



Molntjänster och personuppgiftslagen

Allt fler kommuner, myndigheter och företag överväger att använda sig av så kallade molntjänster. Molntjänster innebär att exempelvis processorkraft, lagring och funktioner tillhandahålls av leverantörer som tjänster över Internet.

Den som använder en molntjänst för lagring av personuppgifter, till exempel i ett löneregister, förlorar den faktiska kontrollen över de personuppgifter som lagras. Till detta kommer att molnleverantörer ofta använder sig av standardavtal, det vill säga i förväg definierade användarvillkor, och anlitar underleverantörer. Det är därför viktigt att den som tänker använda en molntjänst i sin verksamhet är medveten om de krav som ställs enligt personuppgiftslagen.

Den som anlitar en molnleverantör är alltid personuppgiftsansvarig

Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer. Leverantören, och alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden. Det är den personuppgiftsansvarige som ansvarar för att personuppgiftslagen och andra lagar följs, till exempel myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen.



Datainspektionen

Detta måste den personuppgiftsansvarige göra

Laglighetskontroll

Innan en molntjänst tas i bruk måste den personuppgiftsansvarige bedöma om den personuppgiftsbehandling som man vill låta molntjänstleverantören utföra kommer att vara tillåten enligt personuppgiftslagen.

Enligt personuppgiftslagen får personuppgiftsbiträden bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Normalt utformar den personuppgiftsansvarige själv instruktionerna. När man anlitar en molntjänstleverantör är man däremot ofta hänvisad till de villkor som gäller enligt leverantörens standardavtal. I sådana fall måste den personuppgiftsansvarige granska de avtalsvillkor och riktlinjer som molntjänstleverantören erbjuder och göra bedömningen utifrån dessa. Bedömningen måste göras med tanke på personuppgiftslagens bestämmelser och slutsatserna av den personuppgiftsansvariges egen risk- och sårbarhetsanalys. Den personuppgiftsansvarige måste bland annat:

- ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga
- ta ställning till om molntjänstleverantören kan komma att lämna över personuppgifter till ett så kallat tredjeland, det vill säga ett land utanför EU/EES, och om den överföringen i så fall har stöd i personuppgiftslagen
- bedöma vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas
- se till att ett personuppgiftsbiträdesavtal upprättas med molnleverantören samt
- beakta annan lagstiftning, till exempel sekretesslagstiftning.

Risk- och sårbarhetsanalys

Den personuppgiftsansvarige måste genomföra en risk- och sårbarhetsanalys för att bedöma om det är möjligt att anlita molntjänstleverantören för behandling av de tänkta personuppgifterna, vilken säkerhetsnivå som är lämplig och vilka åtgärder som måste vidtas. Ju större integritetsrisker en viss personuppgiftsbehandling innebär desto högre är kraven på säkerhetsåtgärder. Hur stora integritetsrisker som en viss behandling innebär beror bland annat på **antalet** personer som de behandlade uppgifterna avser, **mängden** uppgifter som behandlas om varje person och **känsligheten** hos de behandlade personuppgifterna. Även möjligheten att strukturera personuppgifterna har i det här sammanhanget betydelse. Åtgärder ska övervägas när det gäller bland annat autentisering, behörighetsstyrning, behörighetskontroll, kommunikationssäkerhet, rutiner för säkerhetskopiering och utplåning samt skydd mot obehörig åtkomst och skadlig programvara.

När man behandlar känsliga personuppgifter (till exempel uppgifter om hälsa), brottsuppgifter och sekretesskyddade uppgifter, kräver Datainspektionen bland annat att det ska finnas stark autentisering vid överföring av uppgifter i öppet nät och att



uppgifterna ska skyddas med kryptering. När sådana uppgifter behandlas innebär kraven på åtkomstkontroller ofta att den personuppgiftsansvarige inte bara ska utföra kontroller på förekommen anledning utan också regelbundet och systematiskt följa upp vem som har haft åtkomst till vilka uppgifter.

Det finns flera etablerade metoder för risk- och sårbarhetsanalys. En sådan är att använda checklistor som exempelvis den som tagits fram av EU:s nätverks- och informationssäkerhetsbyrå ENISA; Cloud Computing, Information Assurance Framework. Nackdelen med att använda en checklista är att den inte alltid är anpassad för den molntjänst man tänkt använda och att det finns risk för att man arbetar mekaniskt efter listan och därmed låter bli att tänka själv samt att verkligen analysera resultaten.

Personuppgiftsbiträdesavtal med molnleverantören

Den personuppgiftsansvarige måste i regel se till att det finns ett personuppgiftsbiträdesavtal som lever upp till kraven i personuppgiftslagen.

Personuppgiftsbiträdesavtal upprättas antingen genom att man tecknar ett avtal med varje bolag som behandlar personuppgifter för den personuppgiftsansvariges räkning eller genom att i ett avtal ge ett bolag mandat att ingå avtal med underbiträden. Ger man ett sådant mandat måste det framgå i avtalet att varje underbiträde har samma skyldigheter som det personuppgiftsbiträde som den personuppgiftsansvarige ingått avtal med.

Villkoren i personuppgiftsbiträdesavtalet ska vara urskiljbara från övriga villkor som gäller mellan parterna och de ska inte ensidigt kunna förändras av personuppgiftsbiträdet. Kravet på personuppgiftsbiträdesavtal kan också innebära följande:

Personuppgiftsbiträdesavtalet ska

- föreskriva att personuppgiftsbiträdet är skyldigt att tillämpa svensk lagstiftning när det gäller behandlingen av personuppgifter
- föreskriva att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen
- föreskriva att personuppgiftsbiträden endast får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner och därmed säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som personuppgiftsbiträdet anlitas för
- säkerställa att den personuppgiftsansvarige har kännedom om vilka andra personuppgiftsbiträden som kan komma att behandla den personuppgiftsansvariges personuppgifter
- säkerställa att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder
- säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna samt
- säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter.



Det kan finnas undantag från kravet på personuppgiftsbiträdesavtal då ett sådant avtal inte tillför något mervärde för integritetsskyddet. Ett exempel är när personuppgiftsbiträdet endast lagrar material som är identiskt med sådant som lagligen publicerats på Internet.

Kontroll av biträden

Den personuppgiftsansvarige måste kunna förvissa sig om att alla personuppgiftsbiträden verkligen vidtar de säkerhetsåtgärder som krävs. Ju känsligare uppgifter som behandlas, desto högre är kravet på att kontrollera biträdena. I en molntjänst behandlas ofta uppgifter av flera personuppgiftsbiträden som även behandlar personuppgifter för många andra personuppgiftsansvarigas räkning. Molnleverantörer kan också flytta information inte bara mellan olika underleverantörer utan också mellan olika länder. Därför kan det bli svårt att uppfylla de krav som ställs på kontroll av personuppgiftsbiträden vid behandling av känsliga personuppgifter.

Tredje land

Om personuppgifter kommer att behandlas av personuppgiftsbiträden i ett land utanför EU/EES måste den personuppgiftsansvarige se till att något av undantagen från förbudet mot överföring till tredje land kan tillämpas, till exempel samtycke, standardavtalsklausuler eller anslutande till Safe Harbor-principerna.

Mer information

På www.datainspektionen.se kan du läsa mer om vad som gäller kring personuppgiftsansvar, biträdesavtal, säkerhet och tredjelandsöverföring. Där hittar du också beslut från aktuella inspektioner av molntjänster.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.