personuppgifter i **molnet**

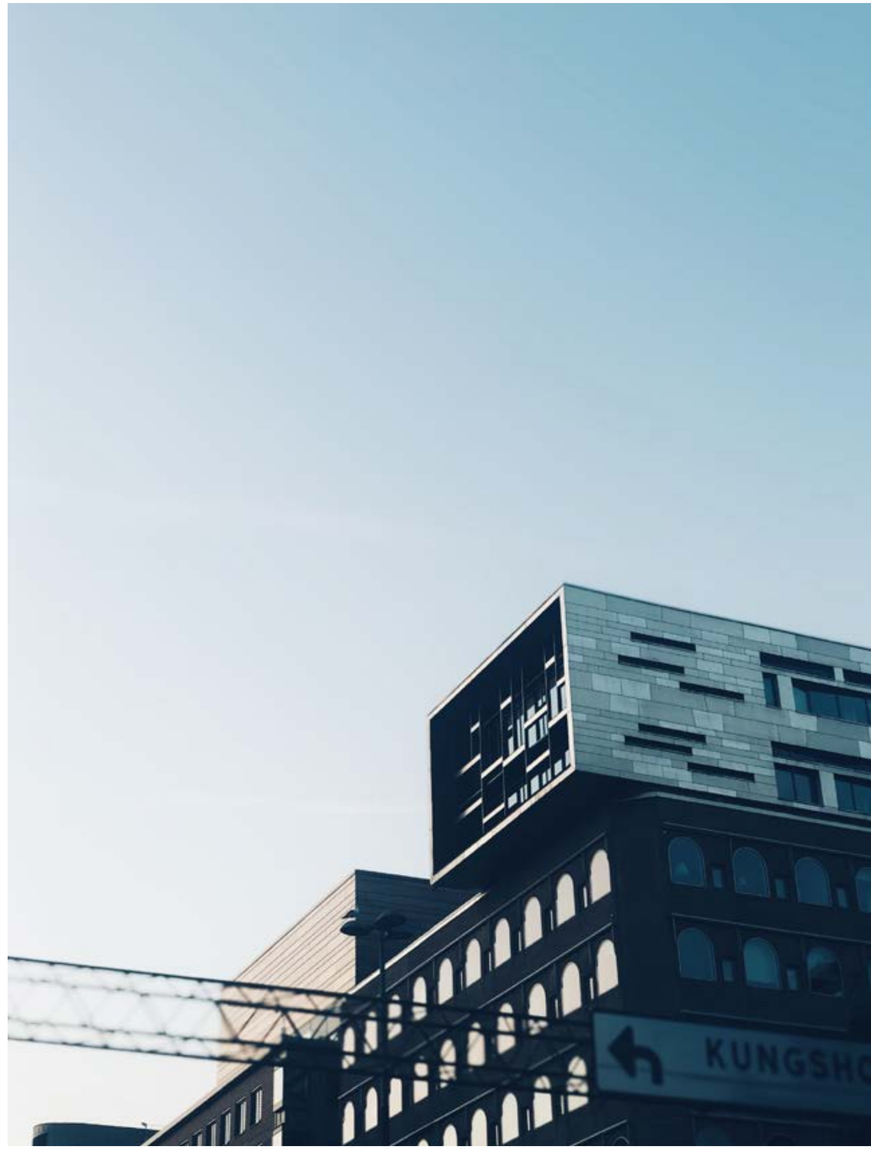
Din guide till Cloud Compliance
och en framtidssäkrad molntjänst

binero

Innehåll

Så påverkar GDPR och CLOUD Act er lagring av personuppgifter i molnet.

De allra flesta organisationer använder någon form av molntjänst idag eller är på väg att flytta delar av sin IT-miljö till molnet. Det innebär att er data inklusive de personuppgifter som lagras och bearbetas hamnar hos den molntjänstleverantör som ni använder er av. Det i sig är inga konstigheter, men när vi pratar om lagring och hantering av just personuppgifter i molnet är det viktigt att även belysa den EU-gemensamma lagstiftningen GDPR (General Data Protection Regulation) samt det amerikanska regelverket CLOUD Act. Anledningen är att dessa två regelverk inte alltid är kompatibla med varandra. Det kan i sin tur innebära juridiska bekymmer för de enskilda europeiska organisationer som nyttjar amerikanska molntjänster. Denna guide syftar till att vägleda dig kring hantering av personuppgifter i molnet så att du säkerställer efterlevnad av regelverket och samtidigt bygger en fratidssäkrad lösning.



GDPR – individens rätt till skydd av personuppgifter

GDPR:s främsta uppgift är att säkerställa alla EU-medborgares rättsliga dataskydd, att säkra individens rätt till sitt privatliv samt kontrollen över sina egna personuppgifter. Regelverket gäller för alla medlemsländer inom EU och således även för alla dföretag som verkar i ett EU-land. Förordningen reglerar även hur personuppgifter får överföras mellan länder EU och till länder utanför EU. Kortfattat gäller följande: det är fritt fram att flytta personuppgifter mellan EU-länder eftersom samma lagstiftning gäller för alla länder inom området. För att överföra personuppgifter utanför EU krävs däremot antingen att mottagarlandet är sedan tidigare godkänt av EU eller att ett separat avtal mellan berörda länder eller företag har upprättats. Detta avtal ska då garantera godkänt personuppgiftsskydd i enlighet med bestämmelserna i GDPR. Det är precis här som svårigheten uppstår när lagring av data sker hos molntjänstleverantörer som lyder under under den amerikanska lagstiftningen CLOUD Act. Här är nämligen dessa två regelverk inte kompatibla.

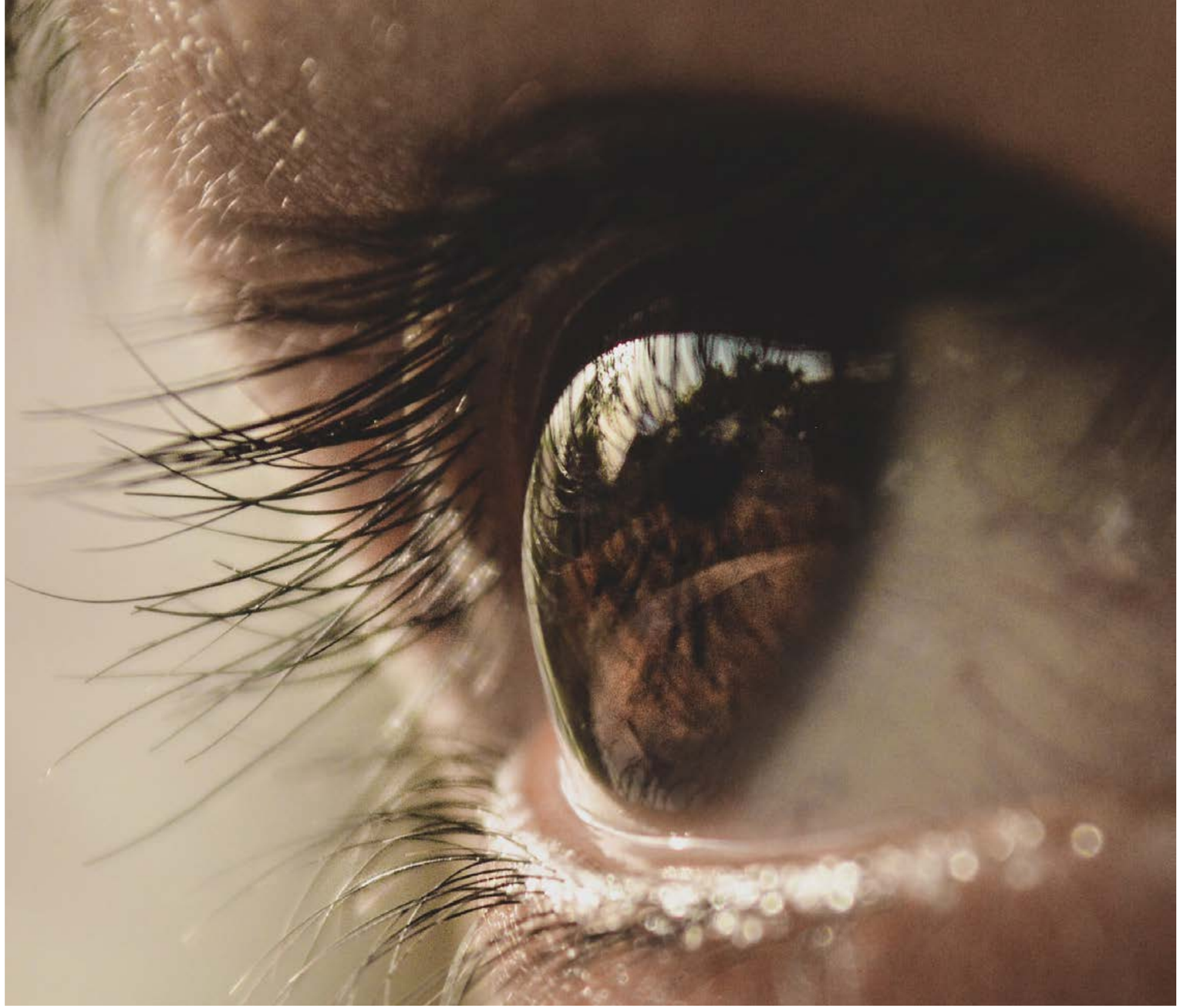
CLOUD Act – amerikanska myndigheters rätt att inhämta information

CLOUD Act är en amerikansk lag som innebär att amerikanska myndigheter, vid misstanke om brott, har rätt att begära ut personuppgifter och annan data från amerikanska molntjänst-leverantörer. Detta gäller även om denna data lagras utanför USA, exempelvis inom EU. Om amerikanska myndigheter nyttjar denna rätt kan det innebära problem för de europeiska organisationer som drabbas eftersom en sådan utlämning av data direkt strider mot GDPR. En sådan överföring av personuppgifter är inte tillåten enligt EU-förordningen GDPR, åtminstone inte utan ett separat avtal.

Det är många svenska bolag som idag lagrar sin data i någon av de amerikanska molnjättarna, AWS, Google eller Microsoft. Det är bra att åt-minstone vara medveten om risken att hamna i dessa juridiska svårigheter kring just hantering av personuppgifter.

”För att ha en trygg och framtidssäkrad moln-tjänst är därför rekommendationen att använda dig av en svensk eller åtminstone europeisk molntjänstleverantör som lagrar din data inom EU. Då vet du att lagringen av personuppgifter uppfyller godkänt skydd enligt bestämmelserna i GDPR. Du kan dessutom vara trygg i att inga andra länders regelverk riskerar att trumfa EU-lagstiftningen.”

Att uppnå och säkerställa compliance



Oavsett vilken typ av molntjänst som din organisation planerar att använda – privat, publikt eller hybrida moln – så är det många lagar och riktlinjer som måste följas för att uppnå Cloud Compliance, det vill säga säkerställa efterlevnad av regelverket. Det är en komplex uppgift som kräver en hel del engagemang från din sida och från din molntjänstleverantör. Det hela blir såklart inte enklare när dessa riktlinjer förändras och uppdateras regelbundet. Men det finns vissa nyckelfaktorer som ger er en bra grund för en trygg och säker molntjänst.

Det spelar alltså ingen roll att en amerikansk molntjänstleverantör har sina servrar fysiskt placerade inom EU. De lyder ändå under CLOUD Act och kan därmed bli tvingade att lämna ut uppgifter till amerikanska myndigheter.

5 steg för att uppnå och upprätthålla Cloud Compliance.

1. Var medveten om vilka lagar och riktlinjer som gäller din verksamhet.

Det viktigaste du behöver göra är att skaffa dig kunskap om vilka lagar och riktlinjer som gäller för din bransch och den typ av data som du planerar att lagra i molnet.

Förutom GDPR som reglerar hantering av personuppgifter i molnet finns det exempelvis olika regler för hur data kopplat till sjukvård och patientsäkerhet får hanteras, hur information om betalningar och kreditkort ska hanteras, samt finansiell information för privatpersoner och företag.

Genom att kartlägga vilka regelverk som gäller för den typ av data som din organisation hanterar så kan du sedan gå vidare och hitta en molnstjänstleverantör som uppfyller just dessa krav. Kräv att få ta del av dokumentationen som stärker leverantörens Cloud Compliance. Detta är dokumentation som även ska kunna användas vid händelse av en översyn, så det är ett viktigt dokument att ta del av när du väljer molntjänst.

2. Säkerhet för access samt inloggning

För att säkerställa Compliance i molnet gäller det även att ha full koll på datasäkerheten inom din organisation. En stor orsak till dataintrång är just brist på bra verifiering vid inloggning samt dåliga rutiner kring vilka som har eller ska ha tillgång till din data. Men det behöver inte vara ett problem, det finns bra rutiner och stöd att ta till här.

Fortfarande idag använder många organisationer enfaktorsverifiering (single sign-on), mest för att det är enklast för användarna. Men metoden innebär dock en betydligt högre risk för att bli hackad, särskilt i jämförelse med multifaktorsverifiering (multi-factor authentication). Med multifaktorverifiering krävs inte enbart ett användarnamn och lösenord utan även information från ytterligare en källa, exempelvis en unik kod som skickas till din telefon eller e-post. Detta gör att multifaktorverifiering är mycket svårare att knäcka och därmed skyddar du tillgången till din data genom denna relativt enkla process.

3. Ha koll på var din data lagras och klassificera den

En av de viktigaste faktorerna för att upprätthålla Cloud Compliance är att ha koll på exakt var din data lagras. Vid händelse av en översyn behöver du kunna styrka informationens exakta position samt redogöra för vilka åtgärder som vidtagits för att skydda den.

Det är en viktig anledning till varför du bör efterfråga tydlig dokumentation från potentiella molntjänstleverantörer som visar var de har sina servrar, det vill säga informationens exakta position. Som vi nämnt tidigare i denna guide spelar det stor juridisk roll om servrarna befinner sig i Sverige, inom EU eller helt utanför EU. Det har också stor betydelse vilket land som molntjänstleverantören är registrerad i. Andra länders lagstiftning kan som sagt orsaka juridiska bekymmer om servrarna ägs av en amerikansk leverantör till exempel, detta även om servrarna befinner sig i Sverige rent fysiskt.

Nästa steg är att klassificera datan för att fastställa rätt nivå av säkerhet. Av säkerhetsskäl, men även för regelefterlevnad (Compliance), kan många välja att inte flytta känslig data till molnet. Det kan givetvis vara en lösning, men om du vill hämta hem nyttan med molnlagring kan lösningen vara att använda privata moln för lagring av just känslig data. Genom att klassificera datan vet du vilken data som kräver särskilt skydd och kan då få hjälp med en kostnadseffektiv lösning som dessutom är säker.

4. Kryptera din data

När du har bestämt vilken data som ska lagras i molnet, samt på vilket sätt, så är det viktigt att säkerställa att datan krypteras på ett tillfredsställande sätt. Genom att kryptera informationen ökar givetvis skyddet vid ett eventuellt dataintrång och kryptering hjälper samtidigt till att uppfylla Compliance-krav. Säkerställ vilken typ av kryptering som din molntjänstleverantör erbjuder samt hur och när den tillämpas. Säkerställ även att leverantören innehar lämpliga certifieringar när det gäller hantering av informationssäkerhet, exempelvis ISO 27001. Tänk dock på att även om din leverantör erbjuder kryptering så är det fortfarande ni själva som ansvarar för att skydda datan, både när den flyttas och när den lagras. Ansvaret kan ni inte outsourca. Mer om ansvar beskriver vi i nästa avsnitt.

Den viktigaste faktorn är dock hur informationen lagras. De allra flesta dataintrång sker nämligen av insiders och personer med direkt access till datan. Det kan vara avsiktligt eller oavsiktligt, men majoriteten av intrången sker inne i din organisation.

Det bästa sättet att skydda sig från sådana dataintrång är att kryptera informationen internt innan den flyttas över till molnet, vilket ger ett extra lager av säkerhet. Det innebär att även om någon obehörig skulle komma åt informationen, avsiktligt eller oavsiktligt, så går den ändå inte att läsa och göra något med.

5. Uppföljning och kontroll av interna rutiner

Sista steget för att säkerställa Cloud Compliance är din uppföljning. Som vi nämner i inledningen till detta avsnitt är lagar och regler ofta under förändring. Särskilt i förhållande till andra länders lagstiftning. Därför är det viktigt att ni inom organisationen har rutiner för uppföljning och kontroll. Det säkerställer att ni regelbundet kan kontrollera att data är skyddad på rätt sätt.

För att summera så gäller det alltså att:

- Ni har kunskap om vilka lagar och regler som gäller vid lagring av information i molnet för er specifika verksamhet.
- Ni ska ha ordning och reda på vilka som har access till informationen samt en hög säkerhetsnivå vid inloggning.
- Ni ska veta exakt var er data lagras, hålla koll på vilken information som kräver extra hög säkerhetsnivå samt att ni ser till att kryptera informationen innan den skickas till molnet.
- Ni skapar en rutin för att bevaka eventuella uppdateringar som sker gällande regelverket.

Ovanstående innebär att ni har lagt en riktigt bra grund för Cloud Compliance i er molntjänst.
Personuppgfiter

Cloud Compliance är ett delat ansvar

Du som äger datan har alltid ett ansvar, åtminstone juridiskt. En del organisationer tror att en migrering av datan till molnet även innebär att hela säkerhetsansvar flyttas till molntjänstleverantören. Detta stämmer dock inte riktigt. Säkerhetsansvar såväl som Cloud Compliance delas av flera olika parter.

Molntjänstleverantören ansvarar för att rätt verktyg för säkerhet och regelefterlevnad finns tillgängliga i tjänsten. Ofta finns där en person som har Compliance-frågor som sitt ansvarsområde. Men det är den enskilda organisationen som i slutändan ansvarar för att dessa verktyg används samt att den egna datan lagras och hanteras på ett sådant sätt att regelefterlevnaden uppnås. Det innebär att om datan hanteras oförsiktigt eller felaktigt så är det den egna organisationen som får ta smällen rent juridiskt. Använder du speciella applikationer tillsammans med din molntjänst så är det applikationsleverantören som ansvarar för säkerheten för just den specifika mjukvaran. Därför är det många partner inblandade i just ansvarsfrågan.

Vem ansvarar för vad?

Det är viktigt att förstå och urskilja gränsdragningen kring vem som har säkerhetsansvararet i vilken del av molnet. En tumregel är att:

- Användaren av molntjänsten ansvarar för att använda tillgängliga verktyg för säkerhet och regelefterlevnad i molnet. Både vad gäller molntjänsten som sådan och för externa applikationer.
- Applikationsleverantören ansvarar för säkerheten i deras specifika mjukvara.
- Molntjänstleverantören ansvarar för säkerheten och tillhandahållandet av verktyg i molntjänsten.

För organisationer som är vana vid att lagra all information lokalt kan detta innebära en förskjutning och förflyttning av ansvar. Från att ha haft totalansvar för hela sin IT-miljö till ett uppdelat ansvar mellan flera olika parter. Det innebär en lättnad i ansvar, men det är samtidigt viktigt att säkerställa gränsdragningen.

Din checklista för rätt hantering av en personuppgiftsincident

Även om du har bra rutiner och processer så kan incidenter ske. Om ett dataintrång eller en incident kring personuppgifter skulle inträffa, trots alla åtgärder ni vidtagit för att förhindra detta, så är det bra att veta hur ni ska hantera ett sådant ärende. Vi har utgått ifrån Datainspektionens rekommendationer och tagit fram en checklista som hjälper dig att se hur bra förberedd din organisation är för att hantera eventuella personuppgiftsincidenter.

Förberedelser för att hantera personuppgiftsincidenter

- [ ] Ni vet hur ni känner igen en personuppgifts-incident. Det vill säga ta reda på vad detta innebär i praktiken.
- [ ] Ni förstår att en personuppgiftsincident inte bara handlar om förlust eller stöld av personuppgifter. Det flesta intrång sker som sagt inom organisationen, avsiktligt eller oavsiktligt.
- [ ] Ni har rutiner för hur ni ska agera inom organisationen om en personuppgiftsincident skulle inträffa.
- [ ] Ni har utsett en person eller en grupp som ansvarig för att hantera personuppgifts-incidenter. Här är det viktigt att även involvera de parter som ni har ett delat ansvar med, exempelvis molntjänst-leverantören.
- [ ] Er personal vet hur de ska rapportera personuppgifts-incidenter till rätt person eller grupp.

Att anmäla personuppgiftsincidenter

- Ni har rutiner för att kunna bedöma riskerna för personer som har drabbats av en personuppgiftsincident.
- Ni vet vilken som är den ansvariga tillsynsmyndig-heten för er verksamhet, det vill säga om det är Datainspektionen eller tillsynsmyndigheten i ett annat EU-land än Sverige.
- Ni har rutiner för att meddela Datainspektionen om det har inträffat en personuppgiftsincident. Rutinen säger att ni ska rapportera inom 72 timmar efter att ni har upptäckt personuppgiftsincidenten. Ni rapporterar då, även om ni inte har alla detaljer ännu.
- Ni vet vilken information ni måste ge Datainspektionen när en personuppgiftsincident har inträffat. Det innebär ofta att ni kommer att behöva samverka med exempelvis molntjänstleverantören i de fall informationen lagras i en molntjänst.
- Ni har rutiner för att informera de registrerade personerna när det är troligt personuppgiftsincident medför en hög risk för deras rättigheter och friheter.
- Ni vet att ni i så fall måste informera de registrerade personerna omedelbart.
- Ni vet vilken information om personuppgifts-incidenten som ni måste ge till de registrerade personerna, och att ni bör ge råd för att hjälpa dem att skydda sig från dess effekter.
- Ni dokumenterar alla personuppgiftsincidenter, även de som inte behöver anmälas till Datainspektionen.

binero.com

facebook | linkedin