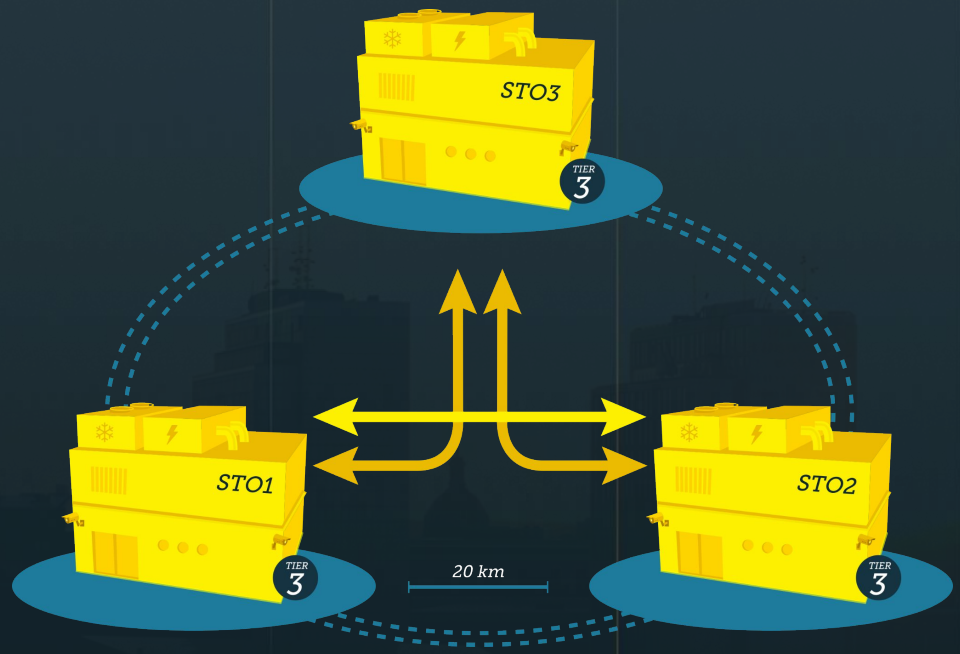

elastx
Public Cloud
made in Sweden

En molnplattform för affärskritiska tjänster med känsligt data

elastx

Vad är viktigt

- Modern och säker plattform
- Support du kan lita på
- Hållbart
- Utan inlåsning
- Regelefterlevnad



elastx

Välkommen Mattias!

elastx

Tredjelandsöverföringar till USA och Schrems III

En **nulägesuppdatering** om **överföringar** av **personuppgifter** till **USA** och förutsättningarna att göra detta på ett **effektivt** och **lagligt** sätt

Vem jag är (urval)

- **Senior juridisk rådgivare** - Data Law Center
- **Vice ordförande** – Forum för dataskydd

- Har **tidigare** arbetat på **advokatbyrå**, **statliga myndigheter** och på **kommun** som jurist.

Agenda

- Vissa dataskyddsgrunder
- Varför är överföring av personuppgifter till USA ett problem?
- Vad gör EU och USA för att lösa problemet?
- Kommer den inslagna vägen att räcka eller kommer det bli ett Schrems III?
- Hur kan vi hantera den osäkerhet som finns?

Dataskyddsgrunder

Kopplat till tredjelandsöverföringar

Skydd för personuppgifter

- Regleras i EU genom bland annat GDPR.
- GDPR är ett regelverk med omfattande skydd för personuppgifter.
- I princip all digital behandling om uppgifter kopplat till individer räknas som personuppgiftsbehandling.

Huvudregeln tillåter inte tredjelandsöverföringar

Att föra ut personuppgifter ut ur EU/EES (GDPR:s tillämpningsområde) är som huvudregel förbjudet.

Detta eftersom rätten till integritet anses vara mänsklig rättighet utifrån

- skyddet för privat och familjelivet (artikel 7 rättighetsstadgan),
- skyddet för personuppgifter (artikel 8 rättighetsstadgan) och
- rätten till effektiva rättsmedel, t.ex. domstol (artikel 47 rättighetsstadgan).

Undantag från huvudregeln

Det finns undantag som gör det möjligt att föra ut personuppgifter till tredjeland i vissa fall bl.a. genom

- Adekvansbeslut
- EU-kommissionens standardavtalsklausuler (SCC)
- Rättsligt bindande och verkställbara instrument mellan myndigheter och offentliga organ
- Godkända uppförandekoder
- Avtalsklausuler eller bestämmelser som är särskilt godkända av tillsynsmyndigheten i det enskilda fallet

Hur genomförs överföringar idag?

De vanligaste överföringsmekanismerna är:

- **Adekvansbeslut** från EU-kommissionen
- Standardavtalsklausuler (**SCC**)

Vid **adekvansbeslut** krävs **inte särskilda åtgärder** för att överföringen ska vara laglig.

Standardavtalsklausuler kräver **normalt omfattande åtgärder** för att vara lagliga.

Det följer skyldigheter med att tredjelandsöverföringar

Sexstegsprocess från EDPB vid överföringar:

1. **Känna till sina tredjelandsöverföringar.**
2. **Känna till vilken mekanism i GDPR som överföringarna grundar sig på.**
3. **Bedöma om det finns några hinder i tredjelandet som påverkar skyddsåtgärderna som mekanismen ger. (finns begränsad vägledning gällande detta): EDPB: Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**
4. **Implementera skyddsåtgärder för att uppnå godtagbart skydd för personuppgifter utifrån bristerna i 3.**
5. **Ta ev. formella steg för att åtgärder i 4 blir bindande.**
6. **Återkommande bedöma om skyddsåtgärderna är tillräckliga och bevaka om förändringar sker vad avser 3.**

Varför är överföring av personuppgifter till USA ett problem?

Överföring USA idag

Utifrån Schrems II huvudsakligen två problem med överföringar till USA:

- Att amerikanska myndigheter kan få del av uppgifterna. Detta då de övervakningsåtgärder etc. som genomförs inte är nödvändiga och proportionella utifrån ett demokratiskt samhälle.
- Att det inte finns effektiva mekanismer för att framföra klagomål för enskilda som anser att dennes uppgifter har hanterats felaktigt.

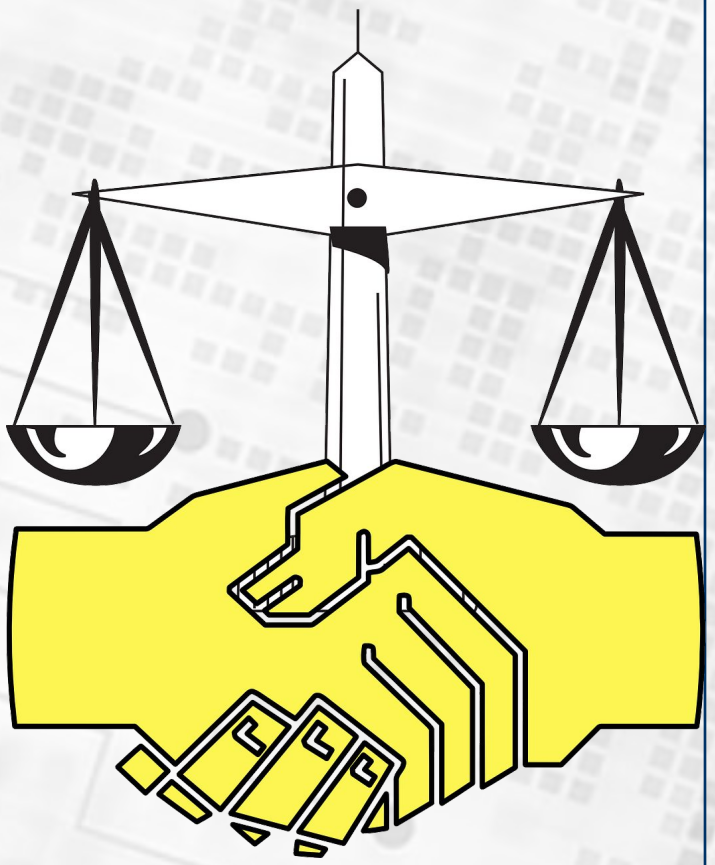
Lagliga överföringar till USA?

Utifrån detta bara tekniska skyddsåtgärder som fungerar (EDPB) såsom:

- **Datalagring för säkerhetskopiering** och **andra ändamål** som **inte kräver** åtkomst till **data i klartext**
- Överföring av **pseudonymiserade uppgifter**
- **Krypterade uppgifter** som endast **transiterar tredjeländer**
- **Skyddad mottagare** (enligt lag)
- Delad bearbetning eller flerpartsbearbetning (**sharding**)

Fungerar inte (EDPB):

- **Överföring** till **molntjänstleverantörer** eller andra personuppgiftsbiträden **som kräver åtkomst** till **läsbar data**
- **Fjärråtkomst** till **data i klartext** (för t.ex. support)



USA specifikt

Tidigare överföringsmekanismer:

- Safe harbour
- Privacy shield

Ny mechanism på väg:

- EU-US Data Privacy Framework

Vad gör EU och USA för att lösa problemet?

Tidslinje åtgärder EU-USA

- **Safe harbour införs,** 26 juli **2000**
- **Schrems I** och **Safe harbour upphävs,** 6 oktober **2015**
- **Privacy shield införs**, 12 juli **2016**
- **Schrems II** och **Privacy shield upphävs**, 16 juli **2020**
- **Vägledningar** från EDPB ang. **tolkning av Schrems II**, **2020-2021**
- 'Offentliga' **förhandlingar mellan EU-USA** inleds om överföring av personuppgifter, augusti **2020**
- "**Agreement in principle**" mellan EU-USA, **25 mars 2022**
- **presidentorder** i USA för att närma sig GDPR "**Enhancing Safeguards for United States Signals Intelligence Activities**", **7 oktober 2022**
- EU-kommissionen publicerar **utkast** på **adekvansbeslut** för **USA**, **13 December 2022**
- **???, idag**
- EU-US Data Privacy Framework införs, ?

Agreement in principle

EU-USA formulerade ett **dokument** där de lyfte fram vilka **principer** som ett **överföringsavtal** skulle bygga på:

- Med det **nya ramverket ska data** kunna **flöda fritt** och säkert mellan **EU** och **deltagande amerikanska företag**.
- **Begränsningar** för **USA:s underrättelsetjänster** till vad som är nödvändigt och proportionellt för att skydda den **nationella säkerheten** i **USA**.
- **Underrättelsetjänster** ska **säkerställa** en **effektiv tillsyn** av medborgerliga **fri- och rättigheter**.
- Ett **nytt överprövningssystem** som omfattar en domstol '**Data Protection Review Court**'.
- **Starka skyldigheter** för **företag** där de kan **självcertifiera**.
- Särskilda övervaknings- och översynsmekanismer.

Enhancing Safeguards for United States Signals Intelligence Activities

DATA LAW CENTER

I korthet innehåller **presidentordern**:

- **Bindande skyddsåtgärder** som **begränsar** de **amerikanska underrättelsemyndigheternas** tillgång till **uppgifter**.
- **Inrättande** av en **ny domstol** som ska **undersöka och lösa klagomål** angående amerikanska **underrättelsemyndigheters tillgång** till **enskildas personuppgifter.**
- **Uppdrag** till amerikanska **underrättelsetjänster** att **se över** sina **interna policys** etc.

OCTOBER 07, 2022

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

BRIEFING ROOM › PRESIDENTIAL ACTIONS

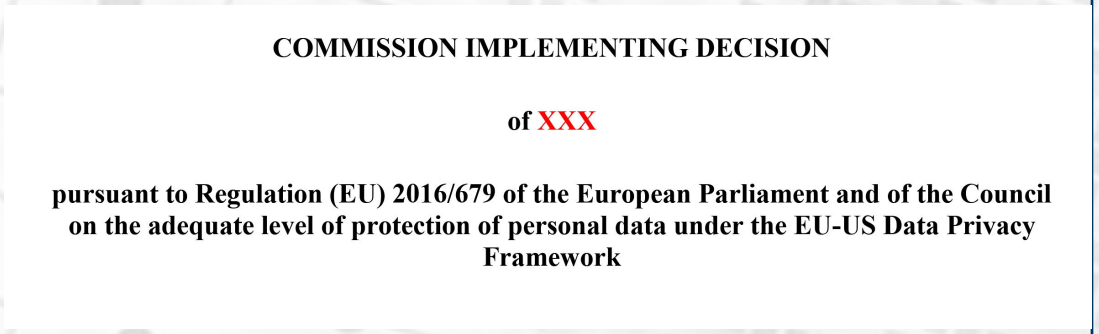
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Utkast adekvansbeslut USA

I en **FAQ** kopplat till **utkastet till adekvansbeslutet** skriver **EU-kommissionen** följande (min översättning):

Varför tror **kommissionen att EU-domstolen inte kommer att riva upp avtalet** igen?

Kommissionens mål i dessa förhandlingar har varit att ta tag med de frågor som EU-domstolen tog upp i Schrems II och tillhandahålla en hållbar och tillförlitlig rättslig grund för transatlantiska dataflöden. Detta återspeglas i **de skyddsåtgärder** som ingår i **presidentordern,** både när det gäller den materiella **begränsningen av USA:s nationella säkerhetsmyndigheters tillgång till uppgifter** […] **och inrättandet av de nya prövningsmekanismerna**.



COMMISSION IMPLEMENTING DECISION

of XXX

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

EU-USA Data Privacy Framework

Adekvansbeslutet i sig **innebär**, utifrån utkastet, i korthet **att företag** som **ansluter sig** till (**självcertifierar**) EU-US Data Privacy Framework anses '**godkända**' enligt **GDPR (för tredjelandsöverföring) om företagen**:

- **Följer** de **regler** (vilka i stort påminner om GDPR) **som ställs** utifrån **adekvansbeslutet** såsom:
  - att **radera personuppgifter** när de inte längre är nödvändiga för det syfte för vilket de samlades in
  - att **säkerställa kontinuitet** i **skyddet** när personuppgifter delas med tredje part
  - **Underställa** sig **rättslig prövning** så att **EU-medborgare** kan få tillgång till **rättsmedel** på **flera sätt** t.ex. genom flera tvistlösningsmekanismer och en domstol (**företagen ska alltså 'frivilligt' underställa sig dessa**).

Vad händer härnäst?

- **Sannolikt** kommer **EU-kommissionen gå vidare** med **adekvansbeslutet**, då måste de först:
  - **Inhämta synpunkter från EDPB**.
  - Få **godkännande** av en **kommitté** bestående av representanter från nationalstaterna i EU.
  - **Möjligen** klara en **granskning** av **EU-parlamentet**.
- **Sedan** kan de **införa adekvansbeslutet**.
- **Det kan möjligen klart till sommaren**.

Kommer den inslagna vägen att räcka eller kommer det bli ett Schrems III?

Recap

Schrems II fällde tidigare ramverk eftersom:

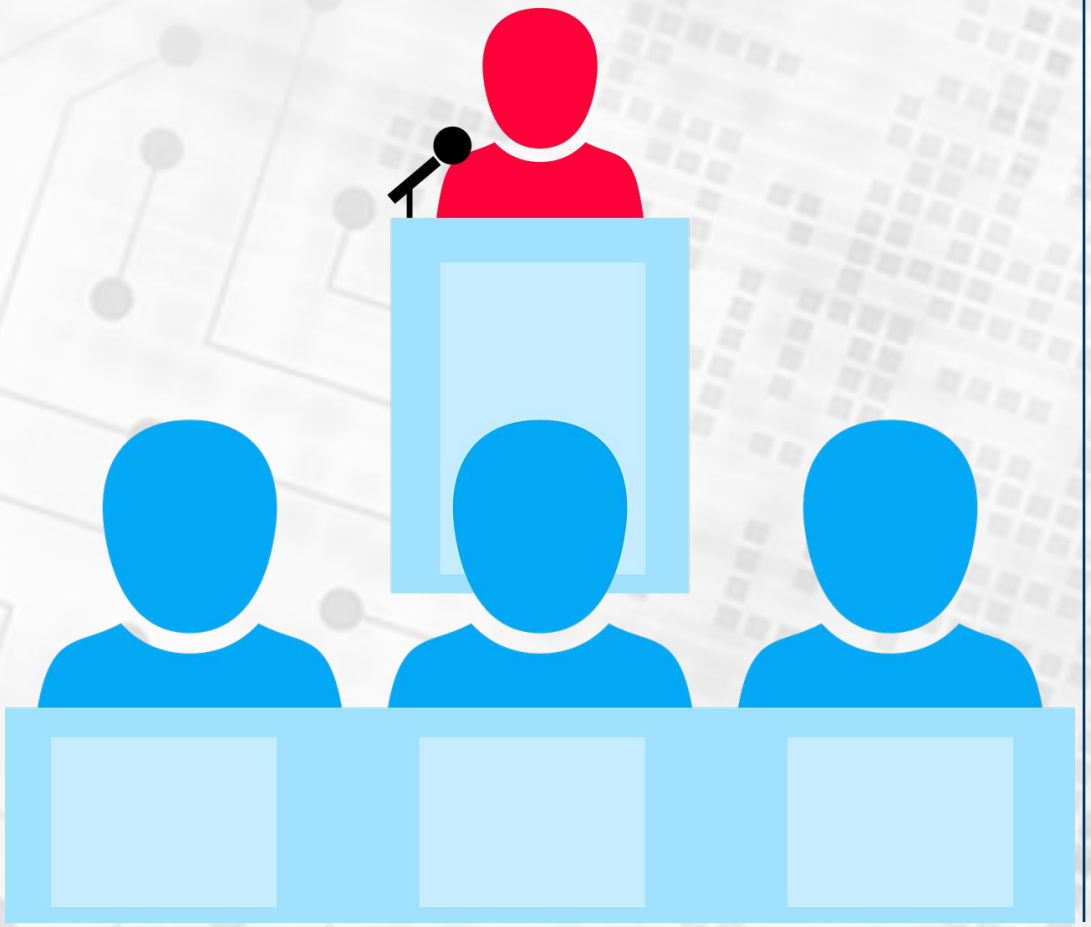
- Att **amerikanska myndigheter** kan få del av **uppgifter**. Detta då de **övervakningsåtgärder** etc. som genomförs **inte** är **proportionella** utifrån ett **demokratiskt samhälle**.
- Att det **inte finns effektiva mekanismer** för att framföra **klagomål**.

Frågor utifrån detta:

- **Innehåller** nya **ramverket begräsningar** för **amerikanska myndigheter** som är **tillräckliga**?
  - **Möjligt**?
- **Finns effektiva mekanismer** för skydd av enskilda?
  - De är **starkare** än **tidigare ramverk** (**men**!)
- **Uppfyller ramverket** m.m. **'god lag'** enligt EU-rätten?

Ett presidentbeslut

- **Tveksamt** om **presidentordern** är **tillräckligt** för att anses vara ‘**lag**’ utifrån **EU-rätten** och utifrån detta tillgodose kraven som ställts av EU-domstolen i Schrems I-II.
- **Beslut** av **kongressen krävs möjligen** för att vara ‘god lag’ enligt EU-rätten. Risk att det skulle strida om USA:s konstitution (?).



Nya ‘Domstolen’

- **Nya domstolen** som ska **pröva** enskildas klagomål **kan anses brista** utifrån **EU-rätt** kopplat till **oberoende**, vilket kan göra att rätten till effektiva rättsmedel (domstol) inte kommer anses vara uppfyllt. Vidare tveksamt om det utifrån EU-rätt är att anse som domstol.

Schrems III

Frågan är alltså om **åtgärderna räcker** för att 'Schrems III' **inte** ska **fälla EU-US Data Privacy Framework**.

- Finns **många kunniga dataskyddare** som bedömer att **det kommer hålla respektive fällas** vid en prövning av EU-domstolen.
- **Personligen** anser jag att det **inte är uppenbart** att de **åtgärder** som vidtagits **tydligt adresserar problemen** som framgår av Schrems I-II. **Det finns** därför **risk** att **ramverket inte** klarar **överprövning**.

Hur kan vi hantera den osäkerhet som finns?

Välja EU-baserat

- Om en väljer **leverantörer baserade i EU** behöver inte regelverket kopplat till tredjelandsöverföringar tas hänsyn till.
- Tips! **Kontrollera underleverantörer-underleverantörer-underleverantörer**!

Välj leverantörer i länder med adekvansbeslut

- **Länder** med **adekvansbeslut** innebär **lägre risk**. Många av de **äldre adekvansbesluten** är det **tveksamt** om de skulle **hålla för rättslig prövning**. I teorin kan de komma att hävas, jfr privacy shield.
- **Sydkorea sannolikt** det **mest stablia adekvansbeslutet** (också senaste).

- Andorra
- Argentina
- Bailiwick of Guernsey
- Färöarna
- Isle of Man
- Israel
- Japan
- Jersey
- Nya Zeeland
- Schweiz
- Storbritannien
- Sydkorea
- Uruguay
- Kanada (om regler för privat sektor gäller)

Använda USA

- **Tveksamt** om **adekvansbeslutet håller** för prövning.
- Max Schrems organisation **NOYB** (None of Your Business) har sagt att de avser att få ev. **adekvansbeslut prövat**. Vi kan alltså vänta oss att **inom kort** (gissningsvis 1-3 år från ikraftträdande) få frågan prövad av EU-domstolen.

Använda USA forts.

- **Var medveten** om **risken** för på nytt **upphävt överföringsavtal**.
- Ha **exitplan** eller **riskbeslut** på riskaccept.
- **Om** vidtar **ytterligare åtgärder** – riskbedömningar enligt GDPR (konsekvensbedömning, transfer impact assessment o dyl) var **medveten** om vad för **syfte** de ska fylla (uppnå regelefterlevnad, riskminskning etc.) och **lägga resurser utifrån målet**.

Använda andra länder

- Formellt ‘ska’ den som är **personuppgiftsansvarig** (PUA) göra **en bedömning** om **lagligheten** i sina **behandlingar**. **Om** ett **land** som **inte** är **EU/EES** eller har **adekvansbeslut** ska i normallfallet **göras prövning** likt **EU-kommissionen gör vid adekvansbeslut** vid **tredjelandsöverföring**.
- **Notera** här att **EU-kommissionen misslyckats** med **EU:s största samarbetspartner** (USA) **två gånger** hittills.

Kontakt

Data Law Center

Mattias Gotthold

E-postadress:
Mattias.gotthold@datalawcenter.se

Telefon: 070 288 27 74

www.datalawcenter.se

Nästa fika, 30 mars.

Hur du säkerhetshärdar Kubernetes för att uppnå kluster som uppfyller de mest strikta dataskyddsföreskrifterna så som GDPR, MSBFS 2020:7 och svenska patientlagar.

Vi ses!