CIRIO

Schrems II-domen och Privacy Shield – vad får det för konsekvenser?

Caroline Olstedt Carlström

27 oktober 2020

Agenda

- Rättslig bakgrund och EU-domstolens slutsatser
- Vad innebär domen i praktiken?
- Vad kommer att ske härnäst?
- Frågor

CIRIO

Rättslig bakgrund och EU-domstolens slutsatser

Överföring av personuppgifter till tredje länder

- **Personuppgifter blir tillgängliga för någon i ett land utanför EU/EES**
  - Striktare regler än när behandling av personuppgifter enbart görs inom EU/EES där medlemsländerna har anslutit sig till GDPR
  - Såväl server i tredje land som extern access från tredje land

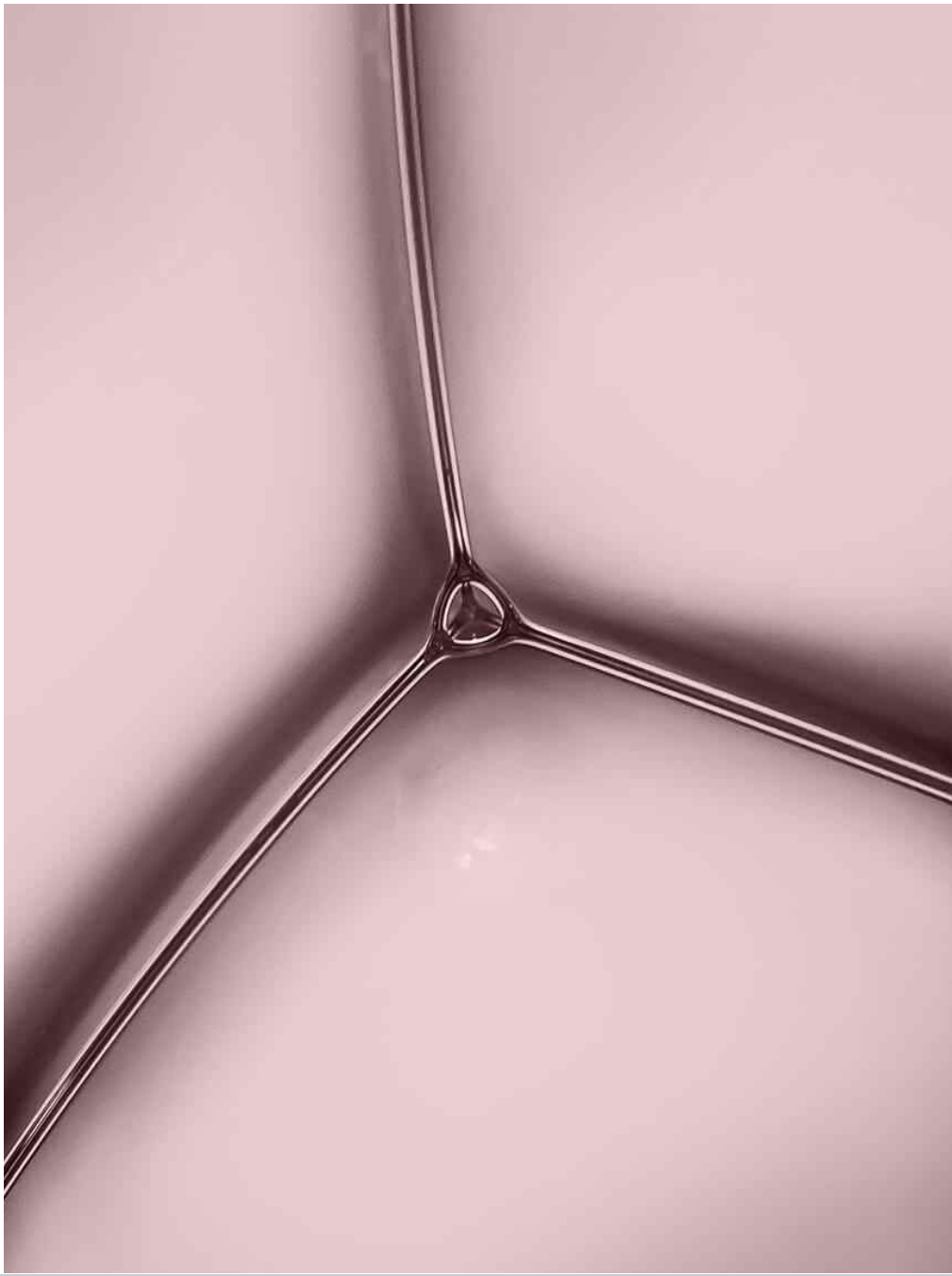
- **Principiellt förbud för överföringar till tredje land (artikel 44)**
  - När får en överföring ske?
    - Jurisdiktionen där mottagaren är belägen anses ge en adekvat skyddsnivå (artikel 45)
    - Exporterande organisation säkerställer att överförda personuppgifter omfattas av lämpligt instrument för överföringen (artikel 46)
    - Uttryckligt undantag är tillämpligt (artikel 49)

.

Överföring av personupp-gifter till tredje länder (USA)

- **I huvudsak två möjligheter:**
  - **EU-US Privacy Shield (numera ogiltigförklarad)**
    - **Mekanism för självcertifiering i USA**
    - **Möjliggjorde för personuppgiftsansvariga i EU att överföra personuppgifter till mottagare som hade anslutit sig till Privacy Shield**
  - **EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till länder utanför EU**

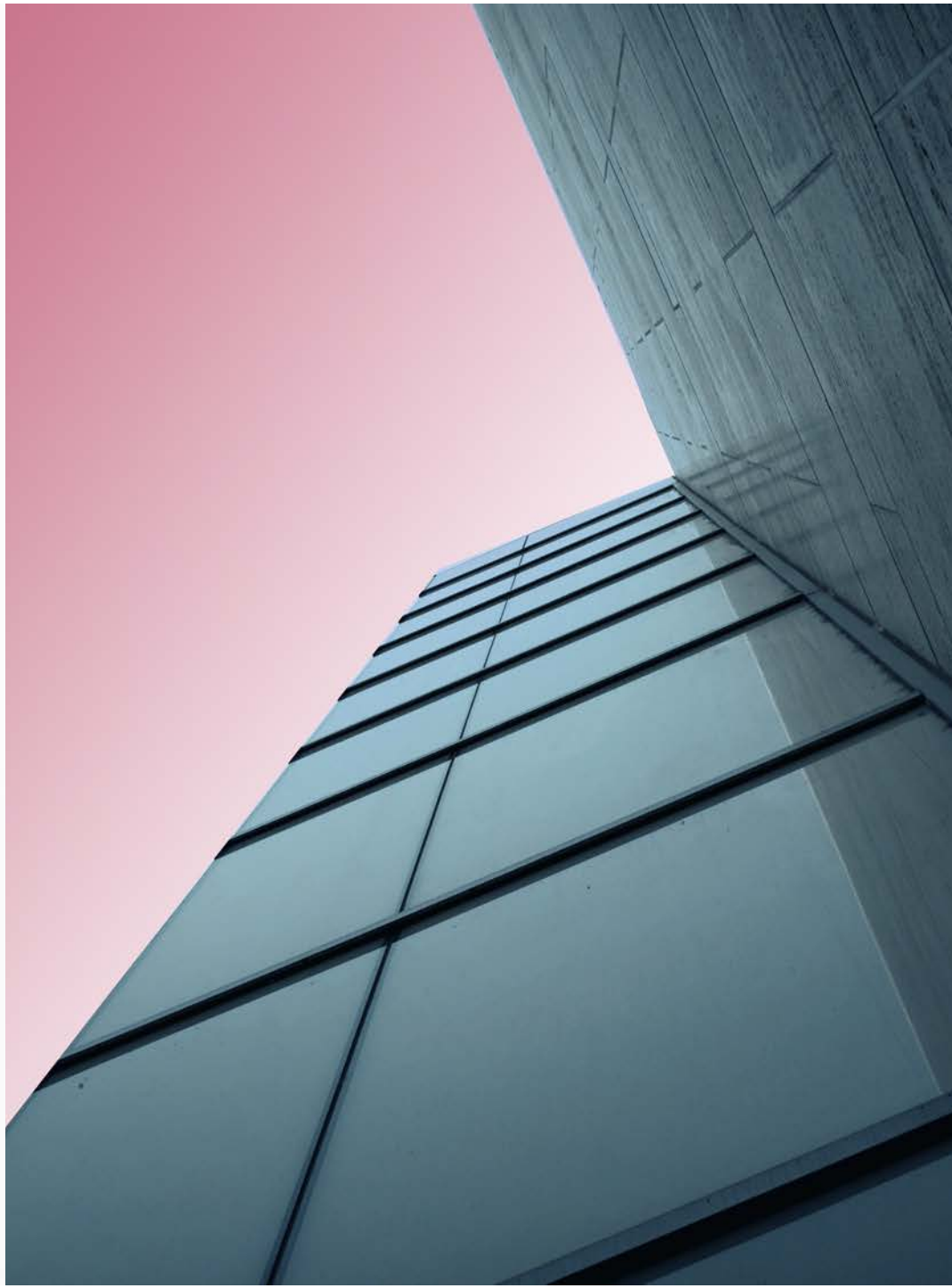
  - Bindande företagsbestämmelser
  - Även vissa ytterligare undantag, såsom samtycke



Schrems II-målet

- Facebook Irlands möjlighet att överföra personuppgifter till amerikanska Facebook Inc.

- Frågor i EU-domstolen:
  - Är det lagligt att överföra personuppgifter till tredje länder med stöd av EU-US Privacy Shield, och
  - EU-kommissionens standardavtalsklausuler?



EU-domstolens slutsatser

- Privacy Shield ogiltigförklaras
- EU-kommissionens standardavtalsklausuler är fortsatt giltiga

EU-domstolens slutsatser

➢ **Ogiltigförklaring av Privacy Shield**

- Det är inte längre tillåtet för personuppgiftsansvariga i EU att överföra personuppgifter till USA med stöd av Privacy Shield.
- Amerikanska myndigheter har för generella möjligheter att få åtkomst till personuppgifter mot bakgrund av generellt utformade intressen som ”nationell säkerhet, allmänintresset och rättsefterlevnaden”.
- Privacy Shield erbjuder inte ett tillräckligt skydd för enskildas rättigheter.

EU-domstolens slutsatser

- **EU-kommissionens standardavtalsklausuler är fortsatt giltiga**
  - Exportören måste säkerställa ”väsentligt likvärdigt skydd” som i EU
  - Kan användas som grund vid tredjelandsöverföringar, men ytterligare skyddsåtgärder för att säkerställa skyddsnivån kan behöva vidtas (punkt 133)
    - ”Ytterligare skyddsåtgärder” definieras inte närmare
    - Kryptering? Endast vissa typer av uppgifter? Vissa mottagare?
  - Importören skyldig att informera exportören om klausulerna inte kan följas
  - Innebär inte att alla tredjelandsöverföringar med stöd av klausulerna är lagliga
    - Bindande mellan den aktör som överför personuppgifterna till tredje land och den aktör som mottar dem – inte myndigheterna i det land där mottagaren befinner sig
    - Krav på bedömning av om rättssystemet i mottagarlandet ger ett tillräckligt starkt skydd för de registrerades personuppgifter
  - Dataskyddsmyndigheterna är skyldiga att stoppa överföringar som inte ger likvärdigt skydd

Praktiska konsekvenser

Krav på personuppgifts-ansvariga

- **Ansvar för att behandlingen och överföringen av personuppgifterna är laglig**
  - Innan varje överföring av personuppgifter till tredje land måste den personuppgiftsansvarige ***visa*** att den har bedömt om mottagarlandets rättssystem erbjuder ett tillräckligt starkt skydd
  - Om det mottagande företaget informerar att den, på grund av nationella bestämmelser, **inte** uppfyller de krav som ställs enligt standardavtalsklausulerna måste personuppgiftsansvarig
    - avsluta överföringen och/eller kontraktet
    - informera behörig tillsynsmyndighet

Lagligheten av överföringar till USA

- **Är överföringar av personuppgifter till USA med stöd av standardavtalsklausuler lagliga?**
  - EU-domstolen uttalar sig inte direkt i frågan
  - EU-domstolen ogiltigförklarade dock Privacy Shield på grund av att det amerikanska rättssystemet gav ett otillräckligt skydd
    - *Utgångspunkt*: användningen av standardavtalsklausuler för överföringar till USA kommer att anses vara olagliga
- **Domen påverkar i princip all användning av moln- och IT-tjänster som innefattar överföringar av personuppgifter till USA**
  - Behov av riktlinjer från dataskyddsmyndigheter
  - EU och USA kommer sannolikt att göra kraftiga ansträngningar för att hitta alternativa lösningar
- **Överföringar till USA kan fortfarande göras med stöd av artikel 49 GDPR**
  - *T.ex.* om den registrerade uttryckligen har samtyckt till överföringen efter att ha blivit informerad om eventuella risker,
  - överföringen är nödvändig för att fullgöra ett avtal eller
  - överföringen är nödvändig för att fastställa, göra gällande eller försvara rättsligt anspråk

Alternativ grund: bindande företagsbestämmelser

- **Schrems II-målet påverkar inte denna möjlighet som det ser ut nu**
- **Regler som en företagskoncern med bolag i flera länder kan ta fram för att reglera sin behandling av personuppgifter**
  - T.ex. avseende registrerades rättigheter och processen för hantering av klagomål samt hur koncernen följer grundläggande principer som ändamålsbegränsning och uppgiftsminimering
- **Ett tredjelands lag kan påverka skyddet som tillhandahålls genom överföringsverktyget**
  - Den som vill överföra personuppgifter till tredje land ska göra bedömningen av om tillräckliga skyddsåtgärder vidtagits där
- **Måste godkännas av Datainspektionen eller annan tillsynsmyndighet i EU**
  - Bedömningen görs inte av lagstiftningen i alla mottagarländer
    - Den som fått sina bindande företagsbestämmelser godkända måste bedöma om de garantier och skydd som ges i bestämmelserna i praktiken upprätthålls
    - Ytterligare skyddsåtgärder kan behöva vidtas
    - Om inte lämpliga skyddsåtgärder kan säkerställas måste överföringen avbrytas

Vad bör man fundera på?

- **Vilka flöden av personuppgifter finns i organisationen?**
  - T ex behandlingsregistret (vilka länder, vilka uppgifter, vilka grunder etc)
  - Stoppa överföring baserat på Privacy Shield
- **I vilka fall kan personuppgifter komma att överföras till tredje land?**
  - Undersök nogsamt såväl leverantörer som underleverantörer.
  - Kan standardavtalsklausulerna tillämpas? Undersök ”ytterligare skyddsåtgärder”
  - Undersök möjligheten att tillämpa även undantagen i artikel 49 (samtycke, avtal etc)
  - Glöm inte andra perspektiv; etik, kundinställning, allmänt riskperspektiv etc
- **Om uppgifter överförs till tredje land**
  - Hur ser skyddet ut i det mottagande landet?
  - Finns det stöd för överföringen?
  - Framgår det av era avtal med personuppgiftsbiträden att personuppgifter överförs till tredje land?
  - Överför era underleverantörer personuppgifter till tredje land?
  - Vilka säkerhetsåtgärder säkerställer överföringen?
  - Se över beslutsprocesserna för verksamhet som innebär överföring till tredje land
  - Följ rättsutvecklingen och uttalanden från dataskyddsmyndigheterna
  - Brexit!
- **Övriga krav i GDPR måste vara uppfyllda för att överföringen ska vara laglig.**
  - Notera t.ex. krav på information till den registrerade om överföringen.

Vad kommer att ske härnäst?

Spaningar framåt

- **Svenska företag och myndigheter behöver vidta åtgärder i avvaktan på politiska beslut**
  - Kartlägg och upprätta handlingsplan
  - Riskbedömning och identifiering av rättsligt stöd
  - Dataklassificering och dataminimering, skyddsåtgärder, beslutsprocesser
  - Håll en dialog och arbeta fram alternativa lösningar med era leverantörer
  - Gäller även personuppgiftsbiträden som använder amerikanska leverantörer som underbiträden
- **Tveksamt att Datainspektionen i närtid kommer att utfärda förbud och/eller sanktionsavgifter mot företag som överför personuppgifter till USA**
  - Dock erbjuds företag ingen uttrycklig övergångsperiod
- **Politiska åtgärder kommer att behöva vidtas för en långsiktig lösning**
- **Arbete pågår!**
  - Håll utkik; EDPB, lokala dataskyddsmyndigheter etc.

Frågor?

CIRIO