Molntjänster och Juridik

Förutse och minimera de avtalsmässiga och juridiska riskerna

Agne Lindberg - Advokatfirman Delphi

Djupdykning i några juridiska aspekter:

GDPR
NIS
Branschspecifika krav
Cloud Act
Myndighetsdata i molnet

GDPR: Grundläggande principer

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
  - Uppgifter ska vara adekvata, relevanta och inte för omfattande i relation till ändamålet
- Korrekthet
  - Uppgifter ska vara korrekta, annars korrigeras/raderas
- Lagringsminimering
  - Uppgifter får inte sparas längre tid än nödvändigt
- Integritet och konfidentialitet
  - Krav på säkerhet, inkl. skydd mot obehörig förlust

Delphi

Säkerhetskrav

- Företag ska vidta tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå
- Kan inbegripa t.ex.
  - kryptering av personuppgifter
  - Inbyggd säkerhet och data privacy i system och tjänster (”privacy by design”)
  - fortlöpande kontroll av de system som behandlar uppgifterna. Uttryckliga krav på att skydda personuppgifter från att förstöras och röjas
- OBS! 1.8 2018: Lagen om informationssäkerhet i samhällsviktiga och digitala tjänster (+ förordning) – NIS direktivet
  - Digitala tjänster: marknadsplats, sökmotor, molntjänster
  - Samhällsviktiga: Energi, transport, bank, finansinfra, hälso/sjukvård, vatten, digital infra.
  - Säkerhetsåtgärder (+riskanalys och åtgärdsplan) och incidentrapportering(betydande inverkan)
  - Kontroll av status under NIS del av risk-och sårbarhetsanalys enligt GDPR?

Informationskrav vid personuppgiftsincident

- Informera om *”personuppgiftsincident”* utan *oskäligt dröjsmål*
- Informera tillsynsmyndigheten
  - Som huvudregel: **Inom 72 timmar** efter vetskap om intrånget
- Informera varje registrerad individ
  - Om sannolikt leder till hög risk för enskildas rättigheter
  - Undantag, t.ex. om system finns för att bevisa att de ”förlorade” uppgifterna gjorts oläsbara för utomstående, t.ex. kryptering
  - Oproportionerlig ansträngning: istället informera allmänheten
- Behov av att stärka säkerhetsåtgärder och införa rutiner för att meddela registrerade individer!
- Avtalspunkt i biträdesavtal. Tydliga interna processer!

Säkerhetskrav/Personuppgiftsincident - case

- British Airways riskerar den hittills högsta sanktionsavgiften – 183 miljoner pund – efter ett intrång som drabbade 500 000 kunder och deras personuppgifter efter vidarehänvisningar till en falsk webbplats. *”a variety of information was compromised by poor security arrangements at the company”*
- Hotellkedjan Marriott International riskerar att drabbas av en sanktionsavgift på 99 miljoner pund efter en personuppgiftsincident som drabbade 339 miljoner gäster, pga. en säkerhetsbrist i ett system Marriott köpt i samband med ett förvärv av en annan hotellkedja. *”Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems”*
- Det franska försäkringsbolaget Active Insurance fick i juli en sanktionsavgift på 180 000 Euro efter att försäkringsbolagets kunders konton kunde hittas genom en sökmotor: *”non-compliance with the obligation to preserve the security of the personal data of its website users, in breach of Article 32 of the GDPR”*

Förbud mot överföring utanför EU/EES

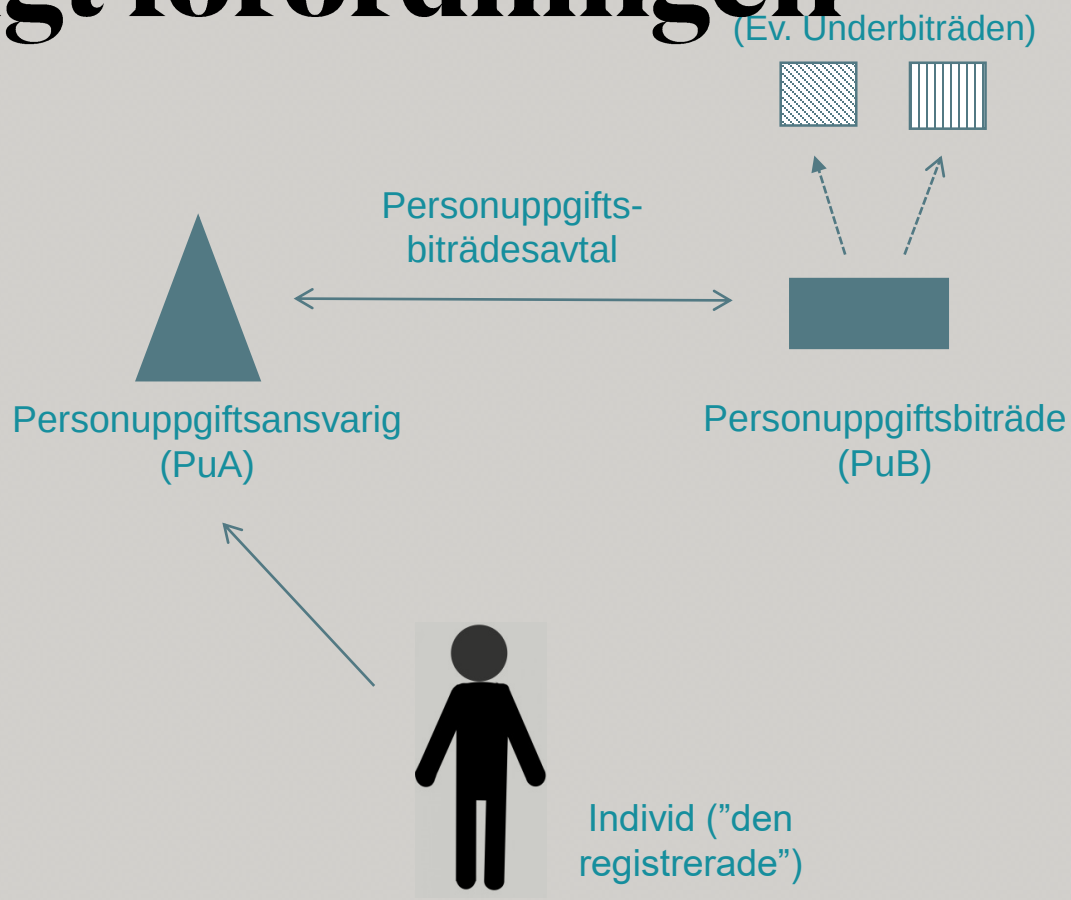
- Liknande regler som tidigare – utgångspunkt är att data inte får accessas eller lagras utanför EU/EES
- Lagstiftningen ska inte kunna kringgås genom att flytta ut data
- Behöver ha koll på var data behandlas
  - Innebär viss tjänst eller support överföring till länder som inte är tillåtna?
  - Supporttjänster
  - Molntjänster

Överföring av personuppgifter till tredje land

- Rättsliga grunder:
  1. adekvat skyddsnivå (Lista från Kommissionen)
  2. standardklausuler
  3. BCR
  4. Privacy shield ”post Safe Harbor”

Personuppgiftsbiträde - Nya krav på avtalens innehåll enligt förordningen

- Art 28.1 – krav på biträde. Garantier för lämpliga tekn/org åtgärder
- Katalogen för vad ett biträdesavtal ska innehålla utökas (se art 28)
  - *dokumenterade* instruktioner
  - Biträdet ska omedelbart informera den ansvariga om biträdet anser att en instruktion strider mot förordningen eller unionens eller medlemsstats dataskyddsbestämmelse
  - Detaljer kring uppgifterna, ändamål, incidenthantering, radering vid avtalets upphörande, kontrollmöjlighet m m.



Avtalskraven – case

- Dataskyddsmyndigheten i den tyska förbundsstaten Hessen valde att bötfälla ett rederi med 5 000 Euro för avsaknad av personuppgiftsbiträdesavtal med en tjänsteleverantör. Riktlinje för sanktionsavgift per avtalsrelation utan personuppgiftsbiträdesavtal?
- Datainspektionen har enligt personuppgiftslagen (PuL) gjort bedömningar av avtalsskrivningar för molntjänster gällande tydligheten av dokumenterade instruktioner, *beslut 2013-05-31 i ärende 1351-2012 (Salems kommun)* och *beslut 2014-04-25 i ärende 1475-2013 (Ale kommun)*. *”.. instruktioner till biträdet i biträdesavtalet ska vara tillräckligt tydliga för att förhindra att biträdet exempelvis behandlar uppgifterna för egna ändamål*”. Exempel: *“will process Customer Personal Data for the purposes of providing, maintaining and improving the services”* – godkändes inte.

Risk och sårbarhetsanalys – inför Cloud tjänster

- Ingen uttrycklig reglering – men följer av laglighetskontroll, privacy by design m m
  - Finns checklistor – ex vis SKL
  - Uttryckligt krav på konsekvensbedömning och förhandssamråd – hög risk behandlingar. (Art 35)
    - Ska innehålla beskrivning av behandlingen, dess proportionalitet, risker och åtgärder för att hantera riskerna
- Laglighetsanalys, inkl kontroll av avtalsvillkor
- Specifik lagstiftning – ex vis Solvens II för försäkring, EBA Guidelines för bank och finans (och försäkring)

EBA Guidelines

- Gäller fr o m 30.9 2019
  - Nuvarande outsourcingavtal ska uppfylla riktlinjerna senast 31.12 2021 (Art 14) .
  - Om avtalet ändras eller förnyas ska uppdatering ske tidigare
- Ersätter tidigare guidelines för molntjänster (Dec 2017) + 2006 guidelines on outsourcing
- Inte bara väsentlig outsourcing (”critical or important functions”) utan all outsourcing. Men vissa krav avser endast väsentlig outsourcing. (Exempel: interna kontrollfunktioner, bankverksamhet eller betalningstjänster)
- Särskilda regler om Cloud (ex: Riskbaserad hantering av var data lagras)
- FI har lagt ut en Podd
- Tillämpas i Sverige även för försäkringsverksamhet

EBA Guidelines

- Outsourcingprocessen (avsnitt 12):
  - Riskbedömning (Risk och sårbarhetsanalys)
  - Due Diligence
- Kontraktsfas – krav på avtalet. Art 75 innehåller lång lista för väsentlig outsourcing. Exempel:
    - Geografisk plats för leverans och lagring
    - Revisionsrätt
    - Servicenivåer
    - Rapportkrav
    - Uppsägningsregler
- Governance. Fortsatt ansvar. Bibehålla egen organisation. Artikel 41 – krav på Outsourcing Policy som löpande uppdateras.
  - Finns även krav på att dokumentera outsourcing och föra register. Art 53 ff.

Cloud Act

- Ger amerikansk domstol rätt att kräva utlämnande av data från USA-baserade tech företag även om lagras i EU eller annat land
  - Även om bolaget är anslutet till “Privacy Shield”
- Förutsättningar:
  - Amerikansk domstol har jurisdiktion över tjänsteföretaget
  - Tjänsteföretaget har en molntjänst / tjänst för elektronisk kommunkation
  - Tjänsteföretaget förvaltar eller kontrollerar datan
- Krock med GDPR

Cloud Act, forts

- Vad ska vi göra?
- Jfr Artikel 28.1 GDPR – får endast anlita PU-biträden som erbjuder ”tillräckliga garantier” för att GDPR efterlevs. Vägledning saknas.
- Del av risk och sårbarhetsanalys
  - Tekniska lösningar, t ex kryptering
- Avtalspunkter att se över:
  - Sekretess
  - Regler om utlämnande enligt domstolsbeslut. Invändningsskyldighet. Rätt att vara med i processen.
  - Hemvistförändring

Molntjänster och myndighetsdata

- En mängd rättsliga utlåtanden: eSam, pensionsmyndigheten, statens inköpscentral
- Särskilda lagkrav: GDPR, säkerhetsskyddslagen, arkivlagen, *offentlighets- och sekretesslagen*
- Sekretessreglerade uppgifter får inte *röjas*
- eSam:
  - *2015 ”Om uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som enligt avtalet inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker, ska uppgifterna enligt expertgruppens bedömning inte anses som röjda i offentlighets- och sekretesslagens mening.”*
  - 2018 ”*Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda.”*
- Slutsats: Föreligger konflikt mellan utländska rättsordningar och svensk sekretesslagstiftning? Exempel – Göteborgs stad – O365 m ”customer lockbox”

Avtalet

Grundbultar och tips för att undvika fällorna

Vad går fel?

- Nr 1 – Scope – innehåll/gränsdragning
- Nr 2 – Prismodell – tolkning
- Nr 3 – SLA/KPI – tillräckliga? Konsekvenser?
- Nr 4 – Flexibilitet
- Nr 5 – Marknadsmässig leverans och kostnad under avtalstiden

Tjänstens innehåll och krav på kvalitet

- Tjänstebeskrivning
  - Beskrivning av tjänsten och scope. Relevans: Bas för SLA, garantier, ansvar
- Kvalitet: Servicenivå
  - Exempel: Tillgänglighet. Responstid. Åtgärdstid.
- Mätperiod
- Mätmetod
- ”Tillåten nedtid”
- Dokumentationskrav/rapportering
- Konsekvenser
  - Vite
  - Andra påföljder?
  - Bonus
  - Tak på exponering för leverantören?
  - Eskalering

Prismodeller

- Fördelning mellan:
  - Fast prisdel – baspris
  - Rörligt pris
    - Resource Units
    - Volymbegräsningar
- Lång avtalsperiod
  - Indexuppräkning
  - Omförhandling

Immateriella rättigheter

- En heltäckande reglering är en nödvändig förutsättning för handlingsutrymme i avtalet
- Betydelsen beror på avtalsföremålet
- Kundens data / Kundens material
  - Kundens rätt att få hem data
  - Leverantörens rätt att använda data? Aggregerad form? OBS – notera om det är personuppgifter!
- Pre-Existing Rights
- Resultat
- Tredjepartsprodukt
- Open Source
- OBS – molntjänstavtalet är inte ett traditionellt licensavtal

Delphi

Ansvarsreglering

- Skadestånd
- Ensidigt - ömsesidigt
- Ansvarsbegränsning
  - Belopp och typ av skada
  - ”carve outs”
    - IPR
    - Sekretess
    - Personuppgiftshantering
      - Konceptet ”supercap”

Hur ska kunden veta vad den köper i avtal om molntjänster?

- “Hjärtat i avtalet”. I en bra tjänstebeskrivning bör det tydligt framgå vilka tjänster som ska utföras.
- …men hur tydligt är det när man köper molntjänster?
  - Exempel: Koppling till gällande dokumentation, innehåll på webbsidor
- ”Off the shelf” -krav på att kunden noggrant har kontrollerat att tjänsten uppfyller behoven.
- Testmöjlighet? Ångerrätt?

”Levande tjänster”, ändringshantering

- Naturlig del av molntjänster (delvis det man köper), men hur undvika försämring?
- Överenskommen ändring vs leverantörens ensidiga
  - Ensidig ändring vanligast och kanske omöjligt att helt förhindra
  - Försök få till en baseline från vilken det inte får bli sämre – särskilt med tanke på säkerhet.
  - ”Materially”?
  - Exit möjlighet?

”Levande tjänster”, ändringshantering, *forts.*

- Byte av underleverantörer
  - Vanligast: bara ett faktum man ska acceptera?
  - Minimum:
    - Rätt att bli meddelad innan (i god tid)
    - Möjligheter att göra invändningar (Jfr GDPR)

Avstängning och exit

- Avstängning av tjänsten
  - När och under vilka förutsättningar
  - Ofta låga krav för när leverantören ska ha rätt till detta – hög risk (kan gå emot regulatoriska krav)!
- Kundens data
  - Ingen rätt för leverantören att hålla inne data
  - På vilket sätt ska migrering av data ske? Kostnad?
  - Skyldighet för leverantören att återlämna/radera data. Back-up lösningar?

Avstängning och exit –praktiskt exempel (1)

Omedelbar avstängning:

- “ *If Customer is late on payment for the Services, Provider may suspend the Services or terminate the Agreement for breach pursuant to Section X.y”*
- Hur hämtar man hem data i denna situationen? (”data hostage”)

Avstängning och exit –praktiskt exempel (2)

Avstängning:

"*Violation of the terms may result in suspension of the Cloud Service. Provider will suspend the Cloud Service only to the extent reasonably necessary. Unless Provider believes an immediate suspension is required, Provider will provide reasonable notice before suspending a Cloud Service*"

Slutsatser – juristens input till din cloud-strategi

- Bygg in juridik och avtal i beslutsprocessen och kravställning
- Gör Risk och sårbarhetsanalys inkl. ev konsekvensbedömning
- Kontroll mot branschspecifika krav
- Ta fram egna mallar för avtal?
  - Biträdesvillkor
  - Molntjänster
- Och/eller: Ta fram checklista för avtalsinnehåll
  - GDPR krav
  - Tjänsteinnehåll
  - Ändringsrätt
  - Servicenivåer
  - Avtalstid – uppsägningar, avstängning
  - Exit – rätt till data

Delphi

Agne Lindberg

Advokat/Partner/Head of Delphi Business Advisory Group

Mobil 0709-25 25 25

agne.lindberg@delphi.se

Advokatfirman Delphi
Adress: Mäster Samuelsgatan 17, P.O. Box 1432, Stockholm, Sweden
Telefon: + 46 (0)8 677 54 00
www.delphi.se