Integritetsskydds myndigheten

Datum:
2022-02-28

Frågeformulär

Allmänna frågor om användningen av molntjänster

1. Använder ni för närvarande en molntjänstleverantör som behandlar personuppgifter eller planerar ni att göra det inom en snar framtid (senast i slutet av 2022)? Om ja, hur många?

2. Om ni för närvarande använder molntjänstleverantörer, vänligen lämna följande information för varje molntjänstleverantör:

Allmän information om molntjänstleverantören och avtalet

a) Vad är namnet på molntjänstleverantören?
b) Vad är namnet på den juridiska person med vilken avtal om molntjänsten har ingåtts?
c) Vilket är avtalets start- och slutdatum och eventuella datum för förlängning eller planerade ändringar av tjänsterna?
d) Vilka är de distributionsmodeller (offentliga/privata/hybridmodeller/samhällsmodeller)[1] och tjänstemodeller (SaaS, PaaS, DSaaS, IaaS osv.)[2] som används?
e) Finns det en konsekvensbedömning avseende dataskydd för denna molntjänstleverantörs behandling av personuppgifter?

Typer av personuppgifter som behandlas

f) Vilka kategorier av personuppgifter behandlas av molntjänstleverantören? Behandlas särskilda kategorier av personuppgifter (t.ex. hälsouppgifter) eller personuppgifter som är särskild skyddsvärda såsom ekonomiska uppgifter? Vänligen precisera.
g) Vems personuppgifter behandlas i molnet (t.ex. anställdas personuppgifter, medborgares eller andra personers personuppgifter)?
h) För vilken funktion används tjänsten (t.ex. intern administration, kommunikation, personalförvaltning, service till medborgarna,

[1] Se bilagan (termerna kommer från ISO 17788).
[2] Se bilagan (termerna kommer från ISO 17788).

Postadress:
Box 8114
104 20 Stockholm
Webbplats:
www.imy.se
E-post:
imy@imy.se
Telefon:
08-657 61 00

utvecklingsverktyg, servrar) och omfattar detta organisationens huvudsakliga verksamhet funktion?

i) Behandlar molntjänstleverantören telemetridata[3] eller diagnostikdata som härstammar från er verksamhet? Ange vilka kategorier av personuppgifter som samlas in.

Identifiering av rollerna

j) Vilka roller har er organisation och molntjänstleverantören (dvs. personuppgiftsansvarig, gemensamt personuppgiftsansvariga eller personuppgiftsbiträde)?

k) Om ni har en relation till molntjänstleverantören där ni är personuppgiftsansvariga och leverantören är personuppgiftsbiträde, finns det ett avtal som följer artikel 28.3 i dataskyddsförordningen[4]? (Observera att fråga 13 avser villkoren i detta avtal, som inte behöver behandlas ytterligare här.)

l) Om ni är gemensamt personuppgiftsansvariga tillsammans med molntjänstleverantören, använder molntjänstleverantören data (inklusive diagnostik- eller telemetridata) för sina egna ändamål? Om ja, besvara följande frågor:
   - I vilket eller vilka syften använder molntjänstleverantören uppgifterna?
   - Har ni gjort en bedömning av vad det är för data som molntjänstleverantören använder för egna syften?
   - Vilken är den rättsliga grunden för molntjänstleverantörens behandling?

m) Har ni identifierat några underleverantörer som används av molntjänstleverantören? Om ja, vad är namnet på underleverantörerna?

Anlitande av en molntjänstleverantör

3. Beskriv den process ni har följt (eller skulle följa), inklusive eventuella riskbedömningar avseende dataskydd för er organisation, för att fastställa om molnet skulle vara en lämplig lösning för era behov och för att välja en specifik molntjänstleverantör. Ange särskilt vilka eventuella obligatoriska dataskyddskrav som måste uppfyllas av en molntjänstleverantör som ni kan tänka er att välja och om kraven utgör uttryckliga tilldelningskriterier i samband med förfarandet för att anlita en molntjänstleverantör.

---

[3] Telemetridata är data som genereras genom användning av tjänsten, även för säkerhetsändamål.

[4] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

4. Gör er organisation någon konsekvensbedömning avseende dataskydd eller begär er organisation en sådan konsekvensbedömning från molntjänstleverantören innan ni anskaffar molnbaserade tjänster?
    - Om ja, på vilket sätt och var ingår en konsekvensbedömning avseende dataskydd i anskaffandeprocessen? Tänk på hur de identifierade riskerna hanterades under anskaffandeprocessen när ni besvarar denna fråga. Detta kan särskilt omfatta applikations- och gränssnittssäkerhet, identitets- och åtkomsthantering, kryptering och nyckelhantering, fysisk säkerhet, säkerhet kring virtualisering och nätverksarkitektur, operativ separation och multitenans, incidenthantering osv.
    - Vilka är era erfarenheter (positiva och negativa) av att genomföra en konsekvensbedömning avseende dataskydd på detta sätt?

5. Använder ni er av nationella/internationella standarder eller ledande praxis vid bedömning av molntjänstleverantören (t.ex. ISO 27001/ISO 27701), antingen för att ni förlitar er på denna certifiering som en del av er egen bedömning eller för att certifiering av molntjänstleverantörer är ett av era krav? Om så är fallet och om molntjänsten är certifierad[5] (genom en ISO-certifiering eller nationell certifiering), vilken information om certifieringen görs tillgänglig för er (certifieringsrapport, sammanfattning av rapporten) och hur ofta?

6. Har er organisation vid anlitande av molnbaserade tjänster för sin databehandling undersökt var uppgifterna (fysiskt) behandlas (överförs till, lagras och görs tillgängliga från)? Om molntjänstleverantören har anlitat underleverantörer, har er organisation undersökt vart de uppgifter som behandlas av dessa underleverantörer (fysiskt) överförs, var de lagras och varifrån de görs tillgängliga?

7. Har er organisation upplevt lagstiftningsrelaterade utmaningar vid användning av molnet (t.ex. strikta regler för offentliga organs användning av molnbaserade tjänster)? Om så är fallet, ange vilka dessa utmaningar är och hur ni har hanterat dem.

8. Rådfrågar er organisation sitt eget dataskyddsombud (oberoende av molntjänstleverantörens eventuella samråd med dataskyddsombudet) under processen för att anlita en molntjänstleverantör? Förklara varför eller varför er organisation inte gör det.

9. Har er organisation någonsin köpt tjänster trots ett negativt yttrande från ert dataskyddsombud?

---

[5] Eller om den följer en uppförandekod.

Avtalet med molntjänstleverantören

Obs! Svara på följande frågor genom att hänvisa till var och en av de molntjänstleverantörer som anges i fråga 1.

10. Om ni är gemensamt personuppgiftsansvariga tillsammans med molntjänstleverantören, har de skyldigheter som anges i artikel 26 i dataskyddsförordningen fullgjorts? Förklara i allmänna ordalag hur ni har sett till att molntjänstleverantören fullgör sina skyldigheter.

11. Om molntjänstleverantören agerar som personuppgiftsbiträde är artikel 28 i dataskyddsförordningen tillämplig på avtalet med personuppgiftsbiträdet. Förklara i allmänna ordalag hur ni har säkerställt att följande skyldigheter fullgörs av molntjänstleverantören.

    - Molntjänstleverantören behandlar personuppgifterna endast på dokumenterade instruktioner från den personuppgiftsansvarige.
    - Molntjänstleverantören vidtar alla nödvändiga åtgärder för att säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
    - Molntjänstleverantören vidtar alla åtgärder som krävs för att säkerställa säkerheten i samband med behandlingen.
    - Molntjänstleverantören anlitar inte någon underleverantör utan ert förhandstillstånd. (Om molntjänstleverantören använder underleverantörer: har ni gett tillstånd till det?)
    - Molntjänstleverantören bistår er så långt det är möjligt för att ni ska kunna fullgöra er skyldighet att svara på en begäran om utövande av den registrerades rättigheter.
    - Molntjänstleverantören hjälper er att garantera behandlingens säkerhet.
    - Molntjänstleverantören raderar eller återlämnar alla personuppgifter till er när avtalet löper ut.
    - Molntjänstleverantören gör det möjligt för er eller någon person som ni bemyndigar att genomföra eller bidra till granskningar. Ange särskilt vilka granskningsrättigheter ni har när det gäller molntjänstleverantören och om de ingår i avtalet.

12. Innehåller avtalet med molntjänstleverantören bestämmelser om kontroller/krav avseende anmälan av dataintrång?

13. Har er organisation samarbetat nationellt eller internationellt vid förhandlingar om villkor eller inställningar med molntjänstleverantören (t.ex. med centrala inköpare eller andra myndigheter i andra länder)? Förklara vilken inverkan detta samarbete har haft på de villkor och inställningar som ingår i avtalet och om ni har informerat de parter som ni har samarbetat med om resultaten av förhandlingarna.

14. Har er organisation lyckats förhandla fram villkor eller inställningar för att minska riskerna i samband med dess behandling?
    - Om så är fallet, beskriv resultatet.
    - Om nej, förklara varför och beskriv eventuella hinder som uppstått under processen.

15. Har organisationen krävt/förhandlat fram ett servicenivåavtal för tjänsterna?

16. Har er organisation vidtagit eller förhandlat fram några avtalsrelaterade, tekniska och/eller organisatoriska åtgärder för att begränsa molntjänstleverantörens behandling av personuppgifter (särskilt för egna ändamål eller med avseende på platsen för behandlingen) vid användning av de upphandlade molnbaserade tjänsterna? Om så är fallet, beskriv de åtgärder som vidtagits och förklara resonemanget bakom införandet av dessa åtgärder. (Observera att ytterligare frågor om internationella överföringar ställs nedan.)

17. Har ni genomfört några kontroller för att säkerställa reversibilitet/uppsägning av ett avtal, t.ex. om ni beslutar er för att byta till en annan leverantör? Förklara i allmänna ordalag vilka kontroller ni har genomfört.

Närmare uppgifter om avtalet: internationella överföringar

Obs! Svara på följande frågor genom att hänvisa till var och en av de molntjänstleverantörer som anges i fråga 1.

18. Överför molntjänstleverantören (och dess underleverantörer) personuppgifter (inklusive diagnostisk- eller telemetridata) till tredje land? Om ja, besvara frågorna nedan.

19. Har er organisation vidtagit eller förhandlat fram några avtalsrelaterade, tekniska och/eller organisatoriska åtgärder för att se till att internationella överföringar följer kraven? Har er organisation i synnerhet begränsat databehandlingen (behandling, överföring och lagring) till specifika platser eller länder? Om ja, beskriv dessa åtgärder.

20. Om er organisation överför personuppgifter (inklusive diagnostik- eller telemetridata) till tredjeländer, beskriv vilket överföringsverktyg i enlighet med kapitel V i dataskyddsförordningen som er organisation använder sig av.

21. Om ni använder er av standardavtalsklausuler, ange vilken mall från kommissionen som används för att upprätta standardavtalsklausuler (datum och typ, t.ex. standardavtalsklausuler mellan

personuppgiftsansvarig och personuppgiftsbiträden/mellan olika personuppgiftsbiträden).

22. Om er organisation har använt standardavtalsklausuler för överföringar, eller om den förlitar sig på molntjänstleverantörens bindande företagsbestämmelser: har det mot bakgrund av Schrems II-domen kontrollerats att det inte finns något i tredjelandets lagstiftning och/eller praxis som förbjuder mottagarna att uppfylla sina avtalsenliga skyldigheter för att säkerställa att den skyddsnivå för personuppgifter för fysiska personer som garanteras inom EES inte undergrävs?

23. Om er organisation anser att den som importerar uppgifterna faktiskt kan garantera att de bindande företagsbestämmelserna uppfylls eller att de avtalsenliga skyldigheterna enligt standardavtalsklausulerna fullgörs: beskriv skälen till denna slutsats.

24. Om er organisation anser att åtgärderna för överföring i kapitel V i dataskyddsförordningen är otillräckliga (t.ex. avtalsförpliktelser i standardavtalsklausulerna eller de bindande företagsbestämmelserna), har ni övervägt att genomföra kompletterande åtgärder och i så fall vilka åtgärder? Har er organisation 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? Beskriv resultatet av denna bedömning och skälen till er slutsats i detalj.

25. Har ni underrättats om någon begäran om utlämnande av uppgifter som utfärdats till molntjänstleverantören (eller någon av underleverantörerna) av statliga myndigheter i ett tredjeland? Om ja, vad var innehållet i den underrättelsen?

Närmare uppgifter om avtalet: Molntjänstleverantörens insamling och behandling av diagnostik- eller telemetridata

Obs! Svara på följande frågor genom att hänvisa till var och en av de molntjänstleverantörer och deras underleverantörer som anges i frågorna 1 och 2.

26. Om molntjänstleverantören samlar in och behandlar diagnostik- eller telemetridata till följd av användningen av molntjänsterna, hur gör molntjänstleverantören det? Dela upp svaret efter tjänst/funktion/komponent.
    a. Samlas dessa uppgifter in på klientsidan eller på molntjänstleverantörens servrar?
    b. Är dessa uppgifter anonymiserade eller pseudonymiserade?
        i. Om de är pseudonymiserade:

1. Var sker pseudonymiseringen? På klientsidan eller på molntjänstleverantörens servrar?
2. Hur utförs pseudonymiseringen (tekniker, identifierare osv.)?

ii. Om de är anonymiserade:

1. Var sker anonymiseringen? På klientsidan eller på molntjänstleverantörens servrar?
2. Hur utförs anonymiseringen (tekniker, aggregeringsnivå, beroende på vad som är tillämpligt)?

c. Samlas dessa uppgifter in som standard eller inte? Om så är fallet, vilka kontroller erbjuder molntjänstleverantören för att begränsa insamlingen och bearbetningen?
d. Vilka säkerhetsåtgärder tillämpar ni för att skydda dessa uppgifter under överföring, i minne och i vila?

27. Samlar molntjänstleverantören in och behandlar diagnostik- eller telemetridata eller annan information till följd av användningen av molntjänster som er organisation och/eller molntjänstleverantören inte anser vara personuppgifter? Dela upp svaret efter tjänst/funktion/komponent.

Efterlevnad

28. Kontrollerar ni molntjänstleverantörens tekniska och organisatoriska åtgärder, inklusive säkerhetsåtgärder, för att säkerställa[6] att denne uppfyller de överenskomna kraven och/eller fullgör sina skyldigheter och/eller uppfyller internationella standarder? Beskriv hur ni gör det och hur ofta.

29. Omfattar denna kontroll huruvida molntjänstleverantören utför regelbundna riskbedömningar av skyddet av personuppgifter, inbegripet bedömningar av informationssäkerhetsrisker (i efterhand) avseende införandet av molnbaserade tjänster? Om ja, hur övervakar ni att molntjänstleverantören utför dessa riskbedömningar? Beskriv hur ni gör det och hur ofta.

30. Utöver de delar som regleras i avtal med molntjänstleverantören, kontrollerar ni hur molntjänstleverantören uppfyller kraven i dataskyddsförordningen i allmänhet, t ex om molntjänstleverantören ser över och uppdatera policyer och åtgärder (t.ex. skyddsåtgärder i samband med internationella överföringar, eller vid utveckling av vägledning och rättspraxis)? Beskriv kortfattat era åtgärder i detta avseende

---

[6] Detta inbegriper kontroll av att åtgärderna är effektiva.

Bilaga – Definitioner

Följande terminologi, som återfinns i detta dokument, kommer från ISO 17788[7].

molnbaserade datortjänster	Ett koncept för nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser med automatisk åtkomst och administration på begäran.
molntjänst	En eller flera funktioner som ingår i molnbaserade datortjänster och anropas via ett definierat gränssnitt.
molntjänstleverantör	Part som tillhandahåller molntjänster.
gruppmoln	Distributionsmodell där molntjänster uteslutande stöder, och delas av, en specifik grupp av molntjänstkunder som har gemensamma krav och en relation till varandra, och där resurserna kontrolleras av åtminstone en medlem i denna samling.
beräkning som tjänst (CompaaS)	Molntjänstkategori där funktionerna som erbjuds molntjänstkunden är leverans och användning av bearbetningsresurser som behövs för att driftsätta och köra program.
datalagring som tjänst (DSaaS)	Molntjänstkategori där funktionerna som erbjuds molntjänstkunden är tillhandahållande och användning av datalagring och tillhörande funktioner.
hybridmoln	Molndistributionsmodell som använder minst två olika molndistributionsmodeller.
infrastruktur som tjänst (IaaS)	Molntjänstkategori där den molnkapacitetstyp som tillhandahålls molntjänstkunden är en typ av infrastrukturkapacitet.
plattform som tjänst (PaaS)	Molntjänstkategori där den molnkapacitetstyp som tillhandahålls molntjänstkunden är en typ av plattformskapacitet.
privat moln	Molndistributionsmodell där molntjänsterna används uteslutande av en enda molntjänstkund och resurserna kontrolleras av den molntjänstkunden.
publikt moln	Modell för införande av molntjänster där molntjänsterna är potentiellt tillgängliga för alla molntjänstkunder och resurserna kontrolleras av molntjänstleverantören.
reversibilitet	Process där molntjänstkunder hämtar sina kunddata och applikationsartefakter i molntjänsten och molntjänstleverantören raderar alla kunduppgifter i molntjänsten samt avtalsenligt specificerade molntjänstdata efter en överenskommen period.

[7] ISO/IEC 17788: Informationsteknik – molnbaserade datortjänster – översikt och vokabulär.

programvara som tjänst (SaaS)	Molntjänstkategori där den molnkapacitetstyp som tillhandahålls molntjänstkunden är en typ av applikationskapacitet.
klientorganisation	En eller flera användare av molntjänster som delar tillgång till en uppsättning fysiska och virtuella resurser.