisatoriska säkerhetsåtgärder som personuppgiftslagen kräver.

4 Riskvärdering och informationssäkerhet

Oavsett vem som behandlar personuppgifterna är det den registeransvariga myndigheten som har ansvar för att se till att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. Den registeransvariga myndigheten bör därför genomföra en risk- och sårbarhetsanalys inklusive en noggrann rättslig analys. Därtill bör undersökas om molntjänster är lämpliga med avseende på den säkerhetsnivå som är lämplig för verksamheten[3]. Om man använder molntjänster bör åtminstone följande åtgärder övervägas:

- Autentisering
- Behörighetskontroll
- Kommunikationssäkerhet
- Rutiner för säkerhetskopiering, och skydd mot obehörig trafik och skadlig programvara

Således ska databehandlingsavtalet innehålla en del som behandlar informationssäkerhet och det är viktigt att den registeransvariga går grundligt igenom avtalet. Avtalet i sig är ingen garanti för att leverantören har en tillfredsställande informationssäkerhet.

Personuppgiftslagens 18 § har en bestämmelse om säkerhetsrevision. Därför bör den registeransvariga kunna lägga fram dokumentation om informationssystemets utformning och säkerhetslösningar. Detta i syfte att den behandlingsansvariga kan förvissa sig om att lösningen har tillfredsställande informationssäkerhet utgående från riskanalysen.

[3] Cloud Sweden som är en verksamhetsgren och ett nätverk inom Dataföreningen www.cloudsweden.se

4.1 Rättsliga hinder

Den rättsliga analysen kan ge vid handen att de krav som lagstiftningen uppställer kan vara svåra att uppfylla vid användningen av molntjänster. Vid behandlingen av personuppgifter kan det finnas rättsliga krav på sekretess och säkerhet som behöver beaktas i samband med val av molntjänstleverantör eller ställas som krav på säkerhet i molntjänstavtalet.

4.2 Informationssäkerhet

En överflyttning av tjänster till molnet ställer särskilda krav på ett systematiskt informationssäkerhetsarbete hos både leverantören och kunden.

4.3 Due diligence

En kund bör inte helt förlita sig på ett välutformat avtal utan bör undersöka leverantörens ställning och historik. Det kan handla om att undersöka leverantörens verksamhet och ställning utifrån ett såväl legalt, finansiellt som tekniskt perspektiv (due diligence) där kunden till exempel får ta del av leverantörens underlag, rutiner och processer för att kunna bedöma leverantörens förmåga att leva upp till kundens krav.

4.4 Riskanalys

Innan beslut fattas om att använda molnet bör kunden analysera vilka risker och krav som är särskilt kopplade till molnanvändningen för att kunna förankra behovet av säkerhetsåtgärder hos leverantören.

4.5 Upphandling

Offentliga organ måste i de flesta fall beakta reglerna om upphandling. Vidare måste bland annat offentlighetsprincipen och arkivreglerna följas.

5 Tredje land

Molntjänster utförs ofta över landsgränser och i olika världsdelar samtidigt. Det är således inte tillräckligt att endast ta reda på var information lagras utan även var den bearbetas. Det innebär att information kan överföras för bearbetning för att sedan återföras och lagras i bearbetad form på överenskommen lagringsplats. Konsekvensen blir att en kund - oavsett vad avtalet anger - kan vara exponerad mot andra länders rättssystem.

Det finns ett förbud i personuppgiftslagen mot att överföra personuppgifter som är under behandling till länder som inte har en adekvat skyddsnivå. En molnleverantör som inte är etablerad inom EU eller EES, eller om denna i sin tur anlitar underentreprenörer som inte är etablerade där, riskerar att överföra personuppgifter till tredje land. Det är den registeransvariga myndighetens (kunden) ansvar att se till att eventuell överföring till tredje land är tillåten, till exempel med de registrerades samtycke, med stöd av standardavtals klausuler eller om en molnleverantör som är etablerad i USA har anslutit sig till det som kallas Safe Harbor.[4]

[4] En samling frivilliga regler om personlig integritet och dataskydd som har tagits fram och beslutats av USA:s handelsdepartement (Department of Commerce - DoC). EU-kommissinen har bedömt att reglerna utgör en adekvat skyddsnivå och därmed är det tillåtet att föra över personuppgifter från EU/EES till organisationer i USA som har anslutit sig till regelverket.

6 Informationsplikt

Den registeransvariga myndigheten har en skyldighet att ge den registrerade följande information:

- Namn och adress på den registeransvariga,
- Ändamålet med behandlingen
- Om uppgifter lämnas ut och vem som är mottagare
- Annan information för den registrerade ska kunna använda sig av de rättigheter han eller hon har enligt personuppgiftslagen

7 Problemställningar

Att särskilt observera

- Identifiering av allmän handling
- Hantering av arbetsmaterial med mera
- Sekretessprövning
- Partsinsyn
- Identifiering av förvaltningsbeslut
- Personuppgiftslagens bestämmelser

Rutiner för såväl arkivering och bevarande, gallring och rensning samt krav på dokumentation behövs (registrering, arkivering/bevarande, gallring/utplåning och dokumentation vid ärendehandläggning). Är det tillåtet för tjänstemän att ladda upp Google applikationer, twittrande och bloggande?

8 Sammanfattning

Definiera aktuell sammansättning av molntjänster

- Privata moln, publika moln eller hybridlösningar
- Nationella, inom EU eller internationella

Precisera verksamhetens art

- Service, ärendehandläggning (eventuellt Inkluderande myndighetsutövning), uppdragsverksamhet, affärsverksamhet)

Kartlägg involverade aktörer såsom

- Sökande, klagande eller annan part
- Registrerad (vid behandling av personuppgifter)
- Enskilda, till exempel företrädare för intresseorganisationer
- Kommersiella, till exempel vidareutnyttjare av myndigheters handlingar
- Tjänsteföretag
- Media