Integritetsskydds myndigheten

Diarienummer:
DI-2022-1985

Datum:
2022-11-16

Användning av molntjänster inom offentlig sektor – en sammanställning av en undersökning av sju myndigheter

Innehåll

Sammanfattning 2
Inledning och bakgrund 2
Hur gick undersökningen till? 3
Resultatet av undersökningen 3
Grundläggande frågor om användningen av molntjänster 3
Personuppgiftsansvarig och personuppgiftsbiträde 3
Anlitande av molntjänstleverantör 4
Överföring av personuppgifter till tredje land 5
Molntjänstleverantörens insamling och behandling av diagnostik- eller telemetridata 6
Myndigheternas kontroll av molntjänstleverantören 6
Övrigt om utmaningarna med att anskaffa och använda molntjänster 7
Bristande kunskap om dataskyddsregelverket hos molntjänstleverantörer 7
Ställer höga krav på myndigheterna 8
Förhandlingar med molntjänstleverantören 8
Avtalsfrågor 8
Tips för fortsatt läsning 8

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Sammanfattning

Integritetsskyddsmyndigheten, IMY, har genomfört en undersökning av offentliga myndigheters användning av molntjänster. Undersökningen har utförts inom ramen för en samordnad åtgärd inom Europeiska dataskyddsstyrelsen, EDBP. Sju myndigheter har svarat på ett frågeformulär som rör myndighetens användning av molntjänster. Då underlaget är begränsat kan enbart övergripande slutsatser dras.

Samtliga myndigheter uppger att det är utmaning att hitta molntjänster som är förenliga med dataskyddsregelverket. Det framkommer att det ofta kan vara svårt att förhandla med molntjänstleverantörer och därmed svårt att på påverka utformningen av eller villkoren för användningen av molntjänsterna.

Enligt undersökningen synes molntjänster huvudsakligen användas som verksamhetsstöd och för behandling av anställdas uppgifter, men det förekommer att även känsliga personuppgifter om medborgare behandlas.

Undersökningen indikerar att det finns vissa utmaningar för myndigheterna att fastställa rollfördelningen mellan personuppgiftsansvarig och personuppgiftsbiträde eller gemensamt personuppgiftsansvar.

Samtliga myndigheter uppger att de har processer och rutiner för att anskaffa molntjänster och merparten att konsekvensbedömningar genomförs innan en molntjänst anskaffas.

Utifrån myndigheternas svar är det oklart om det vid överföring av uppgifter till tredje land alltid finns stöd för överföringen i form av ett tillämpligt överföringsverktyg i kapitel V i dataskyddsförordningen.

Enligt myndigheterna uppges vissa molntjänstleverantörer ha bristande kunskaper om grundläggande dataskyddsregler, vilket ställer stora krav på upphandlande myndigheter. Det handlar till exempel om vad som är personuppgifter och en personuppgiftsbehandling, om roll- och ansvarsfördelningen för personuppgifts-ansvarig och personuppgiftsbiträde samt personuppgiftsbiträdets ansvar vid anlitande av underbiträden. Undersökningen pekar också på att molntjänstleverantörer i vissa fall felaktigt uppger att de har skyddsmekanismer i form av anonymisering och pseudonymisering.

En sammanfattande rapport av den samlade åtgärden kommer från EDPB under 2023.

Inledning och bakgrund

IMY ingår i ett EU-samarbete genom Europeiska dataskyddsstyrelsen, EDPB. Som ett led i EDPB:s strategi för 2021–2023, har EDPB beslutat att inrätta ett ramverk för samordnade åtgärder (Coordinated Enforcement Framework, CEF). Inom ramen för ramverket beslutades att för 2022 genomföra en undersökning av användningen av molnbaserade tjänster inom offentlig sektor, vilket är den första åtgärden som genomförs inom ramen för samordnade åtgärder. 22 dataskyddsmyndigheter valde att medverka i åtgärden och IMY är en av de dataskyddsmyndigheter som medverkar.

Hur gick undersökningen till?

Undersökningen har genomförts genom att ett frågeformulär som tagits fram av EDPB har skickats till totalt över 80 utvalda offentliga organ i EU.

Vissa dataskyddsmyndigheter har genomfört undersökningen som en tillsyn, medan det för andra dataskyddsmyndigheter har handlat om att inhämta information. IMY har inte genomfört undersökningen som en tillsyn, utan syftet har varit att få ökad förståelse för de utmaningar och svårigheter offentliga organ har med att använda molnbaserade tjänster som är förenliga med dataskyddsreglerna.

IMY skickade frågeformuläret till 11 statliga myndigheter som IMY bedömer behandlar stora mängder personuppgifter och har erfarenhet av att använda molntjänster. Sju myndigheter svarade på formuläret.

Då underlaget är begränsat kan enbart övergripande iakttagelser göras och några säkra slutsatser kan inte dras från den svenska undersökningen. En sammanfattande rapport som omfattar underlag från samtliga deltagande i den samordnade åtgärden, 22 medlemsstater, kommer från EDPB under slutet av 2022 eller i inledningen av 2023.

Resultatet av undersökningen

Grundläggande frågor om användningen av molntjänster

Samtliga myndigheter uppger att de använder molntjänster, men antalet molntjänster som varje myndighet använder varierar, från ca ett tiotal tjänster och uppåt. De inkomna svaren ger inte en helt tydlig bild av i vilket syfte myndigheterna använder molntjänster. Mot bakgrund av att flera myndigheter uppger att de kategorier av personuppgifter som behandlas i molntjänsterna är exempelvis anställdas inloggningsuppgifter och kontaktuppgifter, drar IMY slutsatsen att molntjänsterna huvudsakligen verkar användas för olika former av verksamhetsstöd och inte i myndigheternas kärnverksamhet eller ärendehandläggning. En myndighet uppger dock att behandlingen kan omfatta såväl anställdas som medborgares uppgifter och att det även kan bli fråga om behandling av känsliga personuppgifter.

Personuppgiftsansvarig och personuppgiftsbiträde

En förutsättning för att behandlingen av personuppgifter ska vara förenlig med dataskyddsregelverket när en organisation anlitar externa leverantörer för olika tjänster, är att det är tydligt vem som är personuppgiftsansvarig respektive personuppgiftsbiträde, och vad det innebär.

Beträffande myndigheternas respektive molntjänstleverantörens roller, ger svaren inte en entydig bild. De flesta myndigheterna uppger att de är personuppgiftsansvariga och att molntjänstleverantören är personuppgiftsbiträde. Någon enstaka myndighet svarar dock att molntjänstleverantören är personuppgiftsansvarig och några myndigheter lämnar inte ett konkret svar eller uppger att det är oklart ur ansvarsfördelningen ser ut. Det framkommer även att det i ett fåtal fall kan bli fråga om att myndigheter är gemensamt personuppgiftsansvariga, och då har en ansvarsfördelning upprättats.

De myndigheter som uppgett att molntjänstleverantören är personuppgiftsbiträde uppger även att personuppgiftsbiträdesavtal har ingåtts. Flera myndigheter uppger att det anlitas underbiträden.

Anlitande av molntjänstleverantör

För att säkerställa ett gott dataskydd behöver en organisation som planerar att använda molntjänster ha rutiner och processer för att undersöka och bedöma om den behandling av personuppgifter som sker vid användning av molntjänsten är förenlig med dataskyddsförordningen.

Beträffande anskaffande av molntjänster varierar de inkomna svaren i utförlighet och nivå. Vissa myndigheter svarar kort utan att utveckla och vissa svarar inte på vissa frågor.

Samtliga myndigheter uppger att myndigheten har processer och rutiner för att anskaffa molntjänster. Alla myndigheter utom en svarar att konsekvensbedömningar genomförs enligt artikel 35 i dataskyddsförordningen innan en molntjänst anskaffas. De inkomna svaren visar emellertid att konsekvensbedömningar inte verkar genomföras varje gång en molntjänst anskaffas. IMY tolkar detta som att de flesta tillfrågade myndigheterna har rutiner för att genomföra konsekvensbedömningar innan en molntjänst anskaffas och att så görs i de fall myndigheten bedömer att det finns en skyldighet att göra en sådan.

Samtliga myndigheter uppger att de undersöker var uppgifterna lagras vid anskaffande av molntjänster. Samtliga svarar även att det är utmaning att hitta molntjänster som är förenliga med dataskyddsregelverket.

På fråga om myndigheten har samarbetat nationellt eller internationellt vid förhandlingar om villkor eller inställningar med molntjänstleverantören uppger en myndighet att den har samverkat genom eSam[1] i viss utsträckning, resterande svarar att de inte har samarbetat på det sättet.

En fråga tar sikte på myndigheternas möjlighet att förhandla fram villkor eller inställningar för att minska riskerna i samband med personuppgiftsbehandlingen. De flesta myndigheterna uppger att det varit möjligt åtminstone i viss utsträckning, exempelvis gällande överföring av personuppgifter till tredje land.

På frågan om myndigheten vidtagit eller förhandlat fram några avtalsrelaterade, tekniska och/eller organisatoriska åtgärder för att begränsa molntjänstleverantörens behandling av personuppgifter, ger svaren ingen entydig bild. Ett par myndigheter besvarar inte frågan eller svarar kortfattat utan att utveckla. Några svarar att de vidtagit eller förhandlat fram åtgärder och bland de åtgärder som vidtagits nämns skyddsåtgärder vid användning av sociala medier och införande av behörighetsstyrning.

[1] eSam är ett medlemsdrivet program för samverkan mellan 34 myndigheter kring tillgängliga och rättssäkra digitala lösningar. Syftet är också att samla kompetenser inom gemensamma områden.

Överföring av personuppgifter till tredje land

Att använda molntjänster kan medföra att det sker en överföring av personuppgifter till tredje land, det vill säga ett land utanför EU/EES. Dataskyddsförordningen innehåller särskilda regler om under vilka förutsättningar sådana överföringar är tillåtna.

På fråga om användningen av molntjänster innebär att det faktiskt sker en överföring av personuppgifter, inklusive av diagnostisk- eller telemetridata[2], till tredje land, tolkar IMY de inkomna svaren som att tredjelandsöverföring sker i viss utsträckning. Någon myndighet uppger att tredjelandsöverföring sker vid användning av vissa tjänster, en annan myndighet uppger att tredjelandsöverföring sker vid användning av vissa tjänster och avseende vissa uppgifter. Ett par myndigheter svarar att tredjelandsöverföring inte sker eller bara sker i undantagsfall. Ett par myndigheter lämnar inget svar på frågan.

Utifrån myndigheternas svar är det oklart om det vid överföring av uppgifter till tredje land alltid finns stöd för överföringen i form av ett tillämpligt överföringsverktyg i kapitel V i dataskyddsförordningen. På den tidigare ställda frågan om myndigheten har vidtagit eller förhandlat fram några avtalsrelaterade, tekniska och/eller organisatoriska åtgärder för att säkerställa att internationella överföringar följer kraven, uppgav som framgått ett par myndigheter att de har det, medan flera myndigheter svarade nej eller inte svarade på frågan. Mot bakgrund av att ett par myndigheter inte har svarat på frågan om tredjelandsöverföring av personuppgifter förekommer kan det inte uteslutas att sådana överföringar sker i större utsträckning än vad som framkommer av svaren och att överföringarna inte alltid har stöd i kapitel V i dataskyddsförordningen.

På frågan om vilket överföringsverktyg i kapitel V i dataskyddsförordningen som används om myndigheten för över personuppgifter till tredje land ger svaren inte en tydlig bild av hur myndigheterna bedömer att deras möjlighet att föra över personuppgifter till tredje land ser ut. Några myndigheter svarar inte på frågan, medan ett par myndigheter uppger att de tillämpar överföringsverktyg i kapitel V, såsom standardavtalsklausuler, beslut om adekvat skyddsnivå och lämpliga skyddsåtgärder, samt i undantagsfall artikel 49 i dataskyddsförordningen.

Mot bakgrund av den så kallade ”Schrems II-domen”,[3] ställdes en fråga om myndigheterna, för det fall att organisationen använder standardavtalsklausuler för överföringar eller förlitar sig på molntjänstleverantörens bindande företagsbestämmelser, kontrollerar om det finns något i tredjelandets lagstiftning och/eller praxis som förbjuder molntjänstleverantörerna att uppfylla sina avtalsenliga skyldigheter för att säkerställa att den skyddsnivå för personuppgifter för fysiska personer som garanteras inom EES inte undergrävs. De inkomna svaren ger dock inte en tydlig bild av hur myndigheterna arbetar för att leva upp till sina skyldigheter med anledning av Schrems II-domen. Ett par myndigheter svarar att det har undersökts men utvecklar inte vad undersökningen resulterat i eller hur myndigheten agerat med anledning av vad som framkommit. Flertalet uppger att det inte undersöks eller lämnar inget svar.

---

[2] Telemetridata är mätdata över händelser i ett system, vanligen i form av loggposter, som samlas in över ett nätverk och sedan analyseras, ibland också i realtid. Vilka data som samlas in beror på syftet med insamlingen som kan vara t.ex. kvalitetsmätning, prestandamätning, säkerhetsövervakning eller funktionsanvändning. Diagnostikdata är telemetridata för ändamålet diagnostik.
[3] EU-domstolens dom av den 16 juli 2020 i mål C-311/18, Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems.

När det gäller tredjelandsöverföringar som sker med stöd av standardavtalsklausuler eller molntjänstleverantörens bindande företagsbestämmelser, ställdes även en fråga hur myndigheterna bedömer att den som importerar uppgifterna faktiskt kan garantera att de bindande företagsbestämmelserna uppfylls eller att de avtalsenliga skyldigheterna enligt standardavtalsklausulerna fullgörs. Svaren ger inte en tydlig bild av hur myndigheter arbetar i situationer där överföring sker med stöd av standardavtalsklausuler eller bindande företagsbestämmelser. En myndighet uppger att det har ställts frågor till leverantörerna och då väl motiverade svar har erhållits har de uppgifterna godtagits, en annan svarar att myndigheten inte har bedömt att det kan garanteras. Resterande svarar inte eller uppger att de inte har dragit några slutsatser enligt frågan.

På temat överföring till tredje land ställdes även en fråga om myndigheten, för det fall åtgärderna för överföring i kapitel V i dataskyddsförordningen anses vara otillräckliga (t.ex. avtalsförpliktelser i standardavtalsklausulerna eller de bindande företagsbestämmelserna), har övervägt att genomföra kompletterande åtgärder, och i sådana fall vilka. Det ställdes även en fråga om myndigheten har kontrollerat att dessa kompletterande åtgärder kan genomföras i praktiken och att det inte finns något i tredjelandets lagstiftning och/eller praxis som hindrar dem från att tillämpas, för att säkerställa att den nivå på uppgiftsskyddet för fysiska personer som garanteras inom EES inte undergrävs.

Sådana kompletterande åtgärder verkar genomföras i viss utsträckning, då flera myndigheter uppger att de har använt pseudonymisering eller annan form av uppgiftsminimering. Någon uppger de har tänkt undersöka kompletterande åtgärder, och några svarar inte på frågan.

Beträffande överföring av personuppgifter till tredje land, ställdes även frågan om myndigheten har underrättats om att molntjänstleverantören, eller någon av underleverantörerna, har tagit emot någon begäran om utlämnande av uppgifter från statliga myndigheter i tredje land. Ingen myndighet uppgav att den hade underrättats om en sådan begäran; flera myndigheter svarade uttryckligen att så inte hade skett medan ett par myndigheter inte besvarade frågan.

Molntjänstleverantörens insamling och behandling av diagnostik- eller telemetridata

Användningen av molntjänster kan innebära att det sker en behandling diagnostik- eller telemetridata. En fråga rörde därför om molntjänstleverantören samlar in och behandlar diagnostik- eller telemetridata till följd av användningen av molntjänsterna och hur myndigheter hanterar den frågan. IMY bedömer att det inte är ett område som myndigheterna är väl insatta i, då endast en myndighet uppger att all informationsöverföring, inklusive telemetri- och diagnostikdata, utreds. Övriga svarar att de inte vet, att de inte har avtalat om den frågan med molntjänstleverantören eller så lämnas inget svar på frågan. På mer detaljerade frågor om behandling av sådana uppgifter svarar myndigheterna inte alls eller att de inte vet.

Myndigheternas kontroll av molntjänstleverantören

För att säkerställa att den behandling av personuppgifter som sker genom användningen av molntjänster är förenlig med dataskyddsförordningen behöver myndigheter som använder molntjänster kontrollera hur molntjänstleverantören behandlar personuppgifterna.

En fråga tar därför sikte på om myndigheterna kontrollerar molntjänstleverantörernas tekniska och organisatoriska åtgärder, inklusive säkerhetsåtgärder, för att säkerställa att de uppfyller de överenskomna kraven, sina skyldigheter eller internationella standarder. Fem av sju myndigheter svarar att sådan kontroll görs, däremot varierar tidpunkten och tillvägagångssättet för kontrollen; i vissa fall sker det i anskaffningsstadiet, i vissa fall vid indikation och i vissa fall årligen eller vid förändring av behandlingen.

Därutöver ställs en fråga om myndigheternas kontroll även omfattar huruvida molntjänstleverantören gör regelbundna riskbedömningar av skyddet för personuppgifter, såsom bedömningar av informationssäkerhetsrisker, vid användning av molntjänster. De inkomna svaren ger en bild av att myndigheterna kontrollerar om molntjänstleverantörer gör riskbedömningar avseende skyddet för personuppgifter i lägre utsträckning än de kontrollerar tekniska och organisatoriska åtgärder. Endast någon myndighet uppger att vissa kontrollfrågor avseende riskbedömningar ställs, medan resterande myndigheter svarar nej eller inte svarar på frågan.

Avslutningsvis undersöks om myndigheterna kontrollerar hur molntjänstleverantören uppfyller kraven i dataskyddsförordningen i allmänhet, t ex om molntjänstleverantören ser över och uppdaterar policyer och åtgärder. Svaren ger inte en entydig bild, varken avseende huruvida sådan kontroll görs eller på vilket sätt den genomförs. Några myndigheter uppger att sådan kontroll inte görs eller underlåter att svara, medan några svarar att sådan kontroll görs. Av de myndigheter som genomför en sådan kontroll uppger några att kontrollen sker vid anskaffning av molntjänsten, och någon annan att det görs vid regelbunden uppföljning.

Övrigt om utmaningarna med att anskaffa och använda molntjänster

Utöver svaren på frågorna i frågeformuläret har det även framkommit ytterligare information om de svårigheter myndigheter har att anskaffa och använda molntjänster.

Bristande kunskap om dataskyddsregelverket hos molntjänstleverantörer
Ett problem som framkommit är att molntjänstleverantörer överlag har bristande kunskap om dataskyddsregelverket, vilket tar sig uttryck på olika sätt och skapar svårigheter för myndigheter som vill använda molntjänster. Det kan t ex handla om att molntjänstleverantören:

- har bristande kunskaper om vad som är personuppgifter, särskilt när det är fråga om indirekta personuppgifter, eller vad som är en personuppgiftsbehandling. Det är vanligt förekommande att molntjänstleverantören felaktigt uppger att användandet av molntjänster inte utgör en personuppgiftsbehandling
- har bristande kunskaper om roller och ansvarsfördelning enligt dataskyddsförordningen, dvs. vilken organisation som är personuppgiftsansvarig respektive personuppgiftsbiträde. Detta inkluderar bristande förståelse för att underbiträden också är personuppgiftsbiträden, och vilka krav dataskyddsförordningen ställer om underbiträden anlitas
- felaktigt uppger att uppgifter är anonymiserade eller pseudonymiserade
- inte kan skilja på dataskydd och informationssäkerhet.

Ställer höga krav på myndigheterna
Bristande kunskaper om regelverket hos molntjänstleverantörer ställer istället höga krav på organisationer som använder molntjänster, då de måste ha goda kunskaper om både juridik och teknik för att kunna bedöma om molntjänstleverantörens behandling av personuppgifter lever upp till kraven i dataskyddsförordningen.

Förhandlingar med molntjänstleverantören
Även om myndigheterna har de juridiska och tekniska kunskaper som krävs för att kunna bedöma om en molntjänst kan användas kan det ofta vara svårt att förhandla med molntjänstleverantörer. Anledningen till det är att många aktörer förutsätter att molntjänstleverantörer följer tillämpliga lagar och regelverk och därför inte gör någon mer utförlig undersökning och bedömning av om användandet av en molntjänst lever upp till kraven i dataskyddsförordningen. Följaktligen har de aktörer som inte enbart godtar påståenden från molntjänstleverantörerna utan vill ställa krav på eller förhandla med dessa svårt att påverka utformningen av eller villkoren för användningen av molntjänsterna.

Myndigheterna upplever att de har haft störst möjlighet att förhandla med molntjänstleverantören i situationer där myndigheten har varit eller kunnat bli en viktig kund för molntjänstleverantören, där beslutsvägarna hos molntjänstleverantören är korta eller dialog har kunnat föras direkt med molntjänstleverantörens ledning eller där det har funnits en samsyn kring vikten av ett gott dataskydd.

Avtalsfrågor
Det har även framkommit information om att det kan vara svårt att ingå avtal med molntjänstleverantören, då avtalsvillkor inte alltid är transparenta och ofta uppdateras ensidigt.

Tips för fortsatt läsning

- Vad är en personuppgift: Personuppgifter, vad ni inom verksamhet behöver veta | IMY
- Behandling av känsliga personuppgifter: Känsliga personuppgifter | IMY
- Personuppgiftsansvarig och personuppgiftsbiträde – EDPB:s vägledning: Personuppgiftsansvariga och personuppgiftsbiträden | IMY
- Konsekvensbedömning: Konsekvensbedömningar och förhandssamråd | IMY

Överföring till tredje land:

- Överföring till tredjeland | IMY
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)