Advokatfirman Kahn Pedersens skriftserie 2020:3

kahn pedersen

Publika molntjänster i näringslivet

– Rättslig analys och en introduktion till Folke©-modellen

kahn pedersen

ADDENDUM 2020-11-18

EDPB:s rekommendation om kompletterande skyddsåtgärder vid tredjelandsöverföring

Efter rapportens tryckning har den Europeiska dataskyddsstyrelsen (EDPB) publicerat ett utkast till rekommendation[1] för överföring av personuppgifter till länder utanför EU/EES (tredjelandsöverföringar). Bakgrunden till rekommendationen är EU-domstolens avgörande i Schrems II, och de frågetecken som uppkommit avseende bl.a. förutsättningarna för användning av publika molntjänster (se avsnitt 3.2.3 och 3.4 i denna rapport).

I allt väsentligt förändrar inte EDPB:s rekommendation de bedömningar och slutsatser som presenteras i rapporten. Det finns dock några klargöranden och typfall i EDPB:s rekommendation som läsaren av denna rapport bör uppmärksamma. Vi drar följande preliminära slutsatser från rekommendationen:

1. EDPB klargör att *avtal eller organisatoriska åtgärder* inte i sig kan utgöra tillräckliga åtgärder för att säkerställa en adekvat skyddsnivå för personuppgifter vid tredjelandsöverföring.
2. Det finns inga effektiva tekniska skyddsåtgärder för molntjänster som medför att leverantören i ett tredjeland har tillgång till personuppgifter i klartext vilket gäller oavsett om kryptering tillämpas vid överföring och vid "data-at-rest". Detta omfattar typiskt sett de SaaS-tjänster som innebär överföring av personuppgifter till USA.
3. Personuppgifter i klartext får generellt inte överföras via internet i okrypterad form, eller annars göras tillgängliga i klartext i tredjeland. Typiskt sett krävs kryptering och att leverantören/mottagaren inte har, eller enkelt kan skaffa tillgång till, dekrypteringsnyckeln.
4. Pseudonymisering kan vara en effektiv skyddsåtgärd, under vissa förutsättningar. Detsamma gäller för uppdelning av en personuppgiftsbehandling mellan flera personuppgiftsbiträden, så att ingen av dem får tillräcklig information för att identifiera fysiska personer.

Vi konstaterar vidare att EDPB inte uttrycker sig i termer av riskbedömning eller riskbegränsande åtgärder när det gäller tredjelandsöverföring. Det är, enligt EDPB:s rekommendation, således inte möjligt att beakta *sannolikheten* för att personuppgifterna kommer att behandlas på ett sätt som strider mot EU-rätten och *konsekvenserna* för de registrerade om detta trots allt sker. Vi bedömer emellertid att de åtgärder som vi rekommenderar i avsnitt 3.2.4.2 i denna rapport ligger i linje med EDPB:s rekommendation och är lämpliga att beakta i samband med överföring till tredjeland, såsom att minska exponering mot tredjeländers regelverk och att minimera riskerna genom t.ex. uppgiftsminimering, ytterligare säkerhetsfunktioner i molntjänster, kryptering och pseudonymisering. Vid den slutgiltiga bedömningen måste dock hänsyn tas till de särskilda typfall som EDPB redovisar i sin rekommendation.

Vi bedömer att även Folke©-modellen fungerar väl med beaktande av EDPB:s rekommendation om kompletterande skyddsåtgärder. Folke©-modellen tar, när det gäller dataskydd, sin utgångspunkt i den riskbedömning som alltid måste utföras vid behandling av personuppgifter, oaktat tredjelandsöverföring. Den huvudsakliga konsekvensen av EDPB:s rekommendation för tillämpning av Folke©-modellen, är dels att det nu ställs ännu högre krav för att kryptering och andra skyddsåtgärder mot tredjelandsöverföring alls ska påverka slutresultatet av riskbedömningen, dels att risken för att utländska myndigheter vid tredjelandsöverföring får åtkomst till de överförda personuppgifterna inte direkt är relaterad till vilken typ av personuppgift det är fråga om.

// Advokatfirman Kahn Pedersen, dag som ovan

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted – version for public consultations.

Vi på Advokatfirman Kahn Pedersen ser det som en naturlig del av vår roll som specialistbyrå att delta i den offentliga diskussionen. Detta för att bidra till att föra fram och utveckla intressanta och inte sällan svåra rättsfrågor inom våra specialistområden. Ett led i detta arbete är denna skriftserie som publiceras med ett till tre nummer per år. Tanken med skriftserien är att lite mer djupgående utreda aktuella och mer komplexa rättsfrågor, som vi märker är av intresse för våra klienter och samhället i stort.

Eftersom målsättningen är att vårt arbete med rapporterna ska komma inte bara våra klienter och samarbetspartners till del, utan även ska kunna bidra till utvecklingen av de rättsområden som vi är specialiserade inom, tillhandahålls alla nummer av skriftserien kostnadsfritt på vår webbplats under en Creative Commons Erkännande-Inga Bearbetningar 4.0 Internationell Licens. Detta möjliggör mångfaldigande och spridning av materialet förutsatt att inga ändringar görs och att källan anges.

Ämnet för denna rapport, som har nummer 2020:3, är publika molntjänster i näringslivet.

ISBN 978-91-986495-0-5

1. Inledning

1.1 Varför en rapport om publika molntjänster?

"*Det finns inget moln – det är bara någon annans dator*", brukar det lite skämtsamt sägas. Utöver att själva begreppen "moln" och "molntjänst"1 i sig är mångtydiga, så är påståendet i sak nog både sant och falskt. Å ena sidan är det korrekt att molntjänster innebär att man istället för egen it-kapacitet använder leverantörens centraliserade resurser (hårdvara, lagringsutrymme och nätverksåtkomst), vilka typiskt sett delas och används av flera olika kunder. Å andra sidan antyder påståendet att molntjänster skulle vara en mindre viktig företeelse, vilket inte heller är rättvisande. Det är nog ingen som ifrågasätter att framväxten av molntjänster under de senaste 10–15 åren i hög utsträckning påverkat snart sagt alla organisationer – oavsett typ och verksamhet.

Användning av molntjänster innebär att information ofta lagras i olika jurisdiktioner, samt att den leverantör som lagrar och behandlar informationen kan vara underkastad andra lagar och regler än molntjänstkunden. Dessa omständigheter aktualiserar många olika rättsfrågor och risker för molntjänstkunden. Inte sällan handlar det i praktiken om att tolka och tillämpa lagstiftning och regelverk som har inrättats under helt andra förutsättningar och för helt andra tillämpningar. Detta ställer i sin tur stora krav på varje potentiell molntjänstkund, såvitt gäller både juridisk, regulatorisk och teknisk kompetens.

Diskussionerna kring för- och nackdelar med molntjänster samt hur riskerna med dessa tjänster ska hanteras, har pågått under lång tid. I stor utsträckning har diskussionen utgått från ett tekniskt perspektiv och då särskilt informationssäkerhet. Många av de som, mer eller mindre vederhäftigt, har uttalat sig om de juridiska aspekterna på molntjänster har emellertid inte i första hand utgått från de svenska rättsliga förutsättningarna, och debatten har, menar vi, inte sällan präglats av kategoriska och onyanserade ställningstaganden. Behovet av att på djupet analysera de rättsliga förutsättningarna för användning av molntjänster har dock vuxit och har under de senaste åren fått mycket stor uppmärksamhet. EU-domstolens dom i det s.k. Schrems II-målet[2] är det senaste exemplet på denna utveckling.

---

1 Vad som är en "molntjänst" kan diskuteras in absurdum. Vi anser inte att en sådan utdragen och teoretisk diskussion är nödvändig, eftersom den semantiska betydelsen inte är avgörande för den rättsliga bedömningen. Den här rapporten avhandlar generellt användning av "publika molntjänster", med vilket vi menar allmänt och kommersiellt tillgängliga webbaserade tjänster för företag (B2B), där leverantörens hårdvara, lagringsutrymme och nätverksåtkomst delas av flera kunder. Se vidare i avsnitt 3.1.1 där vi beskriver olika typer av sådana molntjänster. Om inte annat särskilt anges menar vi i rapporten samma företeelse/tjänster när vi använder "publika molntjänster" eller bara "molntjänster".

2 EU-domstolens dom av den 16 juli 2020 i mål C-311/18, *Schrems II*.

Vi vill poängtera att de juridiska utmaningarna sällan har med tekniken kring molntjänster att göra. Istället ligger utmaningen, och de stora riskerna, i att leverantörer står under inflytande av främmande jurisdiktion, vilken kan stå i konflikt med de lagar och regler som svenska företag och organisationer har att efterleva. De standardavtal som reglerar molntjänstleverantörens åtagande och ansvar är oftast skrivna utifrån molntjänstleverantörens intressen snarare än kundens rättsliga skyldigheter.

Vidare uppstår risker i och med kategoriska strategier i stil med ”allt i molnet” eller ”molnet först”, genom vilka det inte lämnas utrymme för nödvändiga juridiska nyanser. Sådana strategier medför ofta ett närmast vårdslöst risktagande och innebär en likgiltighet inför lagar och regler. Märkligt nog har tillsynsmyndigheter som Datainspektionen och Finansinspektionen inte ännu tagit sig an dessa viktiga frågor i någon märkbar omfattning. Vi är dock övertygade om att användningen av molntjänster kommer att bli föremål för granskning och juridisk prövning. Det vore en önskvärd utveckling som inte bara skulle medföra en ökad efterlevnad av svensk rätt, utan även tvinga de stora leverantörerna att anpassa sina tjänster och avtal på ett sätt som överensstämmer bättre med svenska och europeiska juridiska förutsättningar.

Vi vill genom denna rapport delge vår syn och vår rättsliga bedömning i några av de frågor som aktualiseras och som har diskuterats i olika sammanhang. Tack vare att vi under de senaste åren haft anledning att utreda dessa frågor på djupet i olika sammanhang, har vi också utarbetat en egen modell för riskbedömning i samband med molnmigrering, den s.k. Folke©-modellen[3], vilken vi presenterar i denna rapport.

1.2 Varför två rapporter om publika molntjänster?

I den svenska debatten kring molntjänster har fokus i stor utsträckning varit på den offentliga sektorns möjligheter, och förutsättningar för, att hantera sekretessreglerade uppgifter och personuppgifter i publika molntjänster. Diskussionerna har även rört sig utanför de rent rättsliga frågorna och berört lämpligheten i att svenska myndigheter avhänder sig kontrollen över information i samhällsbärande verksamhet.[4]

I denna diskussion har bl.a. begreppet ”digital suveränitet” använts för att belysa behovet av att Sverige behåller kontrollen av digital information och utrustning samt förmågan att utveckla it-system.[5]

---

3 Namnet ”Folke©-modellen” har vi främst, men inte enbart, hämtat från det tyska ordet för moln, dvs. ”Wolke”.

4 Försäkringskassan, *Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt*, publicerad den 18 november 2019, dnr. 013428-2019, https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf?MOD=AJPERES&CVID=, hämtad den 3 september 2020.

5 Se vidare Försäkringskassan, *Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt* (2019), s. 26.

Motsvarande diskussion, i synnerhet angående behovet av att minska beroendet av amerikanska molntjänster, har även förts i många andra europeiska länder och av EU-kommissionen. I denna del bör nämnas att framförallt tyska och franska intressen driver ett europeiskt projekt kallat Gaia-X[6], vars målsättning är att skapa europeiska alternativ till marknader som idag domineras av amerikanska leverantörer. I oktober 2020 antog samtliga EU:s medlemsländer en gemensam deklaration om avsikten att samarbeta för att skapa ”a European cloud”.[7]

Då vi menar att de rättsliga utmaningarna med användning av publika molntjänster skiljer sig åt mellan privat och offentlig sektor, så har vi valt att göra två separata rapporter på detta ämne. I den här rapporten, som utgör den första delen, redogör vi för de mest relevanta regelverken för näringslivets användning av publika molntjänster. Den andra delen, om användning av molntjänster i offentlig sektor, planerar vi att publicera under 2021.

1.3 Behovet av praktisk vägledning är stort

De företag, myndigheter och organisationer som köper molntjänster, ställs inför frågan om leverantörernas villkor och erbjudande är förenliga med de lagkrav och regulatoriska krav som ställs på dem. Detta är en komplex bedömning att göra, där oberoende och lättillgänglig rättslig vägledning kan vara svår att finna.

Den rättsliga regleringen, både i Sverige och inom EU, har stegvis uppdaterats till att passa den nya digitaliserade miljön. På grund av den tekniska komplexiteten och att reglerna ska tillämpas på många olika typer av verksamheter, har lagstiftarna varit hänvisade till att utforma reglerna mer som principer än som konkreta handlingsdirigerande regler. Detta lämnar stort utrymme inte bara för tillsynsmyndigheterna att tolka reglerna och ge vägledning efter bästa förmåga, utan placerar även ett stort ansvar på molntjänstkunder som omfattas av regelverket att tillämpa reglerna efter en egen tolkning av reglernas mer eller mindre tydliga syften.

Vi tror att en nyanserad och riskbaserad inställning så långt möjligt är nödvändig. Utgångspunkten för denna rapport är vår grundläggande uppfattning om att det *dels* inte finns absoluta rättsliga hinder mot användning av publika molntjänster som sådana, *dels* att ny teknik (och/eller nya leveransmodeller) som utgångspunkt bör vara tillåten så länge den inte uppenbart är förbjuden.

Vi menar vidare att det finns ett behov av en metod för att väga samman olika risker med användning av publika molntjänster. Vi har där-

6 Se GAIA-X: A Federated Data Infrastructure for Europe, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html, hämtad den 3 september 2020.

7 EU-kommissionens artikel, *Towards a next generation cloud for Europe*, publicerad den 15 oktober 2020, https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe, hämtad den 22 oktober 2020.

för utvecklat en egen metod för detta, den s.k. Folke©-modellen, som vi också presenterar i rapporten. Denna metod är avsedd att fungera som ett beslutstöd som kan visualisera hur olika beslut och ställningstaganden kan och bör påverka den juridiska tillämpningen i praktiken.

Vi tror och hoppas att denna rapport kan fungera som ett inlägg i debatten om publika molntjänster. Vi hoppas också, vilket är minst lika viktigt för oss som advokatbyrå, att rapporten blir en praktiskt användbar vägledning i samband med konkreta överväganden kring användning av molntjänster och digital transformation.

1.4 Vem bör läsa denna rapport?

Den huvudsakliga målgruppen för denna rapport är jurister inom näringslivet som kommer i kontakt med frågor om publika molntjänster. Rapporten innehåller inte enbart renodlad juridik, utan resonerar även kring generella frågor om riskbedömning, lämplighet och hur man i praktiken kan och bör förhålla sig till abstrakta och allmänna principer. Vi hoppas och tror därför att rapporten kan vara intressant även för andra yrkeskategorier som kommer i kontakt med frågor om dataskydd, personlig integritet, molntjänster, riskhantering och hållbarhetsfrågor.

1.5 Disposition

Rapporten utgår från Kahn Pedersens proprietära verktyg *Folke©-modellen* för att visualisera risk förknippad med publika molntjänster. Modellen presenteras närmare i kapitel 2.

Vilka risker som ska beaktas i Folke©-modellen beror bl.a. på vilken information som placeras i ”molnet”, vilka lagar och regler som är tillämpliga på informationen, valet av leverantör och molntjänst samt vilka avtalsvillkor som ska tillämpas. Därför har vi valt att dela in de efterföljande kapitlen i dels *generella juridiska överväganden,* dels *särskilda överväganden* beroende på vilken typ av verksamhet molntjänstkunden bedriver.

Generella juridiska överväganden som bör göras behandlas i kapitel 3. Först redogör vi för den s.k. *jurisdiktionsrisken* (avsnitt 3.2), vilken vi menar är den enskilt största frågan och risken som en organisation behöver bedöma i samband med användning av molntjänster. Därefter går vi i avsnitt 3.3 närmare in på hur man identifierar risker ur ett dataskyddsperspektiv, vilka dataskyddsrisker som typiskt sett aktualiseras i fråga om molntjänster samt hur man genomför en *konsekvensbedömning enligt kraven i dataskyddsförordningen* (GDPR). I avsnitt 3.4 behandlas sedan hur riskerna med användning av molntjänster kan påverkas genom olika *tekniska säkerhetslösningar* och då i synnerhet kryptering. I slutet av kapitlet, avsnitt 3.5, redogör vi, baserat på våra erfarenheter av marknadens större molntjänstleverantörers

standardavtal, för vilka *avtalsmässiga risker* som typiskt sett förekommer i dessa avtal och vilka konsekvenser de aktuella riskerna kan komma att få för molntjänstkunden.

I de efterföljande kapitlen beskriver vi *särskilda överväganden* som bör göras när den potentiella molntjänstkundens verksamhet omfattas av särskild lagstiftning eller regulatoriska krav. Först tar vi, i kapitel 4, upp de särskilda utmaningar avseende informationssäkerhet som användning av molntjänster kan komma att innebära för *verksamheter som omfattas av bl.a. säkerhetsskyddslagen* (2018:585) och lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (även kallad NIS-lagen).

Därefter redogör vi i kapitel 5 för de särskilda överväganden som bör göras av *banker och försäkringsföretag*, dels mot bakgrund av reglerna om bank- och försäkringssekretess, dels med tanke på de bank- och försäkringsregulatoriska krav på utkontraktering och uppdragsavtal som följer av Europeiska bankmyndighetens och Europeiska försäkrings- och tjänstepensionsmyndighetens respektive riktlinjer.

Avslutningsvis har vi i kapitel 6 upprättat ett par *tillämpningsexempel* för att illustrera hur Folke©-modellen kan användas i praktiken vid näringslivets anlitande av en molntjänstleverantör, samt hur modellen påverkas av de överväganden och risker som behandlas i de övriga delarna av rapporten.

1.6 Avgränsningar

Vi vill särskilt betona att denna rapport inte gör anspråk på fullständighet. Det valda ämnet är mycket omfattande och komplext och vi har, för att begränsa omfånget av rapporten, gjort vissa avgränsningar genom att välja ut de perspektiv som vi tycker är mest relevanta och som det, enligt vår erfarenhet, finns flest frågor kring när det gäller användning av publika molntjänster i näringslivet.

Våra redogörelser i rapporten avser endast svensk rätt och EU-rätt och vi vill understryka att vi, utöver den korta redogörelse för relevanta delar av amerikansk rätt som görs i avsnitt 3.2 nedan, inte har beaktat annan utländsk lagstiftning. Som framgår av rapporten kan ytterligare utländsk lagstiftning mycket väl aktualiseras i det enskilda fallet, vilket är en av de många risker som en molntjänstkund måste utreda och ta ställning till.

Vi har i rapporten inte tagit hänsyn till andra rättsområden än de som uttryckligen avhandlas. Således har varken skatte- eller konkurrensrätten behandlats och inte heller anti-korruptionslagstiftning. Vi har heller inte närmare beaktat de immaterialrättsliga eller associationsrättsliga frågeställningar som kan aktualiseras i samband med användning av olika typer av molntjänster. Som nämnts ovan har vi i denna rapport inte behandlat sådan särskild reglering som enbart gäller för myndigheter.

Slutligen ska nämnas att vi i de slutsatser som dras i rapporten utgår från generella förutsättningar och typiska risker förknippade med användning av molntjänster som tillhandahålls av de flesta större molntjänstleverantörerna. Innan en verksamhet fattar beslut om anlitande av en molntjänstleverantör, bör det alltid göras en juridisk helhets- och lämplighetsbedömning i relation till den särskilda molntjänstleverantör som övervägs, den specifika tjänstens innehåll och de konkreta avtalsvillkoren.

Eftersom denna rapport utgår från svensk rätt och EU-rätt, vill vi i detta sammanhang understryka vikten av att anlita lokala juridiska rådgivare för att identifiera potentiella konsekvenser och risker i samband med utländsk lagstiftning, för det fall molntjänstleverantören eller dess underleverantörer lyder under utländsk jurisdiktion. Även då parterna avtalar om att molntjänstavtalet ska tolkas under utländsk rätt bör juridisk rådgivare i aktuell jurisdiktion anlitas för att bedöma avtalet under aktuell jurisdiktion.

1.7 Tillämpningsområdet för Folke©-modellen

Vår modell för juridisk riskanalys för molntjänster utgår, som framgått av kapitel 2 nedan, från ett riskperspektiv. Med ”risk” menar vi genomgående i rapporten produkten av sannolikheten för att något inträffar och hur allvarliga konsekvenserna är av att detta ”något” inträffar.

Enligt vår uppfattning är det naturligt att utgå från ett riskperspektiv i detta fall, både eftersom rättsläget kring publika molntjänster är osäkert men också eftersom många av de rättsregler som är tillämpliga innehåller och förutsätter att en riskbedömning görs i det enskilda fallet. De tydligaste exemplen på detta är att den personuppgiftsansvarige enligt dataskyddsförordningen genom ett riskbaserat synsätt ska bedöma och agera utifrån vad som är ”*lämpliga tekniska och organisatoriska åtgärder*” och tillse att en molntjänstleverantör i avtalet lämnar (och har förmåga att lämna) ”*tillräckliga garantier*”. Liknande relativa kriterier och förutsättningar finns i SSL, NIS-lagen och i EBA:s riktlinjer för outsourcing.

Folke©-modellen är utformad för att kunna beakta, analysera och tillämpa olika rättsregler, oavsett karaktär, som kan aktualiseras vid användning av molntjänster. Modellen är framtagen för att kunna göra en sammanvägd bedömning av många disparata regler och skyddsintressen. Det kan emellertid diskuteras om det är *lämpligt* att på detta sätt kombinera dessa olika regler in i en och samma analysmodell – en sådan metod har ju inte stöd i lag och kan uppfattas som svårförenlig med ett enskilt regelverk. I denna fråga menar vi dels att behovet av ett praktiskt användbart verktyg är så pass stort att denna typ av samordnad modell är *nödvändig*, dels att modellen på ett vederhäftigt sätt beaktar och väger samman tillämpliga lagar och regler.

Samtidigt kan Folke©-modellen naturligtvis aldrig ersätta behovet av juridisk analys i det enskilda fallet.

I vissa fall – såsom vid användning av publika molntjänster för omfattande behandling av känsliga personuppgifter eller kvalificerat hemliga uppgifter enligt SSL – är utrymmet för riskbedömning med Folke©-modellen mycket litet, om ens något. I många andra fall kommer istället tillåtligheten av potentiell molntjänstanvändning nästan helt och hållet vara avhängigt en riskbedömning.

En särskild aspekt av modellen är att den beaktar molntjänstkundens ”riskaptit”. Detta är sannolikt inte kontroversiellt när det gäller kommersiell eller affärsmässig risk, men desto mera intressant i relation till risken för lagöverträdelse (juridisk risk). En molntjänstkund kan givetvis aldrig, med stöd av juridisk analys eller Folke©-modellen, komma fram till att det skulle vara acceptabelt att begå lagöverträdelser med hänvisning till stor/hög riskaptit. Detta är en av anledningarna till att vi infört gränser i Folke©-modellen för hur mycket en molntjänstkund själv kan bestämma sin riskaptit (se avsnitt 2.2). Det finns omständigheter när användning av publika molntjänster klart och tydligt kommer att medföra lagöverträdelse. I dessa fall kan inte Folke©-modellen användas för att berättiga sådan användning.

Sammanfattningsvis, Folke©-modellen bör framförallt användas i de fall när den juridiska analysen och bedömningen *inte* är uppenbar. Vår erfarenhet är att tillämpningsområdet för Folke©-modellen därmed i praktiken är mycket stort.

1.8 Förkortningar

FÖRKORTNING	BESKRIVNING
CLOUD Act	Clarifying Lawful Overseas Use of Data Act, H.R.4943 (amerikansk lag)
Dataskydds-förordningen; GDPR	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)
Delegerade förordningen till Solvens II	Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II)
EBA	Europeiska bankmyndigheten
EDPB	Europeiska dataskyddsstyrelsen
EDPS	Europeiska dataskyddsombudsmannen
EIOPA	Europeiska försäkrings- och tjänstepensionsmyndigheten
ESMA	Europeiska värdepappers- och marknadsmyndigheten
FISA	Foreign Intelligence Surveillance Act (amerikansk lag)
FRL	Försäkringsrörelselag (2010:2043)
IaaS	Infrastructure as a service (”infrastruktur-som-tjänst”)
LBF	Lag (2004:297) om bank- och finansieringsrörelse
NIS-lagen	Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
OSL	Offentlighets- och sekretesslag (2009:400)
PaaS	Platform as a service (”plattform-som-tjänst”)
Privacy Shield	Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna
SaaS	Software as a service (”mjukvara-som-tjänst”)
SCA	Stored Communications Act (amerikansk lag)
SCC-beslutet	Kommissionens beslut 2010/87 av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG, i dess lydelse enligt kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016
Schrems I	EU-domstolens dom av den 6 oktober 2015 i mål C-362/14
Schrems II	EU-domstolens dom av den 16 juli 2020 i mål C-311/18
SSF	Säkerhetsskyddsförordning (2018:658)
SSL	Säkerhetsskyddslag (2018:585)
VpmL	Lag (2007:528) om värdepappersmarknaden

2. Om Folke©-modellen

2.1 Inledning

Kahn Pedersen har under de senaste åren utvecklat Folke©-modellen – en egen metod för att synliggöra och hantera juridiska risker kopplade till publika molntjänster. Modellen utgår från en bedömning av *leverantörsrisk* och *skyddsvärde* för den information som hanteras i molntjänsten. Dessa begrepp förklaras närmare i avsnitt 2.3 nedan.

Folke©-modellen är utvecklad för att utgöra ett dynamiskt beslutstöd för verksamheter som överväger att börja använda en publik molntjänst, t.ex. istället för en s.k. on premises-lösning. Modellen väger samman flera olika riskfaktorer och variabler till ett resultat som indikerar vilken risknivå en sådan planerad användning skulle medföra. Folke©-modellen tar bl.a. hänsyn till tillämplig lagstiftning, regulatoriska krav, rättsliga vägledningar och andra ”externa krav”[8], vilken molntjänstleverantör som anlitas, vilken information som placeras i molnet, vilka tekniska och organisatoriska informationssäkerhetsåtgärder som vidtas, vissa kommersiella risker och även vilken riskprofil eller riskaptit som den aktuella verksamheten typiskt sett har eller bör ha.

Folke©-modellen bygger i grunden på kvalificerade bedömningar och ett riskbaserat angreppssätt. Som framgått av inledningen av denna rapport menar vi att det inte finns några generella absoluta juridiska hinder eller förbud mot att använda molntjänster som sådana. Det är alltså, menar vi, sällan meningsfullt att inom ramen för näringslivets användning, kategorisera en molntjänst som ”laglig” eller ”olaglig” eller som ”tillåten” eller ”otillåten”. Det beror helt på omständigheterna i det enskilda fallet. Vem är leverantören, vilken typ av behandling innefattar tjänsten, vem är kunden, vilka skyddsåtgärder har vidtagits och vilken information omfattas? En och samma molntjänst kan mycket väl vara laglig/tillåten i ett fall, och olaglig/otillåten i ett annat. Det är här som Folke©-modellen fyller sitt huvudsakliga syfte, dvs. att väga samman olika risker och omständigheter i ett sammanhållet och dynamiskt beslutstöd.

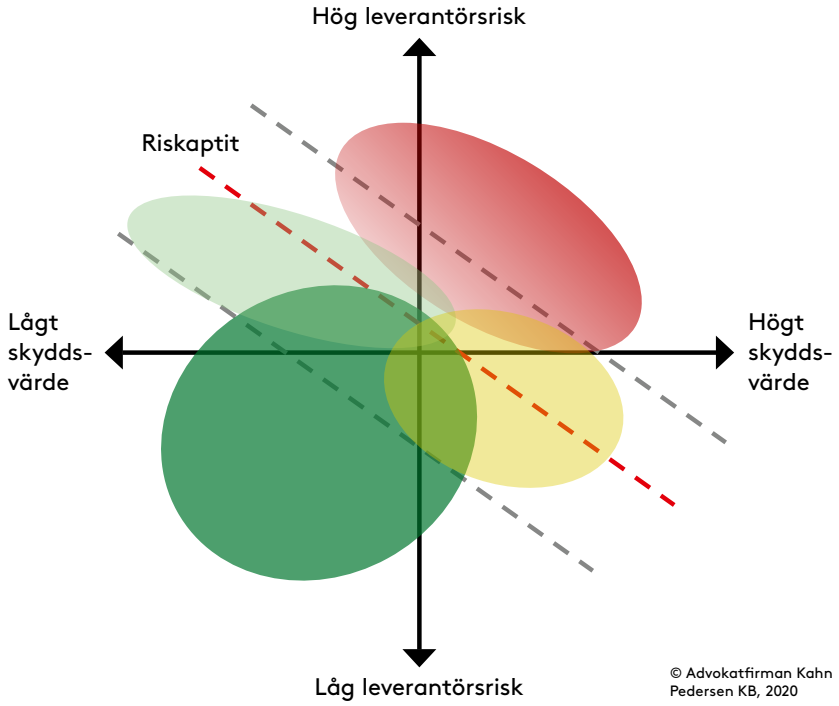
Folke©-modellen är i princip användbar för alla verksamheter och för alla typer av molntjänster.[9] I detta avsnitt presenterar vi modellen och hur den är tänkt att används. I kapitel 6 tillämpar vi sedan modellen praktiskt på tre fiktiva scenarion. Vi redogör inte i detalj för de algoritmer och metoder som krävs för att göra en fullständig analys enligt Folke©-modellen eftersom dessa inte ryms i aktuellt format.

---

8 Angående detta begrepp, se Advokatfirman Kahn Pedersens skriftserie 2020:1, *Juridisk informationssäkerhet – Att samordna arbetet enligt säkerhetsskyddslagen, NIS-lagen, dataskyddsförordningen och annan lagstiftning om informationssäkerhet*. Rapporten finns tillgänglig för nedladdning på https://kahnpedersen.se/publications/reports/.

9 Vissa begränsningar finns emellertid, se vidare i avsnitt 2.4 nedan.

2.2 Övergripande presentation av Folke©-modellen



Figur 2.1: Folke©-modellen.

På ***Y-axeln*** i Folke©-modellen placeras *leverantörsrisken* (se vidare avsnitt 2.3.1 nedan). Denna risk är ofta relativt "statisk" och svår att påverka för den enskilda molntjänstkunden även om större och förhandlingsskickliga molntjänstkunder kan genomdriva förbättringar i vissa fall (se 3.5 nedan). Här krävs istället en omfattande bedömning av den aktuella tjänsten, den leverantör som tillhandahåller tjänsten och tillämpliga avtalsvillkor. Molntjänster och molntjänstleverantörer med *låg* leverantörsrisk, t.ex. en svensk privat molntjänst med robusta och lagenliga avtalsvillkor under svensk rätt, placeras i den undre delen av Y-axeln, medan en publik molntjänst som tillhandahålls av en leverantör i en högriskjurisdiktion utanför EU/EES och omfattas av ensidiga och godtyckliga avtalsvillkor bör anses medföra en *hög* leverantörsrisk och därmed placeras i den övre delen av Y-axeln.

På ***X-axeln*** i modellen illustreras *informationens skyddsvärde* (se vidare avsnitt 2.3.2 nedan). Denna risk är betydligt enklare för molntjänstkunden att disponera över, eftersom det är kunden som bestämmer vilken information som ska omfattas. Information med *lågt* skyddsvärde placeras längst ut till vänster på skalan, medan information med *högt* skyddsvärde placeras längst ut till höger på axeln.

I kapitel 6 nedan har vi, utifrån vår bedömning av leverantörsrisken kopplad till molntjänsterna och informationens skyddsvärde, placerat in några vanliga typer av molntjänster och information på Folke©-modellens Y- respektive X-axel.

Verksamhetens bedömning av leverantörsrisken och informationens skyddsvärde kan sedan placeras in i Folke©-modellen. Information med ett lågt skyddsvärde som behandlas genom en molntjänst med låg leverantörsrisk positionerar den sammanvägda användningen av molntjänsten i ***det mörkgröna området*** i modellen. Den nivå av risk som är acceptabel i det enskilda fallet beror också på organisationens riskaptit (se avsnitt 2.3.3 nedan), men generellt kan sägas att positioner i det mörkgröna området typiskt sett medför en låg juridisk risk.

Information med högt skyddsvärde (exempelvis en stor mängd hälsouppgifter om försäkringstagare) som behandlas i en molntjänst med hög leverantörsrisk placerar den sammanvägda risken i ***det röda området*** i modellen. Användning av molntjänster som hamnar i det röda området medför typiskt sett en hög juridisk risk, se dock avsnitt 2.3.3 nedan.

Om den sammanvägda risken placeras i ***det gula området*** nere till höger i modellen innebär det en *medelhög* sammanvägd risk och placeringar i ***det ljusgröna området*** uppe till vänster innebär en *medellåg* sammanvägd risk.

Vi vill understryka att Folke©-modellen är dynamisk, såtillvida att resultatet kommer att påverkas beroende på vilka juridiska, avtalsmässiga, tekniska och organisatoriska skyddsåtgärder som vidtas. Genom att vidta olika åtgärder kan molntjänstkunden alltså *påverka riskerna* som behandlingen innebär. En framgångsrik förhandling av avtalets villkor innebär exempelvis att den juridiska informationssäkerheten förbättras och att värdet på Y-axeln sjunker. På motsvarande sätt kan en förändring av vilken typ av data som behandlas i molntjänsten och/eller införande av ytterligare tekniska säkerhetsåtgärder innebära ett minskat värde på X-axeln. Detta utvecklas i det följande avsnittet 2.3.

För att tillämpa Folke©-modellen behöver man också ta ställning till vilken riskbenägenhet och riskaptit som kan anses vara lämplig för verksamheten och tjänsten (se vidare avsnitt 2.3.3 nedan). Molntjänstkundens riskbenägenhet och riskaptit illustreras av den ***diagonala röda streckade linjen*** i modellen som bör placeras någonstans i spannet mellan de två grå streckade linjerna. Positioner ovanför den utplacerade röda linjen betraktas som icke-godtagbara och/eller ej tillåtna enligt tillämpliga regler och riktlinjer inom kundens organisation och positioner under linjen betraktas som acceptabla.

2.3 Närmare om Folke©-modellens beståndsdelar

2.3.1 VAD ÄR ”LEVERANTÖRSRISK”?

2.3.1.1 Definition

> **Leverantörsrisk** = Risken (sannolikhet * allvarsgrad) för att information hanteras enligt lagar eller avtalsvillkor som står i konflikt med lagar och regler som informationsinnehavaren (dvs. molntjänstkunden) lyder under.

Bedömningen av leverantörsrisk har ett nära samband med informationssäkerhetsarbetet. Vi menar att en fullgod informationssäkerhet bör inbegripa skyddsåtgärder baserat på både teknisk och juridisk informationssäkerhet. Folke©-modellen har utvecklats bl.a. som ett sätt att kvantifiera och hantera den juridiska informationssäkerheten.[10]

2.3.1.2 Exempel på viktiga riskfaktorer (ej uttömmande)

Vi menar att bl.a. följande omständigheter påverkar leverantörsrisken:

- **Jurisdiktionsrisken,** vars storlek i sin tur beror på bl.a.:

  - Om molntjänstkunden genom avtalsvillkoren godkänner ett utlämnande till utländska myndigheter eller till annan obehörig tredje man i utlandet utan att molntjänstkunden dessförinnan i varje enskilt fall getts möjlighet att bedöma lämpligheten av ett sådant utlämnande och förhindra det. Således, överlåter molntjänstkunden till leverantören att fatta beslut om brytande av sekretess för molntjänstkundens konfidentiella information?

  - Vilken lag som är tillämplig på avtalet. Vilka risker finns för utelämnande som inte är förenligt med de regler som molntjänstkunden omfattas av?

  - Vilken lag som är tillämplig för leverantören och/eller eventuella underleverantörer. Vilka risker finns för obehörigt utlämnande under dessa jurisdiktioner? För att säkerställa detta bör man bl.a. undersöka:
    - graden av rättssäkerhet i aktuell jurisdiktion, och
    - avsaknad eller förekomst av vedertagna och rättssäkra utlämningsmekanismer (t.ex. Mutual Legal Assistance Treaty, ”***MLAT***”) som möjliggör utlämnande i enlighet med lagar och regler som molntjänstkunden lyder under.

10 För en närmare redogörelse av begreppet juridisk informationssäkerhet, se Advokatfirman Kahn Pedersens skriftserie 2020:1, *Juridisk informationssäkerhet*.

  - Om tjänsten innefattar att information regelmässigt lämnar lagringsplatsen (eller kan kommas åt från annan plats, t.ex. genom support), så att informationen därigenom kan bli föremål för annan jurisdiktion.

- **Geopolitisk risk*:*** Förekommer geopolitisk risk kopplad till var informationen är lagrad? Observera att vi här inte avser jurisdiktionsrisken, utan exempelvis risken för politisk instabilitet, terrorism, krig, sanktioner, naturkatastrofer eller revolution.

- **Avvikelser i förhållande till annan tillämplig jurisdiktion*:*** Finns avvikelser i hur avtalet och/eller tjänsten uppfyller tillämpliga bestämmelser i den jurisdiktion som molntjänstkunden lyder under?

- **Motståndskraftiga avtalsvillkor och molntjänstkundens kontroll*:*** Hur robusta är avtalsvillkoren för molntjänstkunden? Förekommer exempelvis ensidig rätt för leverantören att ändra avtalet, finns mer eller mindre godtyckliga möjligheter för leverantören att suspendera molntjänstkundens tillgång till molntjänsten och hur regleras uppsägningstider, avtalstid m.m.?

- **Tillgängligheten till molntjänsten*:*** Hur robust är tjänstens avtalade tillgänglighet för molntjänstkunden (mot bakgrund av avstängningsmöjligheter, SLA-nivåer m.m.)?

- **Tillräckliga sanktioner vid avtalsbrott*:*** Är avtalsbrott tillräckligt sanktionerade för att avskräcka leverantören och således tillräckligt robusta för att verka beteendestyrande?

- **Kundens beroende av tjänsten*:*** Är det i praktiken möjligt för molntjänstkunden att väcka talan mot leverantören eller säga upp avtalet till förtida upphörande, med hänsyn till molntjänstkundens faktiska beroende av tjänsten. Det vill säga, är molntjänstkundens verksamhet helt eller delvis beroende av de aktuella tjänsterna i sådan utsträckning att molntjänstkunden inte rimligen kan riskera att stå utan dessa? Under sådana omständigheter finns heller ingen praktisk möjlighet att inleda en tvist eller stoppa prestationer.

2.3.1.3 Exempel på hur leverantörsrisken kan påverkas/minska (ej uttömmande)

Vi menar att leverantörsrisken huvudsakligen beror på tre aspekter:

1) Valet av leverantör,

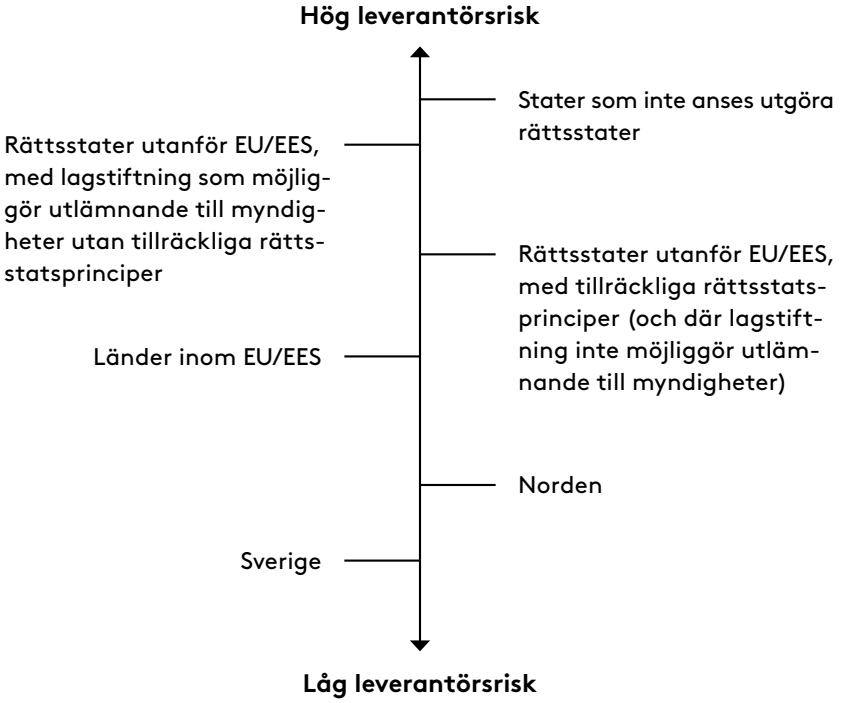
2) valet av molntjänst och dess uppsättning/arkitektur, och

3) vilka avtalsvillkor som är tillämpliga.

Detta innebär att varje molntjänst i utgångsläget medför en viss leverantörsrisk, beroende på vilken leverantör som avses, vilken moln-

tjänst som avses och hur de aktuella standardavtalsvillkoren är formulerade.

Följande bild illustrerar hur molntjänstleverantörens jurisdiktion, utan förhandlade avtalsvillkor, påverkar leverantörsrisken och vilken placering på Y-axeln i Folke©-modellen det normalt sett medför:



Figur 2.2: Närmare beskrivning av Folke©-modellens Y-axel.

Utgångsläget för bedömningen av en molntjänst såvitt avser leverantörsrisk kan påverkas genom förhandling av relevanta avtalsvillkor (se avsnitt 3.5 nedan).

2.3.2 VAD INNEBÄR INFORMATIONENS ”SKYDDSVÄRDE”?

2.3.2.1 Definition

Publika molntjänster kan användas för många olika ändamål och för många olika typer av information. Det finns information som är särskilt skyddsvärd, av t.ex. juridiska, säkerhetsmässiga eller kommersiella skäl. Därför krävs en noggrann analys av vilken information som för den enskilda molntjänstkunden är lämplig att lägga i molnet och därmed exponeras för den juridiska informationssäkerhetsrisk som identifierats. Informationens skyddsvärde definieras i Folke©-modellen som:

> **Informationens ”skyddsvärde”** = den betydelse och det värde som informationen har för informationsinnehavaren (dvs. molntjänstkunden) baserat på rättsliga, konkurrensmässiga eller kommersiella konsekvenser av ett obehörigt utlämnande.[11]

2.3.2.2 Exempel på relevanta riskfaktorer (ej uttömmande)

Vi menar att bl.a. följande faktorer påverkar informationens skyddsvärde:

- **Informationsklassning, tillämpliga lagar och regler:**
  - Är det utrett vilka lagar och regler som är tillämpliga (inklusive sektorspecifika sekretesskrav såsom bank- och försäkringssekretess och/eller annan lagreglerad sekretess såsom exempelvis inom hälso- och sjukvård)?
- **Dess känslighet:**
  - Vad blir konsekvenserna av ett obehörigt utlämnande?
    - För Sveriges nationella säkerhet
    - För Sveriges finansiella stabilitet och banksystem
    - För samhällets funktionalitet om verksamheten är att betrakta som en ”samhällsbärande verksamhet”[12]
    - För integritetsskyddet för det fall informationen utgör personuppgifter, dvs. riskerna för de registrerades fri- och rättigheter, i synnerhet mot bakgrund av:
      - uppgifternas natur/känslighet för den enskilde,
      - om antalet registrerade eller mängden uppgifter skapar risk för kartläggning/övervakning på makro- eller individnivå,

11 Ett ”obehörigt utlämnande” avser utlämnande eller tillgängliggörande som genomföras i strid med informationsinnehavarens (dvs. molntjänstkundens) önskemål och/eller i strid med rättsregler som är tillämpliga för informationsinnehavaren.

12 Begreppet används av Försäkringskassan i syfte att omfatta både samhällsviktig verksamhet och sådana funktioner som i sig inte omfattas av den definitionen, men som samhällsviktig verksamhet är beroende av. Begreppet omfattar även s.k. säkerhetskänslig verksamhet enligt definitionen i säkerhetsskyddslagen (2018:585). Se vidare Försäkringskassan, *Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt,* (2019).

    - om sammanhanget för behandlingen eller dess ändamål medför särskilda integritetsrisker[13], och/eller
    - om uppgifter har exkluderats på grund av sin känslighet, och sådan känslig information ändå kan utläsas från själva utlämnandet.[14]
  - För det skyddsintresse som omfattas av sekretessbestämmelser i lag.
  - För tredje man om informationen omfattas av sekretessåtagande gentemot denne.
  - För molntjänstkundens konkurrenskraft (försämras denna t.ex. vid röjande av företagshemlighet eller äventyrande av immateriella rättigheter?)

  - Är informationen tillgänglig via andra publika källor?

- **Kommersiellt värde** både i sig själv och i form av metadata eller aggregerad med annan information, och huruvida avtalet innebär risk för att detta ”skänks bort” till leverantören. En sådan bestämmelse skulle kunna innebära ett obehörigt beslut att ”skänka” bort bolagets tillgångar till en leverantör.

- **Kundens kontinuitets- och exitplanering**

  - Vilken förväntad längd avseende led-/omställningstid vid leverantörsbyte gäller för molntjänsten?

  - Kan leverantörsbyte/flytt genomföras oberoende av och utan stöd från leverantören?

  - Finns det en detaljerad och användbar exitplanering hos molntjänstkunden?

2.3.2.3 Exempel på hur kan informationens skyddsvärde påverkas/minska (ej uttömmande)

Informationens skyddsvärde avgörs huvudsakligen utifrån följande faktorer:

1) Vilken information som hanteras i molntjänsten,

2) vilka lagar och regler som är tillämpliga på informationen som hanteras i molntjänsten,

3) hur informationen skyddas, och

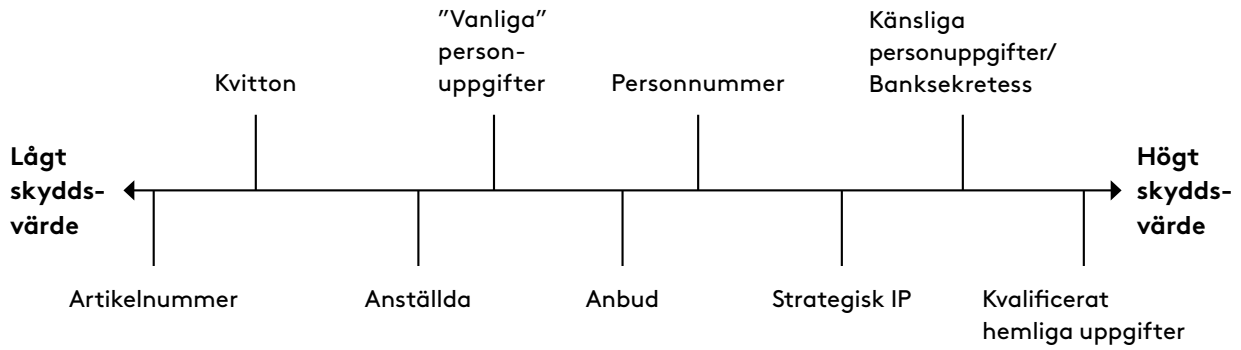
---

13 Exempelvis behandling som avser en privatpersons personliga och ekonomiska förhållanden som sker inom bank- och försäkringsväsendet eller om ändamålet med behandlingen är att diskriminera en person genom att utestänga denne från en viss tjänst (s.k. spärrlista).

14 Ett exempel på detta är om en uppgift om att en viss person har besökt en psykiatrisk mottagning röjs. Även om det inte framgår om eller på vilket sätt personen i fråga är sjuk, för att den informationen exkluderats, skulle sannolikt den röjda uppgiften typiskt sett ändå anses vara en hälsouppgift (dvs. en känslig personuppgift).

4) hur viktig och känslig informationen är för molntjänstkundens kommersiella verksamhet och för andra skyddsintressen (t.ex. nationell säkerhet, finansiell stabilitet, externa samarbetspartners, registrerade).

Följande bild illustrerar olika typer av information och hur de typiskt sett placeras på Folke©-modellens X-axel utifrån dess skyddsvärde:



Figur 2.3: Närmare beskrivning av Folke©-modellens X-axel.

Informationens skyddsvärde kan i allra högsta grad påverkas av molntjänstkunden, primärt genom att denne:

- ändrar eller anpassar vilken information som hanteras av molntjänstleverantören, och/eller

- överväger och implementerar ytterligare tekniska och organisatoriska säkerhetsåtgärder (utöver leverantörens standardlösningar) för att skydda informationen från de konsekvenser som kan följa av ett oönskat utlämnande/röjande.

2.3.3 VILKEN RISKAPTIT HAR VERKSAMHETEN?

Vid bedömningen av vilken riskbenägenhet och riskaptit som kan anses vara lämplig, bör kunden ta sin utgångspunkt i vilka lagar och regler som är tillämpliga för den aktuella verksamheten och på den information som behandlas, men även beakta marknadsspecifika och kommersiella faktorer. Riskaptiten påverkas naturligtvis även av de fördelar som molntjänstkunden antar att molntjänster innebär i förhållande till alternativa lösningar, såsom minskade kostnader, förkortad time-to-market eller ökad flexibilitet.

Mot denna bakgrund får exempelvis en statlig myndighet typiskt sett antas ha en låg riskbenägenhet och riskaptit, medan ett bolag på en oreglerad och starkt konkurrensutsatt marknad däremot kan och bör sannolikt vara benäget att ta en högre risk i detta avseende.

3. Generella juridiska överväganden rörande publika molntjänster

3.1 Inledning

Diskussionerna kring huruvida en verksamhet ska övergå till att använda molntjänster initieras ofta med fokus på de fördelar som molntjänster antas kunna innebära för verksamheten. Det kan exempelvis vara fråga om snabbare ”time-to-market”, ökad flexibilitet och skalbarhet, minskade kostnader och i vissa fall förhöjd teknisk säkerhet.

Samtliga verksamheter som överväger att använda sig av publika molntjänster bör dock inledningsvis göra ett antal *generella juridiska överväganden* avseende de risker som sådan användning innebär.

Mot denna bakgrund redogör vi i detta kapitel för hur en molntjänstkund bör förhålla sig till den särskilda risk som är kopplad till användningen av utländska molntjänster, nämligen den s.k. *jurisdiktionsrisken* (avsnitt 3.2) och de risker som typiskt sett aktualiseras om den information som behandlas i molnet utgör *personuppgifter* (avsnitt 3.3). Vidare behandlas i avsnitt 3.4 hur riskerna med användning av molntjänster kan påverkas genom olika *tekniska säkerhetslösningar* för molntjänster och därefter går vi närmare in på hur en molntjänstkund bör förhålla sig till de vanligt förekommande riskerna som följer av *molntjänstleverantörers standardavtal* (avsnitt 3.5).

3.1.1 OLIKA MOLNTJÄNSTER INNEBÄR OLIKA RISKER OCH AVTALSUTMANINGAR

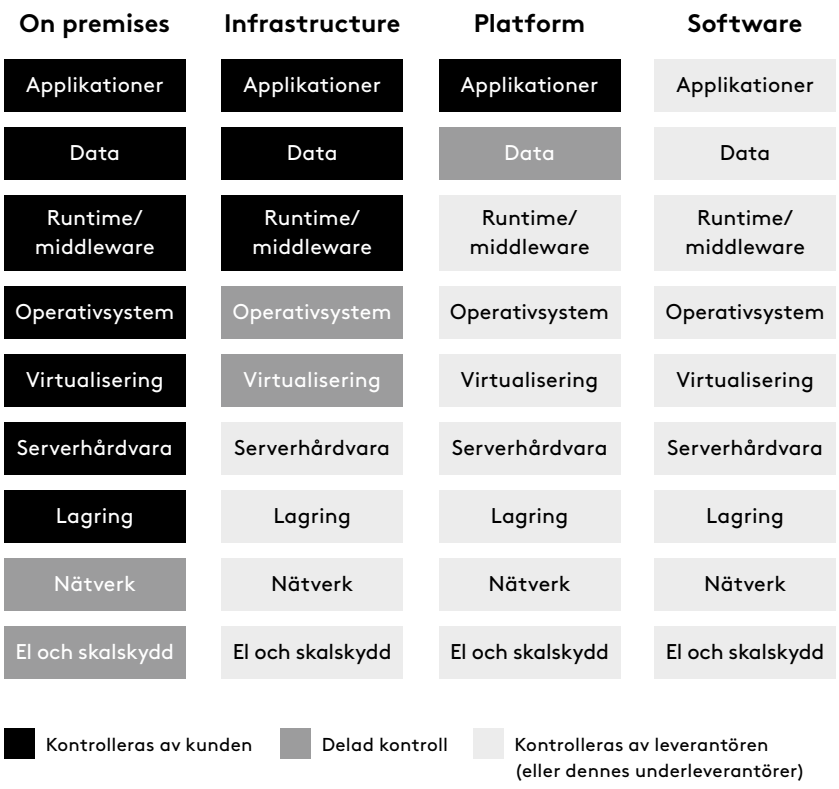
Den riskbedömning som diskuteras i denna rapport varierar beroende på vilken typ av molntjänst som är aktuell. Det finns därför anledning att redogöra för några av de vanligaste typerna av molntjänster som är aktuella på marknaden idag.

3.1.1.1 Typer av molntjänster

Molntjänster delas traditionellt in i ”infrastruktur-som-tjänst” (Infrastructure-as-a-service, ”**IaaS**”), ”plattform-som-tjänst” (Platform-, ”**PaaS**”) och ”mjukvara-som-tjänst” (Software-, ”**SaaS**”). Utöver dessa tre huvudkategorier finns även tjänster som inordnas under andra ”as a services”-kategorier, exempelvis Functions-, Network-, Data- och Backend-as-a-service. Gemensamt för dessa är att en extern leverantör

tar ansvar för hanteringen av ett visst eller flera lager[15] i den s.k. stack som behövs för att kunna leverera it-tjänster. Dessa tjänster kan kontrasteras mot det tidigare dominerande sättet att hantera it-tjänster, när samtliga lager av hård- och mjukvara hanterades inom kundens organisation och ibland även lokaler, dvs. genom en on premises-lösning.

Nedanstående bild illustrerar de olika lagren i en sådan stack och vem som ansvarar för dem i olika molntyper. Det kan förekomma att kontrollen över vissa lager är delad mellan leverantören och kunden, exempelvis för IaaS-lösningar där leverantören tillhandahåller operativsystem och virtualisering för den fysiska hårdvaran[16], medan kunden, åtminstone i vissa fall, ansvarar för operativsystem i den virtualiserade hårdvaran och även kan virtualisera denna i ytterligare steg. Även om kunden då utövar kontroll av vad som lagras på den virtualiserade hårdvaran är det i praktiken omöjligt för kunden att ha *exklusiv* kontroll över information som lagras i en molntjänst, så länge informationen lagras på ett lagringsmedium som molntjänstleverantören har fysisk tillgång till.



Figur 3.1: Vem som i olika molntyper ansvarar för de olika lagren i den stack som behövs för att kunna leverera it-tjänster.

15 Med *lager* avses här teknologier och resurser som bygger på andra teknologier och resurser som utgör lägre lager, och i sin tur utgör grund för andra, högre lager i en stack av sådana teknologier och resurser.

16 Med *virtualisering* avses teknik som låter mjukvara utgöra virtuell hårdvara, på så sätt att en särskild programvara (hypervisor) kan låta flera olika operativsystem finnas och köra samtidigt på en fysisk dator, och koordinerar hur mycket varje sådant system får förbruka av den fysiska datorns olika resurser. Detta gör det möjligt för dessa virtualiserade system att tas i drift, ändras, säkerhetskopieras och flyttas med ett minimum av manuell administration.

IaaS-tjänster: En tjänsteleverantör hanterar hårdvara för beräkning, lagring och nätverk i traditionella datacenter, och gör denna kapacitet tillgänglig för kunder på så sätt att kunden kan få tillgång till valfri mängd kapacitet på ett enkelt eller till och med automatiserat sätt. I princip kan molntjänstkunden beställa en eller flera serverdatorer, bestyckade på valfritt sätt samt datalagring för och nätverk till dessa. Molntjänstkunden bestämmer sedan vad som ska köras på dessa datorer, från operativsystem och uppåt i ovanstående stack.

Den stora skillnaden mellan IaaS-tjänster och forna tiders it-drift eller s.k. co-location (dvs. när kunden placerar sin egenägda hårdvara i en tjänsteleverantörs driftsmiljö) är att de serverdatorer som kunden får tillgång till, inte motsvaras av faktisk fysisk hårdvara, utan är virtualiserade. Med hjälp av virtualisering kan en molntjänsteleverantör erbjuda långt flera virtuella servrar än det antal fysiska servrar som denne förfogar över. En annan fördel är att molntjänstkunderna med ett minimum av administration kan skala upp eller ned sitt användande av kapaciteten.

PaaS-tjänster: I en IaaS-lösning är molntjänstkunden ansvarig för att installera, konfigurera och administrera alla lager av programvara som behövs för en it-tjänst (operativsystem, databashanterare, webbservrar m.m.). Det är inte alla kunder som har behov av (eller fallenhet för) att sköta sådan hantering. Inte ens för molntjänstkunder som utvecklar egna it-tjänster är det alltid befogat att lägga resurser på de undre lagren i den stack av olika teknologier som krävs för att leverera it-tjänster. Istället vill verksamheten kunna utveckla tjänster ovanpå en bestämd plattform av funktionalitet som en molntjänstleverantör ansvarar för (dvs. PaaS), och på så vis fokusera på de övre lagren i stacken. En sådan plattform kan exempelvis bestå av ett ramverk för att utveckla webbtjänster i något visst programspråk. Vissa plattformar, exempelvis sådana som använder stora datamängder för analys eller artificiell intelligens, är särskilt lämpade att leverera som en tjänst, då dessa är svåra eller omöjliga för en kund att realisera själv.

De stora molntjänstleverantörerna på den amerikanska marknaden (Amazon Web Services, Google Cloud Platform och Microsoft Azure) erbjuder hundratals olika tjänster, varav vissa kan betecknas som IaaS-tjänster och andra PaaS-tjänster. En leverantörs tjänster är ofta utformade på liknande sätt och interagerar väl med varandra, varför en viss inlåsningseffekt till den specifika leverantören lätt uppstår. För varje nytt behov av någon form av molntjänst, är det typiskt sett ”enklast” att välja en tjänst från den befintliga molntjänstleverantören.

SaaS-tjänster: IaaS- och PaaS-tjänster vänder sig i allt väsentligt till kunder som har förmåga och behov av att utveckla och utforma egna it-tjänster. Många kunder – även de som använder IaaS/PaaS för vissa ändamål – har dock inget behov av att skräddarsy all sin it. Många it-tjänster kan därför utformas på i stort sätt samma sätt för en bred marknad, exempelvis för ordbehandling, samarbetsverktyg eller kundvård. SaaS-leverantörer tillhandahåller molntjänster som kan användas direkt av slutanvändare hos molntjänstkunden för sådana ändamål. SaaS-tjänster tillhandahålls normalt sett via ett webbgränssnitt eller

mobilappar som kontinuerligt uppdateras. Molntjänstleverantören tar hand om samtliga lager i stacken för att tillhandahålla den funktionalitet som behövs. Exempel på SaaS-tjänster med breda tillämpningsområden är Microsoft 365, Salesforce, Workday och Google Apps.

3.1.1.2 Kontroll över data och infrastruktur

IaaS- och PaaS-tjänster kan anpassas och användas på flera olika sätt, bl.a. beroende på hur en applikation designas och sätts upp på infrastrukturen. Det är möjligheten att som kund styra över viktiga aspekter såsom var, hur och hur länge informationen lagras, vart den skickas, hur kryptering och andra tekniska åtgärder används samt informationshantering i övrigt, som gör att en IaaS-/PaaS-tjänst på ett avgörande sätt skiljer sig från SaaS-orienterade tjänster. Detta innebär att PaaS- och framförallt IaaS-orienterade tjänster i en sammanlagd riskbedömning erbjuder större möjligheter att införa skyddsåtgärder som adresserar identifierade risker jämfört med SaaS-tjänster. I en SaaS-tjänst har molntjänstkunden typiskt sett endast viss insyn i hur informationen hanteras och än mindre möjlighet att styra vilka skyddsåtgärder som ska implementeras.

Det ska även tilläggas att många SaaS-leverantörer i sin tur använder sig av andra PaaS- och IaaS-leverantörer. En sådan SaaS-leverantör har därför inte exklusiv kontroll över exempelvis var och hur länge data lagras eftersom även dennes underleverantörer har faktisk kontroll över datalagringen.

3.2 Jurisdiktionsrisken

3.2.1 INLEDNING

I detta avsnitt fokuserar vi på en specifik risk i anknytning till molntjänster som tillhandahålls av utländska leverantörer, nämligen den s.k. jurisdiktionsrisken. Jurisdiktionsrisken är en central del av den sammanvägda leverantörsrisken som beskrivs i avsnitt 2.3 ovan. Med jurisdiktionsrisk menar vi dock enbart risken för ett obehörigt utlämnande och röjande enligt främmande rätt i strid med lagar och regler som molntjänstkunden lyder under.

Jurisdiktionsrisk har alltid existerat i någon utsträckning i förhållande till it-leverantörer som omfattas av utländska regler och jurisdiktion, men har särskilt aktualiserats i fråga om amerikanska leverantörer dels med anledning av ökad överföring av personuppgifter till USA, dels med anledning av att amerikansk lagstiftning ändrades (eller åtminstone klargjordes) år 2018 genom antagandet av CLOUD Act[17]. Lagändringen innebar att amerikanska myndigheter under vissa förutsättningar kan få tillgång till uppgifter även om de finns lagrade

17 Clarifying Lawful Overseas Use of Data Act (H.R.4943).

utanför USA och att ett sådant utlämnande kan ske utan föregående information, godkännande och/eller rättslig prövning enligt svensk rätt.

Den 16 juli i år (2020) meddelade dessutom EU-domstolen dom i mål C-311/18, *Schrems II*. Genom domen har EU-domstolen bl.a. ogiltigförklarat det beslut som låg till grund för en av de huvudsakliga mekanismerna för överföring av personuppgifter till USA, nämligen EU-kommissionens beslut om adekvat skyddsnivå, *Privacy Shield*. Domstolen prövade även giltigheten av EU-kommissionens beslut som möjliggör överföring av personuppgifter till tredjeland med stöd av standardavtalsklausuler.[18] Kommissionens beslut om standardavtalsklausulerna ansågs förvisso vara giltigt, men bedömdes även medföra sådana skyldigheter som innebär att möjligheterna att överföra personuppgifter till tredjeland är betydligt mer begränsade än vad många verksamheter hittills har antagit.

Mot denna bakgrund har vi i detta avsnitt också valt att fokusera på just konsekvenserna av amerikansk lagstiftning. Det ska dock nämnas att motsvarande problem även finns i många andra länder och att vare sig standardavtalsklausulerna eller EU-domstolens avgörande i Schrems II är begränsat till att avse enbart USA.

Frågan är alltså om och i vilken utsträckning anlitandet av en amerikansk, eller för all del även en indisk eller kinesisk, molntjänstleverantör kan vara förenligt med tillämpliga lagar och regler för en svensk molntjänstkund, trots förekomsten av jurisdiktionsrisken. I detta avsnitt har vi fokuserat på bedömningen i förhållande till dataskyddsförordningen som är en central reglering för jurisdiktionsrisken. Dataskyddsförordningen är också generell på det sättet att den aktualiseras vid de flesta överföringar till USA eftersom så gott som all information innehåller någon form av personuppgifter.

För att kunna göra en sådan bedömning krävs ingående förståelse och analys av relevant amerikansk lagstiftning. Vi har i korta drag sammanfattat relevanta delar av amerikansk rätt i avsnitten 3.2.2 och 3.2.3 nedan. Det bör understrykas att vår sammanfattning inte beaktar annan utländsk lagstiftning än de amerikanska rättsakterna Stored Communication Act (”**SCA**”) och CLOUD Act samt de rättsakter som inom ramen för amerikansk underrättelseverksamhet diskuteras i Schrems II-domen, dvs. Section 702 Foreign Intelligence Surveillance Act (”**FISA**”), Executive Order 12333 (”**E.O. 12333**”) samt Presidential Policy Directive 28 (”**Presidentdirektiv 28**”).

3.2.2 OM UTLÄMNANDE AV PERSONUPPGIFTER TILL USA OCH CLOUD ACT

3.2.2.1 CLOUD Act och SCA

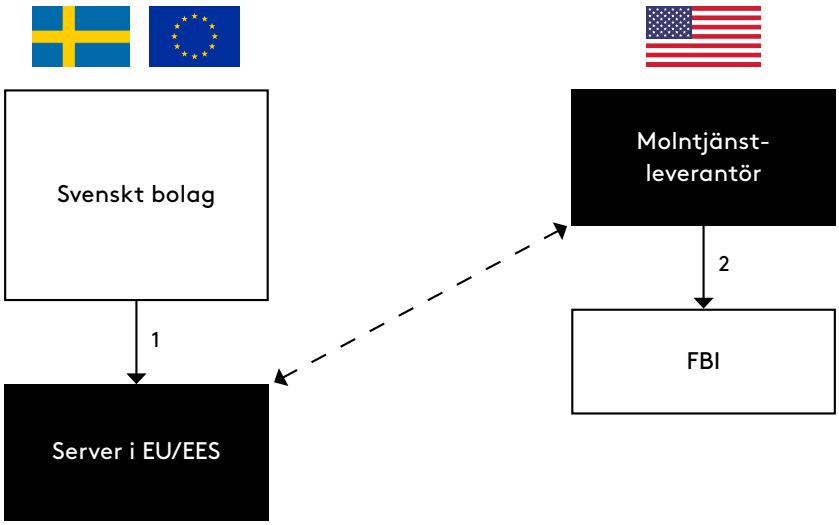
Enligt såväl svensk rätt som enligt EU-rätten finns särskilda rättssäkerhetsåtgärder som aktualiseras när personuppgifter lämnas ut

18 Artikel 46.2 c dataskyddsförordningen.

till myndigheter i ett brottsbekämpande syfte eller för syften som har med nationell säkerhet att göra. Vad gäller utlämnande från EU/EES till myndigheter i tredjeland i brottsbekämpande syften, är huvudregeln att detta endast får ske med stöd av internationella överenskommelser (t.ex. genom ett MLAT).[19]

Genom CLOUD Act tydliggjordes emellertid att företag som lyder under amerikansk jurisdiktion enligt SCA[20] kan åläggas att lämna ut information till amerikanska myndigheter, oavsett var uppgifterna finns under förutsättning att uppgifterna är inom företagets kontroll (”possession, custody or control”). Detta gäller således även om personuppgifterna rör en s.k. icke-amerikansk person[21] och lagras på svenskt territorium eller inom EU/EES.

En typisk CLOUD Act-situation kan illustreras med följande figur (jfr. med ”Överföring till tredjeland” i avsnitt 3.2.3 nedan):



Figur 3.2: CLOUD Act-situationen.

CLOUD Act innebär därmed att amerikanska myndigheter inte behöver ta stöd av internationella överenskommelser för att begära att molntjänstleverantörer lämnar ut uppgifter som lagras i andra länder. Begäran om utlämnande kan prövas av amerikansk domstol och uteslutande enligt amerikansk rätt.[22] En skyldighet att lämna ut uppgifter enligt amerikansk rätt kan dessutom förenas med ett förbud för molntjänstleverantören att informera sin kund om att en begäran inkommit eller att ett utlämnande har skett, en s.k. gag order.

19 Artikel 48 dataskyddsförordningen.

20 Stored Communications Act reglerar förutsättningar för utlämnande av vissa uppgifter från bl.a. molntjänstleverantörer.

21 Se begreppet ”*non-United States person*” i CLOUD Act.

22 I denna prövning kan domstolen i viss begränsad omfattning ta hänsyn till att utlämnandet kan strida mot bestämmelser i andra länder genom s.k. *comity analysis*, en rättsprincip under common law. Den närmare innebörden av denna princip är dock oklar.

En amerikansk molntjänstleverantör som behandlar personuppgifter, i egenskap av antingen personuppgiftsbiträde eller underbiträde, för den personuppgiftsansvariges räkning kan därför komma att bli skyldig att lämna ut personuppgifter till amerikanska myndigheter i strid med svensk rätt och EU-rätt.

CLOUD Act innehåller förvisso förutsättningar för att amerikanska myndigheter ska kunna ingå särskilda ömsesidiga avtal (s.k. executive agreements) med andra länder om utlämnade av personuppgifter för brottskämpande syfte, men såvitt känt har endast ett sådant avtal ingåtts, nämligen mellan Storbritannien och USA. De bestämmelser i CLOUD Act som gäller sådana avtal är således inte tillämpliga i förhållande mellan USA och EU eller mellan USA och Sverige.

3.2.2.2 Vissa begränsningar i CLOUD Act

CLOUD Act innebär alltså att amerikanska myndigheter kan kräva att en amerikansk molntjänstleverantör lämnar ut information som leverantören har kontroll över, oavsett var informationen lagras. Det finns dock ett antal begränsningar i de amerikanska myndigheternas rätt att kräva att sådan information lämnas ut. Dessa begränsningar avser framför allt hur en begäran om utlämnande av information ska vara utformad och vad den får avse. Det bör understrykas att begränsningarna inte ändrar på det förhållande att molntjänstkunden berövas kontroll över den information som hanteras i molntjänsten och att en obehörig tredje man, nämligen amerikansk myndighet, har tillgång till information när amerikansk domstol anser att förutsättningar för sådan tillgång föreligger. Några av de mest relevanta begränsningarna är:

- För det första måste en begäran avse information som är hänförlig till en *pågående utredning* inom amerikansk jurisdiktion.

- För det andra kan en begäran endast omfatta sådan information som molntjänstleverantören har *kontroll över vid tidpunkten för begäran*.

- För det tredje kan amerikanska myndigheter inte kräva att molntjänstleverantören, i syfte att senare lämna ut informationen, *lagrar mer eller annan information* än vad molntjänstleverantören annars skulle göra.

- För det fjärde kan en amerikansk myndighet inte kräva att molntjänstleverantören *genomför ändringar* i sin tjänst, sitt system eller överför informationen från en server till en annan.

- För det femte ska en begäran vara *avgränsad i omfattning* och *precis till sin utformning*. Myndigheten måste därför specificera (i) personen som avses, (ii) typen av information som avses, (iii) den geografiska platsen där informationen lagras, och (iv) under vilken tidsrymd transaktionerna ägt rum.

3.2.2.3 Relevanta bestämmelser i dataskyddsförordningen

I dataskyddsförordningen är det primärt följande bestämmelser som aktualiseras med anledning av den del av jurisdiktionsrisken som uppstår till följd av CLOUD Act:

- Principen om laglig behandling (artikel 5.1 a)
- Förbud mot överföringar och utlämnanden som inte är tillåtna enligt unionsrätten (artikel 48)
- Skyldigheten att anlita personuppgiftsbiträden som lämnar "*tillräckliga garantier*" (artikel 28.1 och 28.4)

a) Principen om laglig behandling (artikel 5.1 a)

Personuppgifter ska, enligt principen i artikel 5.1 a dataskyddsförordningen behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Kravet på att behandlingen ska vara laglig innebär i första hand att uppgifterna ska behandlas i enlighet med dataskyddsförordningen och kompletterande nationell rätt.

Utlämnande av personuppgifter till utländska myndigheter som sker utan stöd i dataskyddsförordningen kan därför strida mot principen om laglighet. När begäran om utlämnande riktas mot personuppgiftsbiträdet (som i typsituationen är molntjänstleverantören) är det denne som måste göra bedömningen om utlämnandet är förenligt med principen om laglighet. Såvida leverantören inte har stöd i avtalet med kunden, fattar leverantören detta beslut i egenskap av personuppgiftsansvarig (jfr artikel 28.10 dataskyddsförordningen).

Det anses emellertid inte heller förenligt med principen om laglighet att överföra eller lämna ut personuppgifter till någon annan, om det kan antas att denne kommer att behandla personuppgifterna i strid med dataskyddsförordningen.[23] Ett utlämnande till ett personuppgiftsbiträde som kan tvingas att lämna ut personuppgifter i strid med artikel 48 dataskyddsförordningen (se underavsnitt b) nedan), kan därför komma i konflikt med principen om laglighet. För att ett sådant utlämnande ska vara olagligt, krävs dock att den personuppgiftsansvarige kan anta att ett sådant utlämnande kan komma att ske. Detta gäller även i situationer där personuppgiftsbiträdet i sin tur använder sig av en amerikansk molntjänstleverantör som underleverantör, vilken kan tvingas att lämna ut personuppgifter i strid med artikel 48.

Principen om laglighet har ännu inte prövats av EU-domstolen i detta avseende. Den aktualiserades inte heller i Europeiska dataskyddsstyrelsens ("**EDPB**") och Europeiska dataskyddsombudsmannens ("**EDPS**") yttrande angående CLOUD Act och dess relation till det europeiska dataskyddsregelverket (se vidare underavsnitt b) nedan).

23 Se Öman, Sören, *Dataskyddsförordningen (GDPR) m.m. En kommentar* (2019), s. 113.

Enligt vår bedömning är det – trots avsaknaden av vägledande uttalanden – inte uteslutet att det kan strida mot principen om laglighet att lämna ut personuppgifter till en molntjänstleverantör som i sin tur kan komma att tvingas lämna ut personuppgifter i strid med dataskyddsförordningen. Detta är, enligt vår uppfattning, en fråga om riskbedömning. I en sådan bedömning bör beaktas dels sannolikheten för att ett utlämnande i strid med dataskyddsförordningen förverkligas, dels vilka konsekvenser ett sådant utlämnande innebär för de registrerade (angående dessa risker, se vidare avsnitt 3.2.4.1 nedan).

b) Förbud mot överföringar och utlämnanden som inte är tillåtna enligt unionsrätten (artikel 48)

I artikel 48 dataskyddsförordningen anges att:

"*[d]omstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt* [kapitel V om överföring av personuppgifter till tredjeländer eller internationella organisationer]."

I juli 2019 publicerade EDPB och EDPS ett gemensamt yttrande avseende CLOUD Act och dess relation till det europeiska dataskyddsregelverket.[24] EDPB och EDPS framhåller att ett utlämnande av personuppgifter till amerikanska myndigheter enligt CLOUD Act kräver stöd i en internationell överenskommelse. Genom en internationell överenskommelse kan nämligen ett utlämnande ske med stöd av bestämmelser i nationell rätt och den rättsliga grunden att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse.[25]

EDPB:s och EDPS:s preliminära slutsats, som vi instämmer i, är att ett utlämnande till amerikanska myndigheter utan stöd i en internationell överenskommelse endast kan ske när det föreligger exceptionella omständigheter och där utlämnandet är nödvändigt för att skydda intressen som är av grundläggande betydelse för den registrerade, dvs. fara för liv och hälsa enligt artikel 6.1 d dataskyddsförordningen.

Då begäran om utlämnande riktas mot personuppgiftsbiträdet eller dess underbiträde, är det i första hand denne som måste göra bedömningen av om det finns rättsligt stöd för utlämnandet. Ett eventuellt utlämnande av personuppgiftsbiträdet sker alltså under dennes självständiga personuppgiftsansvar. Som nämns nedan kan emellertid

24 EDPB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, publicerad den 10 juli 2019, ref. OUT2019-0007, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf, hämtad den 3 september 2020.

25 Artikel 6 dataskyddsförordningen.

den personuppgiftsansvarige, vid bedömning om personuppgiftsbiträdet eller dess underbiträde kan lämna tillräckliga garantier för att följa dataskyddsförordningen, behöva ta hänsyn till risken för att personuppgiftsbiträdet eller dess underbiträde kan komma att behöva lämna ut personuppgifterna i strid med dataskyddsförordningen.[26]

EDPB och EDPS har i det ovan nämnda yttrandet ansett att hänvisningen till ”*andra grunder för överföringen*” innebär att utlämnandet kan prövas enligt de grunder för överföring till tredjeland som anges i artikel 49 dataskyddsförordningen. EDPB och EDPS konstaterar emellertid att stöd för utlämnande enligt CLOUD Act i princip saknas i artikel 49. Ett sådant utlämnande kan eventuellt vara förenligt med artikel 48, endast om det föreligger exceptionella omständigheter och utlämnandet är nödvändigt för att skydda den registrerades grundläggande intressen, dvs. vid fara för liv och hälsa.[27]

Bestämmelsen i artikel 48 dataskyddsförordningen om överföringar och utlämnanden som inte är tillåtna enligt unionsrätten gäller både personuppgiftsansvariga och personuppgiftsbiträden. Den situation som är aktuell inom ramen för den här rapporten är dock när begäran om utlämnande riktas mot en molntjänstleverantör som omfattas av amerikansk jurisdiktion och som behandlar personuppgifter som personuppgiftsbiträde eller underbiträde för en svensk molntjänstkunds räkning och uppgifterna finns sparade inom EU/EES. Det är för närvarande oklart om bestämmelsen ska tillämpas även när personuppgifterna redan har förts ut till tredjeland av den personuppgiftsansvarige eller ett personuppgiftsbiträde och myndigheterna i mottagarlandet därefter begär tillgång till uppgifterna.[28]

Anlitandet av ett personuppgiftsbiträde eller godkännandet av ett underbiträde, som omfattas av amerikansk jurisdiktion, innebär inte i sig enligt vår uppfattning att personuppgifter lämnas ut till amerikanska myndigheter. Det kan dock medföra en förhöjd risk för att personuppgifter i ett senare skede kommer att lämnas ut till amerikanska myndigheter av personuppgiftsbiträdet. Vi bedömer dock att förbudet mot att lämna ut personuppgifter i artikel 48 dataskyddsförordningen inte i sig utgör ett hinder mot anlitande av sådana personuppgiftsbiträden eller underbiträden.

c) Skyldigheten att endast anlita personuppgiftsbiträden som lämnar ”tillräckliga garantier” (artikel 28.1 och 28.4)

En personuppgiftsansvarig får endast anlita personuppgiftsbiträden som ”*ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas*”.[29]

---

26 Se artikel 28.1 dataskyddsförordningen.

27 Artikel 49.1 f dataskyddsförordningen.

28 Se Kuner et al, *The General Data Protection (GDPR) A Commentary* (2020), s. 832.

29 Artikel 28.1 dataskyddsförordningen.

Skyldigheten att endast anlita personuppgiftsbiträden som lämnar sådana tillräckliga garantier gäller den personuppgiftsansvarige.[30] Det innebär att den personuppgiftsansvarige åläggs en skyldighet att granska personuppgiftsbiträden innan de anlitas. Om ett anlitat personuppgiftsbiträde i något steg behandlar personuppgifter i strid med dataskyddsförordningen kan det således medföra ansvar för överträdelse av dataskyddsförordningen och sanktioner för den personuppgiftsansvarige, redan på den grunden att denne inte har försäkrat sig om att det anlitade personuppgiftsbiträdet har lämnat tillräckliga garantier. Detta gäller även i förhållande till underbiträden. Den personuppgiftsansvarige måste därför också granska och godkänna alla de underbiträden som anlitas av ett personuppgiftsbiträde.[31]

Kraven på tillräckliga garantier avser ”*tekniska och organisatoriska åtgärder*”, vilket i första hand avser åtgärder som har samband med informationssäkerheten kring behandlingen.[32] Av skäl 81 i dataskyddsförordningen framgår att det avser garantier ”*i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser* [...] *bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter*”.[33]

Det kan antas att det i första hand handlar om åtgärder som vidtas för att förhindra ”*oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats*”.[34]

Skyldigheten att endast anlita biträden och underbiträden som lämnar tillräckliga garantier är dock inte begränsad till garantier avseende teknisk informationssäkerhet, vilket vi menar är en vanlig missuppfattning. Att tillräckliga garantier avser en bredare bedömning framgår inte minst av att syftet med de tekniska och organisatoriska åtgärderna ska vara att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Det är, enligt vår uppfattning, uppenbart att formuleringen ”tillräckliga garantier” ger utrymme för en bedömning i det enskilda fallet.

Personuppgiftsbiträden omfattas, som nämnts ovan, uttryckligen av förbudet i artikel 48 mot att överföra eller lämna ut personuppgifter enligt beslut från domstol eller myndighet i tredjeland, om inte beslutet grundar sig på en internationell överenskommelse. En avgörande fråga är således om personuppgiftsbiträden och underbiträden är skyldiga att lämna tillräckliga garantier enligt artikel 28.1 och 28.2 dataskyddsförordningen för att dessa genom tekniska och organisatoriska åtgärder ska förhindra ett otillåtet utlämnande enligt artikel 48 dataskyddsförordningen.

---

30 Artikel 28.1 dataskyddsförordningen.

31 Detta följer även av bestämmelserna i artikel 28.2 och 28.4 dataskyddsförordningen.

32 Notera att personuppgiftsbiträden (inklusive underbiträden) även kan visa ”*tillräckliga garantier*” genom anslutning till en godkänd uppförandekod eller certifieringsmekanism, se artikel 28.5 dataskyddsförordningen. Någon sådan relevant uppförandekod eller certifiering existerar emellertid inte i nuläget, såvitt vi känner till.

33 Se även EDPB, *Guidelines 7/2020 on the concept of controller and processor in the GDPR. Version 1.0*, antagen den 2 september 2020, s. 29 f, hämtad den 22 oktober 2020.

34 Artikel 32 dataskyddsförordningen.

Frågan bör besvaras med beaktande av att den personuppgiftsansvarige alltid bär huvudansvaret för personuppgiftsbehandling som sker för dennes räkning. Anlitande av ett personuppgiftsbiträde eller underbiträde påverkar inte detta ansvar.

En annan utgångspunkt är att de registrerades skydd enligt dataskyddsförordningen inte ska försämras på grund av att den personuppgiftsansvarige anlitar ett personuppgiftsbiträde eller underbiträde. Denna utgångspunkt står även i överensstämmelse med en sådan syftestolkning av dataskyddsregleringen som EU-domstolen vid ett flertal tillfällen har gjort.[35] Vidare ska de garantier som ett personuppgiftsbiträde ska lämna enligt artikel 28.1 även omfatta skyddandet av de registrerades rättigheter.

Mot den bakgrunden bör bestämmelsen i artikel 28 dataskyddsförordningen inte tolkas för snävt. Skyldigheten att vidta tekniska och organisatoriska åtgärder bör därför, enligt vår bedömning, även innefatta åtgärder för att förhindra utlämnanden som är otillåtna enligt artikel 48 dataskyddsförordningen. Den personuppgiftsansvarige bör därför se till att endast anlita personuppgiftsbiträden och underbiträden som kan lämna tillräckliga garantier att personuppgifter inte kommer att lämnas ut i strid med artikel 48 dataskyddsförordningen.

Att garantierna som personuppgiftsbiträdet och underbiträdet ska lämna enligt artikel 28.1 ska vara ”tillräckliga” torde innebära att åtgärderna som vidtas för att lämna sådana garantier ska vara proportionerliga i förhållande till riskerna med den behandling som utförs av personuppgiftsbiträdet. Det innebär att man vid bedömningen, bör ta hänsyn till de faktorer som nämns i bestämmelsen om säkerhet i artikel 32 dataskyddsförordningen. I artikel 32 anges att man vid fastställande av vad som avses med lämplig säkerhetsnivå i förhållande till risken med en behandling, ska beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

3.2.2.4 Sammanfattande bedömning av risken för utlämnande

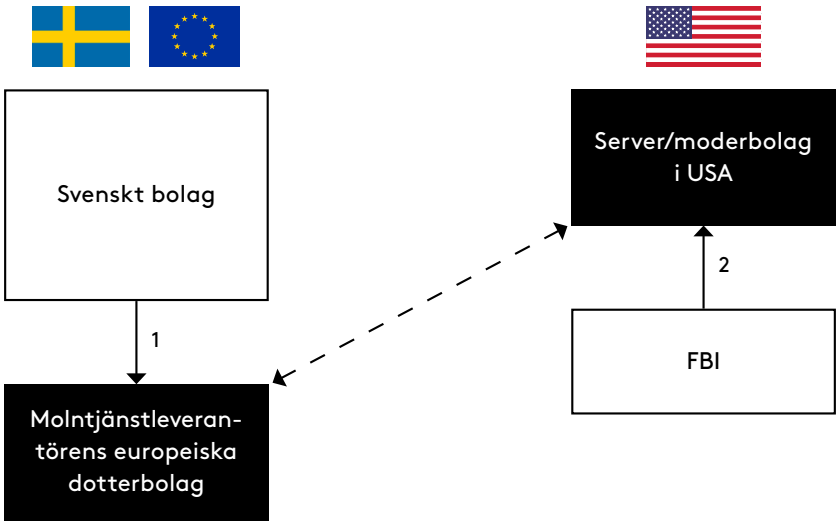
Sammanfattningsvis bör en personuppgiftsansvarig som står i begrepp att anlita eller redan har anlitat en molntjänstleverantör (som personuppgiftsbiträde eller underbiträde) som omfattas av amerikansk jurisdiktion (återigen) bedöma *riskerna med behandlingen* som ska utföras av den amerikanska molntjänstleverantören, bedöma *molntjänstleverantörens möjligheter att uppfylla kraven* enligt dataskyddsförordningen, vidta *riskbegränsande åtgärder*, för att därefter bedöma om de *kvarvarande riskerna är proportionerliga* i förhållande till de faktorer som anges i artikel 32 dataskyddsförordningen. En sådan bedömning sker lämpligast i form av en konsekvensbedömning enligt artikel 35 dataskyddsförordningen (se vidare avsnitt 3.3 nedan).

35 Se exempelvis *Schrems II*, p. 132.

3.2.3 OM ÖVERFÖRING AV PERSONUPPGIFTER TILL USA OCH SCHREMS II

Utmaningen kring CLOUD Act-situationen består främst i att en obehörig myndighet i tredjeland kan komma åt personuppgifter som lagras på svenskt territorium eller inom EU/EES. Jurisdiktionsrisk kan även aktualiseras när personuppgifter överförs till ett tredjeland av den personuppgiftsansvarige eller av personuppgiftsbiträdet på uppdrag av den personuppgiftsansvarige och uppgifterna avlyssnas innan de nått personuppgiftsbiträdet eller därefter begärs ut enligt bestämmelser i det tredjelandet.

Vad som avses med ”Överföring till tredjeland” kan illustreras med följande bild, där vi använt USA som exempel (jfr. med CLOUD Act-situationen i avsnitt 3.2.2 ovan):



Figur 3.3: Överföring till tredjeland.

3.2.3.1 Relevanta bestämmelser i dataskyddsförordningen

De bestämmelser i dataskyddsförordningen som primärt aktualiseras med anledning av den del av jurisdiktionsrisken som uppkommer till följd av överföring till tredjeland är:

- Den allmänna principen för överföring av uppgifter till tredjeländer (artikel 44)
- Tredjelandsöverföring på grundval av ett beslut om adekvat skyddsnivå (artikel 45)
- Tredjelandsöverföring som omfattas av lämpliga skyddsåtgärder (artikel 46)

För att det ska vara tillåtet att överföra personuppgifter till tredjeland krävs enligt artikel 44 dataskyddsförordningen att överföringen har stöd i förordningen. Detta gäller även vid tredjelandsöverföringar från molntjänstleverantören till dennes underbiträden.[36]

För vissa länder har EU-kommissionen fattat beslut om att dessa har s.k. adekvat skyddsnivå för skyddet av personuppgifter. Ett sådant beslut utgör i sig ett stöd för att överföra personuppgifter till det landet.[37] Fram till i juli 2020 var det s.k. Privacy Shield-beslutet[38] ett exempel på ett sådant beslut i förhållande till överföring av personuppgifter till USA, i vilket EU-kommissionen bedömt att skyddsnivån i USA var adekvat om mottagaren hade anmält att denne uppfyllde de krav som ställdes i Privacy Shield, till det amerikanska handelsdepartementet (Department of Commerce).

I avsaknad av beslut om adekvat skyddsnivå, kan även tredjelandsöverföringar ske under förutsättning att den personuppgiftsansvarige eller dess personuppgiftsbiträde har vidtagit lämpliga skyddsåtgärder samt att det finns lagstadgade rättigheter och effektiva rättsmedel tillgängliga för de registrerade.[39] Lämpliga skyddsåtgärder kan exempelvis vara EU-kommissionens standardavtalsklausuler eller bindande företagsbestämmelser (s.k. Binding Corporate Rules, ”**BCR**”).[40]

3.2.3.2 Bakgrunden till Schrems II

I oktober 2015 ogiltigförklarade EU-domstolen i Schrems I-målet föregångaren till Privacy Shield, det s.k. Safe Harbor-beslutet, som grund för överföring av uppgifter till tredjeland då det inte ansågs säkerställa en adekvat skyddsnivå för personuppgifter som överfördes till USA.[41] Detta skedde efter att Maximilian Schrems, en österrikisk medborgare, gjort en anmälan till den irländska dataskyddsmyndigheten med anledning av att Facebook Ireland Ltd vid Schrems användning av Facebooks tjänster, överförde dennes personuppgifter till servrar som tillhör Facebook Inc. i USA, där uppgifterna fortsatte att behandlas.

Efter Safe Harbor-domen fortsatte den irländska tillsynsmyndigheten att utreda Schrems anmälan. Schrems vidhöll att USA inte säkerställer en tillräcklig skyddsnivå för personuppgifter om europeiska Facebookanvändare som överförs till USA och att det därmed fanns skäl för att avbryta den aktuella överföringen. När Safe Harbor ogiltigförklarats, genomförde Facebook istället överföringen på grundval av

36 Notera att en förutsättning för att kraven och skyldigheterna i dataskyddsförordningen ska kunna uppfyllas är att den personuppgiftsansvarige måste ha kontroll, inbegripet bl.a. en spårbarhet, över hur dennes personuppgifter behandlas i alla led.

37 Artikel 45 dataskyddsförordningen.

38 Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

39 Artikel 46.1 och 46.2 dataskyddsförordningen.

40 Artikel 46.2 c dataskyddsförordningen.

41 EU-domstolens dom av den 6 oktober 2015 i mål C-362/14, *Schrems I*.

EU-kommissionens beslut om standardavtalsklausuler[42] (nedan kallat SCC-beslutet). Den irländska tillsynsmyndigheten ansåg därför att det var nödvändigt att även utreda giltigheten av SCC-beslutet. Tillsynsmyndigheten vände sig till Förvaltningsöverdomstolen i Irland som i sin tur begärde ett förhandsavgörande från EU-domstolen.

Mot denna bakgrund ombads EU-domstolen att i Schrems II-målet klargöra tillämpligheten av dataskyddsförordningen på överföringar av personuppgifter som grundar sig på SCC-beslutet, dels vad avser den skyddsnivå som krävs i samband med en sådan överföring, dels vad avser de skyldigheter som åvilar tillsynsmyndigheterna. Därutöver väcktes även frågan om giltigheten av såväl SCC-beslutet som Privacy Shield-beslutet (då det senare hade antagits av EU-kommissionen strax efter att förfarandet inletts).

3.2.3.3 USA:s övervakningsprogram

Begreppet *adekvat skyddsnivå* ska, utan att det krävs att det berörda tredjelandet ska säkerställa en skyddsnivå som är identisk med den som garanteras i EU, förstås så att det krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, *de facto* säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är *väsentligen likvärdig* med den skyddsnivå som garanteras inom EU enligt dataskyddsförordningen jämförd med Europeiska unionens stadga om de grundläggande rättigheterna.[43]

I Schrems II ifrågasattes EU-kommissionens konstaterande i Privacy Shield-beslutet att USA säkerställer en sådan skyddsnivå som är ”*väsentligen likvärdig*”, bl.a. mot bakgrund av de ingrepp som följer av de s.k. *övervakningsprogram* som genomförs i USA baserat på Section 702 FISA[44] och E.O. 12333.

Enligt vad som angetts i den irländska Förvaltningsöverdomstolens begäran om förhandsavgörande möjliggör Section 702 FISA för den amerikanska riksåklagaren och direktören för den nationella underrättelsetjänsten att gemensamt ge tillstånd till övervakning av icke-amerikanska medborgare utanför USA i syfte att inhämta ”*uppgifter från utländsk underrättelseinformation*”. Ett sådant tillstånd får ges under förutsättning att den amerikanska domstolen för underrättelseinformation (FISC) dessförinnan lämnat sitt godkännande. I skälen till

42 Kommissionens beslut 2010/87 av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG, i dess lydelse enligt kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016.

43 Jfr. *Schrems II*, punkt 94.

44 Section 702 i FISA gäller alla leverantörer av elektroniska kommunikationstjänster (se definitionen i 50 USC § 1881(b)(4)) medan E.O. 12333 omfattar elektronisk övervakning, vilket definieras som att ta del av icke-offentlig kommunikation på elektronisk väg utan samtycke från en person som deltar i den elektroniska kommunikationen eller, vid icke-elektronisk kommunikation, utan samtycke från en person som är synligt närvarande på platsen för kommunikationen. Det omfattar dock inte användning av radiopejlingsutrustning som endast syftar till att fastställa var en sändare befinner sig (se definitionen i E.O. 12333, 3.4 (b)).

Privacy Shield-beslutet anges dock att FISC inte godkänner individuella övervakningsåtgärder, utan snarare övervakningsprogram och att dessa typiskt sett inte innehåller någon information om de enskilda personer som den målinriktade övervakningen avser, utan snarare anger kategorier av utländska underrättelseuppgifter. Detta utgör bl.a. grund för övervakningsprogrammen *Prism*[45] och *Upstream*[46].

Vidare anges i begäran om förhandsavgörande att E.O. 12333 möjliggör för den nationella säkerhetsmyndigheten i USA, NSA, att få åtkomst till uppgifter som befinner sig ”in transit” på väg till USA, genom att NSA har åtkomst till undervattenskablar på Atlantens botten. Det framgår att NSA, utan att detta regleras i lag, på så sätt kan samla in och lagra dessa uppgifter redan *innan* de anländer till USA, där de omfattas av bestämmelserna i FISA.

Även Presidentdirektiv 28 utgör ett centralt rättsliga instrument i fråga om USA:s underrättelseverksamhet, eftersom det ska införa ett antal begränsningar av USA:s signalspaningsverksamhet. Av en bilaga till Privacy Shield-beslutet framgår dock att Presidentdirektiv 28 gör det möjligt att genom ”’*bulkinsamling*’ [inhämta] *en relativt stor mängd signalunderrättelser under omständigheter där underrättelsegemenskapen inte kan använda en identifierare som är förknippad med ett specifikt mål för att rikta insamlingen*”. I målet har det betonats att det i den del som avser icke-amerikaner endast anges att underrättelseverksamheten ska vara ”*så riktad som möjligt*”.

3.2.3.4 Utfallet av Schrems II

Vid prövningen av giltigheten av Privacy Shield-beslutet, påpekade EU-domstolen att Privacy Shield, i likhet med Safe Harbor, ger företräde för krav avseende nationell säkerhet, allmänintresset och efterlevnaden av amerikansk lagstiftning. Detta, menade domstolen, möjliggör ingrepp i personers grundläggande rättigheter när deras personuppgifter överförs från EU till USA.

En lagstiftning som innebär ett ingrepp i de grundläggande rättigheterna såsom i det aktuella fallet måste, för att uppfylla kravet på proportionalitet, i synnerhet precisera under vilka omständigheter och på vilka villkor en åtgärd för behandling av personuppgifter får vidtas och på så sätt säkerställa att ingreppet begränsas till vad som är *strikt nödvändigt*.

---

45 Inom ramen för Prism-programmet är leverantörerna av internettjänster, enligt vad den hänskjutande domstolen har konstaterat, skyldiga att tillhandahålla NSA all kommunikation som skickats och mottagits av en ”väljare” (eng. selector), varvid en del av dessa meddelanden även överförs till FBI och CIA.

46 Vad gäller Upstream-programmet konstaterade nämnda domstol att de telekommunikationsföretag som driver internets ”stamnät” – det vill säga kabelnätet, switchar och routrar – är skyldiga att låta NSA kopiera och filtrera trafikflödena på internet i syfte att samla in kommunikation som skickas eller mottas av eller rör en icke-amerikansk medborgare som uppmärksammats av en ”väljare”. Enligt den hänskjutande domstolen har NSA inom ramen för nämnda program åtkomst till såväl metadata som innehållet i de berörda kommunikationerna.

EU-domstolen konstaterade vidare att de begränsningar av skyddet av personuppgifter som följer av USA:s interna bestämmelser om åtkomst till och användning av sådana uppgifter, inte är reglerade på ett sådant sätt att de uppfyller krav som är väsentligen likvärdiga med dem som i EU-rätten uppställs genom proportionalitetsprincipen. De övervakningsprogram som grundar sig på dessa bestämmelser är nämligen inte begränsade till vad som är strikt nödvändigt. Detta då det, när det gäller vissa övervakningsprogram, inte framgår att det föreligger några begränsningar av behörigheten att genomföra dessa övervakningsprogram och att det inte heller finns några garantier för icke-amerikaner som eventuellt omfattas av dessa eftersom de inte innehåller några rättigheter till förmån för berörda personer som kan göras gällande mot amerikanska myndigheter vid domstol. Privacy Shield-mekanismen ansågs inte heller kunna tillhandahålla dessa personer något rättsmedel som är väsentligen likvärdigt med dem som krävs enligt EU-rätten.

Mot bakgrund av dessa skäl ogiltigförklarade EU-domstolen Privacy Shield-beslutet.

Domstolen prövade vidare giltigheten av SCC-beslutet. Detta beslut ansågs vara giltigt, bl.a. mot bakgrund av att EU-kommissionens standardavtalsklausuler ansågs innehålla sådana effektiva mekanismer som i praktiken gör det möjligt att:

- säkerställa att den skyddsnivå som krävs enligt dataskyddsförordningen iakttas, och att

- överföringar av personuppgifter som sker med stöd av dessa dataskyddsbestämmelser kan avbrytas eller förbjudas om bestämmelserna åsidosätts eller är omöjliga att iaktta.

Domstolen framhöll bl.a. att standardavtalsklausulerna innebär dels en skyldighet för den personuppgiftsansvarige och mottagaren av uppgifterna att i förväg kontrollera att den skyddsnivå som krävs enligt EU-rätten iakttas i det berörda tredjelandet, dels en skyldighet för mottagaren att informera den personuppgiftsansvarige, om att mottagaren eventuellt inte kan iaktta standardavtalsklausulerna. I det sistnämnda fallet åligger det den personuppgiftsansvarige att avbryta överföringen av personuppgifter och/eller häva avtalet med mottagaren.

Domstolen uttalade även att man vid bedömningen av den skyddsnivå som säkerställs i samband med en överföring till tredjeland ska ta hänsyn till:

- de avtalsvillkor som överenskommits mellan den personuppgiftsansvarige och mottagaren av överföringen i det berörda tredjelandet, samt

- de relevanta delarna av rättssystemet i det berörda tredjelandet såvitt avser den åtkomst som myndigheterna i det landet eventuellt har till överförda personuppgifter.

Avslutningsvis konstaterade EU-domstolen att kravet på att den skyddsnivå för fysiska personer som säkerställs genom dataskyddsförordningen inte får undergrävas, innebär att det kan bli nödvändigt att komplettera skyddsåtgärderna i dessa standardavtalsklausuler med ”*ytterligare skyddsåtgärder*”.[47] Det framgår dock inte av domen vad sådana ytterligare skyddsåtgärder skulle kunna vara.

3.2.4 KAN ANLITANDE AV EN AMERIKANSK MOLNTJÄNSTLEVERANTÖR TROTS JURISDIKTIONSRISKEN VARA FÖRENLIGT MED GDPR?

3.2.4.1 Särskilt om risken för utlämnande i strid med GDPR (med anledning av CLOUD Act)

Som framgått av avsnitt 3.2.2.3 ovan finns det ett antal krav i dataskyddsförordningen som måste uppfyllas för att ett utlämnande enligt amerikansk rätt (utan stöd av en internationell överenskommelse) ska vara förenligt med dataskyddsförordningen. Flera av de nämnda kraven aktualiseras först när en begäran om utlämnande riktas mot molntjänstleverantören och denne måste bedöma om utlämnandet ska göras.

Det avgörande kravet på molntjänstkunden vid anlitande av ett personuppgiftsbiträde eller underbiträde som omfattas av amerikansk jurisdiktion är att bedöma huruvida molntjänstleverantören kan lämna *tillräckliga garantier* enligt artikel 28.1 dataskyddsförordningen. I denna bedömning får molntjänstleverantörens möjligheter att uppfylla kraven på rättslig grund, principen om laglighet och förbudet mot utlämnande utan stöd i unionsrätten betydelse.

Motsvarande bedömning måste även göras enligt principen om laglighet i artikel 5.1 a dataskyddsförordningen, närmare bestämt om det kan antas att personuppgifterna efter molntjänstkundens utlämnande till ett personuppgiftsbiträde och eventuellt underbiträde kan antas komma att behandlas i strid med dataskyddsförordningen.

Enligt vår bedömning innebär exponeringen mot amerikansk lagstiftning en tydlig risk för att en molntjänstleverantör som omfattas av amerikansk jurisdiktion kan komma att lämna ut personuppgifter i strid med dataskyddsförordningen. Därmed riskerar molntjänstkunden att inte uppfylla kraven i dataskyddsförordningen genom att endast anlita personuppgiftsbiträden som lämnar tillräckliga garantier enligt artikel 28.1 dataskyddsförordningen och att utlämnandet kan komma i strid med principen om laglighet i artikel 5.1 a.

Risken för överträdelse av artiklarna 5.1 a och 28.1 dataskyddsförordningen uppstår för molntjänstkundens räkning i och med att personuppgifter lämnas ut till en molntjänstleverantör som omfattas av amerikansk jurisdiktion. Bedömningen bör dock göras redan när leverantören anlitas av molntjänstkunden.

---

47 *Schrems II*, punkt 134. Jfr. skäl 109 dataskyddsförordningen.

I båda fallen behöver molntjänstkunden bedöma de anlitade personuppgiftsbiträdenas och underbiträdenas möjligheter att behandla personuppgifterna i överensstämmelse med dataskyddsförordningens krav. Enligt vår bedömning finns det ett utrymme för att göra en riskbedömning vad gäller både tillräckliga garantier enligt artikel 28.1 och vid bedömningen enligt principen om laglighet i artikel 5.1 a.

Riskbedömningen är beroende av såväl omständigheterna i det enskilda fallet som en helhetsbedömning. Den risk som, enligt vår mening, ska bedömas består dels av sannolikheten för att personuppgiftsbiträdet inte uppfyller kraven i dataskyddsförordningen, dels av de konsekvenser som de registrerade kan drabbas av om biträdet inte uppfyller kraven enligt dataskyddsförordningen.

Enligt vår bedömning innebär själva förekomsten av CLOUD Act att sannolikheten för att ett personuppgiftsbiträde eller underbiträde lämnar ut uppgifterna i strid med dataskyddsförordningen i nuläget får anses vara högre än innan CLOUD Act trädde ikraft. Det bakomliggande syftet med CLOUD Act är ju att underlätta för amerikanska myndigheter att begära ut uppgifter som finns lagrade i andra länder.

Den risk som kan uppkomma för de registrerade vid ett eventuellt utlämnande enligt amerikansk rätt utan stöd i dataskyddsförordningen eller internationell överenskommelser, består i att de registrerade går miste om det skydd som dataskyddsförordningen ger bl.a. vad gäller möjligheten att få information och kunna kontrollera personuppgiftsbehandlingen samt att kunna klaga till tillsynsmyndigheten och därigenom få en rättslig prövning av behandlingens laglighet.

Risken för att de registrerade drabbas av konsekvenser vid ett utlämnande i strid med dataskyddsförordningen är i helt beroende av vilken typ av behandling och personuppgifter det rör sig om.[48]

Förutom att kräva att molntjänstleverantören organiserar tjänsten så att denne helt saknar faktisk och rättslig åtkomst till uppgifterna, något som i de flesta molntjänster är mycket svårt att säkerställa i praktiken (se vidare avsnitt 3.4.3 angående faktisk åtkomst), har vi svårt att se vilka åtgärder som molntjänstkunden skulle kunna vidta för att minska sannolikheten för att molntjänstleverantören kan tvingas lämna ut uppgifterna till amerikanska myndigheter. Däremot ser vi flera åtgärder som kan vidtas för att minska risken för att de registrerade drabbas av negativa konsekvenser av ett sådant utlämnande (se vidare avsnitt 3.3.5.1 nedan). Genom att minska konsekvenserna för de registrerade menar vi att risken, under vissa försättningar, kan minskas till en sådan nivå att det *kan vara möjligt* att anlita av en amerikansk molntjänstleverantör på ett sätt som kan vara förenligt med dataskyddsförordningen, även om det alltid kommer finnas en

48 Vid behandling av särskilda kategorier av personuppgifter (”känsliga personuppgifter”), uppgifter om brott, person- och samordningsnummer och integritetskänsliga personuppgifter, såsom finansiella uppgifter som skulle kunna användas för betalningsbedrägeri och andra personuppgifter av mycket personlig karaktär måste risken typiskt sett anses hög, i synnerhet om det gäller omfattande behandling.

kvarvarande risk för att uppgifterna lämnas ut till amerikanska myndigheter under CLOUD Act. Som framgår av avsnitt 3.2.3 ovan, kan man vid anlitandet av en amerikansk molntjänstleverantör dock även komma att behöva beakta risken för tredjelandsöverföring i strid med dataskyddsförordningen.

3.2.4.2 Särskilt om risken för tredjelandsöverföring i strid med GDPR (mot bakgrund av Schrems II)

Vid bedömningen av huruvida en personuppgiftsansvarig kan överföra personuppgifter till en mottagare i tredjeland på grundval av de standardavtalsklausulerna, ska hänsyn tas till (i) *omständigheterna* kring överföringen (bl.a. de avtalsvillkor som överenskommits och de relevanta delarna av rättssystemet i det tredjelandet), och (ii) de *ytterligare skyddsåtgärder* som kan vidtas.[49]

Sådana kompletterande skyddsåtgärder måste, tillsammans med standardavtalsklausulerna, säkerställa att den adekvata skyddsnivå som dessa bestämmelser garanterar kan upprätthållas i praktiken, dvs. att den lagstiftningen i det aktuella tredjelandet inte inkräktar på detta skydd.[50] Om man i sin bedömning kommer fram till att en lämplig skyddsnivå inte kan säkerställas, måste den aktuella överföringen avbrytas eller avslutas. Även de nationella tillsynsmyndigheterna är skyldiga att avbryta eller förbjuda fortsatt överföring, om de bedömer att standardavtalsklausulerna inte ger det garanterade skyddet, för det fall den personuppgiftsansvarige själv inte har gjort detta.

Som framgår av avsnitt 3.2.3.4 ovan har EU-domstolen emellertid bedömt att amerikansk lagstiftning *inte* säkerställer en skyddsnivå som är väsentligen likvärdig med den som uppställs i EU-rätten. Det juridiska läget avseende användning av amerikanska molntjänster får därför anses vara osäkert i nuläget. Det kan därmed konstateras att Schrems II får konsekvenser även för andra överföringsmekanismer, såsom användningen av bindande företagsbestämmelser (BCR) i enlighet med artikel 47.

EDPB arbetar för närvarande med att ta fram en vägledning avseende vilka ”ytterligare säkerhetsåtgärder” det faktiskt kan vara fråga om.[51]

Även om rättsläget får anses vara osäkert är det enligt vår bedömning inte sannolikt att dataskyddsförordningen ska tolkas på ett sådant sätt att det skulle vara absolut omöjligt/förbjudet att använda amerikanska molntjänster; eller kinesiska, indiska eller ryska för den delen. Allt är som sagt avhängigt förhållandena i det enskilda fallet och den enskilda bedömningen.

---

49 Detta följer av EU-domstolens uttalanden i *Schrems II*.

50 EDPB, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, antagen den 23 juli 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf, hämtad den 3 september 2020.

51 EDPB, Nyhetsmeddelande av den 4 september 2020, https://edpb.europa.eu/news/news_en, hämtad den 15 september 2020.

Vår rekommendation är att i första hand och i största möjliga utsträckning minska verksamhetens exponering mot tredjeländers regelverk.

Vad gäller befintliga avtal med amerikanska molntjänstleverantörer, anser vi att ett rimligt förhållningssätt är att, i avvaktan på vägledande uttalanden från tillsynsmyndigheten, i så stor utsträckning som möjligt minimera de risker som den aktuella behandlingen kan komma att innebära genom att vidta olika typer av riskbegränsande åtgärder.

Sådana *riskbegränsande åtgärder* kan exempelvis bestå av de dataskyddsrelaterade säkerhetsåtgärder som framgår av avsnitt 3.3.5.1 nedan, såsom att säkerställa högsta grad av uppgifts- och lagringsminimering vid den aktuella överföringen.

Därutöver kan även följande exempel på riskbegränsande åtgärder vara tänkbara:

- **Säkerställa att personuppgifterna lagras inom EU/EES** och om möjligt, kräva att uppgifterna inte heller behandlas utanför EU/EES.

- **Begränsa den faktiska användningen av molntjänsten**, exempelvis genom att i en situation där det endast är en supportfunktion för molntjänsten i fråga som medför att överföring till tredjeland aktualiseras (vilket är en typisk risk för molntjänster, se avsnitt 3.3.4.2 nedan), överväga om verksamheten verkligen behöver använda supporttjänsten.

- **Lägga till ytterligare säkerhetsfunktioner i molntjänsten**. Det förekommer exempelvis funktioner som innebär att en molntjänstleverantör och eventuella underleverantörer, för att få tillgång till molntjänstkundens data, dessförinnan måste skicka en förfrågan som ska godkännas av molntjänstkunden vid varje enskilt tillfälle. Det kan också finnas olika sätt att använda den aktuella molntjänsten (t.ex. deployment utan permanent lagring) som bör beaktas.

- **Aktivt arbeta med exit- och kontinuitetsplanering**. Exempelvis genom att utforma arkitekturen ovanpå sådana driftplattformar som flera molntjänstleverantörer kan erbjuda, fortlöpande bevaka alternativa molntjänstleverantörers erbjudande och kartlägga vilka hinder som finns för att genomföra en sådan flytt samt upprätta en backup-hantering som är oberoende av molntjänstleverantören.

- **Utvärdera möjliga alternativ för kryptering och pseudonymisering**, inbegripet att säkerställa en säker nyckelhantering.

- **Ta fram interna rutiner för användning av molntjänsten** i syfte att se till att tjänsten inte används på ett otillåtet sätt.

- **Följa rättsutvecklingen i det aktuella tredjelandet** för att bedöma om riskerna med molntjänsten ökar eller minskar.

Vi vill understryka att det i nuläget inte är möjligt att med säkerhet

avgöra huruvida ovanstående riskbegränsande åtgärder (tillsammans eller var för sig) når upp till kravet på ”ytterligare skyddsåtgärder”. Vi menar dock att ovanstående åtgärder bör övervägas och om möjligt implementeras för att minska de risker som aktualiseras i Schrems II. Oavsett utgången av dessa överväganden, är det som alltid i dataskyddsarbetet viktigt att dokumentera den bedömning man gjort i det enskilda fallet i syfte att kunna presentera för tillsynsmyndighet och i domstol.

Om det, efter att ha vidtagit tillgängliga och lämpliga skyddsåtgärder, ändå bedöms att det är sannolikt att molntjänsten innebär en hög risk för de registrerades rättigheter och friheter är man skyldig att utföra en konsekvensbedömning enligt artikel 35 dataskyddsförordningen.

3.3 Konsekvensbedömning enligt GDPR

3.3.1 INLEDNING

En verksamhet som vill använda sig av en publik molntjänst för att hantera viss information som kan innehålla personuppgifter, kommer i typfallet att vara personuppgiftsansvarig i dataskyddsförordningens mening, medan molntjänstleverantören är personuppgiftsbiträde.

Som personuppgiftsansvarig ska molntjänstkunden ”*säkerställa och kunna visa att*” all personuppgiftsbehandling som utförs under den personuppgiftsansvariges ansvar utförs i enlighet med kraven i dataskyddsförordningen.[52] Den personuppgiftsansvarige är även skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till de risker som uppstår för fysiska personers rättigheter och friheter.[53]

Sådana risker vid personuppgiftsbehandling ska tolkas brett och innefattar risker för såväl fysiska och materiella som immateriella skador. De risker som, enligt dataskyddsförordningen, särskilt bör beaktas vid behandling av personuppgifter är:

- om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel;

- om den registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter;

- om personuppgifterna som behandlas avslöjar känsliga person-

52 Artikel 5 och 24 dataskyddsförordningen.

53 Artikel 32 dataskyddsförordningen.

uppgifter (artikel 9) eller personuppgifter som rör fällande domar i brottmål samt överträdelser (artikel 10);

- om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör exempelvis arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlighet eller beteende, vistelseort eller förflyttningar i syfte att skapa eller använda personliga profiler;

- om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn; eller

- om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.[54]

Dataskyddsförordningen bygger på ett riskbaserat förhållningssätt vilket innebär att det ansvar som personuppgiftsansvariga och personuppgiftsbiträden bär ska bedömas utifrån riskerna med den aktuella personuppgiftsbehandlingen.[55] Det riskbaserade förhållningssättet förutsätter således att personuppgiftsansvariga och personuppgiftsbiträden utför *en inledande riskanalys*.[56] Om riskanalysen utvisar att den planerade behandlingen sannolikt kommer leda till en *hög* risk för fysiska personers rättigheter och friheter, ska den personuppgiftsansvarige även genomföra en *konsekvensbedömning* i enlighet med artikel 35 dataskyddsförordningen.

I detta avsnitt 3.3 redogör vi för hur en riskbedömning enligt dataskyddsförordningen kan genomföras när en verksamhet planerar att anlita en molntjänstleverantör, vilka faktorer som avgör huruvida en konsekvensbedömning enligt artikel 35 krävs för den planerade behandlingen och vad en sådan konsekvensbedömning ska innehålla. Vi har även identifierat ett antal typiska dataskyddsrisker som uppkommer i samband med anlitande av en molntjänstleverantör.

3.3.2 INLEDANDE DATASKYDDSRÄTTSLIG RISKANALYS

För att kunna bedöma vilka säkerhetsåtgärder som verkligen är ”lämpliga”, och på så sätt uppfylla kraven i dataskyddsförordningen, måste all behandling av personuppgifter som ska ske i molntjänsten identifieras, beskrivas och analyseras noggrant, innan behandlingen påbörjas.

Genom en sådan analys ska det kunna bedömas dels vilka dataskyddsrisker behandlingen kan innebära, dels hur sannolik och allvarlig respektive risk är och dels vilka skyddsåtgärder som kan vara relevanta för att minska sådana risker. Bedömningen av hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är

54 Skäl 75 dataskyddsförordningen.

55 Se bl.a. artikel 24 och skäl 74 dataskyddsförordningen.

56 Jfr. artikel 35 samt skäl 76 dataskyddsförordningen.

bör göras utifrån behandlingens art, omfattning, sammanhang och ändamål.[57]

3.3.2.1 Krävs en konsekvensbedömning enligt artikel 35 dataskyddsförordningen?

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, "*sannolikt leder till en hög risk för fysiska personers rättigheter och friheter*" ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (en s.k. konsekvensbedömning).[58]

I dataskyddsförordningen anges tre fall[59] då det är obligatoriskt att genomföra en konsekvensbedömning, nämligen när det är fråga om:

a) behandling som innebär en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

b) behandling i stor omfattning av känsliga uppgifter, som avses i artikel 9.1 dataskyddsförordningen, eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott, som avses i artikel 10 dataskyddsförordningen.

c) systematisk övervakning av en allmän plats i stor omfattning.

Dessa fall utgör inte någon uttömmande lista. Datainspektionen har upprättat och offentliggjort en vidare förteckning[60] över behandlingsverksamheter som omfattas av kravet på konsekvensbedömning.[61] Enligt förteckningen ska en sådan bedömning upprättas om den planerade behandlingen uppfyller minst två av följande kriterier:

57 Se bl.a. artikel 24 och 32 samt skäl 74 och 76 dataskyddsförordningen.

58 Artikel 35.1 dataskyddsförordningen.

59 Artikel 35.3 dataskyddsförordningen.

60 Se Datainspektionen, *Förteckning enligt artikel 35.4 i Dataskyddsförordningen*, 16 januari 2019, dnr. DI-2018-13200, https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/.

61 Jfr. artikel 35.4 dataskyddsförordningen.

	DATAINSPEKTIONENS KRITERIER
1.	***utvärderar eller poängsätter människor**, t.ex. ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar eller ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare*
2.	*behandlar personuppgifter **i syfte att fatta automatiserade beslut** som har rättsliga följder eller liknande betydande följder för den registrerade*
3.	***systematiskt övervakar människor**, t.ex. genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer*
4.	***behandlar känsliga personuppgifter** enligt artikel 9 **eller uppgifter som är av mycket personlig karaktär**, t.ex. ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter*
5.	*behandlar personuppgifter **i stor omfattning***
6.	***kombinerar personuppgifter** från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, t.ex. när man samkör register*
7.	*behandlar personuppgifter om **personer som** av något skäl **befinner sig i ett underläge eller i beroendeställning** och därför är sårbara, t.ex. barn, anställda, asylsökande, äldre och patienter*
8.	*använder **ny teknik** eller **nya organisatoriska lösningar***
9.	*behandlar personuppgifter **i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal**, t.ex. när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån*

När en molntjänstkund planerar att använda en molntjänst är det inte ovanligt att det är fråga om behandling av personuppgifter i stor omfattning (femte kriteriet), behandling av personuppgifter om personer i beroendeställning, t.ex. anställda (sjunde kriteriet) och/eller behandling av känsliga personuppgifter eller uppgifter som är av mycket personlig karaktär, t.ex. en bank som hanterar finansiella uppgifter[62] (fjärde

62 Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679*, senast reviderade och antagna den 4 oktober 2017, WP 248 rev. 01, s. 11, https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-konsekvensbedomning-avseende-dataskydd.pdf, hämtad den 3 september 2020.

kriteriet). Det påstås ibland att molntjänster i sig är att betrakta som ”ny teknik” på så sätt som avses i det åttonde kriteriet, vilket vi generellt menar är tveksamt men det kan inte helt uteslutas utifrån en bedömning av omständigheterna i det enskilda fallet.

Vidare ska nämnas att det finns ***ett antal undantag*** i dataskyddsförordningen som medför att den personuppgiftsansvarige inte behöver genomföra en konsekvensbedömning när:

- behandlingens art, omfattning, sammanhang och ändamål är mycket lik en annan behandling för vilken den personuppgiftsansvarige redan har genomfört en konsekvensbedömning, varpå resultatet från den första konsekvensbedömningen även kan användas för den andra behandlingen som medför liknande höga risker,[63]

- behandlingen i fråga har sin rättsliga grund i unionsrätten eller i en medlemsstats nationella rätt (som den personuppgiftsansvarige omfattas av) av vilken det framgår att den specifika behandlingsåtgärden omfattas och att en konsekvensbedömning inte behöver utföras, eftersom en konsekvensbedömning redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av den lagliga grunden för behandlingen (dvs. när behandlingen är nödvändig för att den personuppgiftsansvarige antingen ska kunna fullgöra en rättslig förpliktelse, eller ska kunna utföra en uppgift av allmänt intresse enligt artiklarna 6.1 c och e),[64] eller

- behandlingen finns uppräknad i den förteckning, som Datainspektionen får upprätta och offentliggöra, över det slags behandlingsverksamheter för vilka det inte kommer att krävas att en konsekvensbedömning genomförs.[65] I dagsläget har Datainspektionen dock inte upprättat någon sådan lista.

3.3.3 METOD FÖR KONSEKVENSBEDÖMNING

3.3.3.1 Vad ska en konsekvensbedömning innehålla?

För att uppfylla de krav som uppställs i dataskyddsförordningen[66] ska en genomförd konsekvensbedömning *åtminstone* innehålla:

a) en ***systematisk beskrivning*** av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,

b) en ***bedömning av behovet*** av ***och proportionaliteten*** hos behandlingen i förhållande till syftena,

63 Artikel 35.1 dataskyddsförordningen.

64 Artikel 35.10 dataskyddsförordningen.

65 Artikel 35.5 dataskyddsförordningen.

66 Artikel 35.7 dataskyddsförordningen.

c) en ***bedömning av de risker*** för de registrerades rättigheter och friheter som identifierats, och

d) de ***åtgärder som planeras för att hantera riskerna***, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att dataskyddsförordningen efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

För att klargöra vad kraven innebär har den tidigare Artikel 29-gruppen (Europeiska dataskyddsstyrelsens företrädare) utfärdat särskilda riktlinjer för konsekvensbedömning.[67] Därtill finns det flera formella modeller för genomförande av en konsekvensbedömning och vi har i detta avsnitt, utöver Artikel 29-gruppens riktlinjer, i första hand beaktat PIA-metodologin från franska dataskyddsmyndigheten CNIL[68] samt ISO/IEC 29134.[69]

Skyldigheten att utföra en konsekvensbedömning åligger den personuppgiftsansvarige men personuppgiftsbiträdet ska, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå, bistå den personuppgiftsansvarige i arbetet med konsekvensbedömningen.[70]

Vidare bör den personuppgiftsansvarige, om tillämpligt, även vidta följande åtgärder vid genomförandet av konsekvensbedömningen:

- **Rådfråga utsett dataskyddsombud**. Om det utsetts ett dataskyddsombud hos den personuppgiftsansvarige ska ombudet rådfrågas vid, och även övervaka, genomförandet av konsekvensbedömningen. Dataskyddsombudets råd ska sedan dokumenteras i konsekvensbedömningen.[71]

- **Inhämta synpunkter från de registrerade**. Den personuppgiftsansvarige ska också, när det är lämpligt, inhämta synpunkter från de registrerade (eller deras företrädare), om den planerade behandlingen. Exempelvis genom en intern eller extern undersökning i samband med fastställande av en behandlings ändamål och medel, eller om det är fråga om personaluppgifter en formell fråga till intern företrädare för personalen eller fackförening. Detta ska göras utan att det påverkar vare sig skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.[72]

---

67 Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679.*

68 Den franska nationella tillsynsmyndigheten, se https://www.cnil.fr/en/PIA-privacy-impact-assessment-en, hämtad den 3 september 2020.

69 ISO/IECI 29134:2017, *Information technology – security techniques – Guidelines for privacy impact assessment.*

70 Artikel 35.1 och 28.3 f dataskyddsförordningen.

71 Artikel 35.2 och 39.1 c dataskyddsförordningen.

72 Artikel 35.8 och 35.9 dataskyddsförordningen.

- **Iaktta godkända uppförandekoder**. Om det (exempelvis av en branschorganisation) upprättats någon särskild uppförandekod för att tillgodose särdragen hos en viss behandling, och den uppförandekoden är tillämplig på behandlingen i fråga, så kan denna användas vid genomförandet av konsekvensbedömningen.[73]

- **Samråda med Datainspektionen**. Om en konsekvensbedömning visar att den planerade behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken[74], ska man samråda med Datainspektionen innan behandlingen utförs. Sådana oacceptabelt höga risker kan exempelvis vara att de registrerade kan uppleva betydande, eller till och med oåterkalleliga, konsekvenser som de inte kan övervinna eller när det verkar vara uppenbart att risken kommer att inträffa. Om Datainspektionen vid ett sådant förhandssamråd anser att den planerade behandlingen skulle strida mot dataskyddsförordningen, i synnerhet om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska Datainspektionen ge den personuppgiftsansvarige skriftliga råd.[75]

3.3.3.2 Kräver en flytt till molntjänst en konsekvensbedömning?

Även om den behandling som planeras ske i molntjänsten inte per se alltid innebär någon ”ny behandling” för de registrerade/den personuppgiftsansvarige, som på så sätt utlöser krav på att genomföra en riskanalys och konsekvensbedömning, så kan en flytt från en on premises-lösning till en molntjänst innebära att en konsekvensbedömning ändå behöver genomföras eller uppdateras. Anledningen till detta är att flytten till molnet i sig kan innebära ökade och nya risker för de registrerades fri- och rättigheter. En genomförd konsekvensbedömning inte är någon engångsaktivitet utan en fortlöpande process och en personuppgiftsansvarig som står i begrepp att välja nya tekniska eller organisatoriska åtgärder som kan påverka allvaret eller sannolikheten för de risker som uppkommer vid behandlingen kan således behöva uppdatera sin konsekvensbedömning.[76] Vid en uppdatering är det dock inte givet att samtliga steg i en formell konsekvensbedömning behöver upprepas.[77]

3.3.3.3 Genomförande av översyn

Efter att konsekvensbedömningen har genomförts ska den personuppgiftsansvarige vid behov genomföra en översyn för att bedöma

---

73 Artikel 40 dataskyddsförordningen.

74 En skyldighet att begära förhandssamråd föreligger troligen inte när den personuppgiftsansvarige bedömer att det de planerade skyddsåtgärderna medför att det inte längre föreligger en hög risk, se skäl 94 dataskyddsförordningen.

75 Artikel 36.1 och 36.2 dataskyddsförordningen.

76 Jfr. artikel 35.1 ”*före behandlingen utföra en bedömning*”.

77 Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679,* s. 16.

om den aktuella behandlingen genomförs i enlighet med konsekvensbedömningen. Detta ska i vart fall göras när den risk som behandlingen medför förändras.[78] Risker kan bl.a. förändras till följd av en ändring av någon av komponenterna i behandlingen (såsom förändring av uppgifterna, riskkällor, tänkbara konsekvenser, hot etc.) eller till följd av att behandlingens sammanhang utvecklas (såsom förändring av ändamålet med behandlingen eller dess funktion). System för personuppgiftsbehandling kan utvecklas snabbt och på så sätt innebära att nya sårbarheter uppstår.

3.3.4 TYPISKA DATASKYDDSRISKER VID ANVÄNDNING AV PUBLIKA MOLNTJÄNSTER

Nedan redogör vi för några av de dataskyddsrisker som typiskt sett uppkommer vid användning av olika typer av molntjänster, dvs. de risker för de registrerades rättigheter och friheter som kan uppstå i samband med att deras personuppgifter behandlas i en sådan molntjänst.

> Vänligen observera särskilt att nedan angivna risker är ett urval och att flera, och i vissa fall kritiska aspekter, inte omnämns.

Det bör nämnas att dessa risker ser olika ut beroende på vilken typ av molntjänst det är fråga om, t.ex. om det är en SaaS-, PaaS- eller IaaS-tjänst (se avsnitt 3.1.1 ovan). Nedanstående är ett urval av de dataskyddsrisker som kan aktualiseras vid användning av molntjänster och ska inte betraktas som en fullständig förteckning.

3.3.4.1 Jurisdiktionsrisken

Jurisdiktionsrisken, som behandlas i avsnitt 3.2 ovan, är av avgörande betydelse vid bedömningen av huruvida det är lämpligt för en verksamhet att övergå till att använda sig av en publik molntjänst och den kan uppstå på flera olika sätt. I detta sammanhang är det även viktigt att uppmärksamma att många molntjänstavtal innehåller ett uttryckligt civilrättsligt godkännande från molntjänstkunden till molntjänstleverantören att leverantören får lämna ut uppgifter till utländsk ”myndighet” när detta följer av ”lag” (detta kallar vi nedan ”avtalad rätt till utlämnande till utländsk myndighet”, se avsnitt 3.5.3.1 nedan).

Jurisdiktionsrisken kan också i viss mån påverkas genom dels valet av leverantör och underleverantörer (se avsnitt 3.5.3.2 nedan), dels valet av vilken lag som är tillämplig för avtalet.

De bestämmelser i dataskyddsförordningen som primärt riskerar att åsidosättas till följd av jurisdiktionsrisken redogörs för i avsnitt 3.2.2.3 och 3.2.3.1 ovan.

78 Artikel 35.11 dataskyddsförordningen.

3.3.4.2 Risk för tredjelandsöverföring enligt dataskyddsförordningen, p.g.a. tjänsten i sig

En annan typisk risk vid anlitande av en molntjänstleverantör är att tjänsten *i sig* innebär att leverantören och/eller eventuella underleverantörer av olika skäl kommer föra över information lagrad i molntjänsten från den lagringsmiljö inom EU som avtalet vanligtvis avser när det är fråga om kunder i Sverige, till andra lagringsmiljöer utanför EU. Anledningen till detta kan bl.a. vara att uppnå redundans (t.ex. för katastrofhantering) eller att kunna utföra teknisk support vid kundens användning av tjänsterna. Det är exempelvis inte ovanligt med en omfattande lista på koncerninterna leverantörsbolag/underleverantörer som kan komma att ha tillgång till tjänsten samt villkor som innebär att molntjänstleverantören ges möjlighet att ensidigt ändra vilka dessa bolag/underleverantörer är.

Det bör vidare understrykas att tredjelandsöverföringar kan öka jurisdiktionsrisken, eftersom ytterligare jurisdiktioner kan bli tillämpliga på behandlingen.

3.3.4.3 Minskad kontroll över faktisk datahantering

Risken för att den personuppgiftsansvarige förlorar den direkta kontrollen över personuppgifterna uppkommer om och i den mån uppgifter lagras på lagringsmedia hos tredje man. Detta är givetvis en relevant risk vid all utkontraktering, men när det är fråga om molntjänster förbehåller sig ofta molntjänstleverantören rätten att behandla de aktuella personuppgifterna för sina egna ändamål (såsom för att ”förbättra tjänsten”), vilket innebär att den faktiska kontrollen av personuppgiftsbehandlingen går förlorad. Detta kan dessutom leda till förvirring/oklarheter avseende ansvarsförhållandena enligt dataskyddsförordningen, i relation till dessa behandlingar.

Risk med anledning av förlorad kontroll kan även uppstå i samband med flytt till molntjänsten och/eller när kunden väljer att lämna avtalet/sluta använda molntjänsten. Uppgifter som en gång lagrats i molnmiljön kan nämligen vara svåra att i praktiken radera på ett förutsebart sätt p.g.a. den infrastruktur som används för att säkerhetskopiera och vid behov återskapa informationen (backup). Av denna anledning förbehåller sig ofta molntjänstleverantören möjligheten att radera uppgifter först efter en angiven tidsfrist (som kan uppgå till flera månader). Under denna tidsfrist kan de registrerades personuppgifter alltså fortsätta behandlas i dataskyddsförordningens mening, trots att den registrerade/personuppgiftsansvarige begärt att uppgiften skulle raderas. Fortsatt tillgång till personuppgifterna för molntjänstleverantören, efter den personuppgiftsansvariges instruktion om radering, innebär även att samtliga övriga avtalsrisker föreligger fram till dess att personuppgifterna *de facto* raderas.

3.3.4.4 Risk för obehörig åtkomst, ändring eller radering

All information som lagras i ett system med nätanslutning riskerar teoretiskt sett att utsättas för obehörig åtkomst, om någon säkerhetsbrist uppstår som möjliggör för en obehörig person inom eller utanför molntjänstleverantören att få tillgång till, ändra eller radera personuppgifterna genom dataintrång eller liknande. Denna risk kan dock vara lägre när man använder en molntjänst jämfört med en on premises-lösning, eftersom molntjänstleverantörer generellt erbjuder en hög nivå av teknisk it- och informationssäkerhet och gör omfattande investeringar för att upprätthålla en hög säkerhetsnivå. Trots detta är det fortfarande en risk ur ett dataskyddsperspektiv eftersom det inte är möjligt för någon att garantera ett fullständigt skydd mot antagonistiska angrepp eller obehörig åtkomst i övrigt. Med anlitande av en molntjänstleverantör uppkommer även risken för att leverantörens anställda eller anställda hos leverantörens underleverantörer obehörigen bereder sig åtkomst till personuppgifterna.

3.3.4.5 Risk för avbrott som påverkar kundens tillgång till personuppgifterna

Med denna risk avses risken för att vissa delar av molntjänsten inte är tillgängliga för molntjänstkunden, exempelvis genom att molntjänstleverantören förbehåller sig en ensidig rätt att mer eller mindre godtyckligt ”suspendera” molntjänstkunden eller enskild användare hos molntjänstkunden. Även om ett sådant avbrott i tjänstens tillgänglighet inte i sig orsakar något oavsiktligt röjande av personuppgifter, kan det fortfarande inbegripa en risk för att de registrerades rättigheter och friheter kränks under specifika omständigheter. Rättigheter och friheter i detta sammanhang är enligt dataskyddsförordningen inte begränsade till integritetsrisker, utan kan t.ex. avse rätten till fri rörlighet eller en rättvis rättegång.[79] Om avbrottet leder till kränkning av sådana rättigheter kan det vara en överträdelse av dataskyddsförordningen trots att inget obehörigt röjande eller otillåten behandling sker.

3.3.4.6 Risk för ensidiga avtalsändringar

Molntjänstleverantörernas standardavtal innehåller i regel långtgående möjligheter för molntjänstleverantören att (med viss frist samt rätt för molntjänstkunden att säga upp avtalet) genomföra ensidiga ändringar av såväl avtalets villkor som tjänsterna (se även avsnitt 3.5.4.1 nedan). Ur ett dataskyddsperspektiv riskerar detta typiskt sett att ha en negativ påverkan på (i) molntjänstkundens tillgång de personuppgifter som överförts, (ii) valda skyddsåtgärder för personuppgifterna eller att (iii) inskränka den personuppgiftsansvariges instruktionsrätt, vilket i samtliga fall kan komma ställa den personuppgiftsansvarige inför valet att antingen inte fullt kunna styra den personuppgiftsbe-

79 Se skäl 75 dataskyddsförordningen.

handling som molntjänstleverantören utför, och/eller att vara tvungen att frånträda avtalet under fristen. Det är inte heller ovanligt att molntjänstleverantören förbehåller sig rätt att säga upp avtalet utan att kunden har någon möjlighet att påverka detta, vilket leder till förlust av i vart fall tillgängligheten till tjänsten.

3.3.5 HANTERING AV RISKER FÖR DE REGISTRERADES RÄTTIGHETER OCH FRIHETER

När riskerna med den planerade behandlingen har identifierats återstår att bedöma dessa baserat på riskens sannolikhet och allvarlighetsgrad.

Varken dataskyddsförordningen eller Artikel 29-gruppens särskilda riktlinjer för konsekvensbedömning innehåller några krav på hur en kvantifiering av risker ska göras men ett vanligt sätt att göra detta är att kategorisera sannolikhet respektive allvarlighetsgrad i olika nivåer som ges en specifik innebörd. Antalet nivåer och innebörden av respektive nivå kan bestämmas helt efter vad som kan anses vara lämpligt med hänsyn till verksamheten.

Kategoriseringen kan sedan användas för att bedöma sannolikhet respektive allvarlighetsgrad för respektive risk som har identifierats i den hypotetiska situation som molntjänstkunden befinner sig i dels utan att några riskbegränsande åtgärder har vidtagits, dels efter att molntjänstkunden har genomfört sådana åtgärder som identifierats för respektive risk.

En vanlig metod för sådan riskbedömning är att använda sig av de ***fyra kategorierna***: försumbar, begränsad, signifikant och maximal med den innebörd som presenteras i tabellen nedan. Denna indelning används i såväl CNIL:s PIA-modell för konsekvensbedömningar[80] som i relevant ISO-standard[81]. I riskbedömningen beaktas såväl de informationstekniska förutsättningarna som omgivande organisatoriska och rättsliga förutsättningar, tillsammans med riskkällor som kan innefatta tekniska, organisatoriska, rättsliga och andra risker.

80 Dessa kriterier härstammar från CNIL:s PIA-modell, se särskilt avsnitt 1.5 och 1.6 i *Privacy Impact Assessment (PIA) Knowledge Bases*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, hämtad den 3 september 2020.

81 Se Annex A i ISO/IEC 29134:2017.

	SANNOLIKHET	ALLVAR
Försumbar	Det framstår **inte som möjligt** för de beskrivna riskkällorna att realisera risken genom att utnyttja egenskaper hos informationssystem eller organisatoriska förutsättningar.	De registrerade blir antingen inte påverkade alls, eller kan utsättas för vissa besvär som de kan avhjälpa.
Begränsad	Det framstår som **svårt** för de beskrivna riskkällorna att realisera risken genom att utnyttja egenskaper hos informationssystem eller organisatoriska förutsättningar.	De registrerade kan utsättas för betydande besvär, som de med viss svårighet kan avhjälpa, eller ett stort antal registrerade utsätts för en Försumbar skada.
Signifikant	Det framstår som **möjligt** för de beskrivna riskkällorna att realisera risken genom att utnyttja egenskaper hos informationssystem eller organisatoriska förutsättningar.	De registrerade kan utsättas för betydande besvär, som de bör kunna avhjälpa, dock med verkliga och betydande svårigheter, eller ett stort antal registrerade utsättför en Begränsad skada.
Maximal	Det framstår som **mycket lätt** för de beskrivna riskkällorna att realisera risken genom att utnyttja egenskaper hos informationssystem eller organisatoriska förutsättningar.	De registrerade kan utsättas för betydande eller oåterkalleliga besvär som de kan vara oförmögna att avhjälpa, eller ett stort antal registrerade utsätts för en Signifikant skada.

3.3.5.1 Exempel på åtgärder för att hantera vissa typiska dataskyddsrisker

För att minska dataskyddsriskerna i samband med att den personuppgiftsansvarige anlitar en molntjänstleverantör kan den personuppgiftsansvarige exempelvis vidta följande åtgärder:

- Begränsa vilka personuppgifter som behandlas i molntjänsten
- Begränsa omfattningen av personuppgiftsbehandlingen som ska utföras av personuppgiftsbiträdet
- Upprätta och genomföra lämpliga processer för att säkerställa uppgiftsminimering och ändamålsbegränsning
- Se över avtalsvillkoren (inklusive personuppgiftsbiträdesavtalet) och förhandla om konsekvenser av dataskyddsriskerna (i synnerhet jurisdiktionsrisk, i den mån det är möjligt) och övriga avtalsmässiga risker så långt som möjligt (se vidare avsnitt 3.5 nedan)

3.4 Tekniska säkerhetslösningar för molntjänster

3.4.1 INLEDNING

Som framgått av rapportens föregående avsnitt, och även i avsnitt 3.5 nedan, medför användning av publika molntjänster ett stort antal risker med ursprung i olika källor. De åtgärder som kan aktualiseras för att hantera, eller i bästa fall eliminera, dessa risker är också av olika karaktär.

I dataskyddsförordningen hittar vi exempelvis det ofta återkommenade uttrycket ”tekniska och organisatoriska åtgärder”. Vad som är skillnaden mellan en teknisk och en organisatorisk åtgärd är inte alltid självklart, särskilt för sådana åtgärder som har både en teknisk och en organisatorisk aspekt. Ett sådant exempel är då en personuppgiftsbehandlande arbetsgivare utformar sin behandling på ett sådant sätt att endast de anställda som behöver få tillgång till de aktuella personuppgifterna för att kunna utföra sina arbetsuppgifter får sådan tillgång. Att analysera och besluta vem som behöver tillgång till vilken information är en *organisatorisk* åtgärd, och att verkställa detta beslut genom behörighetsstyrning i de it-system som används är en *teknisk* åtgärd.

I detta avsnitt 3.4 har vi valt att fokusera på de tekniska åtgärderna, eftersom det är dessa åtgärder som molntjänstleverantören i huvudsak har kontroll över och som typiskt sett bör regleras i molntjänstavtalet. Genom att vidta tekniska skyddsåtgärder kan den potentiella molntjänstkunden, enligt vår bedömning, påverka både X- och Y-axeln i Folke©-modellen (jfr kapitel 2 ovan). Detta gäller i synnerhet olika typer av kryptering, varför vi valt att går närmare in på detta i avsnitt 3.4.3 nedan.

3.4.2 OLIKA TEKNISKA SÄKERHETSLÖSNINGAR

De tekniska åtgärder som står till buds för att hantera olika typer av risker är givetvis många. Följande säkerhetslösningar utgör exempel på sådana tekniska åtgärder som typiskt sett diskuteras i samband med användning av molntjänster:

- **Säker hantering av verksamhetens enheter och media**. Detta innefattar centraliserad styrning av exempelvis de laptops och mobiltelefoner som används i en organisation, i syfte att skapa översikt över vilka enheter som finns, vilken data som finns på dessa enheter. På detta sätt möjliggör man för att vid behov av t.ex. säkerhetsskäl kunna avskära enheternas tillgång till andra system eller att på distans kunna radera data på en sådan enhet.

- **Behörighetsstyrning**, vilket avser åtgärden att på tjänste- och/eller filnivå centralt kunna styra vem som får läsa eller ändra vilken information. Detta innefattar även införande av sådan teknik som

används för att med tillräcklig säkerhet kunna fastställa identiteten på den person eller det system som använder en viss tjänst, t.ex. genom användning av lösenord, flerfaktorsautentisering eller andra metoder.

- **Kryptering** (se följande avsnitt)

- **Fysisk säkerhet**, dvs. att se till att obehöriga personer inte kan få fysisk tillgång till interna nätverk eller till enheter med information som ska skyddas.

- **Brandväggar och nätverkssegmentering**, dvs. att utforma datornätverk så att kommunikation mellan olika enheter på nätverket passerar knutpunkter som kan styras till att exempelvis inspektera trafiken för att identifiera misstänkta beteenden eller spärra trafiken.

Vilka åtgärder som är relevanta för att åtgärda en identifierad risk varierar naturligtvis beroende på vilken risk det är fråga om i det enskilda fallet. Ofta kan flera olika åtgärder aktualiseras för att hantera en viss risk och kan i bästa fall även samverka för att öka skyddet.

I molntjänstsammanhang kan en leverantör förväntas ha förmåga att tillämpa de flesta av de ovan nämnda åtgärderna för att öka säkerheten i den aktuella behandlingen. Det är vanligt förekommande att molntjänstleverantörer är certifierade enligt standarden ISO/IEC 27001. ISO 27000-serien är en uppsättning av standarder som bl.a. innehåller en katalog över olika lämpliga säkerhetsåtgärder, som är långt mer omfattande än den exemplifierande uppräkningen ovan. En certifierad molntjänstleverantör bör kunna redogöra för om och i vilken utsträckning de implementerat de olika skyddsåtgärderna som anges i ISO 27000-katalogen.

3.4.3 SÄRSKILT OM KRYPTERING

I sin mest översiktliga form är kryptering[82] processen att med hjälp av en krypteringsnyckel transformera en viss datamängd till en form som i sig är oläslig, men som kan återtransformeras till sin ursprungliga form genom en dekrypteringsprocess, av den som har tillgång till samma nyckel.[83] Tekniska lösningar som involverar kryptering kan utformas på avancerade sätt där mer begränsade nycklar har möjlighet att avkryptera delar av den lagrade informationen, och att access till olika nycklar kan hanteras med behörighetsstyrning och spårbarhet för vilka användare eller delsystem som ska ha tillgång till dessa. Sådana implementationer av kryptering i molntjänster benämns ofta Key

82 Här bortser vi från s.k. envägskryptering, som är en process för att transformera en viss datamängd (indata) till en annan (utdata) på ett förutsägbart/deterministiskt sätt, dvs så att samma indata alltid ger samma utdata, men där det inte finns ett sätt att från utdata rekonstruera indata.

83 Här beskrivs symmetrisk kryptering som är det som huvudsakligen används vid lagring av information (data at rest). För kommunicering av information (data in transit) är det vanligt med detta kompletteras asymmetrisk kryptering där olika nycklar – som har ett matematiskt samband – används för kryptering respektive dekryptering.

Management Services (”**KMS**”) och i den utsträckning som dessa tillåter molntjänstkunden att själv kontrollera vilka nycklar som används, benämns tjänsten ”**BYOK**” (bring your own key). Även med sådan kontroll måste nycklarna dock vara tillgängliga för molntjänstleverantören i någon form för att tjänsterna ska fungera. Grundproblemet i en sådan lösning är därmed att säkerställa att molntjänstleverantören inte kan dekryptera informationen utan molntjänstkundens medverkande eller godkännande.

I väldigt grundläggande användande av molntjänster, där tjänsten används som lagringsyta för information, är det möjligt för kunden att inte röja krypteringsnyckeln för någon utomstående, inklusive molntjänstleverantören. Med en sådan åtgärd är det teoretiskt omöjligt att molntjänstleverantören eller någon tredje part kan dekryptera informationen.[84] Sådana lösningar beskrivs ibland med termen ”**HYOK**” (hold your own key), men har inte slagit igenom på bred front eftersom en sådan lösning dels ställer stora krav på kunden och framförallt att denne kan hantera sina krypteringsnycklar på ett säkert sätt, dels omöjliggör sådan behandling av information i molnmiljön som är själva värdet i molntjänstanvändning. Molntjänstkunden får därför ofta nöja sig med att använda molntjänsten som en renodlad lagringstjänst, och trots de risker det medför, behandla informationen i samma miljö som där krypteringsnyckeln förvaras. Det kan dock konstateras att HYOK-baserade uppsättningar på ett relevant sätt torde minska de olika risker som förknippas med användning av publika molntjänster.

I de flesta former av molntjänstanvändning förutsätts dock en mer ingående behandling av informationen, exempelvis att informationen kan skapas, ändras, sammanställas och förmedlas till slutanvändare i själva tjänsten. Om informationen ska kunna behandlas så måste den också kunna dekrypteras i själva molnmiljön[85], vilket förutsätter att molntjänstleverantören i någon form har tillgång till nyckeln. Om man som molntjänstkund har möjlighet att utforma hur denna behandling går till, inklusive hur och när dekryptering sker, kan man göra det svårare för molntjänstleverantören att få tillgång till krypteringsnyckeln i användbart skick (något som framförallt är möjligt vid IaaS- eller PaaS-tjänster). I sina mest sofistikerade former använder molntjänstleverantören ett KMS där nycklar lagras i en för kunden dedikerad Hardware Security Module (”**HSM**”) – en hårdvaruenhet för nyckelhantering och kryptering där den fysiska innehavaren av enheten inte nödvändigtvis kan bereda sig tillgång till de krypteringsnycklar som lagras i enheten. När BYOK kombineras med HSM på ett korrekt sätt kan detta göra det mycket svårt för molntjänstleverantören att dekryptera information oberoende av molntjänstkunden.

---

84 I praktiken kräver detta att en bra krypteringsalgoritm utan kända brister används, att algoritmen för kryptering och algoritmen för nyckelgenerering är korrekt implementerade, att kundens exklusiva besittning av nyckeln inte röjs genom exempelvis dataintrång, och att det under informationens livslängd inte upptäcks avgörande brister i algoritmen.

85 Metoder för att behandla information utan att dekryptera den är ett växande forskningsområde (homomorfisk kryptering). Dessa metoder möjliggör dock idag inte den omfattande behandling som krävs i typiska molntjänster.

Grundproblemet är dock att det är svårt att säkerställa att molntjänstleverantören eller någon tredje part inte kan bereda sig faktisk tillgång till krypteringsnyckeln (eller den information som krypterats med nyckeln) i användbar form. Grundorsaken till denna svårighet är att nyckeln *de facto* måste befinna sig inom molntjänstleverantörens miljö i någon form. Vidare ställer sådana tekniska lösningar krav på en hög teknisk kompetens hos kunden, framförallt vad gäller nyckelhantering men också på säkert utformande av it-tjänster, något som kanske inte alltid finns på plats i kundens organisation och som kan vara en av anledningarna till att man överväger molntjänster från första början.

3.5 Exempel på typiska avtalsmässiga risker i molntjänstavtal

3.5.1 KAN MOLNTJÄNSTAVTAL FÖRHANDLAS?

Vi vill understryka att detta avsnitt inte gör anspråk på att vara en uttömmande beskrivning av alla avtalsmässiga risker som aktualiseras i samband med avtal om publika molntjänster.[86]

Det påstås emellanåt att molntjänstleverantörernas standardavtal inte går att förhandla, eftersom dessa tjänster är hårt standardiserade och att det skulle vara nödvändigt för leverantören att tillämpa samma avtalsvillkor för alla sina kunder. Detta påstående är både sant och falskt. Det finns avtalsvillkor som en leverantör av organisatoriska eller tekniska skäl typiskt sett inte kan reglera på ett kundspecifikt sätt och som leverantören därför överhuvudtaget inte är beredd att diskutera. Detta gäller typiskt sett för sådana villkor som kräver ändrade interna processer eller som påverkar hur tjänsten är uppbyggd. Ett avtal om molntjänster innehåller dock även andra, rent kommersiella eller riskhanterande bestämmelser såsom t.ex. ansvarsbegränsningar eller reglering av tillämplig lag. För att framgångsrikt kunna förhandla molntjänstavtal är det helt avgörande att som molntjänstkund förstå vilka bestämmelser som hör till respektive kategori.

Från molntjänstkundens perspektiv innebär detta att molntjänstavtal dels innehåller förhandlingsbara risker, dels ”inneboende” risker som behöver bedömas och hanteras utifrån ett riskperspektiv. I detta avsnitt 3.5 fokuserar vi främst på de avtalsbestämmelser som medför inneboende risk och de tekniska, organisatoriska eller avtalsmässiga åtgärder som kan vara relevanta för att påverka och minska dessa risker för kunden.

86 För en mer allmän bild av avtalsmässiga risker i molnavtal hänvisar vi till Cloud Sweden, *Rättsliga frågor vid flytten till molnet – en checklista* (2011), Kammarkollegiets förstudierapport, *Webbaserat kontorsstöd* (2018) och Pensionsmyndighetens rapport, *Molntjänster i staten* (2015).

Jurisdiktionsrisken, som beskrivs närmare i avsnitt 3.2 ovan, är det viktigaste exemplet på en sådan ”inneboende” avtalsmässig risk. Därutöver finns bestämmelser i standardavtalen som typiskt sett kan medföra eller påverka operativ risk (avsnitt 3.5.4), risk för bristande uppfyllelse av regulatoriska krav (avsnitt 3.5.5) och andra affärsjuridiska risker (avsnitt 3.5.6). Avslutningsvis vill vi även nämna den omständighet att standardavtalen ofta är utformade som omfattande och svårlästa avtalspaket, vilket i sig innebär en risk för att molntjänstkunden inte uppmärksammar eller ens har en rimlig möjlighet att identifiera ofördelaktiga villkor.

3.5.2 JURISDIKTIONSRISKEN

Jurisdiktionsrisken kan påverkas av avtalsvillkoren och kan, till viss del, minskas (men inte elimineras) genom förhandling av specifika avtalsvillkor i molntjänstavtalet.

3.5.2.1 Avtalad rätt till utlämnande till bl.a. utländsk myndighet

Med ”avtalad rätt till utlämnande till utländsk myndighet” avser vi den del av jurisdiktionsrisken som kommer till uttryck i avtal. Denna risk uppstår om molntjänstkunden *genom avtalsvillkoren godkänner ett utlämnande* till en icke-önskvärd mottagare och/eller utländsk myndighet utan att molntjänstkunden dessförinnan i varje enskilt fall ges möjlighet att bedöma lämpligheten av ett sådant utlämnande och att motsätta sig detta. Typexemplet är att molntjänstleverantören förbehåller sig rätt att lämna ut kundens information när så krävs enligt (ospecificerad) ”lag” eller till ”myndighet” och då ofta genom undantag från avtalets bestämmelser om sekretess, t.ex. med en reglering i stil med att ”*konfidentiell information kan röjas (av båda parter) om det krävs enligt lag eller av myndighet. Om det är tillåtet enligt lag, ska den andra parten meddelas innan sådant röjande sker.*”

I dessa sammanhang bör särskild uppmärksamhet riktas mot begreppet ”lag” eller ”myndighet” *inte* avser det lands lag som enligt avtalet är ”tillämplig lag” för avtalet. Denna typ av reglering bör läsas som att molntjänstkunden civilrättsligt godkänner att leverantören röjer information för vilken myndighet som helst, var helst i världen, så länge myndigheten anser att leverantören lyder under myndighetens jurisdiktion. Eftersom de större molntjänstleverantörerna är globala aktörer innebär regleringen att molntjänstkunden riskerar att utsätta sin information för ett mycket stort antal jurisdiktioner, i princip genom att molntjänstkunden väljer att använda den aktuella molntjänsten.

Som molntjänstkund bör man vara medveten om att ett fullständigt avtalsmässigt skydd mot jurisdiktionsrisken inte är möjligt. Det enda sättet att eliminera denna risk är att välja en leverantör respektive tjänst som inte innebär exponering mot främmande jurisdiktioner. Det är helt naturligt att en leverantör/underleverantör inte kommer att, och inte heller rimligen kan förväntas, acceptera eller följa en av-

talsreglering om detta i sig skulle utgöra en överträdelse av tillämplig lag för leverantören/underleverantören.

För att kunna bedöma jurisdiktionsrisken i sin helhet behöver man därför granska vilka jurisdiktioner som kan aktualiseras under avtalet och beakta vilka risker som finns för obehörigt utlämnande eller röjande under dessa jurisdiktioner. Med detta avser vi alltså både *vilken lag som är tillämplig för avtalet* (se följande avsnitt 3.5.3.2) och *vilken lag som är tillämplig för leverantören och/eller eventuella underleverantörer* (jfr. Schrems II-målet, avsnitt 3.2.3.2 ovan). Dessutom bör det beaktas att jurisdiktionsrisk kan uppkomma genom att *molntjänsten i sig innebär att information regelmässigt lämnar den överenskomna lagringsplatsen* (eller kan kommas åt från annan plats, t.ex. genom support), så att informationen därigenom kan bli föremål för annan jurisdiktion.

För att kunna säkerställa vilka risker som finns för obehörigt utlämnande under respektive jurisdiktion bör molntjänstkunden undersöka dels graden rättssäkerhet i den aktuella jurisdiktionen, dels avsaknad eller förekomst av vedertagna och rättssäkra utlämningsmekanismer som möjliggör utlämnande i enlighet med lagar och regler som molntjänstkunden lyder under (t.ex. MLAT). Mot bakgrund av den marknadsdominans som amerikanska molntjänstleverantörer har, bör noteras att EU-domstolen i Schrems II, enligt vår mening, får anses ha klargjort att amerikansk lag i skrivande stund *inte* innehåller nödvändiga rättssäkerhetsgarantier för att på ett adekvat sätt skydda personuppgifter som förs över från EU till USA.

3.5.2.2 Tillämplig lag

Tillämplig lag regleras i de allra flesta avtal mellan en svensk och en utländsk part.

Som ovan framgått innebär en sådan reglering inte att molntjänstavtalet endast kommer att lyda under den lag och jurisdiktion som överenskommits för avtalet. Vi menar ändå att en svensk kund typiskt sett bör sträva efter att avtalet ska tolkas i enlighet med svensk rätt. Vi menar också att den avtalade tillämpliga lagen kan tänkas påverka/minska jurisdiktionsrisken i viss utsträckning, beroende på omständigheterna i det enskilda fallet.

3.5.2.3 Exempel på avtalsvillkor som är relevanta för att minska jurisdiktionsrisken (ej uttömmande)

Följande avtalsvillkor utgör exempel på bestämmelser som typiskt sett är de mest relevanta för att minska jurisdiktionsriken:

- Tillämplig lag

- Sekretess/konfidentiell information – på vilka villkor och enligt vilken process tillåts utlämnande till utländsk myndighet?

- Avtalad datalokalisering
- Process för anlitande av underleverantörer
- Process för hur uppgifter är åtkomliga inom ramen för teknisk support eller felsökning etc.

Det bör särskilt noteras att relevanta bestämmelser kan finnas i olika avtalsdokument. Normalt sett finns t.ex. sekretessklausulen och reglering av tillämplig lag i tjänsteavtalet, medan frågor om utlämnande till myndighet, underleverantörer och datalokalisering ofta placerats i personuppgiftsbiträdesavtalet. Bestämmelser om datahantering inom ramen för teknisk support eller felsökning kan finnas i SLA-dokumentet och/eller i tjänstebeskrivningar. Detta är ett tydligt exempel på att molntjänstavtalens komplexitet, udda disposition och omfattning är en avtalsmässig risk i sig.

3.5.3 AVTALSMÄSSIGA OPERATIVA RISKER

Med avtalsmässiga operativa risker avser vi risken för negativ verksamhetspåverkan för molntjänstkunden till följd av molntjänsten eller molntjänstleverantören. Ett typiskt exempel är den risk som uppstår till följd av att molntjänstkunden inte har direkt kontroll över verksamhetskritiska system och resurser då dessa kontrolleras av molntjänstleverantören. Om och i den mån avtalet innehåller regleringar som ger molntjänstleverantören rätt att begränsa eller stänga av tillgången till tjänsten uppkommer en sådan avtalsmässig operativ risk.

För att kunna bedöma omfattningen av de avtalsmässiga operativa riskerna bör man särskilt beakta kundens beroende av *tjänsten*. I sådana fall där molntjänstkundens verksamhet helt eller delvis är beroende av de aktuella tjänsterna i sådan utsträckning att molntjänstkunden inte rimligen kan riskera att stå utan dessa, finns heller ingen praktisk möjlighet att säga upp avtalet till förtida upphörande, inleda en tvist eller stoppa avtalade prestationer.

3.5.3.1 Ensidiga avtalsändringar som negativt påverkar informationens tillgänglighet

Molntjänstleverantörernas standardavtal innehåller i regel långtgående möjligheter för molntjänstleverantören att genomföra *ensidiga ändringar* av såväl avtalets villkor som tjänsterna, på ett sätt som riskerar att negativt påverka molntjänstkundens tillgång till tjänsten, inbegripet den information som överförts. Exempelvis genom att hänvisa till en (ständigt föränderlig) beskrivning av tjänsten på molntjänstleverantörens egen webbplats. Detta är å ena sidan en naturlig del av att köpa en standardiserad molntjänst, men innebär å andra sidan potentiellt en operationell, strategisk och kommersiell risk för molntjänstkunden. Vi gör i denna rapport ingen bedömning av utsikterna för eventuellt åberopande av 36 § avtalslagen (SFS 1915:218) eller om

sådana villkor utgör ett oskäligt avtalsvillkor enligt lagen (1984:292) om avtalsvillkor mellan näringsidkare eller för all del om sådan bestämmelse skulle kunna utgöra missbruk av dominerande ställning under vissa omständigheter.

Avtalen innehåller normalt vissa, men ofta otillräckliga, *begränsningar för ändringsrätten*, exempelvis en viss tidsfrist under vilken kunden kan ta ställning till eventuell påverkan av ändringen eller en ”rätt” för kunden att säga upp avtalet om den genomförda ändringen har för stor påverkan på kundens möjligheter att använda tjänsten.

Om molntjänsten innefattar behandling av *personuppgifter* kan en ensidig ändringsrätt för leverantören dessutom bl.a. påverka molntjänstkundens instruktionsrätt som personuppgiftsansvarig (se avsnitt 3.3.4.6 ovan). En sådan ensidig ändringsrätt för leverantören när det gäller personuppgiftsbiträdesavtalet kan typiskt sett inte accepteras av molntjänstkunden, eftersom det uppenbart strider mot dataskyddsförordningen.

3.5.3.2 Avstängningsrätt och leverantörsberoende

Det är även vanligt att standardavtalen innehåller en alltför omfattande rätt för molntjänstleverantören att efter egen bedömning *stänga av molntjänsten*, i vissa fall t.o.m. baserat på att en enda slutanvändare hos kunden bryter mot användarvillkoren. En bred och generell avstängningsrätt för leverantören innebär en uppenbar operativ risk för kunden och, ytterst, ett mycket högt leverantörsberoende för molntjänstkunden.

Molntjänstleverantörernas standardavtal innehåller i regel inte heller *tillräckliga sanktioner vid avtalsbrott* för att avskräcka leverantören från oönskat beteende. Molntjänstleverantörens *ansvar* är exempelvis ofta begränsat till ett mycket lågt belopp, som typiskt sett motiveras av att molntjänstkunden köper en ”färdigpaketerad” standardprodukt. Ansvarsbeloppet för leverantören motsvarar inte sällan det som kunden har betalat för tjänsten under ett visst antal månader. Är det då fråga om en relativt sett ”billig” molntjänst, vars pris inte reflekterar hur viktig tjänsten är för kundens verksamhet, kan detta innebära en omfattande operativ risk för molntjänstkunden.

Det kan även vara fråga om att avtalade servicenivåer avseende molntjänstens tillgänglighet är låga eller, vilket det typiskt sett gäller, att den kompensation som ska utgå till molntjänstkunden vid icke-uppfyllelse av *avtalade servicenivåer* är alltför låg (t.ex. begränsat till endast ett mindre prisavdrag på nästkommande månads faktura).

I detta sammanhang bör man även granska standardavtalens bestämmelser om *avtalstid* och *uppsägning*. Utöver den risk för brist på kontroll som en kort avtals- respektive uppsägningstid kan medföra, innebär det dessutom en risk för att kommersiella förutsättningar förändras till molntjänstkundens nackdel.

3.5.3.3 Risk för inlåsningseffekter

För att undvika inlåsningseffekter finns många olika avtalsmässiga verktyg som molntjänstkunden bör överväga innan molntjänsten börjar användas. Särskilt viktigt är att molntjänstkunden redan när avtalet ingås säkerställer att det tydligt framgår hur och i vilken omfattning som leverantören ska assistera kunden i samband med avveckling av tjänsten och/eller byte av leverantör. För molntjänster är det särskilt viktigt hur processen för återlämning av informationen ser ut. Det bör exempelvis vara tydligt på vilket sätt och i vilket format kundens information ska återlämnas samt att leverantören även ska förstöra eventuella kopior eller annan information som kan hänföras till kundens information. Det bör nämnas att det inte är ovanligt att standardavtalens bestämmelser medför en rätt för leverantören att hålla inne kundens data. En sådan reglering skapar naturligtvis en betydande operativ risk för kunden.

3.5.3.4 Bristande uppföljningsmöjligheter av avtalsvillkoren

Standardavtalen innehåller sällan tillräckliga möjligheter för en molntjänstkund att genomföra granskningar och annan typ av uppföljning av molntjänstleverantörens efterlevnad av de villkor som överenskommits mellan parterna. Det är typiskt sett molntjänstleverantören som har kontroll över molntjänstkundens information samtidigt som kunden saknar insyn i hur molntjänstleverantörens tjänst utförs.

Molntjänstkunden bör därför se över villkoren för samverkan och rapportering samt säkerställa att kunden har rätt att genomföra för avtalet nödvändig uppföljning. En fråga som vi menar har diskuterats i oproportionerligt stor utsträckning, inte minst avseende molntjänstkunder som omfattas av regulatoriska krav (se avsnitt 3.5.5 nedan), är möjligheten för molntjänstkunden att genomföra revision på plats hos leverantören. Vi har svårt att se att just denna möjlighet skulle vara avgörande för att kunden ska upprätthålla kontroll och uppföljningsmöjlighet över sin information och sin verksamhet. Vi ser i praktiken ytterst få situationer när det skulle vara nödvändigt för molntjänstkunden att insistera på att få göra fysiska besök i leverantörens datahall. I de allra flesta fall torde det vara acceptabelt för kunden att förlita sig på s.k. tredjepartsrevision, där leverantören i en ordnad process granskas av en oberoende tredje part. Det bör också nämnas att de större molntjänstleverantörerna numera har särskilda avtalsregleringar för molntjänstkunder som lyder under regulatoriska krav, och att sådana särskilda villkor innehåller en rätt till revision på plats under särskilda omständigheter.

3.5.3.5 Exempel på avtalsvillkor som är relevanta för att minska de avtalsmässiga operativa riskerna (ej uttömmande)

Följande avtalsvillkor utgör exempel på bestämmelser som typiskt sett är de mest relevanta för att identifiera och minska de operativa riskerna:

- Suspendering/avstängning av tjänsten
- Servicenivåavtal (SLA)
- Ändringshantering – förekommer ensidiga ändringsmöjligheter för leverantören (avseende avtalet, tjänsten och SLA)?
- Sanktioner – finns kännbara/tillräckliga sanktioner vid avtalsbrott för att avskräcka leverantören från oönskat beteende (t.ex. rätt att innehålla betalning)?
- Avtalstid, uppsägning.
- Exit- och kontinuitetsplanering/aktiviteter vid avtalets upphörande

3.5.4 RISK FÖR BRISTANDE EFTERLEVNAD AV REGULATORISKA KRAV

Denna risk avser att molntjänstkunden genom att använda molntjänsten inte efterlever de regulatoriska krav som molntjänstkunden omfattas av, t.ex. bestämmelserna i dataskyddsförordningen eller, för det fall det är fråga om bank- eller försäkringsverksamhet, reglerna om banksekretess i lagen (2004:297) om bank- och finansieringsrörelse (”**LBF**”) och/eller Europeiska bankmyndighetens (”**EBA**”) riktlinjer för utkontraktering[87] respektive Europeiska försäkrings- och tjänstepensionsmyndighetens (”**EIOPA**”) riktlinjer för uppdragsavtal med molntjänstleverantörer[88] (se kapitel 5 nedan).

3.5.4.1 Dataskyddsförordningen

Vid användning av molntjänster är det i de allra flesta fall ofrånkomligt att personuppgifter behandlas, i större eller mindre omfattning. Risker i dataskyddsförordningens mening avser de risker för de registrerades rättigheter och friheter som uppstår i samband med att deras personuppgifter behandlas i en molntjänst. Några av de vanligaste riskerna som typiskt sett kan uppkomma vid användning av en molntjänst för behandling av personuppgifter har sammanställts i avsnitt 3.3.4 ovan.

3.5.4.2 Bank- och försäkringsregulatoriska krav

Om molntjänstkunden är en bank eller ett försäkringsföretag bör det även säkerställas att standardavtalen inte innehåller bestämmelser

87 EBA, *Riktlinjer för utkontraktering*, publicerad den 25 februari 2019, EBA/GL/2019/02. https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/91e517b9-9267-4bc9-bd36-911d1d93d0a5/EBA%20revised%20Guidelines%20on%20outsourcing_SV.pdf, hämtad den 3 september 2020.

88 EIOPA, *Riktlinjer om uppdragsavtal med molntjänstleverantörer*, publicerad den 31 januari 2020, EIOPA-BoS-20-002. https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cor_sv_0.pdf, hämtad den 3 september 2020.

som innebär att efterlevnaden av de regulatoriska kraven äventyras. Det är exempelvis inte ovanligt att molntjänstkunden både har inskränkta rättigheter och faktiska möjligheter att genomföra revisioner hos molntjänstleverantören eller att det saknas andra uppföljningsmöjligheter i avtalet.

De risker som typiskt sett kan uppkomma vid bankers och försäkringsföretags användning av molntjänster utvecklas vidare i kapitel 5 nedan.

3.5.4.3 Exempel på avtalsvillkor som är relevanta för att minska risken för bristande uppfyllnad av regulatoriska krav (ej uttömmande)

Följande avtalsvillkor utgör exempel på bestämmelser som typiskt sett är de mest relevanta för att minska risken för bristande uppfyllnad av regulatoriska krav:

- Transparens/revision/granskning
- Exitprocess och planering
- Rapportering/uppföljningsmöjligheter
- Ändringshantering – finns möjlighet och process för ändringar i avtalet eller tjänsten på grund av ändringar i tillämpliga regulatoriska krav?
- Personuppgiftsbiträdesavtal

3.5.5 AFFÄRSJURIDISKA RISKER

Med detta avsnitt 3.5.6 vill vi särskilt belysa sådana bestämmelser som typiskt sett förekommer i molntjänstavtal men som enligt vår uppfattning avviker från svensk praxis för kommersiella avtal.

3.5.5.1 Otillräckliga sanktioner vid avtalsbrott

Molntjänstkundens möjligheter att ta till tillräckliga sanktioner vid molntjänstleverantörens avtalsbrott är ofta alltför begränsade i molntjänstleverantörernas standardavtal för att säkerställa att leverantören avskräcks från oönskat beteende. Standardavtalen saknar exempelvis ofta rätt för molntjänstkunden att innehålla betalning i samband med oenighet/tvist. Dessutom har leverantören typiskt sett avstängningsrätt för tjänsten om molntjänstkunden inte betalar utestående fakturor, oberoende av om kunden bestrider fakturan med hänvisning till att tjänsten varit felaktig/otillgänglig. Detta är ett tydligt exempel på otillräckliga sanktioner som leder till ett obalanserat kund-/leverantörsförhållande och att kunden i praktiken inte har rimliga möjligheter att göra gällande sin rätt i relation till leverantören.

Detta är tveklöst svårförhandlade bestämmelser och slutresultatet av sådan förhandling är normalt ett avtalsförhållande som avviker från vad som enligt vår uppfattning är praxis för andra typer av svenska kommersiella avtalsförhållanden.

3.5.5.2 Ansvarsbegränsning

Som nämnts i avsnitt 3.5.4.2 ovan, är molntjänstleverantörens ansvar vid avtalsbrott ofta begränsat till ett lågt belopp i förhållande till den skada som kan uppkomma och/eller till tjänstens väsentlighet för kunden. Detta kan få stora konsekvenser och molntjänstkunden bör därför säkerställa att leverantörens ansvar är proportionerligt i förhållande till den betydelse som tjänsten har för kundens verksamhet. Denna fråga går i viss mån att förhandla men vi menar ändå att molntjänstleverantörens ansvar normalt sett kommer vara lägre än vad som är praxis för andra kommersiella avtal i Sverige.

3.5.5.3 Betalningsvillkor

Standardavtalens villkor för betalning är typiskt sett ofördelaktiga för kunden och innebär exempelvis ofta korta betalningsfrister och bestämmelser om att en utebliven betalning innebär förlorad tillgång till tjänsten till dess att molntjänstkunden har betalat avgiften.

3.5.5.4 Kommersiella värden ”skänks bort” till leverantören

Molntjänstkundens information kan ofta ha ett kommersiellt värde, både i sig själv och i form av metadata eller aggregerad med annan information. Molntjänstkunden bör därför även säkerställa att avtalet inte innehåller någon bestämmelse som medför att sådan värdefull information ”skänks bort” till molntjänstleverantören.

Standardavtalen innehåller exempelvis ofta en rätt för molntjänstleverantören att behandla kundens information för diverse egna syften såsom produktutveckling, intern resursallokering, statistik m.m.[89]

89 Vi menar att data generellt sett inte kan ”ägas”, utan är en potentiell tillgång som i hög utsträckning måste skyddas genom avtal. Det innebär bl.a. att en avtalad rätt för leverantören att ”använda” data *de facto* innebär en rätt för leverantören att ”få” det kommersiella värdet i informationen. Det är visserligen inte samma sak som att kunden fråntas möjligheten att också nyttja det kommersiella värdet men vi menar att bara det faktum att även leverantören får rätt att kommersialisera detta värde bör uppmärksammas och övervägas av kunden. En annan aspekt på samma tema är att leverantören på motsvarande sätt får del av data från flera/många olika kunder. Detta ger i sin tur leverantören en unik marknadsposition och möjliggör för leverantören att skapa nya ”datadrivna” erbjudanden som potentiellt direkt kan konkurrera med kunden. Exempelvis påstås ibland Amazon eller Google i princip kunna ge sig på vilken marknad som helst och konkurrera ut etablerade aktörer, enbart p.g.a. den data som dessa aktörer har kunnat samla på sig och förädla från olika källor/kunder.

3.5.5.5 Exempel på avtalsvillkor som är relevanta för att minska affärsjuridiska risker (ej uttömmande)

Följande avtalsvillkor utgör exempel på bestämmelser som är de mest relevanta för att minska de affärsjuridiska riskerna:

- Priser och ansvarsbegränsning
- Ersättning vid skada
- Betalningsvillkor
- Immateriella rättigheter

3.5.6 AVSLUTANDE KOMMENTARER

Utöver de generella avtalsmässiga risker som vi särskilt belyser i detta avsnitt 3.5, kan den potentiella molntjänstkunden komma att behöva göra särskilda överväganden till följd av att den verksamhet som bedrivs gör att kunden omfattas av särskild lagstiftning eller regulatoriska krav, såsom säkerhetsskyddslagen (se kapitel 4) och/eller reglerna om bank- och försäkringssekretess (se kapitel 5).

Sådana särskilda överväganden leder typiskt sett till att ytterligare risker kan identifieras i molntjänstleverantörernas standardavtal och att villkoren måste justeras ytterligare för att möjliggöra användning av molntjänster för sådan verksamhet.

4. Särskilda överväganden för verksamheter som omfattas av säkerhets-skyddslagen eller NIS-lagen

4.1 Inledning

För vissa verksamheter med mer samhällsviktig inriktning finns särskilda regleringar kring uppgiftshantering och informationssäkerhet, utöver den lagreglering som följer av dataskyddsförordningen och det generella skyddet för personuppgifter. I detta avsnitt går vi igenom två centrala regleringar som kan vara aktuella både för myndigheter och företag.

Säkerhetsskyddslagen (2018:585) (”**SSL**”), lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (”**NIS-lagen**”) samt de följdregleringar som utfärdats med stöd av någon av dessa lagar, ställer ett antal krav på informationssäkerhet. Det innebär att den som omfattas av någon av lagarna, kan ställas inför särskilda utmaningar vid användningen av molntjänster.

För såväl SSL som NIS-lagen utgör informationssäkerhet en central del för att uppnå det skydd som regleringarna kräver. Det är således nödvändigt för de aktörer vars verksamheter helt eller delvis omfattas av någon eller båda dessa regleringar att noga överväga den juridiska informationssäkerheten[90] innan en molntjänstleverantör används.

4.2 Säkerhetsskyddslagen

4.2.1 INLEDNING

SSL kompletteras av säkerhetskyddsförordningen (2018:658, ”**SSF**”) och ett antal myndighetsföreskrifter, framförallt Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2. Syftet med säkerhetsskyddsregleringen är att genom förebyggande åtgärder skydda Sveriges säkerhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamhet som omfattas av lagen samt även i övrigt skydda säkerhetsskyddsklassificerade uppgifter.[91] En grundläggande princip för lagen är att skyddet för det skyddsvärda objektet eller

90 Angående detta begrepp, se avsnitt 2.3.1 ovan.

91 Med *säkerhetsskyddsklassificerade* uppgifter menas sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400, ”**OSL**”) eller som skulle ha omfattats av sekretess enligt OSL, om den hade varit tillämplig, se 1 kap. 2 § 2 st. SSL.

intresset ska vara detsamma oavsett i vilken verksamhet det förekommer. Inte heller ska säkerhetsskyddet försämras till följd av att en utomstående leverantör anlitas. Med andra ord ska säkerheten vara lika hög, oaktat vem som behandlar informationen eller var den behandlas.

SSL gäller för den som till någon del bedriver verksamhet (verksamhetsutövare) som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).[92] Lagen tar ingen hänsyn till verksamhetens eller verksamhetsutövarens juridiska form, utan det avgörande är om den verksamhet som utövas är av betydelse för Sveriges säkerhet. Det innebär att det är av underordnad betydelse för lagens tillämplighet om verksamhetsutövaren är ett privat företag, en statlig myndighet eller en kommun. En av anledningarna till att säkerhetsskyddslagen utformats på detta sätt är att syftet med lagen ska uppnås även om samhället eller hotbilder förändras. Det medför även att det inte finns någon sammanfattande beskrivning över eller exemplifiering av vilka verksamheter som är att anse som säkerhetskänsliga verksamheter, eftersom detta varierar över tid. De verksamhetsutövare som omfattas av SSL identifieras istället utifrån huruvida det uppstår skada för Sveriges säkerhet ifall en angripare inhämtar information om verksamheten, förstör information eller på annat sätt hindrar att verksamheten kan bedrivas. Annorlunda uttryckt, den som bedriver säkerhetskänslig verksamhet, omfattas av SSL:s tillämpningsområde.[93]

Idag bedöms it-angrepp i olika former vara ett av de allvarligaste hoten mot rikets säkerhet. Enligt Säkerhetspolisen står teknisk inhämtning, exempelvis genom dataintrång, för en allt större del av det utländska spionaget.[94] Vidare har Försvarets radioanstalt uppmärksammat att antagonistiska angripare nu för tiden ofta använder sig av nya tillvägagångssätt där angreppen inte riktas direkt mot slutmålet, utan istället i första hand mot olika tjänsteleverantörer, i syfte att ta kontroll över myndigheter eller företag. Det blir även allt vanligare att viktiga informationssystem som inte i första hand behandlar hemliga uppgifter, men som av andra skäl ändå har ett högt skyddsvärde, t.ex. system för styrning av kraftförsörjning, utsätts för intrångsförsök och sabotage. Det är därför av stor vikt att det finns

92 1 kap. 1 § SSL. Vad som är av betydelse för Sveriges säkerhet är inte uttryckligt och tydligt definierat, men i prop. 2017/18:89, s. 44 f. presenteras ett antal typsituationer, nämligen (i) verksamhet som rör Sveriges yttre säkerhet (territoriell suveränitet och politisk självständighet), (ii) verksamhet som rör Sveriges inre säkerhet (framförallt kritiska anläggningar, funktioner och informationssystem för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga), (iii) viss samhällsviktig verksamhet för vilken en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på nationell nivå, (iv) verksamhet i vilken det hanteras säkerhetsskyddsklassificerade uppgifter, stora mängder uppgifter som av andra skäl kan betraktas som säkerhetskänslig, eller i vissa sammanhang även större mängder personuppgifter, och (v) verksamhet som ansvarar för drifttjänster åt ett flertal myndigheter och det samlade uppdraget kan ha betydelse för Sveriges säkerhet.

93 1 kap. 1 och 2 kap. 5 §§ SSL.

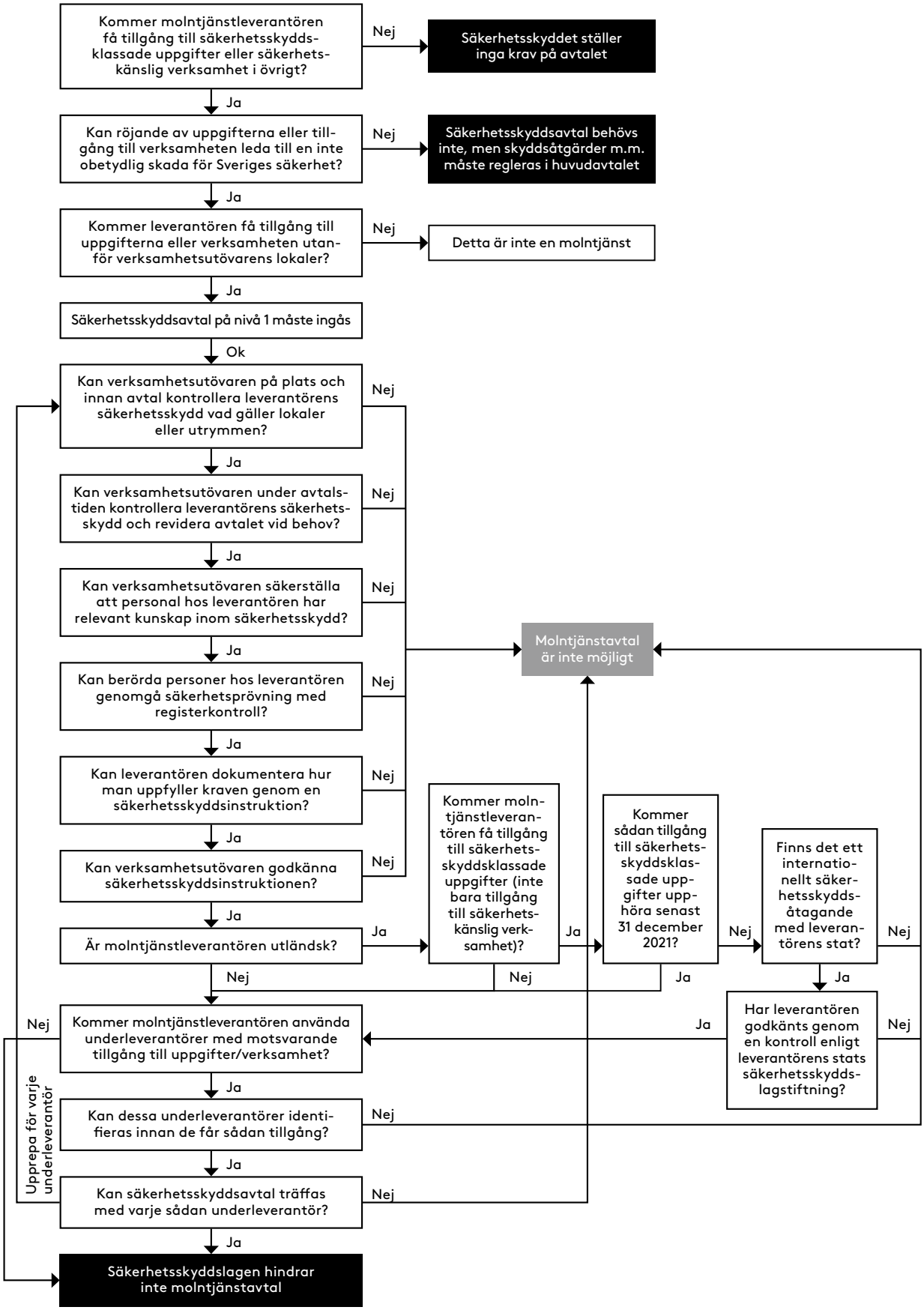
94 Säkerhetspolisen, *Hotbild mot säkerhetskänslig verksamhet*, juni 2019, https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64a/1560776860929/Hotbild-mot-sakerhetskanslig-verksamhet-juni-2019.pdf, hämtad den 3 september 2020.

en medvetenhet hos verksamhetsutövare om att det ständigt pågår intrångsförsök och operationer som syftar till att bedöma olika informationssystems robusthet. Mot denna bakgrund är det särskilt angeläget att verksamhetsutövare som omfattas av SSL noggrant överväger huruvida en molntjänstleverantör kan användas i enlighet med bestämmelserna i SSL, vilka risker som det potentiellt kan innebära och vilka åtgärder som behöver vidtas för att förhindra att Sveriges säkerhet äventyras.

4.2.2 ANVÄNDANDET AV MOLNTJÄNSTER FÖR VERKSAMHET SOM OMFATTAS AV SSL

Om verksamhetsutövaren har bedömt att verksamheten i dess helhet eller i delar omfattas av SSL ställs mycket långtgående krav på organisationen vad gäller inrättande av roller, säkerhetsskyddsklassificering av uppgifter m.m. I denna framställning fokuserar vi på vilka krav som aktualiseras vid anlitande av en molntjänstleverantör.[95] Följande process kan användas för att fastställa exakt hur dessa krav ser ut i det enskilda fallet.

95 För en mer djupgående redogörelse, se Advokatfirman Kahn Pedersens skriftserie 2020:1, *Juridisk informationssäkerhet*, särskilt avsnitt 2.



Figur 4.1: Process för att fastställa förutsättningar för molntjänstavtal. Observera att detta är en schematisk och icke-fullständig översikt.

Inledningsvis måste verksamhetsutövaren bedöma om molntjänstleverantören alls kommer att få tillgång till säkerhetsskyddsklassade uppgifter eller säkerhetskänslig verksamhet i övrigt. Det är möjligt att molntjänster används av säkerhetskänslig verksamhet utan att tjänsteleverantören får tillgång till sådana uppgifter eller sådan verksamhet. Om så är fallet, ställer säkerhetsskyddslagen inte några krav på molntjänstleverantören eller avtalsförhållandet mellan verksamhetsutövaren och molntjänstleverantören. Sett till det typiska syftet med att använda molntjänster är dock sådana fall ovanliga.

Därefter måste en bedömning göras av de uppgifter eller den verksamhet som görs tillgänglig för molntjänsten. Detta för att avgöra om ett röjande av uppgifterna kan medföra en inte obetydlig skada för Sveriges säkerhet (säkerhetsskyddsklass konfidentiell eller högre), eller om tillgång till verksamheten kan medföra motsvarande skada. Verksamhetsutövaren måste ingå ett säkerhetsskyddsavtal med molntjänstleverantören om leverantören kommer att få tillgång till uppgifter i säkerhetsskyddsklass konfidentiell eller högre, eller till verksamhet av motsvarande känslighet.[96] Ett säkerhetsskyddsavtal är ett särskilt avtal som är separat från själva huvudavtalet om molntjänsten, och ska anmälas till tillsynsmyndigheten. Kraven på säkerhetsskyddsavtal framgår framförallt av Säkerhetspolisens föreskrifter om säkerhetsskydd.[97]

Om det istället är fråga om relativt okänsliga uppgifter eller verksamhet, behöver verksamhetsutövaren inte teckna något säkerhetsskyddsavtal med molntjänstleverantören. Säkerhetsskyddet för uppgifterna eller verksamheten får dock inte försämras genom användandet av molntjänsten, varför verksamhetsutövaren ändå måste säkerställa att säkerhetsskyddet regleras på något annat sätt än genom ett säkerhetsskyddsavtal (exempelvis genom krav på skyddsåtgärder i tjänsteavtalet).

Ett säkerhetsskyddsavtal ingås på en av tre olika nivåer.[98] Nivåerna styrs av i vilken utsträckning molntjänstleverantören kan få tillgång till uppgifter eller verksamheten (*kommer att* resp. *kan komma att*), och om detta kan ske i verksamhetsutövarens lokaler eller om tillgången kan ges utanför lokaler. Molntjänster innebär per definition att de aktuella uppgifterna behandlas utanför verksamhetsutövarens lokaler.

Detta är en stor utmaning för säkerhetsskyddslagstiftningen, vars utgångspunkt är att det är verksamhetsutövaren som förvarar och kontrollerar säkerhetsklassade uppgifter. Om uppgifterna är mer känsliga än begränsat hemliga, eller den aktuella verksamheten har motsvarande känslighetsgrad, kräver detta ett säkerhetsskyddsavtal på nivå 1 (högsta nivån).

---

96 2 kap. 6 § SSL och 2 kap. 6 § SSF.

97 7 kap. PMFS 2019:2.

98 7 kap. 3 § PMFS 2019:2.

För säkerhetsskyddsavtal på nivå 1 krävs att:

- Verksamhetsutövaren kontrollerar på plats molntjänstleverantörens säkerhetsskydd beträffande aktuella lokaler eller utrymmen innan säkerhetsskyddsavtal ingås;

- Verksamhetsutövaren kontrollerar molntjänstleverantörens säkerhetsskydd enligt säkerhetsskyddsavtalet för att säkerställa att detta är fullgott, samt löpande bedömer om säkerhetsskyddsavtalet behöver revideras;

- Verksamhetsutövaren säkerställer att personal hos molntjänstleverantören har relevant kunskap inom säkerhetsskydd för arbetet de ska utföra;

- Molntjänstleverantörens ledning eller berörda delar av ledningen samt övriga hos molntjänstleverantören som avses delta i den säkerhetskänsliga verksamheten genomgår säkerhetsprövning med registerkontroll; och

- Molntjänstleverantören dokumenterar hur denne uppfyller kravet på säkerhetsskydd enligt avtalet i en säkerhetsskyddsinstruktion som godkänns av verksamhetsutövaren.

Dessa krav är mycket långtgående och medför sannolikt att de flesta större molntjänstleverantörerna inte är ett alternativ för verksamhetsutövaren. Verksamhetsutövaren måste även få kännedom om alla underleverantörer till den primära molntjänstleverantören och träffa säkerhetsskyddsavtal direkt med dessa.

Ytterligare en omständighet att beakta är om molntjänstleverantören direkt eller indirekt är ett utländskt bolag, exempelvis ett amerikanskt bolag. I praktiken är detta en mycket vanlig utgångspunkt såsom marknaden för molntjänster ser ut idag. Den omständigheten att molntjänstleverantören lyder under utländsk jurisdiktion är i sig inte ett förbud mot att anlita leverantören för säkerhetsskyddad verksamhet. Om uppdraget innefattar hantering av säkerhetsskyddsklassificerade uppgifter (oavsett klassificering) måste dessa också lämnas ut till den utländska leverantören, annars är det inte fråga om en molntjänst. För detta krävs dock att Sverige har ingått ett internationellt säkerhetsskyddsåtagande med den stat i vilken molntjänstleverantören befinner sig, och att molntjänstleverantören har godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning.[99] Motsvarande krav ställs däremot inte om avtalet endast ger molntjänstleverantören tillgång till verksamheten på ett sådant sätt att detta kan medföra skada för Sveriges säkerhet.

De internationella åtagandena publiceras vanligtvis i Sveriges internationella överenskommelser (SÖ) och finns i regel tillgängliga på

99 3 kap. 9 § 2 st. SSF.

regeringens webbplats.[100] Det finns, såvitt vi känner till, ingen komplett lista över vilka länder som Sverige har ingått sådana åtaganden med eller dess omfattning, varför det kan vara svårt att säkerställa att det finns ett lämpligt säkerhetsskyddsåtagande.[101] Det kan också vara förenat med praktiska svårigheter att säkerställa att leverantören har godkänts enligt den andra statens lagstiftning.

Under alla omständigheter kan det dock av flera skäl vara svårt att få in tillräckligt underlag för att från ett säkerhetsperspektiv kunna bedöma en utländsk molntjänstleverantörs lämplighet.[102] I detta sammanhang finns ingen principiell skillnad mellan länder inom och utanför EU. I sammanhanget bör dock noteras att den bestämmelse (3 kap. 9 § SSF) som ställer detta krav inte behöver tillämpas förrän den 1 januari 2022.[103]

Mot bakgrund av ovan är ändå vår uppfattning att för sådana molntjänster som kan komma att hantera säkerhetsskyddsklassad information av klass konfidentiellt eller högre, eller få tillgång till verksamhet av motsvarande känslighet, bör man enbart överväga svenska leverantörer som i sig hanterar sin egen it-infrastruktur och inte använder underleverantörer på ett sådant sätt att underleverantörerna kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet i övrigt. Det bör noteras att leverantörer på den svenska marknaden i allmänhet har goda förutsättningar att kunna uppfylla säkerhetsskyddslagens krav, även om de i allmänhet inte kan leverera samma bredd av molntjänster som de stora amerikanska leverantörerna.

4.3 NIS-lagen

4.3.1 INLEDNING

NIS-lagen är det svenska genomförandet av NIS-direktivet[104], och kompletteras av förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (”**NIS-förordningen**”) och ett antal föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB) som utfärdats med stöd av NIS-förordningen. Vi benämner dessa regleringar gemensamt för ”**NIS-regleringen**”.

NIS-regleringen är en del av EU:s övergripande strategi för informations-

100 Sveriges regering, *Sveriges internationella överenskommelser,* https://www.regeringen.se/rattsliga-dokument/sveriges-internationella-overenskommelser/, hämtad den 3 september 2020.

101 Såvitt vi känner till finns ingen publicerad sammanställning av åtaganden som fokuserar på överlämning av säkerhetsskyddade uppgifter till utländska leverantörer (se 3 kap. 9 § 2 st. SSF). En (inofficiell) sammanställning över åtaganden och jämförelser av säkerhetsskyddsklasser finns tillgänglig på https://blogg.mrpoyz.net/sveriges-internationella-sakerhetsskyddsavtal/, hämtad den 3 september 2020.

102 Se vidare resonemanget i nuvarande säkerhetsskyddslagens förarbeten, särskilt SOU 2015:25, s. 433 ff.

103 3 kap. 9 § SSF. Se 6 p. ikraftträdandebestämmelserna till SSF.

104 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

säkerhet.[105] Strategin utgår från att hot och angrepp mot informationssystem utgör ett hot mot säkerhet, stabilitet och ekonomiskt välstånd, och att en hög nivå på informationssäkerhet är en förutsättning för att potentialen i samhällets digitalisering ska kunna realiseras. Syftet med NIS-regleringen är därför att höja nivån på säkerheten i nätverk och informationssystem för vissa samhällsviktiga och digitala tjänster, främst genom åtgärder för att främja en hög nivå på informationssäkerhet hos myndigheter, företag och i samhället överlag.

NIS-lagen gäller enbart för tillhandahållare av vissa samhällsviktiga och digitala tjänster. Vad som utgör en samhällsviktig respektive digital tjänst inom lagstiftningens tillämpningsområde är detaljreglerat, och betydligt snävare än vad vanligt språkbruk antyder. För samhällsviktiga tjänster anges sex olika sektorer (energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten, samt digital infrastruktur), och för digitala tjänster tre olika typer av tjänster (internetbaserad marknadsplats, internetbaserad sökmotor samt molntjänster[106]).[107] Lagen gäller dock inte för verksamhet som omfattas av säkerhetsskyddslagen.[108]

Beroende på om en viss tjänst är samhällsviktig eller digital enligt lagens systematik åläggs leverantören av tjänsten olika förpliktelser vad gäller anmälan, informationssäkerhet och incidentrapportering.[109] Förpliktelserna är mer långtgående för samhällsviktiga tjänster än för digitala tjänster.[110]

4.3.2 ANVÄNDANDET AV MOLNTJÄNSTER FÖR VERKSAMHET SOM OMFATTAS AV NIS-LAGEN

NIS-regleringen ställer ett antal krav på de som omfattas av regleringen, bl.a. vad gäller att bedriva ett strukturerat och riskbaserat informationsarbete och att rapportera vissa incidenter till CERT-SE (som är en del av MSB).

---

105 Denna strategi inleddes 2013 (se särskilt Europaparlamentets resolution av den 12 september 2013 om EU:s strategi för it-säkerhet: en öppen, säker och trygg cyberrymd (2013/2606[RSP])) och omfattar även ett utökat mandat för EU:s cybersäkerhetsbyrå (”**ENISA**”) och antagandet av 2019 års ”cybersäkerhetsakt”, dvs. Europaparlamentets och Rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013) NIS-direktivet kompletteras av genomförandeförordningen (EU) 2018/151. På nationell nivå har regeringen antagit en nationell strategi för samhällets informations- och cybersäkerhet (se Regeringens skrivelse 2016/17:213, *Nationell strategi för samhällets informations- och cybersäkerhet* av den 22 juni 2017).

106 2 § 4 p. NIS-lagen.

107 Enligt NIS-direktivets definition av samhällsviktiga tjänster inom digital infrastruktur avses (i) internetknutpunkter, (ii) DNS-tjänster, och (iii) registreringsenheter för toppdomäner (se Bilaga II till NIS-direktivet). Detta är särskilt viktigt att notera, eftersom de lätt kan sammanblandas med digitala tjänster, vars definition utesluter just dessa tjänster.

108 8 § NIS-lagen.

109 För mer ingående information om de krav som ställs på en leverantör som omfattas av NIS-regleringen avseende informationssäkerhet, se Advokatfirman Kahn Pedersens skriftserie 2020:1 *Juridisk informationssäkerhet*, s. 34 f.

110 Vad gäller vilka tjänster som är samhällsviktiga inom de olika sektorerna finns grunden för sådan bedömning i bilaga 2 i NIS-direktivet, som i sin tur anknyter till många definitioner i annan EU-lagstiftning. Den nationellt bindande regleringen finns i MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7.

Kraven på en leverantör av *digitala tjänster* är i korthet att leverantörerna ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella, men saknar krav på att arbeta efter en systematisk process.[111]

Det centrala kravet på en leverantör av *samhällsviktiga tjänster* är däremot att leverantören ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete vad gäller de nätverk och informationssystem som används för att tillhandahålla tjänsten. Detta krav preciseras i MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster som anger att arbetet ska bedrivas med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.[112] Liksom nämnts ovan är förpliktelserna för samhällsviktiga tjänster mer långtgående än för digitala tjänster. Vi kommer därför i det följande fokusera på vilka krav som NIS-regleringen ställer på sådana molntjänster som används som en del i att leverera samhällsviktiga tjänster.

NIS-regleringen innehåller, till skillnad från säkerhetsskyddslagstiftningen, i sig inga detaljerade krav på hur informationssäkerhetsarbetet ska bedrivas. Regleringen har även förhållandevis få krav på hur en utkontraktering (outsourcing) till en extern aktör, såsom en molntjänstleverantör, ska ske. För samhällsviktiga tjänster ska dock kravet på systematiskt och riskbaserat informationssäkerhetsarbete omfatta även den hantering av nätverk och informationssystem som utkontrakteras till en extern aktör.[113] Inför utkontraktering ska risker för den samhällsviktiga tjänsten identifieras och hanteras. De säkerhetsåtgärder som den externa aktören ska vidta ska regleras i avtal.

Observera att det, till skillnad från i säkerhetsskyddslagstiftningen, inte ställs några krav på att underleverantören, i detta fall molntjänstleverantören, själv tillämpar ett systematiskt och riskbaserat informationssäkerhetsarbete. Däremot ansvarar kunden, som omfattas av NIS-regleringen, för informationssäkerhetsarbetet även avseende de delar av verksamheten som utkontrakteras till molntjänstleverantören.

I de allmänna råden till MSBFS 2018:8 förordas att tjänsteavtalet tydliggör hur uppföljning av överenskomna säkerhetsåtgärder och det systematiska och riskbaserade informationssäkerhetsarbetet ska ske, och hur den externa aktören ska överlämna information till kunden om misstänkta eller inträffade incidenter, avvikelser och sårbarheter. Även krav på tillräcklig kunskap och kompetens avseende informationssäkerhet bör framgå av avtalet.

Vår bedömning är att dessa krav och rekommendationer bör kunna tillgodoses för de allra flesta molntjänster. Det centrala är kundens

111 15-16 §§ NIS-lagen samt 6 § NIS-förordningen.

112 5 § MSBFS 2018:8.

113 2 § MSBFS 2018:8.

egen bedömning av vilka risker som uppstår i och med användningen av molntjänster, val av lämpliga säkerhetsåtgärder och avtalsmässiga mekanismer för att följa upp informationssäkerhetsarbetet inklusive incidenthantering.

5. Särskilda överväganden för banker och försäkrings-företag

5.1 Inledning

”[Finansinspektionen] *ser inte någon principiell anledning till varför finansiella företag inte skulle kunna använda molntjänster hos externa leverantörer.* […]”[114]

Molntjänster inom finanssektorn är ingen ny företeelse. Det har förekommit under flera år, om än i varierande omfattning. Det är dock först de senaste åren som bankers och försäkringsföretags användning av molntjänster kommit upp till diskussion och väckt normgivarnas intresse, och då särskilt i relation till de bank- och försäkringsregulatoriska regelverken kring s.k. utkontraktering och uppdragsavtal.

”[…] *Men företag som tänker använda molntjänster behöver vara specifikt uppmärksamma på avtalsvillkoren och säkerställa att de avtal som de ingår, eller har ingått, inte innehåller begränsningar som försvårar eller omöjliggör riskhantering, kontroll och tillsyn.*”[115]

Även om flera rättsliga frågetecken gällande molntjänster har rätats ut finns det samtidigt många utmaningar som alltjämt saknar en given lösning. Kan uppgifter som omfattas av bank- eller försäkringssekretess lagras hos en molntjänstleverantör som står under inflytande av ett annat lands jurisdiktion? Vad innebär jurisdiktionsrisken för en bank eller ett försäkringsföretag? Vilka krav måste ställas för att de bank- och försäkringsregulatoriska regulatoriska kraven ska uppfyllas? Hur förhåller sig de regulatoriska regelverken till dataskyddsregleringen?

Det är mot bakgrund av dessa frågor som detta avsnitt kommer att redogöra för (vissa aspekter av) bankers och försäkringsföretags förutsättningar för att anlita utländska molntjänstleverantörer.

Inledningsvis behandlas bank- och försäkringssekretessen och vad sekretessen innebär för banker och försäkringsföretag som överväger att låta en molntjänstleverantör sköta delar av driften av en verksamhet i vilken uppgifter som skyddas av sekretess behandlas. Särskilt fokus riktas mot den jurisdiktionsrisk som är förknippad med utländska molntjänstleverantörer. Därefter tas de bank- och försäkringsregulatoriska kraven på arrangemang kring utkontraktering och uppdragsavtal upp, då särskilt enligt EBA:s riktlinjer för utkontraktering

114 Finansinspektionen, https://www.fi.se/sv/bank/utlagd-verksamhet/, under rubriken *Det sägs att FI motsätter sig användning av molntjänster, stämmer det?*, hämtad den 3 september 2020.

115 A.a.

respektive EIOPA:s riktlinjer för uppdragsavtal med molntjänsteleverantörer. Framställningen fokuserar på sådana krav och överväganden som är särskilt viktiga i förhållande till molntjänstleverantörer.

Även om de huvudsakliga områdena för detta avsnitt är bank- och försäkringsregulatoriska krav, kommer kraven på utkontraktering och uppdragsavtal i värdepappersrörelse, då Europeiska värdepappers- och marknadsmyndigheten ("**ESMA**") relativt nyligen publicerade ett utkast till riktlinjer för utkontraktering till molntjänstleverantörer, att beröras.[116]

5.2 Bank- och försäkringssekretess

5.2.1 BANKSEKRETESSEN

5.2.1.1 Sekretessens innebörd och omfattning

Banksekretessen innebär inte ett absolut förbud för banker att röja uppgifter om kunder. Vad som däremot är otillåtet, är att *obehörigen* röja enskildas förhållanden till banker. Detta följer redan av 1 kap. 10 § LBF, där det anges att "*[e]nskildas förhållanden till [banker] får inte obehörigen röjas*".

För att förstå innebörden av banksekretessen, särskilt i relation till molntjänster, krävs först en förståelse för vad som ligger i begreppen (i) *enskilda*, (ii) enskildas *förhållanden*, (iii) *röja*, och (iv) *obehörigen*.

Begreppet *enskilda* innefattar såväl fysiska som juridiska personer. Det är i detta avseende ovidkommande om kundförhållandet har upphört eller aldrig ens inletts, t.ex. om en person utan framgång har förhandlat med banken om att inleda ett kundförhållande.[117]

Med *förhållanden till banker* avses varje upplysning eller uppgift om kunden som banken har kännedom om, oavsett om uppgifterna är av ekonomisk eller annan karaktär. Banksekretessen omfattar därmed samtliga omständigheter hänförliga till kundförhållandet eller relationen mellan banken och kunden, och detta gäller oavsett på vilken väg informationen har kommit till bankens kännedom, t.ex. direkt från kunden, genom bankens egna iakttagelser eller från tredje man.[118] Banksekretess gäller information om såväl framtida, pågående som historiska bankrelationer.

Banksekretessen innebär, som sagt, ett förbud mot att obehörigen röja uppgifter för tredje man, dvs. någon annan än kunden själv eller banken.[119]

---

116 ESMA, *Consultation Paper – Draft Guidelines on Outsourcing to Cloud Service Providers*, publicerad den 3 juni 2020, ESMA50-164-3342, https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf, hämtad den 3 september 2020.

117 Prop. 2002/03:139 del 2, s. 477.

118 Jansson, Per-Ola, *Banksekretess och annan finansiell sekretess* (2010), utgiven av Svenska Bankföreningen, s. 51.

119 Prop. 2002/03:139 del 2, s. 477-478; Jansson (2010), s. 45-47.

Även om banksekretessen regleras genom svensk lag, är den relevant också utifrån regleringen av bankregulatoriska uppdragsavtal. EBA hänvisar nämligen till upprätthållandet av banksekretessen som en sådan aspekt som särskilt bör säkerställas vid utkontraktering (se vidare avsnitt 5.3.2 nedan).

5.2.1.2 Innebörden av LBF:s röjandebegrepp

Den närmare innebörden av röjandebegreppet i LBF är oklar. Detsamma gäller tolkningen av vad som ska anses vara obehörigt röjande. Varken LBF, förarbeten eller doktrin ger något fullständigt svar på frågan om när ett röjande ska anses ha ägt rum, utan vad som diskuterats är t.ex. vad som avses med enskildas förhållanden, när ett röjande kan anses behörigt och gentemot vilka sekretessen gäller.[120]

I brist på vägledande uttalanden, finns det i huvudsak två möjliga tolkningar av röjandebegreppet.

Den ena tolkningen är att ett röjande har skett när tredje man *de facto* tagit del av uppgifterna i fråga. Förenklat uttryckt, denna tolkning innebär att det sker ett röjande när tredje man (obehörigen) läser eller på annat sätt tar del av uppgifterna.

Den andra tolkningen är att ett röjande sker redan när en uppgift har gjorts tillgänglig för tredje man under sådana omständigheter att man måste räkna med att tredje man obehörigen har tagit del av uppgiften. Detta synsätt ligger i linje med den tolkning av röjandebegreppet i OSL som bl.a. eSams juridiska expertgrupp har framfört.[121]

Även om banker inte omfattas av OSL, finns flertalet omständigheter som tillsammans talar för att det är möjligt att göra samma bedömning av LBF:s röjandebegrepp, bl.a. eftersom:

- Både LBF och OSL använder begreppet *röjande*.
- LBF hänvisar till OSL i direkt anslutning till banksekretessen.[122]
- Banksekretess och sekretess enligt OSL hanteras i viss mån överlappande i lagstiftningsarbetet.[123]

---

120 Se t.ex. prop. 2002/03:139, s. 476 ff.; Jansson (2010), kapitel 5.1 och kapitel 7; SOU 1999:82, avsnitt 2.

121 eSam, som är ett samverkansprogram för 27 myndigheter och SKR, har ansett att uppgifter som omfattas av sekretess enligt OSL ska anses röjda i OSL:s mening om en uppdragstagare omfattas av regler i främmande rätt som kan tvinga uppdragstagaren att röja uppgifterna samt att omständigheterna i övrigt medför att det är osannolikt att leverantören får ta del av eller vidarebefordra uppgifterna. Detta gäller även om uppdragstagaren enligt avtalet med uppdragsgivaren förbjuds att ta del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga för leverantören (s.k. sanktionerad avtalssekretess). Se vidare Rättsligt uttalande om röjandebegreppet enligt offentlighets- och sekretesslagen av den 17 december 2015, dnr/ref: VER 2015-190; Rättsligt uttalande om röjande och molntjänster av den 23 oktober 2018, dnr/ref: VER 2018:57; Kompletterande information om molntjänster, promemoria av den 20 september 2019.

122 1 kap. 10 § 1 respektive 2 st. LBF.

123 Se t.ex. prop. 2002/03:139.

- Vi kan inte se att det skydd som sekretessen enligt OSL innebär, skulle vara strängare än det skydd som banksekretessen ger. OSL tar t.ex. sikte på enskildas ekonomiska förhållanden, medan banksekretessen även omfattar icke-ekonomiska förhållanden. Vidare tar OSL i större utsträckning tar hänsyn till om den enskilde *de facto* kan antas lida skada av ett röjande.[124]

Vi kan dock samtidigt konstatera att det saknas uttryckligt stöd – för eller emot – för att göra samma tolkning av röjandebegreppet i LBF som i OSL.

5.2.1.3 Förbudet mot att obehörigen röja uppgifter

Banksekretessen innebär, som nämnts ovan, inget absolut förbud mot röjande, utan endast ett förbud mot att *obehörigen* röja uppgifter för tredje man, dvs. för någon annan än kunden själv eller banken.[125] Det anses exempelvis inte röra sig om ett obehörigt röjande om röjandet är nödvändigt för att skydda den egna verksamheten, t.ex. vid tvist mellan banken och kunden,[126] eller om röjandet av en uppgift sker med stöd av den enskildes samtycke.[127] Samtycke anses dock inte kunna inhämtas genom bankens allmänna villkor där kunden generellt och på förhand avtalar bort banksekretessen.[128]

Banksekretessen innebär inte heller något förbud mot att en bank låter en uppdragstagare ta del av nödvändiga uppgifter för att uppdraget ska kunna utföras.[129] Det är således ett behörigt röjande. Det är emellertid alltid banken som gentemot kunden bär ansvaret för att banksekretessen upprätthålls, varför en bank som lämnar ut uppgifter som omfattas av banksekretess till en uppdragstagare måste säkerställa att uppdragstagaren omfattas av en minst lika långtgående sekretess som banken och att uppdragstagare således inte röjer uppgifterna obehörigen. Detta innebär bl.a. att uppdragsavtalet[130] bör ange i vilka situationer uppdragstagaren i sin tur får lämna ut uppgifterna.[131]

Därutöver handlar det inte om ett obehörigt röjande om banken är skyldig att röja uppgifter om bankens mellanhavanden med dess kunder enligt svensk lag eller enligt EU-rätten. Det kan t.ex. röra sig om att förhindra eller beivra brottslig verksamhet.[132]

---

124 Se t.ex. 31 kap. 1-3 §§ OSL.

125 Prop. 2002/03:139 del 2, s. 477-478; Jansson (2010), s. 102.

126 Jansson (2010), s. 129 ff.

127 Prop. 2002/03:139 del 2, s. 478-479; Jansson (2010), s. 106-107.

128 SOU 1999:82, s. 126; prop. 2002/03:139 del 2, s. 479.

129 Prop. 2002/03:139 del 2, s. 478.

130 Här avses även sådana uppdragsavtal som inte omfattas av bankens anmälningsplikt gentemot Finansinspektionen, jfr. 6 kap. 7 § LFB.

131 Jansson (2010), s. 218-220.

132 Se t.ex. 4 kap. 3 och 6 §§ lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, och 3 kap. 1 § lag (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning.

Varken LBF, förarbeten eller doktrin behandlar frågan om skyldigheter enligt utländsk lagstiftning kan göra ett röjande av sekretesskyddade uppgifter behörigt. Vi bedömer dock att inte finns möjlighet enligt svensk rätt för en svensk bank att hänvisa till utländsk lagstiftning för att bryta igenom den svenska banksekretessen, såvida inte annat följer av svensk lag eller EU-rätten.[133] Detta innebär att för det fall att en bank anlitar en utländsk leverantör som genom uppdraget får ta del av sekretesskyddade uppgifter om bankens kunder, är det enligt vår bedömning inte förenligt med LBF att leverantören i sin tur röjer sådana uppgifter till följd av krav i utländsk lagstiftning, även om leverantören är bunden av den lagstiftningen (dvs. om det landet har jurisdiktion).

Denna bedömning stöds bl.a. av LBF:s bestämmelser om uppgiftsskyldighet i relation till utländska brottsbekämpande myndigheter. En bank är nämligen skyldig att röja sekretesskyddade uppgifter ”*om det under en utredning enligt bestämmelserna om förundersökning i brottmål begärs av undersökningsledaren eller om det begärs av åklagare i ett ärende om rättslig hjälp i brottmål, på framställning av en annan stat eller en mellanfolklig domstol, eller i ett ärende om erkännande och verkställighet av en europeisk utredningsorder*” [vår understrykning tillagd].[134] Utan denna bestämmelse skulle svenska banker inte ha någon laglig möjlighet att röja enskildas uppgifter för utländska brottsbekämpande myndigheter. Dessutom är sådant röjande inte möjligt om inte framställan görs av svensk åklagare.

Liknande regler finns i fråga om uppgifter som lämnas ut för beskattningsändamål, även när rapporteringsplikten följer av svensk lag. Svenska banker har under vissa förutsättningar en skyldighet att lämna ut uppgifter om sina kunder för att utländska stater ska kunna beskatta dessa på ett korrekt sätt. Trots att denna skyldighet följer av skatteförfarandelagen (2011:1244), får banker inte rapportera informationen direkt till de utländska myndigheterna. Informationen måste istället lämnas till Skatteverket, som i sin tur lämnar ut uppgifterna till den utländska skattemyndigheten.[135]

Mot denna bakgrund gör vi bedömningen att banker endast får röja uppgifter som omfattas av banksekretessen med hänvisning till en lagstadgad skyldighet när denna skyldighet följer av svensk rätt. Motsatsvis kan en bank inte *behörigen* röja sekretesskyddade uppgifter enbart på grundval av utländsk lagstiftning. Det talar för att en viss försiktighet bör iakttas vid anlitandet av molntjänstleverantörer som kan omfattas av lagstiftning som kan möjliggöra utlämnande av sekretesskyddade uppgifter till utländska myndigheter. En noggrann

133 Jfr. situationen där en person i Sverige utför en handling som är brottslig enligt svensk rätt, men laglig i ett annat land.

134 1 kap. 11 § LFB.

135 Själva skyldigheten följer av 22 a och 22 b kap. skatteförfarandelagen (2011:1244), medan den närmare regleringen kring rapporteringspliktens omfattning följer av lag (2015:62) om identifiering av rapporteringspliktiga konton med anledning av FATCA-avtalet respektive lag (2015:911) om identifiering av rapporteringspliktiga konton vid automatiskt utbyte av upplysningar om finansiella konton.

bedömning i det enskilda fallet måste göras. Vikten av banksekretessens upprätthållande ska inte underskattas då ett obehörigt röjande, utöver juridiska konsekvenser, allvarligt kan skada kundernas förtroende för banken.

5.2.2 FÖRSÄKRINGSSEKRETESS

Till skillnad från banksekretessen är försäkringssekretessen, med undantag för bestämmelserna i försäkringsrörelselagen (2010:3043, ”**FRL**”) om sekretess till förmån för förmånstagare samt genetisk undersökning och information,[136] inte uttryckligen reglerad i lag. Den har främst kommit att utvecklas genom försäkringsbranschens handelsbruk. Försäkringsbranschen har sedan länge tillämpat en frivilligt anammad sekretess.[137] Utöver ovan nämnda lagbestämmelser följer försäkringssekretessen i regel av avtalet mellan försäkringsgivaren och försäkringstagaren, samt av en allmän lojalitetsplikt mellan parterna till följd av parternas avtalsförhållande.[138]

I den svenska försäkringsrörelsen anses försäkringssekretessen ha fått en så långtgående omfattning att den väsentligen anses kunna jämföras med banksekretessen.[139] Detta bör, enligt vår bedömning, innebära att om ett röjande anses vara behörigt enligt banksekretessen, ska ett sådant röjande sannolikt även vara förenligt med försäkringssekretessen. Om röjandet innefattar information om förmånstagare eller genetisk undersökning och information, måste dock de särskilda sekretessreglerna i FRL iakttas.

Det saknas även särskilda bestämmelser kring försäkringssekretess vid anlitandet av uppdragstagare[140]. I avsaknad av ett förbud mot röjande till uppdragstagare och eftersom ett sådant röjande under vissa förutsättningar är behörigt enligt banksekretessen, ser vi det inte som sannolikt att anlitandet av uppdragstagare som tar del av nödvändiga uppgifter för att kunna genomföra sitt uppdrag skulle utgöra obehörigt röjande enligt försäkringssekretessen. Detta förutsatt att försäkringsföretaget i avtalet med sådan uppdragstagare ålägger uppdragstagare en minst lika långtgående sekretess som åligger försäkringsföretaget självt.

Svensk Försäkring, försäkringsföretagens branschorganisation, har tagit fram vägledningar och rekommendationer för branschen, avseende bl.a. möjligheten för försäkringsföretag att lämna ut uppgifter till polisen, domstolar, andra myndigheter samt andra försäkrings-

136 4 kap. 14 och 16 §§ FRL.

137 Svensk Försäkring, *Grundläggande principer för skadebehandling*, s. 9, https://www.svenskforsakring.se/globalassets/rekommendationer/rekommendationer-om-skadereglering/grundlaggande-principer-for-skadebehandling.pdf, hämtad den 3 september 2020.

138 Jansson (2010), s. 66-64; s. 69.

139 Jansson (2010), s. 66-64; s. 69.

140 Med *uppdragstagare* avses här alla externa aktörer vilka utför arbete åt en bank eller ett försäkringsföretag.

företag. Enligt rekommendationerna ska försäkringsföretag lämna ut uppgifter till myndigheter, som med stöd i svensk lag begär upplysningar. Försäkringsföretag får även använda uppgifterna i samband med rättslig prövning vid allmän domstol eller lämna uppgifter till polisen och annan myndighet i samband med anmälan om misstänkt brott. Därutöver får försäkringsföretag samarbeta och biträda varandra i utredningsärenden, i syfte att upptäcka och förebygga brott och bedrägerier.[141] Försäkringsföretag uppmanas även att be att en myndighet som begär att uppgifter om viss person ska lämnas ut, anger det lagstöd som finns för sådan begäran.[142] Riktlinjerna nämner inget om utlämnande av uppgifter till utländska myndigheter eller utländska försäkringsföretag. Frågan om skyldigheter enligt utländsk lagstiftning kan göra ett röjande av sekretesskyddade uppgifter behörigt, behandlas inte inom försäkringssekretessen heller.

Det kan konstateras att försäkringssekretessen har givits en relativt långtgående omfattning, låt vara med vissa undantag. Detta, i kombination med avsaknaden av närmare vägledning från t.ex. Svensk Försäkring, talar för att en viss försiktighet bör iakttas vid anlitandet av molntjänstleverantörer som kan omfattas av lagstiftning som kan möjliggöra utlämnande av sekretesskyddade uppgifter till utländska myndigheter. I sammanhanget bör noteras att uppgifter som hanteras inom försäkringsföretag svårligen kan anses ha ett lägre skyddsvärde än uppgifter som hanteras inom bankverksamhet, särskilt då det kan förekomma uppgifter av ännu känsligare natur inom försäkringsföretag (t.ex. hälsodeklarationer). En noggrann bedömning i det enskilda fallet måste göras. Vikten av försäkringssekretessens upprätthållande ska inte underskattas då ett obehörigt röjande utöver juridiska konsekvenser allvarligt kan skada kundernas förtroende för försäkringsföretaget.

5.3 Bank- och försäkringsregulatoriska frågor kring uppdragsavtal

5.3.1 ALLMÄNT OM UTKONTRAKTERING OCH UPPDRAGSAVTAL

Med *utkontraktering* avses i bank- och försäkringsregulatoriska sammanhang *”ett arrangemang eller en överenskommelse, oavsett form, mellan en bank eller ett försäkringsföretag och en tjänsteleverantör där denna tjänsteleverantör utför en process, en tjänst eller en verksamhet som annars skulle ha utförts av banken eller försäkringsföretaget självt”*.[143]

---

141 Svensk Försäkring, *Riktlinjer för försäkringsföretagens utredningsverksamhet*, s. 4, https://www.svenskforsakring.se/globalassets/riktlinjer/riktlinjer-for-forsakringsforetagens-utredningsverksamhet.pdf, hämtad den 3 september 2020.

142 Svensk Försäkring, *Rekommendation om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet*, s. 6, https://www.svenskforsakring.se/globalassets/rekommendationer/rekommendationer-om-personuppgifter/rekommendation-om-behandling-av-personuppgifter-inom-forsakringsforetagens-utredningsverksamhetdoc.pdf, hämtad den 3 september 2020.

143 Jfr. punkt 12 i EBA:s riktlinjer för utkontraktering och artikel 13.28 Solvens II-direktivet. Notera att detta inte är ett ordagrant citat, utan rent redaktionella ändringar har gjorts för att samordna definitionen för banker och försäkringsföretag. Definitionerna är dock likalydande i sak.

Både banker och försäkringsföretag har ett stort antal rättsakter och regler, såväl nationella som EU-rättsliga, att förhålla sig till vid utkontraktering. Dessa regler tar bl.a. sikte på interna styrprocesser, riskbedömning inför utkontrakteringar och krav på det avtal med tjänsteleverantören som reglerar utkontrakteringen (det s.k. uppdragsavtalet). Hur omfattande reglerna är beror till viss del på huruvida det är fråga om ”vanlig” utkontraktering eller utkontraktering som avser funktioner, processer eller arbete som är av väsentlig betydelse[144] för verksamheten. Kraven på utkontraktering som anses vara av väsentlig betydelse är mer omfattande och ställer högre krav på både banken/försäkringsföretaget och dess tjänsteleverantör, särskilt i fråga om uppdragsavtalets innehåll. Gemensamt för banker och försäkringsföretag är att uppdragsavtal avseende utkontraktering av väsentlig betydelse ska anmälas till Finansinspektionen.[145]

Själva anmälningsplikten följer av nationell lagstiftning, men det är främst på EU-nivå som definitionen av och kraven på utkontraktering förtydligas. Av det skälet kommer den fortsatta framställningen främst ta sikte på EU:s regelverk.[146]

> Vi vill understryka att framställningen belyser ett urval av relevanta bestämmelser men att den på intet sätt är fullständig.

Banker ska följa EBA:s riktlinjer för utkontraktering, som publicerades i februari 2019. Tidigare gällde dels Europeiska banktillsynskommitténs riktlinjer om utkontraktering,[147] dels EBA:s rekommendationer för utkontraktering till molntjänstleverantörer.[148] Regelverken upphävdes dock i samband med att 2019 års riktlinjer trädde i kraft.[149]

Försäkringsföretag har å sin sida att förhålla sig till Kommissionens delegerade förordning (EU) 2015/35[150] (”**delegerade förordningen till Solvens II**”), och då närmare bestämt artikel 274 i förordningen. Artikel 274 innehåller ett antal krav som är generellt tillämpliga, dvs. oavsett vad för typ av tjänsteleverantör som anlitas. Därtill har EIOPA, såsom

144 Detta används som ett samlingsbegrepp för vad som benämns som *viktiga*, *kritiska* eller *avgörande*.

145 6 kap. 7 § LBF och 10 kap. 21 § FRL. För bankers vidkommande, se även Finansinspektionens allmänna råd till 10 kap. 2 § Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut.

146 Till sak hör även att Finansinspektionen åtagit sig att följa EBA:s och EIOPA:s respektive riktlinjer. Avseende EBA, se *Guidelines compliance table: Guidelines on outsourcing arrangements*. https://eba.europa.eu/sites/default/documents/files/document_library//EBA%20GL%202019%2002%20-%20CT%20GLs%20on%20outsourcing%20arrangements.pdf, hämtad den 3 september 2020. Avseende EIOPA, se https://www.fi.se/sv/publicerat/nyheter/2020/fi-kommer-tillampa-eu-riktlinjer-om-uppdragsavtal-med-molntjanstleverantorer/, hämtad den 3 september 2020.

147 Europeiska banktillsynskommittén, *Guidelines on Outsourcing*, publicerade den 14 december 2006. Europeiska banktillsynskommittén var föregångaren till EBA.

148 EBA, *Rekommendationer om utkontraktering till molntjänstleverantörer*, EBA/REC/2017/03, publicerade den 28 mars 2018.

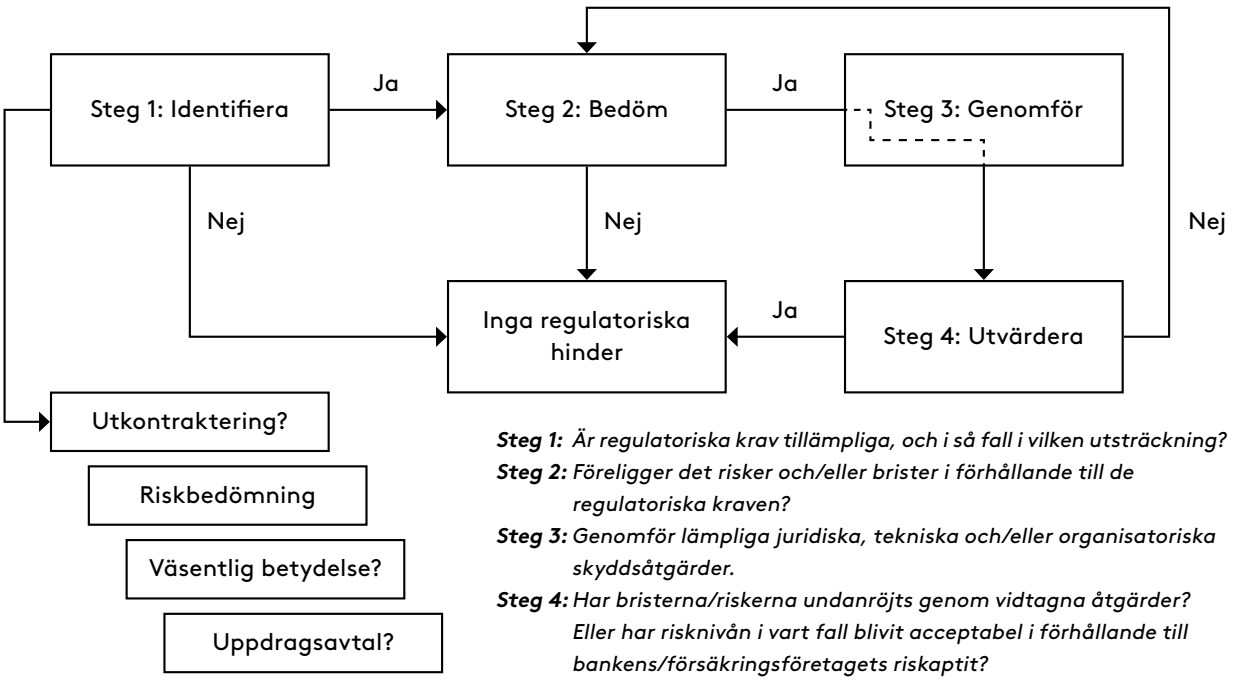
149 Punkt 17 i EBA:s riktlinjer för utkontraktering.

150 Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II).

nämns ovan, publicerat riktlinjer om uppdragsavtal med molntjänstleverantörer. Den delegerade förordningen till Solvens II och EIOPA:s riktlinjer är parallellt tillämpliga vid utkontraktering till molntjänstleverantörer, vilket, som kommer framgå nedan, är viktigt att ha i åtanke.

EBA:s riktlinjer ger banker vägledning om *vad* som egentligen utgör utkontraktering, *när* en utkontraktering ska anses vara av väsentlig betydelse och *vilka* krav som dels ställs på banken, dels som banken måste ställa på sin tjänsteleverantör. För försäkringsföretags vidkommande ges alltså motsvarande vägledning i delegerade förordningen till Solvens II och, såvitt avser utkontraktering till molntjänstleverantörer, EIOPA:s riktlinjer.

Innan vi går vidare och närmare redogör för vad de bank- och försäkringsregulatoriska kraven innebär när en bank eller ett försäkringsföretag önskar utföra en utkontraktering till en molntjänstleverantör, ska något sägas om den generella processen vid en potentiell utkontraktering. Genom figuren nedan vill vi ge en förenklad, schematisk och översiktlig bild av bedömningen *inför* en potentiell utkontraktering, dvs. vid prövningen av huruvida en viss tjänsteleverantör kan anlitas. I detta sammanhang är det av underordnad betydelse om det är fråga om en molntjänstleverantör, men som framgår nedan krävs vissa särskilda överväganden när det är fråga om utkontraktering till molntjänstleverantörer.



Figur 5.1: Bedömningen inför ev. utkontraktering.

Det är inte samtliga utkontrakteringar som per definition är utkontrakteringar i bank- eller försäkringsregulatorisk mening. En bank eller

ett försäkringsföretag måste, som ett första steg, överväga huruvida de regulatoriska kraven alls är tillämpliga. Det finns ibland en tendens att utgå från att det finns ett likhetstecken mellan att anlita en tjänsteleverantör och utkontraktering i regulatorisk bemärkelse. Vidare, även om det är fråga om regulatorisk utkontraktering behöver det inte innebära stora hinder eller kräva omfattande åtgärder från bankens eller försäkringsföretagets sida. Vad som krävs i det enskilda fallet beror istället på vad som identifieras i riskbedömningen och företagsbesiktningen (due diligence), och huruvida utkontrakteringen kan säga vara av väsentlig betydelse.

En utkontraktering medför *per se* tredjepartsrisker. Regelverken syftar inte till att samtliga risker ska elimineras, utan det som är relevant är att banken eller försäkringsföretaget kan *hantera* de risker som uppstår i och med utkontrakteringen.

För att hantera de risker som uppstår kan banken eller försäkringsföretaget genomföra säkerhetsåtgärder. Som exempel kan nämnas avtalsförhandlingar för att säkerställa att uppdragsavtalet uppfyller regulatoriska krav, kryptering av data som överförs till tjänsteleverantören och rätten att göra noggranna och regelbundna revisioner.

Syftet är att genomförda säkerhetsåtgärder ska medföra att utkontrakteringen sammantaget medför en acceptabel risknivå. Det bör dock noteras att i figuren ovan har ett i praktiken högst relevant alternativ utelämnats, nämligen när utkontrakteringen, säkerhetsåtgärderna till trots, medför sådana brister avseende kontrollen av verksamheten eller att riskerna i övrigt inte kan hanteras på ett tillfredsställande sätt, varvid utkontrakteringen inte kan genomföras.

5.3.2 BANK- OCH FÖRSÄKRINGSREGULATORISKA KRAV OCH ÖVERVÄGANDEN VID UTKONTRAKTERING TILL MOLNTJÄNSTLEVERANTÖRER

5.3.2.1 Krav på uppdragsavtalets utformning och innehåll

När en bank eller ett försäkringsföretag väljer att utkontraktera verksamhet av väsentlig betydelse, ställer både EBA och EIOPA uttryckliga krav på uppdragsavtalets utformning och innehåll. Det är därför av central betydelse att bedöma om utkontrakteringen är av väsentlig betydelse (jfr. figur 6.1 ovan). Vi kommer inte att gå in på *hur* bedömningen av vad som utgör utkontraktering av väsentlig betydelse går till, utan endast nämna några aspekter att ta hänsyn till vid bedömningen, nämligen (i) att fel eller brister i den utkontrakterade funktionen försämrar bankens eller försäkringsföretagets regelefterlevnad, finansiella resultat eller kontinuiteten i övriga tjänster, (ii) att interna kontrollfunktioners operativa uppgifter utkontrakteras, och (iii) inlåsningseffekter.[151]

151 För en fullständig uppräkning, se punkt 29-31 i EBA:s riktlinjer för molntjänstleverantörer, respektive punkt 28-29 i EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

EBA:s och EIOPA:s respektive riktlinjer innehåller i huvudsak motsvarande regleringar i detta avseende och skillnaderna är främst redaktionella. Exempel på materiella skillnader är att EIOPA ställer krav på att uppdragsavtalet ska ange behörig domstol och att EBA ställer krav på uttrycklig hänvisning till bankens resolutionsmyndighet (och dess befogenhet i händelse av resolution).[152] Med detta sagt, räcker det inte att endast gå igenom kravkatalogerna i EBA:s och EIOPA:s respektive riktlinjer.

I tillägg till de krav som följer av EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer, har försäkringsföretag, som sagt, att efterkomma kraven i den delegerande förordningen till Solvens II. Det är därför viktigt att ha i åtanke att artikel 274 i förordningen ställer ett antal krav på försäkringsföretags uppdragsavtal som inte följer av EIOPA:s riktlinjer – några exempel är:

- Molntjänstleverantören ska åta sig att efterleva tillämpliga lagar, föreskrifter, allmänna råd och försäkringsföretagets styrdokument, samt samarbeta med och besvara frågor från tillsynsmyndigheter;[153]

- Uppdragsavtalet ska ange en tillräckligt lång uppsägningstid för att säkerställa att försäkringsföretaget kan hitta en alternativ lösning;[154] och

- Försäkringsföretaget ska ha rätt till information om de funktioner och verksamheter som omfattas av uppdragsavtalet och dessas resultat, och ha en instruktionsrätt.[155]

Motsvarande krav ställs också på bankers uppdragsavtal, om än inte lika tydligt. EBA:s riktlinjer innehåller nämligen krav som endast kan tillgodoses genom uppdragsavtalet. Som exempel kan nämnas att banker har en skyldighet att ”[säkerställa att] *de kan fatta och genomföra beslut som gäller deras affärsverksamhet och kritiska eller viktiga funktioner, även beträffande dem som har utkontrakterats*”.[156] Detta är förvisso inget formellt krav som framgår av EBA:s kravkatalog, men vi har svårt att se hur denna skyldighet kan tillgodoses om det inte anges en instruktionsrätt i uppdragsavtalet. På motsvarande sätt är ett kontraktuellt krav på att följa bankens styrdokument[157] det effektivaste sättet att säkerställa *”att tjänsteleverantörerna agerar på ett sätt som överensstämmer med deras värderingar och uppförandekod*”.[158]

De flesta, för att inte säga samtliga, större molntjänstleverantörer

152 Punkt 74-75 i EBA:s riktlinjer för molntjänstleverantörer, respektive punkt 36-37 i EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

153 Artikel 274.4 b) och i) delegerade förordningen till Solvens II.

154 Artikel 274.4 d) delegerade förordningen till Solvens II.

155 Artikel 274.4 f) och j) delegerade förordningen till Solvens II.

156 Punkt 40 a) i EBA:s riktlinjer för utkontraktering.

157 Typiskt sett en uppförandekod för leverantörer (eng. *code of conduct*).

158 Punkt 73 i EBA:s riktlinjer för molntjänstleverantörer.

erbjuder idag någon form av särskilt tilläggsavtal för kunder inom bank eller försäkring. Dessa ska vara särskilt anpassade till bankers och försäkringsföretags regulatoriska verklighet, och tydliga förbättringar har skett bara under det senaste året.

Ett särskilt tillägg avseende bank- eller försäkringsregulatoriska krav brukar till viss del förbättra bankens eller försäkringsföretagets förutsättningar för att uppfylla sina regulatoriska skyldigheter, särskilt i fråga om de formella kraven i EBA:s och EIOPA:s respektive kravkatalog med avseende på revision och rapportering. Dock har vi inte sett något sådant tillägg som uppfyller samtliga regulatoriska krav. Banker och försäkringsföretag måste därför noggrant granska dels det särskilda tillägget i sig, dels villkoren tillsammans med avtalet i dess helhet. Det är inte alltid helt enkelt att identifiera samtliga krav, och det är ofta en utmaning att förstå vilka bestämmelser i molntjänstleverantörers villkor som kan vara problematiska ur ett regulatoriskt perspektiv, trots att det finns ett särskilt tillägg. Som exempel kan följande nämnas:

- Det är sällan en bank kan ”*fatta och genomföra beslut*” avseende de utkontrakterade funktionerna. Detsamma gäller i fråga om försäkringsföretags instruktionsrätt.

- Brister i avtalsstrukturen som i praktiken gör det särskilda tillägget betydelselöst i förhållande till andra bestämmelser i avtalet. Gäller det särskilda tillägget före de övriga bestämmelser i avtalet?

- Det förekommer att molntjänstleverantörer, ensidigt och utan att några objektiva förutsättningar ska vara uppfyllda, kan besluta att det särskilda tillägget inte ska gälla ifall det skulle stå i strid med molntjänstleverantörens ”intressen”. Därmed reduceras betydelsen av det särskilda tillägget till närmast en avsiktsförklaring.

- Servicenivåer[159] kanske anges, men är de tillräckliga givet bankens eller försäkringsföretagets beroende av tjänsten? Är de stringent formulerade och sanktionerade? Det förekommer inte sällan att molntjänstleverantörer ensidigt kan påkalla undantag från servicenivåerna utan några möjligheter till motkrav från banken eller försäkringsföretaget.

Banker och försäkringsföretag måste även beakta övrig relevant lagstiftning och normgivning. Riskerar utkontrakteringen, antingen på grund av dess utformning eller på grund av avtalsvillkoren, att leda till att uppgifter som omfattas av bank- eller försäkringssekretessen obehörigen röjs? Ett parallellt problem, som utvecklas i avsnitt 5.3.2.3 nedan, är att otjänliga förutsättningar och reglering av dataskyddet i sig kan leda till bristande efterlevnad av bank- eller försäkringsregulatoriska krav.

159 Eng. *service level,* regleras typiskt sett genom ett *Service Level Agreement*, eller ”SLA”.

5.3.2.2 Jurisdiktionsrisken och kravet på kontroll över och av utkontrakterade funktioner och verksamheter

Både EBA:s och EIOPA:s riktlinjer är en viktig del i kraven på banker och försäkringsföretag att kunna hantera tredjepartsrisker och därmed säkerställa kontroll över utkontrakterade verksamheter. Det måste därför vara möjligt att fatta och genomföra beslut rörande verksamheten, behålla ordningen i den utkontrakterade verksamheten och säkerställa att den utkontrakterade verksamheten kan hämtas hem.[160] Mot denna bakgrund blir det särskilt relevant att knyta an till den jurisdiktionsrisk som diskuterats i avsnitt 3.2 ovan.

Som konstaterats ovan kan en molntjänstleverantör tvingas lämna ut uppgifter till utländska myndigheter med stöd av utländsk lagstiftning. Utöver det faktum att det sannolikt innebär ett åsidosättande av bank- respektive försäkringssekretessen, ställer vi oss frågan om en bank eller ett försäkringsföretag som anlitar en uppdragstagare, som utan bankens eller försäkringsföretagets vetskap kan komma att lämna ut dennes kunduppgifter, verkligen kan sägas ha kontroll över den utkontrakterade funktionen eller dess data?

Denna utmaning har, såvitt vi känner till, inte diskuterats närmare av vare sig EBA, EIOPA, Finansinspektionen eller annan normgivare,[161] men vi ser det som en tydlig risk ur ett regulatoriskt perspektiv att en bank eller ett försäkringsföretag inte kan påverka eller ens känna till hur exempelvis kunduppgifter som molntjänstleverantören har tillgång till, *de facto* hanteras. Banker och försäkringsföretag måste, för att bibehålla kontrollen över sin verksamhet, både känna till och kunna påverka vad som sker inom ramen för den utkontrakterade delen av verksamheten.

5.3.2.3 Dataskydd och sekretess – särskilt om den bank- och försäkringsregulatoriska kopplingen till dataskyddsförordningen

Inför och löpande under en utkontraktering ska banker och försäkringsföretag, enligt EBA:s och EIOPA:s respektive riktlinjer, bedöma risker kopplade till utkontrakteringen. I riskbedömningen ingår att beakta bl.a. juridiska risker, vilka länder de utkontrakterade tjänsterna tillhandahålls från och uppgifterna lagras i, konsekvenserna av var molntjänstleverantören har hemvist, men även gällande lagar, inklusive lagar för dataskydd, i den aktuella jurisdiktionen.[162]

---

160 Se t.ex. punkt 40 a)-b) och f i EBA:s riktlinjer för utkontraktering. Se vidare punkterna 37-43 i (första delen av) EBA:s *Final Report on EBA Guidelines on outsourcing arrangements*, där risken i förhållande till molntjänstleverantörer framhålls särskilt. Såvitt avser försäkringsföretag, se t.ex. skäl 37, artikel 38 och artikel 49 Solvens II-direktivet, samt skäl 101 och artikel 274 delegerade förordningen till Solvens II.

161 European Banking Federation ("**EBF**"), de europeiska ländernas gemensamma bankförening, publicerade den 4 juni 2020 tre s.k. technical papers, nämligen *The use of Cloud Computing by Financial Institutions, Cloud exit strategy – testing of exit plans*, och *Cloud Outsourcing Register.* EBF ger god vägledning och praktiska råd om hur riskbedömning ska gå till, exit-planer utformas och utkontrakteringsregister fyllas i, men dessvärre saknas djupare problematiseringar och de närmare juridiska resonemangen. https://www.ebf.eu/cybersecurity-innovation/ebf-cloud-banking-forum-releases-three-technical-papers/, hämtad den 3 september 2020.

162 Punkt 68 b)-d.i) i EBA:s riktlinjer för utkontraktering, respektive punkt 29 f), 31 b) och 37 f) i EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

För banker ställs även ett uttryckligt krav på att ta hänsyn till skillnader i nationella bestämmelser när det gäller skydd av personuppgifter, i synnerhet vid utkontraktering till tredjeländer. Detta korresponderar sin tur med kravet på att uppdragsavtal ska innehålla en skyldighet för molntjänstleverantören att skydda konfidentiell, personlig eller på annat sätt känslig information och följa alla juridiska krav på dataskydd som gäller för banken.[163]

I vissa delar ställer EBA och EIOPA uttryckliga krav på att banker och försäkringsföretag måste ta hänsyn till dataskyddsförordningen och att säkerställa att såväl de själva som tjänsteleverantörer uppfyller samtliga krav enligt dataskyddsförordningen.[164] För banker betonas detta särskilt i relation till molntjänstleverantörer, som även i andra avseenden adresseras särskilt av EBA medan EIOPA:s riktlinjer som nämnts ovan uteslutande tar sikte på just molntjänstleverantörer.[165] EBA anger t.ex. att banker bör anta ett riskbaserat förhållningssätt till platsen/platserna för datalagring och behandling av uppgifter och beakta informationssäkerheten vid utkontraktering till molntjänstleverantörer och andra lösningar som innebär hantering eller överföring av personuppgifter eller konfidentiella uppgifter.[166]

Kopplingen mellan å ena sidan EBA:s och EIOPA:s respektive riktlinjer och dataskyddsrätten å andra sidan, innebär, annorlunda uttryckt, att om det skulle finnas dataskyddsrättsliga brister inom ramen för en utkontraktering, t.ex. genom att inte kraven enligt dataskyddsförordningen uppfylls, medför detta att utkontrakteringen inte uppfyller de bank- och försäkringsregulatoriska kraven på utkontraktering och uppdragsavtal.

Vad som i övrigt anges i denna rapport avseende dataskyddsrättsliga risker förknippade med utländska molntjänstleverantörer blir därför aktuellt även ur ett regulatoriskt perspektiv.[167] På samma sätt kan ett åsidosättande av banksekretessen innebära ett åsidosättande av EBA:s riktlinjer för utkontraktering, eftersom EBA uttryckligen hänvisar till upprätthållandet av banksekretessen.[168] EIOPA:s riktlinjer är inte fullt så tydliga, utan uttalar i mer generella ordalag att försäkringsföretag ska definiera en *"lämplig skyddsnivå för konfidentiella uppgifter"*.[169]

---

163 Punkt 84 i EBA:s riktlinjer för utkontraktering.

164 Se punkterna 31 j), 34 och 40 g) och 68 d.i) i EBA:s riktlinjer för utkontraktering, respektive punkt 29 f) och 31 b.iv) i EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

165 Se särskilt punkterna 54 h), 83 och 97 i EBA:s riktlinjer för utkontraktering.

166 Punkt 83 i EBA:s riktlinjer för utkontraktering.

167 I förekommande fall kan också SSL och/eller NIS-lagens krav kan behöva beaktas inom ramen för den bank- eller försäkringsregulatoriska bedömningen, eftersom banker försäkringsföretag har att efterkomma samtliga lagar som gäller för verksamheten.

168 Punkt 84 i EBA:s riktlinjer för utkontraktering.

169 Punkt 49 b) i EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

5.3.3 NÅGOT OM UTKONTRAKTERING OCH UPPDRAGSAVTAL I VÄRDEPAPPERSRÖRELSE

I fråga om uppdragsavtal inom ramen för bankers värdepappersrörelse följer anmälningsskyldigheten av lagen (2007:528) om värdepappersmarknaden ("**VpmL**").[170] Med uppdragsavtal avses enligt VpmL ett uppdrag där någon annan utför "*ett visst arbete och vissa funktioner som är av väsentlig betydelse för verksamheten*". Anmälningsskyldigheten uppstår när uppdragsavtalet innebär en väsentlig förändring av förutsättningarna för tillståndet att driva värdepappersrörelse.[171]

Enligt Europaparlamentets och rådets direktiv 2014/65/EU om marknaden för finansiella instrument ("**MiFID II**") ska värdepappersföretag som ingår uppdragsavtal avseende operativa funktioner som är av avgörande betydelse för tjänsternas tillhandahållande, vidta åtgärder för att undvika ytterligare operativa risker.[172] Kraven vid utkontraktering av avgörande eller viktiga operativa funktioner har fått sin närmare utformning genom Kommissionens delegerade förordning (EU) 2017/565 ("**delegerade förordningen till MiFID II**").[173]

Kraven enligt VpmL och delegerade förordningen till MiFID II ligger i linje med EBA:s riktlinjer för utkontraktering och är i vart fall inte mer långtgående eller omfattande. Vad som kanske är mest intressant i den delegerade förordningen, såvitt avser utkontraktering, är uppräkningen av funktioner som *inte* ska anses vara avgörande eller viktig.[174] Man kan i sammanhanget fråga sig i vilken utsträckning detta kan ge vägledning också för EBA:s och EIOPA:s respektive riktlinjer. Vi är av uppfattningen att vägledning kan hämtas från delegerade förordningen till MiFID II, låt vara med viss försiktighet och med beaktande av om det finns något konflikterande uttalande i EBA:s eller EIOPA:s respektive riktlinjer.

Det ska dock sägas att delegerade förordningen till MiFID II skiljer sig från EBA:s riktlinjer i fråga om vissa tjänsteleverantörer som är belägna i tredjeländer.[175] Dessa krav tar dock endast sikte på uppdragsavtal där värdepappersföretaget utkontrakterar funktioner "*relaterade till en investeringstjänst i form av portföljförvaltning som tillhandahålls kunder*", vilket gör att vi bedömer att detta inte är av relevans för de frågor som vi behandlar i denna rapport om molntjänster.

Som nämndes inledningsvis i detta avsnitt, publicerade ESMA relativt nyligen utkast till riktlinjer för utkontraktering till molntjänstleverantörer. Riktlinjerna var öppna för konsultation fram till september 2020, och en slutlig version kan väntas senast första kvartalet 2021.[176] Det

---

170 Se 6 kap. 7 § 2 st. LBF med hänvisning till 8 kap. 22 § VpmL. För definitionen av värdepappersrörelse, se 1 kap. 4 c § 7 st. jämförd med 2 kap. 1 § VpmL.

171 8 kap. 22 § 2 st. VpmL.

172 Artikel 16.5 MiFID II.

173 Artikel 30-32 delegerade förordningen till MiFID II.

174 För fullständig uppräkning, se artikel 30.2 delegerade förordningen till MiFID II.

175 Artikel 32 delegerade förordningen till MiFID II.

176 Se ESMA:s *Draft Guidelines on Outsourcing to Cloud Service Providers*, s. 5.

är svårt att dra några slutsatser kring riktlinjerna innan den slutliga versionen publicerats, men vi vill redan nu göra vissa observationer:

- ESMA riktar ett stort fokus mot informationssäkerhet och de inneboende risker som är förknippade med molntjänster, särskilt i fråga om dataskydd.[177] Detta uttalas redan i bakgrunden till riktlinjerna, men blir särskilt tydliga vid en jämförelse med EBA:s och EIOPA:s respektive riktlinjer.

- ESMA:s riktlinjer är mer teknikorienterade både vad gäller informationssäkerhet och riskbedömning inför utkontraktering, men också i fråga om åtkomst- och revisionsrättigheter.[178]

- Sitt teknikorienterade fokus till trots, ger ESMA:s riktlinjer inte en heltäckande bild av vad som krävs i informationssäkerhetsarbetet, exempelvis saknas krav på informationsklassning och uppföljning.[179]

177 Se avsnitt 2 i ESMA:s *Draft Guidelines on Outsourcing to Cloud Service Providers*.

178 Se t.ex. punkt 33 i)-v), 43, 51, och 54 i ESMA:s *Draft Guidelines on Outsourcing to Cloud Service Providers*.

179 Punkt 43 i ESMA:s *Draft Guidelines on Outsourcing to Cloud Service Providers*.

6. Tillämpningsexempel med Folke©-modellen

6.1 Inledning

Vi har i kapitel 2 ovan beskrivit Kahn Pedersens Folke©-modell och hur den är uppbyggd från ett teoretiskt perspektiv. I detta avsnitt kommer vi att presentera tre olika fiktiva scenarion som exempel på hur man kan tillämpa Folke©-modellen i praktiken. Genom dessa tillämpningsexempel kan vi illustrera hur de risker som diskuteras i rapportens olika kapitel kan värderas och inte minst påverkas vid anlitande av en molntjänstleverantör.

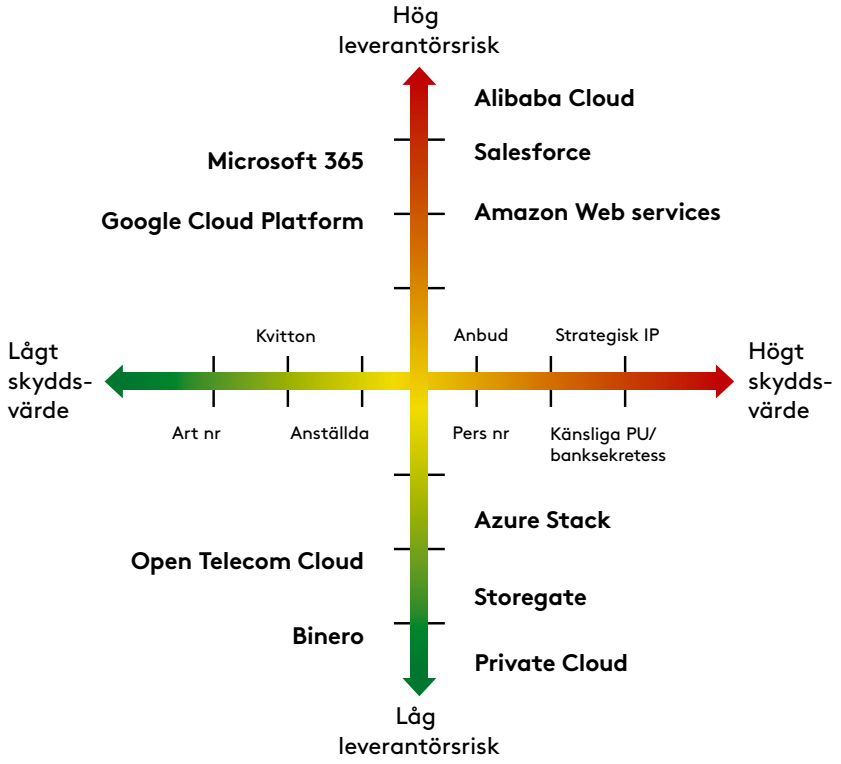
Av utrymmesskäl är det i detta sammanhang inte möjligt att inkludera en fullständig redogörelse och bedömning av alla de risker som aktualiseras i de aktuella exemplen. Vi har istället lyft fram avgörande aspekter och riskfaktorer i respektive scenario.

> Det är således på intet sätt fråga om fullständiga analyser utan enbart exempel på hur Folke©-modellen fungerar.

Sammanfattningsvis påverkas *leverantörsrisken* (Y-axeln) i Folke©-modellen huvudsakligen av (i) vilken leverantör molntjänstkunden anlitar, (ii) valet av molntjänst och dess uppsättning/arkitektur, samt (iii) vilka avtalsvillkor som är tillämpliga för tjänsten.

Informationens skyddsvärde (X-axeln) avgörs framför allt av (i) vilken information som placeras i molnet, (ii) vilka lagar och regler som är tillämpliga på informationen, (iii) hur informationen skyddas, och (iv) hur viktig och känslig informationen är för den potentiella molntjänstkundens kommersiella verksamhet och för andra skyddsintressen (t.ex. nationell säkerhet, finansiell stabilitet, externa samarbetspartners, registrerade). De olika faktorer som påverkar Folke©-modellen beskrivs mer detaljerat i kapitel 2.3 ovan.

Med följande översiktsbild vill vi illustrera hur några av de olika vanligaste molntjänsterna och olika uppgiftstyper enligt vår bedömning kan placeras ut på de två axlarna i Folke©-modellen:



Figur 6.1: Några av de vanligaste molntjänsterna och uppgiftstyper utplacerade i Folke©-modellen.

I sammanhanget bör det nämnas att leverantörsrisken för molntjänster som tillhandahålls av etablerade amerikanska molntjänstleverantörer typiskt sett, med oförändrade standardavtal, enligt vår bedömning bör placeras i den övre delen av skalan, mot bakgrund av de risker för röjande till amerikanska myndigheter som en sådan tredjelandsöverföring kan komma att innebära, bl.a. på grund av CLOUD Act, USA:s övervakningsprogram och EU-domstolens bedömning i Schrems II (som utvecklats i avsnitt 3.2.3 ovan). Detta innebär inte att användning av molntjänster från amerikanska molntjänstleverantörer alltid skulle vara otillåten eller olaglig. Som framgått tidigare i rapporten krävs alltid att molntjänstkunden gör en bedömning i det enskilda fallet. Här använder vi Folke©-modellen för sådana bedömningar.

För att tillämpa Folke©-modellen måste molntjänstkunden även bedöma sin egen generella ”riskaptit” i förhållande till de legala risker som aktualiseras. I exemplen nedan illustreras riskaptiten med den röda diagonala streckade linjen. Diagrammet i Folke©-modellen ska läsas så att positioner *ovanför* linjen indikativt betraktas som icke-godtagbar risknivå och positioner *under* linjen indikativt betraktas som acceptabla ur ett riskperspektiv.

Det tål att upprepas att Folke©-modellen inte utgör eller bygger på objektivt mätbara risker och skyddsvärden. Istället bygger den på en kvalificerad juridisk bedömning och uppskattning av dessa och syftet med modellen är att utgöra ett stöd för en kvalificerad bedömning i det enskilda fallet som är aktuellt för molntjänstkunden.

6.2 Exempel 1: Ett industribolag överväger publik molntjänst för resursplanering (SaaS)

6.2.1 BAKGRUND OCH AVGÖRANDE FIKTIVA FÖRUTSÄTTNINGAR

Ett industribolag med säte i Sverige vill effektivisera sin interna resursplanering och överväger att ingå avtal med en amerikansk molntjänstleverantör gällande en SaaS-tjänst för resursplanering.

Den information som i ett sådant fall skulle hanteras inom ramen för molntjänsten avser främst verksamhetens redovisning, pågående projekt, ekonomiska förvaltning och upphandling, vilken kan komma att innehålla information som utgör personuppgifter och information som är kommersiellt känslig för industribolaget.

Molntjänstleverantören skulle vid ett anlitande agera såsom personuppgiftsbiträde åt industribolaget som är personuppgiftsansvarig. Informationen kommer att lagras på molntjänstleverantörens datacenter inom EU/EES.

Industribolaget har, mot bakgrund av de fördelar som molntjänsten förväntas innebära för verksamheten och de övriga faktorer som framgår nedan, bestämt att bolaget har en medelhög riskaptit.

6.2.2 EXEMPEL PÅ TILLÄMPNING AV FOLKE©-MODELLEN

a) Läge 1 (utgångsläget)

LEVERANTÖRSRISK: Medium/Hög, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Leverantören	• Leverantör som lyder under amerikansk jurisdiktion → Risk för utlämnande/röjande
2. Molntjänsten	• SaaS-tjänst som kommer att medföra behandling av information i okrypterad form • Data lagras på servrar inom EU/EES
3. Avtalsvillkoren	• Alla sedvanliga risker i molntjänstavtal bedöms vara aktuella, se avsnitt 3.5 • Molntjänstleverantörens standardavtal bedöms dock vara mera balanserat än många andra standardavtal för molntjänster • Molntjänstleverantörens standardavtal regleras av svensk rätt • Molntjänstleverantörens personuppgiftsbiträdesavtal uppfyller i huvudsak kraven i dataskyddsförordningen

INFORMATIONENS SKYDDSVÄRDE: Medium, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Informationen	• Den huvudsakliga kategorin av information är uppgifter om industribolagets ekonomi/ finansiella information, projekt, personal-uppgifter, och transaktionsuppgifter • Behandlingen omfattar personuppgifter (ev. även personnummer) • Kommersiellt känslig information kommer att behandlas (dvs. företagshemligheter) • Inga uppgifter som omfattas av svensk säkerhetsskyddslagstiftning • Inga särskilda kategorier av personuppgifter (”känsliga personuppgifter”) • Inga uppgifter som innefattar brottslig verksamhet, barn eller andra särskilt sårbara kategorier av registrerade. • Inga uppgifter som omfattas av OSL
2. Tillämpliga lagar för informationen	• Dataskyddsförordningen med tillhörande regelverk • Lagen (2018:558) om skydd mot företags-hemligheter
3. Säkerhets-lösningar	• Den tekniska säkerhetsnivån bedöms vara god och innehålla sådan funktionalitet man kan förvänta sig av en publik moln-tjänst (t.ex. kryptering at rest och in transit, behörighetsstyrning, hög fysisk säkerhet etc.) • Det saknas vissa specifika säkerhets- och uppföljningsmöjligheter för molntjänst-kunden, t.ex. möjlighet att genomföra penetrationstest
4. Informationens betydelse för bolaget i övrigt (kommersiellt, tekniskt, strategiskt etc.)	• Ett röjande av informationen för främmande makt bedöms medföra stor kommersiell skada för industribolaget

KUNDENS GENERELLA RISKAPTIT: Medium/Hög, pga. följande faktorer:	
Avgörande faktorer	**Beskrivning**
1. Tillämpliga lagar och regler för verksamheten och på den information som behandlas	• Lagen (2018:558) om företagshemligheter • Dataskyddsförordningen med tillhörande regelverk
2. Marknadsspecifika och kommersiella faktorer	• Starkt konkurrensutsatt marknad, där konkurrenter genom att använda molntjänster bedöms ha viktig konkurrensfördel • Ett röjande av informationen för främmande makt bedöms medföra stor kommersiell skada för industribolaget
3. Antagna fördelar i förhållande till alternativa lösningar	• Minskade kostnader • Ökad flexibilitet • Omedelbar tillgång till nya versioner och säkerhetspatchar för mjukvaran • Tillgång till infrastrukturkompetens på högre nivå än egen drift • Generellt högre nivå på tekniska säkerhetsåtgärder

Industribolaget bedömer att den sammanvägda risken av att använda tjänsten utan att vidta ytterligare åtgärder, placeras i det röda området i Folke©-modellen, vilket överstiger bolagets riskaptit. Bolaget bör därför inte, enligt analys med Folke©-modellen, acceptera en sådan användning (se det röda krysset i figur 6.2 nedan).

För att justera risken i sådan mån att det överhuvudtaget ska vara möjligt för industribolaget att använda en molntjänst för den aktuella behandlingen, har industribolaget därför på eget initiativ vidtagit ett antal riskbegränsande åtgärder. Dessa åtgärder är:

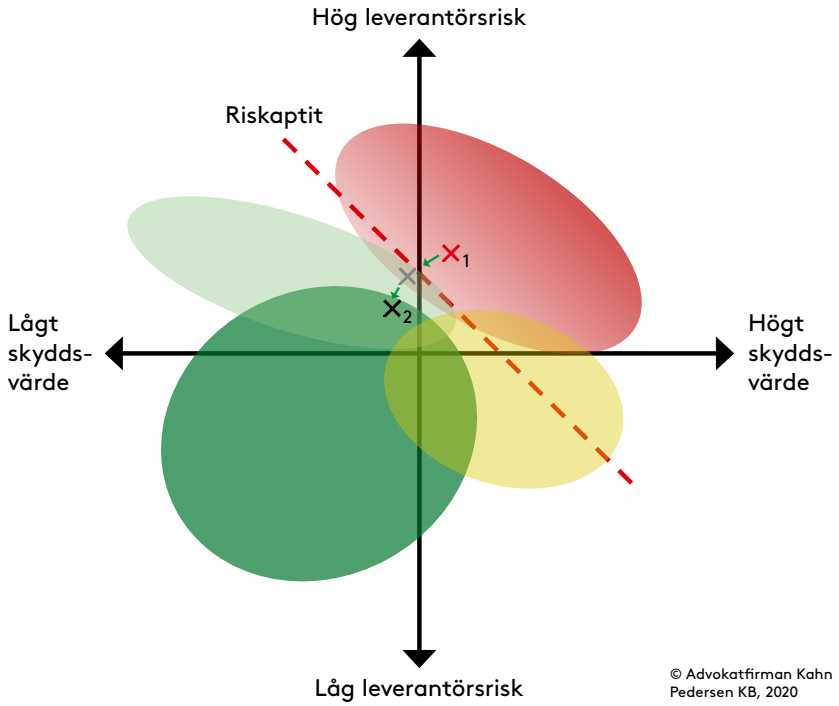
- Kartläggning av de personuppgifter som aktualiseras för tjänsten som en del av industribolagets GDPR-projekt
- Uteslutning av känsliga personaluppgifter från behandlingen
- Säkerställande av att industribolagets information separeras från andra molntjänstkunders information
- Kryptering av industribolagets information
- Säkerställande av att informationen lagras inom EU/EES

b) Läge 2 (med föreslagna förändringar)

De initiala riskåtgärder som bolaget vidtagit placerar den sammanvägda risken med användningen i det ljusgröna området i Folke©-modellen, vilket innebär en medellåg leverantörsrisk (se det grå krysset i figur 6.2 nedan).

Om industribolaget utöver de initiala riskåtgärderna även väljer att vidta de ytterligare åtgärder som föreslås nedan kommer den sammanvägda risken att justeras på så sätt att den placeras i det mörkgröna området (se det svarta krysset i figur 6.2 nedan).

Ytterligare riskbegränsande åtgärder	**Beskrivning**
1. Förhandling av avtalsvillkoren	• Lägga till uttryckliga och tydliga skyldigheter gällande avgörande it-säkerhetsåtgärder, inklusive villkor som minimerar möjligheten att informationen röjs för utländska myndigheter • Lägga till skyldighet för molntjänstleverantören att inte omlokalisera industribolagets data till något annat datacenter inom EU/EES, utan att först ha erhållit industribolagets godkännande • Införa en process som möjliggör för industribolaget att testa, följa upp och granska molntjänstleverantörens it-säkerhetsåtgärder
2. Dataskyddsrättsliga säkerhetsåtgärder	• Säkerställ att industribolaget inte är personuppgiftsbiträde åt exempelvis sina kunder för några personuppgifter som ska omfattas av tjänsten. I sådana fall krävs ytterligare åtgärder • Granska och uppdatera informationstexter till registrerade • Dokumentera industribolagets inledande dataskyddsrättsliga riskanalys (dvs. ingen konsekvensbedömning krävs) • Upprätta och genomför lämpliga processer för att säkerställa uppgiftsminimering och ändamålsbegränsning



Figur 6.2: Industribolagets riskbedömning av dess planerade användning av SaaS-tjänsten illustrerad i Folke©-modellen.

6.2.3 RESULTAT OCH REKOMMENDATION

Industribolaget skulle således, förutsatt att bolaget vidtar de föreslagna åtgärderna i avsnitt 6.2.2, kunna använda SaaS-tjänsten för dess resursplanering på ett sätt som innebär en låg risknivå för bolaget. Sådan användning ryms inom ramen för bolagets generella riskaptit, varför bolaget – enligt analys med Folke©-modellen – bör kunna gå vidare och använda den aktuella molntjänsten.

6.3 Exempel 2: En bank överväger publik molntjänst för kontorstjänster (SaaS)

6.3.1 BAKGRUND OCH AVGÖRANDE FIKTIVA FÖRUTSÄTTNINGAR

En svensk mindre bank överväger att ingå avtal med en amerikansk molntjänstleverantör gällande användning av en SaaS-tjänst för kontorstjänster.

Den information som banken skulle hantera inom ramen för molntjänsten kan både komma att innehålla information som utgör personuppgifter och sådan information om bankens kunder som omfattas av reglerna om banksekretess i LBF och EBA:s riktlinjer för utkontraktering.

Molntjänstleverantören skulle vid ett anlitande vara personuppgifts-

biträde åt banken som är personuppgiftsansvarig. Informationen i molntjänsten är avsedd att lagras på molntjänstleverantörens datacenter inom EU/EES.

Banken har med beaktande av de fördelar som banken antar att molntjänsten innebär för verksamheten och de övriga faktorer som framgår nedan, bedömt att verksamheten har en *låg/medellåg riskaptit*.

6.3.2 EXEMPEL PÅ TILLÄMPNING AV FOLKE©-MODELLEN

a) Läge 1 (utgångsläget)

LEVERANTÖRSRISK: Hög, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Leverantören	• Leverantör som lyder under amerikansk jurisdiktion → Risk för utlämnande/röjande
2. Molntjänsten	• SaaS-tjänst som kommer att medföra behandling av information i okrypterad form • Data lagras på servrar inom EU/EES
3. Avtalsvillkoren	• Alla sedvanliga risker i molntjänstavtal bedöms vara aktuella, se avsnitt 3.5 • Molntjänstleverantörens standardavtal bedöms vara mer obalanserat än många andra standardavtal för molntjänster • Molntjänstleverantörens standardavtal regleras inte av svensk rätt • Molntjänstleverantörens personuppgiftsbiträdesavtal uppfyller inte kraven i dataskyddsförordningen i lika stor utsträckning som många andra standardavtal för molntjänster

INFORMATIONENS SKYDDSVÄRDE: Högt, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Informationen	• Banken har inte begränsat vilken typ av information som får behandlas i tjänsten • Behandlingen omfattar personuppgifter (inkl. personnummer) • Behandlingen omfattar uppgifter om bankens kunder • Behandlingen kan ev. komma att omfatta särskilda kategorier av personuppgifter (”känsliga personuppgifter”) • Kommersiellt känslig information kommer ev. att behandlas (dvs. företagshemligheter) • Inga uppgifter som omfattas av svensk säkerhetsskyddslagstiftning • Behandlingen avser ett stort antal registrerade
2. Tillämpliga lagar för informationen	• Dataskyddsförordningen med tillhörande regelverk • Lagen om bank- och finansieringsrörelse och andra regulatoriska krav • Lagen (2018:558) om skydd mot företagshemligheter
3. Säkerhetslösningar	• Den tekniska säkerhetsnivån bedöms vara god och innehålla sådan funktionalitet man kan förvänta sig av en publik molntjänst (t.ex. kryptering at rest och in transit, behörighetsstyrning, hög fysisk säkerhet etc.) • Det saknas vissa specifika säkerhets- och uppföljningsmöjligheter för molntjänstkunden, t.ex. möjlighet att genomföra penetrationstest
4. Informationens betydelse för banken i övrigt (kommersiellt, tekniskt, strategiskt etc.)	• Ett obehörigt röjande kan få konsekvenser för de registrerades integritetsskydd (dvs. dess fri- och rättigheter) och medför även en risk för sanktionsavgifter från tillsynsmyndigheter och, potentiellt, en risk för att bankens tillstånd att bedriva bankverksamhet förloras • Ett röjande av informationen till främmande makt bedöms medföra stor kommersiell skada för banken

KUNDENS GENERELLA RISKAPTIT: Låg/Medium, pga. följande faktorer:	
Avgörande faktorer	**Beskrivning**
1. Tillämpliga lagar och regler för verksamheten och på den information som behandlas	• Lagen om bank- och finansieringsrörelse • EBA:s riktlinjer för utkontraktering • Lagen (2018:558) om företagshemligheter • Dataskyddsförordningen med tillhörande regelverk
2. Marknadsspecifika och kommersiella faktorer	• Reglerad marknad • Starkt konkurrensutsatt marknad • Beroende av stort kundförtroende • Obehörigt röjande medför risk för sanktionsavgifter från tillsynsmyndigheter och, potentiellt, en risk för att bankens tillstånd att bedriva bankverksamhet förloras • Ett röjande av informationen för främmande makt bedöms medföra stor kommersiell skada för banken
3. Antagna fördelar i förhållande till alternativa lösningar	• Minskade kostnader • Smidigare handläggning av ärenden för kunder och anställda • Ökad flexibilitet

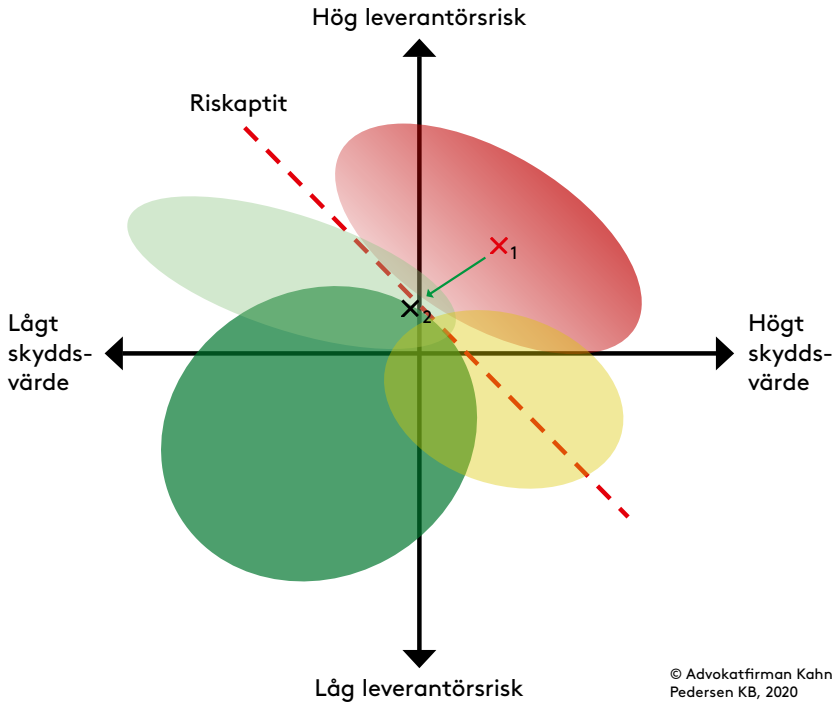
Banken har i utgångsläget inte vidtagit några särskilda tekniska skyddsåtgärder och bedömer att den sammanvägda risken av den planerade användningen utan sådana åtgärder, placeras i det röda området i Folke©-modellen (se det röda krysset i figur 6.3 nedan) vilket överstiger bankens riskaptit. Banken bör därför inte, enligt analys med Folke©-modellen, använda sig av den aktuella molntjänsten på det sätt som ursprungligen avsetts.

b) Läge 2 (med föreslagna förändringar)

Den obegränsade behandlingen av verksamhetens information som banken planerar skulle även innefatta uppgifter om bankens kunder, vilket bl.a. skulle stå i strid med reglerna om banksekretess i LBF (jfr. avsnitt 5.2 ovan). En nödvändig åtgärd för att banken ska kunna använda molntjänsten är därför att begränsa användningen av tjänsten på så sätt att den information som behandlas inte omfattar bankens kunduppgifter. Vid närmare analys bedöms detta inte vara någon större nackdel eftersom banken har särskilda system för kärnverksamheten som uppfyller högt ställda säkerhetskrav och dessutom ska vara de enda system som hanterar vissa processer. Bara för att mailfunktionen tillhandahålls som en SaaS-tjänst innebär det ingen förändring i bedömningen av lämpligheten att använda mail för att dela kundinformation.

Banken väljer därutöver att även vidta de ytterligare åtgärder som föreslås nedan, vilket enligt bankens bedömning kommer att medföra att den sammanvägda risken justeras och placeras i det mörkgröna området (se det svarta krysset i figur 6.3 nedan).

Ytterligare riskbegränsande åtgärder	**Beskrivning**
1. Begränsningar avseende bankens användning av tjänsten	• Uteslutning av kunduppgifter från behandlingen. Upprätta alternativa kontaktvägar för kunder att kommunicera med banken som inte utgör en molntjänst. Införa interna processer för hantering av felaktigt mottagen kundkommunikation • Minimera personuppgiftsbehandlingen i molntjänsten genom att lagra känsliga personuppgifter i ett separat system som inte utgör en molntjänst
2. Förhandling av avtalsvillkoren	• Lägga till uttryckliga och tydliga skyldigheter gällande avgörande it-säkerhetsåtgärder, inklusive separering av bankens information från andra kunders information, kryptering av datalager och villkor för röjanden för utländska myndigheter. • Lägga till skyldighet för molntjänstleverantören att inte omlokalisera bankens data till något annat datacenter inom EU/EES, utan att först ha erhållit bankens godkännande • Införa en process som möjliggör för banken att testa, följa upp och granska molntjänstleverantörens it-säkerhetsåtgärder • Säkerställ att molntjänstleverantörens personuppgiftsbiträdesavtal uppfyller kraven i dataskyddsförordningen
3. Dataskyddsrättsliga säkerhetsåtgärder	• Granska och uppdatera informationstexter till registrerade • Dokumentera bankens inledande dataskyddsrättsliga riskanalys och konsekvensbedömning • Upprätta och genomför lämpliga processer för att säkerställa uppgiftsminimering och ändamålsbegränsning
4. Tekniska och organisatoriska skyddsåtgärder	• Säkerställa stark kryptering av bankens information • Gå med i molntjänstleverantörens ”compliance program” • Förstärka kontinuitetsskydd och exit-planering



Figur 6.3: Bankens riskbedömning av dess planerade användning av SaaS-tjänsten illustrerad i Folke©-modellen.

6.3.3 RESULTAT OCH REKOMMENDATION

Under förutsättning att banken vidtar de föreslagna åtgärderna i avsnitt 6.3.2, skulle banken kunna använda SaaS-tjänsten för kontorstjänster på ett sätt som ryms inom ramen för bankens generella riskaptit, varför banken – enligt analys med Folke©-modellen – bör kunna gå vidare och använda den aktuella molntjänsten.

6.4 Exempel 3: En privat vårdgivare överväger publik molntjänst för it-drift (IaaS)

6.4.1 BAKGRUND OCH AVGÖRANDE FIKTIVA FÖRUTSÄTTNINGAR

En svensk privat vårdgivare inom psykiatrin överväger att ingå avtal med en amerikansk molntjänstleverantör gällande användning av en IaaS-tjänst för verksamhetens it-drift.

Den information som bolaget hanterar, och som kommer att bearbetas inom ramen för molntjänsten, innehåller bl.a. personuppgifter i form av patientuppgifter och andra känsliga personuppgifter. Det är vidare fråga om en stor mängd personuppgifter avseende ett stort antal registrerade. Informationen i molntjänsten kommer att lagras i molntjänstleverantörens datacenter utan någon särskild geografisk begränsning. Molntjänstleverantören kommer använda en global leveransorganisation som innebär att personal runt om i världen kan

få tillgång till uppgifterna om detta krävs (enligt molntjänstleverantörens uppfattning) för att tillhandahålla tjänsterna.

Avtalsvillkoren innehåller flera godtyckliga bestämmelser som innebär att molntjänstleverantören bl.a. kan suspendera tillgång till tjänsten vid enskild användares felaktiga användning av tjänsten, vid oenighet om betalning eller om det krävs ”av säkerhetsskäl”. Molntjänstleverantören har inte kunnat vare sig bekräfta eller begränsa vilka jurisdiktioner som leverantören lyder under. Därtill innehåller avtalet bestämmelser genom vilka molntjänstkunden accepterar att molntjänstleverantören får exploatera informationen för sina egna syften såsom att utveckla nya tjänster och produkter.

Bolaget har, mot bakgrund av de faktorer som framgår nedan, bedömt att bolaget har en låg/medellåg riskaptit.

6.4.2 EXEMPEL PÅ TILLÄMPNING AV FOLKE©-MODELLEN

a) Läge 1 (utgångsläget)

LEVERANTÖRSRISK: Hög, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Leverantören	• Leverantör som lyder under amerikansk jurisdiktion → Risk för utlämnande/röjande
2. Molntjänsten	• IaaS-tjänst som möjliggör goda förutsättningar för olika former av kryptering av bolagets information • Data lagras på servrar utan geografisk begränsning
3. Avtalsvillkoren	• Alla sedvanliga risker i molntjänstavtal bedöms vara aktuella, se avsnitt 3.5 • Molntjänstleverantörens standardavtal bedöms vara mer obalanserat än många andra standardavtal för molntjänster • Molntjänstleverantörens standardavtal regleras inte av svensk rätt • Molntjänstleverantörens personuppgiftsbiträdesavtal uppfyller inte kraven i dataskyddsförordningen

INFORMATIONENS SKYDDSVÄRDE: Högt, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
1. Informationen	• Behandlingen omfattar personuppgifter (inkl. personnummer) • Behandlingen omfattar patientuppgifter och journaler, s.k. ”känsliga personuppgifter” i dataskyddsförordningen mening • Behandlingen avser en stor mängd personuppgifter • Behandlingen avser ett stort antal registrerade • De patienter vars personuppgifter behandlas tillhör kategorin särskilt sårbara registrerade och det kan inte uteslutas att det är fråga om uppgifter om barn • Det kan inte uteslutas att informationen innehåller uppgifter som innefattar uppgift om den registrerades egen eller annans lagöverträdelse • Inga uppgifter som omfattas av svensk säkerhetsskyddslagstiftning
2. Tillämpliga lagar för informationen	• Dataskyddsförordningen med tillhörande regelverk • Patientsäkerhetslagen (2010:659 med tillhörande regelverk • Patientdatalagen (2008:355) med tillhörande regelverk • Hälso- och sjukvårdslagen (2017:30) • Eventuell ytterligare lagstiftning
3. Säkerhetslösningar	• Den tekniska säkerhetsnivån bedöms vara god och innehålla sådan funktionalitet man kan förvänta sig av en publik molntjänst (t.ex. kryptering at rest och in transit, behörighetsstyrning, hög fysisk säkerhet etc.) • Det saknas effektiva säkerhets- och uppföljningsmöjligheter för molntjänstkunden, t.ex. möjlighet att genomföra revision eller penetrationstest

Fortsättning på nästa sida.

INFORMATIONENS SKYDDSVÄRDE FORTS.: Högt, pga. följande faktorer:	
Avgörande riskfaktorer	**Beskrivning**
4. Informationens betydelse för bolaget i övrigt (kommersiellt, tekniskt, strategiskt etc.)	• Ett obehörigt röjande kan få allvarliga konsekvenser för patienternas integritetsskydd (dvs. dess fri- och rättigheter), i synnerhet mot bakgrund av uppgifternas natur/känslighet • Ett obehörigt röjande kan medföra att molntjänstkunden tappar viktiga avtal med olika vårdhuvudmän

KUNDENS GENERELLA RISKAPTIT: Låg/Medium, pga. följande faktorer:	
Avgörande faktorer	**Beskrivning**
1. Tillämpliga lagar och regler för verksamheten och på den information som behandlas	• Patientsäkerhetslagen (2010:659), i synnerhet bestämmelserna om sekretess och tystnadsplikt inom hälso- och sjukvården • Patientdatalagen (2008:355) med tillhörande regelverk • Hälso- och sjukvårdslagen (2017:30) • Dataskyddsförordningen med tillhörande regelverk • Eventuell ytterligare lagstiftning
2. Marknadsspecifika och kommersiella faktorer	• Patienternas säkerhet/integritet/trygghet är av största vikt • Konsekvenserna av ett obehörigt röjande pga. uppgifternas känslighet, mängden personuppgifter, antalet registrerade samt att de registrerade anses vara särskilt sårbara • Bolagets lönsamhet är beroende av att bibehålla viktiga avtal med sina uppdragsgivare (regioner och kommuner), vilket förutsätter ett mycket högt förtroende när det gäller informationshantering och säkerhet
3. Antagna fördelar i förhållande till alternativa lösningar	• Minskade kostnader för it-drift med ca 20 % • Ökad flexibilitet • Generellt högre nivå på tekniska säkerhetsåtgärder

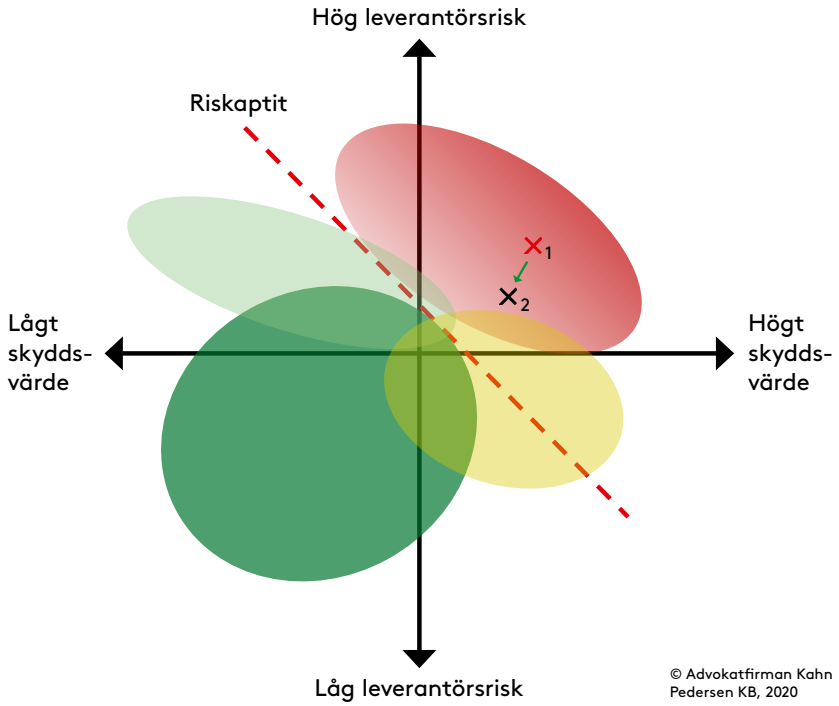
Bolaget har i utgångsläget inte vidtagit några särskilda skyddsåtgärder, vilket innebär att användning av molntjänsten överstiger verksamhetens generella riskaptit. Bolaget bör därför inte, enligt analys med Folke©-modellen, använda den aktuella molntjänsten på det aktuella sättet.

b) Läge 2 (med föreslagna förändringar)

Som illustreras i figur 6.4 nedan bör bolaget inte använda sig av den aktuella molntjänsten då bolaget bedömer att den sammanvägda risken av den planerade användningen placeras i det röda området i Folke©-modellen (se det röda krysset i figur 6.4 nedan). Detta bl.a. mot bakgrund av att det inte kan uteslutas att den avsedda behandlingen, utan ytterligare skyddsåtgärder, skulle innebära ett röjande av patientuppgifterna i strid med de bestämmelser om sekretess och tystnadsplikt inom hälso- och sjukvården som följer av tillämpliga regler i patientsäkerhetslagen.

En teknisk åtgärd som kan öka säkerheten är kryptering (se avsnitt 3.4 ovan). Bolaget bör använda sig av så avancerad kryptering som möjligt. På grund av tjänstens syfte och utformning är det dock inte möjligt att med hjälp av HYOK helt hantera krypteringsnycklar lokalt, eftersom det inte är fråga om en ren lagringstjänst. Om molntjänstleverantören erbjuder kraftfulla KMS-funktioner, exempelvis med stöd för BYOK och där nycklar lagras i en dedikerad HSM, skulle detta möjligen, åtminstone enligt vissa molntjänstleverantörer, förhindra att leverantören får teknisk tillgång till informationen. Det är dock svårt för en utomstående att bedöma vilket skydd en sådan lösning *de facto* ger, i vilken utsträckning bolaget har möjlighet att hantera sin sida av nyckelhantering och utformning av tjänsten på ett korrekt sätt, och i förlängningen om skyddet är tillräckligt mot jurisdiktionsrisken och risken för att informationen ska anses röjd under patientsäkerhetslagen.

Trots att bolaget överväger de krypteringsåtgärder som diskuteras ovan kommer det således inte gå att säkerställa att en sådan säkerhetsåtgärd påverkar den sammanvägda risken i tillräckligt hög utsträckning för att bolagets användning av tjänsten ska vara lämplig/acceptabel (se det svarta krysset i figur 6.4 nedan). Med anledning av detta kommer inte heller några ytterligare åtgärder, i form av exempelvis förhandling av avtalsvillkor etc., att ha någon avgörande effekt på den sammanvägda risken. Det noteras särskilt att kryptering inte hade haft en avgörande effekt på bedömningen då informationen vid körning är okrypterad utom bolagets kontroll, och då under otjänliga avtalsvillkor och med full global exponering för främmande jurisdiktioner.



Figur 6.4: Bolagets riskbedömning av dess planerade användning av IaaS-tjänsten illustrerad i Folke©-modellen.

6.4.3 RESULTAT OCH REKOMMENDATION

Det är, till följd av de risker som en sådan behandling skulle innebära, inte lämpligt för bolaget att använda den tänkta molntjänsten inom ramen för bolagets generella riskaptit, varför bolaget – enligt analys med Folke©-modellen – bör hitta en alternativ lösning som är laglig och lämplig utifrån de förutsättningar som gäller för bolaget.

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mer information om vår verksamhet.

Författarna till denna rapport är:

Karin Angemark Öman, Senior Specialist.

Hanna Bogsjö Österberg, Advokat, Senior Associate.

Martin Brinnen, Senior Specialist.

Johan Kahn, Advokat, Partner.

Daniel Lundqvist, Advokat, Partner.

Staffan Malmgren, Legal Technology Officer.

Albin Svensson, Associate.

www.kahnpedersen.se

ISBN 978-91-986495-0-5