Schrems II och lagförslag om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

Peter Nordbeck

Adam Odmark

Delphi

Agenda

- **Schrems II-domen**
- Bakgrund
- Vad är/var Privacy Shield?
- Vad kom EU-domstolen fram till i sin dom?
- Domens innebörd för standardavtalsklausulerna m.m.
- Avslutande reflektioner

Agenda, forts.

- **Lagrådsremiss om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter**
- Bakomliggande problem med offentlighets- och sekretesslagstiftningen
- Lagförslagets innehåll
- Analys
- Avslutande reflektioner

Schrems II

Schrems II

- **Bakgrund**
- Facebooks överföring av personuppgifter till USA
- Max Schrems klagomål till irländska datainspektionen
- Irländsk domstol begärde förhandsavgörande (Schrems I) – Safe Harbour ogiltigförklarades
- Schrems omformulerade klagomål till att gälla standardavtalsklausuler (SCC) – målet på nytt i irländsk domstol som begärde förhandsavgörande

Delphi

Schrems II, forts.

- **Vad kom EU-domstolen fram till i sin dom?**
- I ett nötskal:
- Privacy Shield (beslut 2016/1250) ogiltigförklarades
- Standardavtalsklausulerna (beslut 2010/87/EU) ogiltigförklarades inte
- De redan stränga kraven för att en överföring till tredje land med stöd av SCC inskärptes ytterligare

Schrems II, forts.

- **Vad var Privacy Shield?**
- Politisk överenskommelse mellan USA och Kommissionen
- Självcertifieringsmekanism för amerikanska organisationer
- På basis av överenskommelsen beslutade Kommissionen att Privacy Shield erbjöd adekvat skydd för personuppgifter hos självcertifierade organisationer i USA

Delphi

Schrems II, forts.

- **Varför upphävde EU-domstolen giltigheten av Privacy Shield-beslutet?**
- I korthet: Innehållet i Privacy Shield-beslutet i kombination med USA:s lagstiftning
- Innehållet i Privacy Shield: Efterlevnaden får begränsas bland annat med hänsyn till ”*krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden*” – dessa intressen har företräde framför skyddet för Privacy Shield i övrigt och rätten till privatliv enligt EU-stadgan
- USA:s lagstiftning: Omfattande möjligheter till inhämtning av personuppgifter enl. säkerhetslagstiftning
- Trots detta ansåg Kommissionen att Privacy Shield säkerställde en adekvat skyddsnivå för personuppgifter i USA
- EU-domstolen: USA erbjuder inte *väsentligen motsvarande* skydd för personuppgifter som GDPR. USAs övervakningsprogram innebär oproportionerlig inskränkning av art. 45(1) GDPR i ljuset av EU-stadgan

Delphi

Schrems II, forts.

- **Vad är problematiskt i amerikansk lagstiftning enl. EU-domstolen?**
- Domstolen analyserar section 702 i FISA och Executive Order 12333
- Avser inte individuella övervakningsåtgärder utan övervakning*sprogram* (ex: PRISM och UPSTREAM – Snowden)
- Övervakningsprogrammen ges årliga godkännanden
- Icke-amerikaner har inga bindande rättigheter som kan göras gällande mot am. myndigheter. Ombudsmansmekanismen i Privacy Shield ger inte effektiva möjligheter för icke-amerikaner att hävda sin rätt

Delphi

Schrems II, forts.

- **Vad hände med modellklausulerna (SCC)?**
- Ogiltigförklarades inte därför att:
- Erbjuder effektiva mekanismer för att säkerställa den nivå av skydd som krävs vid överföringar enl. EU-rätten
- Erbjuder möjlighet att stoppa överföringar vid brott mot klausulerna el. om ej möjligt i praktiken att efterleva dem i mottagarlandet
- Användning av SCC innebär dock inte automatiskt att överföring till tredje land blir tillåten i enskilda fallet

Schrems II, forts.

- **Vad måste vi göra nu?**
- Identifiera situationer med överföring till tredje land
- Identifiera vilka skyddsmekanismer som tillämpas
- Privacy Shield måste ersättas med annan rättslig grund – alternativt stoppa överföring
- Ingen ”grace period”
- Uttryckligt samtycke, BCR eller SCC återstår som alternativ (Tetra Pak fick nyligen BCR godkända)
- BCR-godkännande EJ landspecifikt och krånglig process

Schrems II, forts.

- **Kan SCC användas för fortsatt tredjelandsöverföring och till vilka länder?**
- Bedömning av om registrerade i mottagarlandet (med stöd av SCC) erbjuds en skyddsnivå som *väsentligen motsvarar* den som garanteras enligt GDPR och EU-stadgan
- Om negativt utfall enligt bedömning: vidtagande av ”ytterligare skyddsåtgärder” – vad är det?
- Om inte heller med ytterligare skyddsåtgärder möjligt att uppnå ”rätt skyddsnivå”: stoppa överföringen av personuppgifter/avbryt planerna

Delphi

Schrems II, forts.

- **Kan SCC användas för fortsatt tredjelandsöverföring och till vilka länder? (forts.)**
- Måste bedöma om mottagarlandets lagstiftning (och myndigheternas faktiska agerande) erbjuder väsentligen likvärdigt skydd som enl. GDPR och Stadgan
- USA: uppenbara problem – skälen till ogiltigförklarande gör sig gällande även i SCC-scenario
- Datainspektionen om USA: ”idag VÄLDIGT svårt att se hur SCC ska kunna användas för att överföra till USA”

Delphi

Schrems II, forts.

- **Hur går man i praktiken tillväga för att bedöma om SCC kan användas?**
- I väntan på eventuella EDPB-riktlinjer och rättspraxis: osäkert
- Konsultera lokal expertis för att:

i) bekräfta att mottagarlandets lagstiftning (och myndigheternas faktiska agerande) möjliggör efterlevnad och verkställighet av SCC

ii) kontrollera vilket skydd som rättsordningen erbjuder för personuppgifter generellt;

iii) kontrollera hur vidsträckta möjligheter myndigheterna i landet har att inhämta/kräva tillgång till personuppgifter – finns det bulkövervakningsprogram liknande PRISM och UPSTREAM?

iv) vilka rättigheter registrerade har

Delphi

Schrems II, forts.

- **Hur går man i praktiken tillväga för att bedöma om SCC kan användas? (forts.)**
- Analys av svar från lokal expertis i ljuset av EU-domstolens dom
- Stöd kan ev. tas i kommissionsbeslut om att tredje land säkerställer adekvat skydd för personuppgifter
- Lagstiftning ”som inte går utöver vad som är nödvändigt i ett demokratiskt samhälle för att bl.a. skydda nationell säkerhet, försvaret och allmän säkerhet” strider inte mot SCC (se p. 141 i EU-domstolens dom)
- Beroende av leverantör som envisas om att fortsätta överföra personuppgifter till USA – kräv leverantörsutredning

Delphi

Schrems II, forts.

- **Avslutande reflektioner**
- Väldigt integritetsvänlig EU-domstol
- Uttryckligt samtycke? Artikel 5 i GDPR
- Pågående tillsynsärenden – Facebook Ireland
- Svårt att se EU-politiska lösningar – Stadgan lär inte gå att rucka på
- Ändringar i USA:s lagstiftning?
- Framtida vägledning från EDPB – vilken praktisk nytta?

Delphi

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

- **Bakgrund**
- Myndigheter behöver kunna köpa IT-tjänster (t.ex. molntjänster) från det privata näringslivet
- Sekretesskyddade uppgifter enl. OSL ofta tekniskt tillgängliga för leverantören
- ”Kan vi köpa den här tjänsten externt eller blir det Transportstyrelsen-gate då?”
- Vad myndigheten sammanfattningsvis måste göra:

i) Bedöma om sekretesskyddade uppgifter *röjs* till leverantören/u-leverantörer

ii) Om ja, bedöma om sekretessen gäller i förhållande till leverantören/u-leverantörer (sekretessprövning)

iii) Om sekretessen gäller, finns det någon sekretessbrytande grund?

Delphi

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Om röjande-begreppet**
- Röjande-begreppet saknar legaldefinition (rättsfall från 1991 och gamla förarbeten)
- Om leverantör under amerikansk jurisdiktion, CLOUD Act och eSams rättsliga uttalande från 2018 om röjandebegreppet:
- *”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. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående.”*

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Om sekretessprövning**
- Bulkprövning ofta nödvändigt
- Oförutsägbart vilka uppgifter som leverantören faktiskt kommer få tillgång till (jfr Office 365)
- Ofta underleverantörer i flera led
- Dessutom – innebär CLOUD Act att uppgifter anses röjda till amerikanska myndigheter (vilket är förbjudet enligt OSL)?

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Om sekretessbrytande grund**
- Vore praktiskt om t.ex. avtalssekretess = sekretessbrytande
- I övrigt svårt att hitta sekretessbrytande grund
- Lösning i vissa fall: personal som ”deltar i myndighetens verksamhet” (resurskonsulter) – ej sekretessbrytande grund men sådan personal kan ta del av sekretesskyddade uppgifter

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Nya lagförslaget**
- ”*Den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller tekniskt lagra uppgifter får inte obehörigen röja eller utnyttja dessa uppgifter. I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).*”
- Motsvarande föreslås gälla underleverantörers personal
- Ny sekretessbrytande grund

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **”Tekniskt bearbeta eller tekniskt lagra uppgifter”**
- Exempel:
- *”förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration mot andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster”*
- *”säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering”*
- *”migrer[ing] eller exporter[ing]” av data.*
- Ska huvudsyftet med att anlita leverantören vara att den ska vidta sådana åtgärder eller hur är det tänkt?

Delphi

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Begränsningar med det nya lagförslaget**
- Förutom det oklara begreppet ”tekniskt bearbeta eller tekniskt lagra uppgifter”…
- Förutsätter att leverantörens (och u-leverantörers) personal kan dömas för brott mot tystnadsplikt
- Om brott mot tystnadsplikt begås utanför Sveriges gränser har svensk domstol endast domsrätt om:

i) den som begått brottet är svensk medborgare eller en utlänning med hemvist i Sverige; och

ii) gärningen är straffbar även på gärningsorten.

- Vår tolkning: tystnadsplikten kan endast åberopas för tjänsteleverantörer som kan garantera att den egna (och ev. underleverantörers) personalstyrka är bosatt i Sverige.

Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, forts.

- **Avslutande reflektioner**
- Egen lag, fristående till OSL
- Att främja digitalisering (även) inom offentlig sektor såväl en svensk som EU-gemensam målsättning
- Pågående utredning ”Säker och kostnadseffektiv it-drift för den offentliga förvaltningen” – redovisas 15 januari (förlängd tid)
- Förhoppning om att komma bort ifrån röjande-diskussionen

Delphi Team

Peter Nordbeck

Partner / Advokat
+ 46 709 25 25 01
peter.nordbeck@delphi.se

Adam Odmark

Associate
+ 46 709 25 25 28
adam.odmark@delphi.se

Delphi


Delphi