Transfer Impact Assessments (TIA)

Computerworld

8. februar 2022

SIRIUS advokater

- **Cand.jur. i november 2000**
- **Fuldmægtig ved Datatilsynet pr. 1. december 2000**
  - *Persondataloven var trådt i kraft 1. juli 2000*
- **Fuldmægtig ved Domstolsstyrelsen pr. 15. august 2005**
  - *Domstolsstyrelsen var også dengang tilsynsmyndighed for domstolene efter persondataloven (jf. databeskyttelseslovens § 37)*
- **Dommerfuldmægtig ved Højesteret pr. 1. februar 2008**
  - *Højesteret afsagde bl.a. dom den 27. maj 2011 om godtgørelse på 25.000 kr. til kvinde for ulovlig videregivelse (telefonisk videregivelse af elektronisk registrerede oplysninger – U 2011.2343 H)*
- **Elmer Advokater – Advokatfuldmægtig pr. 1. august 2011 – Partner og Møderet for Højesteret i 2020**
  - *Primært person- og arbejdsskade, men i foråret 2016 blev mit speciale officielt også Databeskyttelsesret – navnlig rådgivning af fagforeninger og forbund*
- **Sirius Advokater pr. 1. oktober 2021**

ANDET:

- Medlem af Danske Advokaters "Fagudvalg for databeskyttelse" oprettet i 2022
- Desuden medlem af Danske Advokaters oprindelige fagudvalg for databeskyttelse, der blev nedsat i forbindelse med vedtagelsen af databeskyttelsesforordningen i 2016
- Var bl.a. en af penneførerne på Danske Advokaters *"Guide om håndtering af personoplysninger i advokaters sagsbehandling"* fra maj 2018
- ⬆ ***Alt sammen baseret på "analog" rådgivning / "analoge" vurderinger og papirer***

SIRIUS advokater

Hvad er en Transfer Impact Assessment (TIA)?

- EU-Domstolen har ved Schrems II (præmis 105) afgjort, at en lovlig overførsel til tredjelande forudsætter, at der *"gælder et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i Unionen ved denne forordning, sammenholdt med chartret"*

- Som dataansvarlig skal man altså sikre sig, at de beskyttelsesgarantier, som gælder for de registrerede i EU ved behandling af deres oplysninger, "følger med", når oplysninger overføres til tredjelande

- En Transfer Impact Assessment (TIA) er den dataansvarliges *dokumenterede* vurdering af lovligheden af igangværende eller planlagte overførsler til tredjelande – altså om der gælder sådanne beskyttelsesgarantier

=> kan hurtigt blive til en tung analog proces

SIRIUS advokater

Hvornår sker der overførsel til tredjelande?

- Det Europæiske Databeskyttelsesråds (EDPB) *Vejledning om samspillet mellem artikel 3 og kapitel V i databeskyttelsesforordningen* af 18. november 2021
  - https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

- Vejledningen fastlægger begrebet "tredjelandsoverførsel" af hensyn til afklaring af behovet for overførselsgrundlag, og der opstilles tre kumulative kriterier for, at der er tale om en tredjelandsoverførsel:

  - Dataansvarlige eller databehandler skal være underlagt databeskyttelsesforordningen i forhold til den konkrete behandling *(hvis etableret i Unionen, hvis udbyder varer/tjenester til registrerede i Unionen eller hvis foretager overvågning af disse)*
  - Eksportøren af data (uanset om det er den dataansvarlige eller databehandleren) skal videregive data omfattet af behandlingen eller stille disse data til rådighed for en anden dataansvarlig, fælles dataansvarlig eller databehandler (dvs. dataimportøren), og
  - Denne dataimportør skal enten
    - være beliggende i et tredjeland eller
    - være en international organisation (uanset om organisationen er underlagt GDPR eller ej)

Eksempel fra EDPB's vejledning:

Eksempel: XYZ Inc., der er etableret uden for EU, sender persondata om sine ansatte/kunder, som også alle er bosiddende uden for EU, til sin databehandler ABC Ltd, der er etableret inden for EU. ABC Ltd. behandler herefter de pågældende data på vegne af XYZ Inc. og sender dataene tilbage til den dataansvarlige XYZ Inc.

- **Fordi** databehandleren ABC er etableret i EU, er den behandling, der udføres af ABC, omfattet af databeskyttelsesforordningens databehandlerspecifikke regler, jf. artikel 3, stk. 1.
- **Fordi** den dataansvarlige XYZ er etableret i et tredjeland, **er** videregivelsen/ tilbagesendelsen af data fra ABC til XYZ en *tredjelandsoverførsel*, der kræver særligt grundlag.

SIRIUS advokater

Kortlægning i forbindelse med Transfer Impact Assessment (TIA)

- Vurdering af lovligheden af *igangværende eller planlagte* overførsler til tredjelande forudsætter:
  - Kortlægning af samarbejdspartnere, som indebærer overførsel af personoplysninger
  - Kortlægning af leverandører, der udfører databehandling af personoplysninger (databehandlere)
  - Kortlægning af leverandørers placering af dataansvarliges data
  - Kortlægning af leverandørernes *underleverandører*
  - Kortlægning af *underleverandørernes* placering af data

Ny vejledning fra Datatilsynet om dataansvaret mellem private leverandører og offentlige myndigheder - 15. november 2021:

Eksempel 11 – It-support som biydelse

En kommune køber et softwareprodukt af virksomheden TechX i form af et system. Virksomheden TechX hverken hoster eller drifter systemet, men i aftalen indgår der som biydelse support og vedligeholdelse af softwareproduktet (patch-opdateringer og fejlrettelser) på systemniveau, dog uden systematisk adgang til kommunens personoplysninger. I supporthenvendelserne kan der i særlige tilfælde indgå filer indeholdende personoplysninger, som er nødvendige for, at it-supporten kan lave fejlrettelser.

Selvom de behandlede filer kun i særlige tilfælde indeholder personoplysningerne, er forekomsten ikke tilfældig. Da det således er forventeligt (og uundgåeligt), at TechX vil behandle personoplysninger på vegne af kommunen, må TechX anses for **databehandler** for kommunen, da det ikke er afgørende, hvor ofte der vil forekomme personoplysninger.

Hvis det modsat ville være rent tilfældigt, at personoplysninger forekommer i de pågældende filer, som it-supporten behandler – og derfor ikke er nødvendige for at lave fejlrettelser – vil TechX ikke være databehandler. Da personoplysninger ikke forventes at forekomme, vil TechX blive anset for tredjepart. Kommunen vil i dette tilfælde skulle foretage de nødvendige beskyttelsesforanstaltninger efter artikel 32 – såsom indgåelse af en fortrolighedserklæring.

Er behandlingen af personoplysninger:

1) **Uundgåeligt?**
2) **I det hele tilfældigt?**

Link til vejledning:

https://www.datatilsynet.dk/Media/637727515566649442/Vejledende%20tekst%20om%20rollefordelingen%20.pdf

SIRIUS advokater

Datatilsynets vejledende tekst om databehandling ved udvikling og test af IT-systemer

- OK at anvende personoplysninger ved eksempelvis afsluttende tests af integrationen og i forbindelse med fejlsøgning/fejlretning, samt også hvis forbundet med betydelige vanskeligheder at skabe retvisende anonymiserede testdata

- Ved anvendelse af personhenførbare produktionsdata i testmiljøer skal etableres samme sikkerhedsforanstaltninger, som er vurderet passende i produktionsmiljøet

- **=> bl.a. databehandleraftale og TIA om nødvendigt**

- *https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/testdata-brug-af-personoplysninger-ved-udvikling-og-test-af-it-systemer*

Hvad indebærer en Transfer Impact Assessment (TIA)?

- Dataansvarliges *dokumenterede* vurdering vedrørende lovligheden af igangværende eller planlagte tredjelandsoverførsler. Ifølge EDPB indebærer den følgende trin:

1. *Undersøg modtagerlandets lovgivning og praksis => Vurdér, om der i forhold til den konkrete overførsel er mulige hindringer for en effektiv beskyttelse af personoplysningerne*

2. *Hvis vurderingen er, at modtagerlandet ikke giver den tilstrækkelige beskyttelse => Identificér og udvælg supplerende foranstaltninger*

3. *Implementér de mulige supplerende foranstaltninger*

4. *Revurdér løbende beskyttelsesniveauet og gennemfør tilsyn med mulige forandringer, der kan påvirke beskyttelsen*

=> kan også hurtigt blive til en tung analog proces – og hvad med opfølgning?

SIRIUS advokater

Analogt skema til kortlægning ifm Transfer Impact Assessment (TIA)

Leverandør	Behandling	Databehandler?	Databehandleraftale?	Underleverandører?	Overførsel til tredjelande	Hvilke tredjelande	Antal registrerede	Omfang af data .....

SIRIUS advokater

Analogt skema til kortlægning ifm Transfer Impact Assessment (TIA)

Kategorier af registrerede	Kategorier af data	Sikkerhedsforanstaltninger	Lovgivning i tredjelandet	Supplerende sikkerhedsforanstaltninger	Andre supplerende foranstaltninger	Samlet risikovurdering	Seneste tilsyn	Senest e opdatering ift ændret risikovurdering

SIRIUS advokater

Supplerende sikkerhedsforanstaltninger?

- EDPB – Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger – af 10. november 2020
  - *https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_da.pdf*

- Persondata behandles ved anvendelse af stærk kryptering før overførsel

- Persondata bliver pseudonymiseret før overførsel, og dataeksportøren beholder krypteringsnøglen

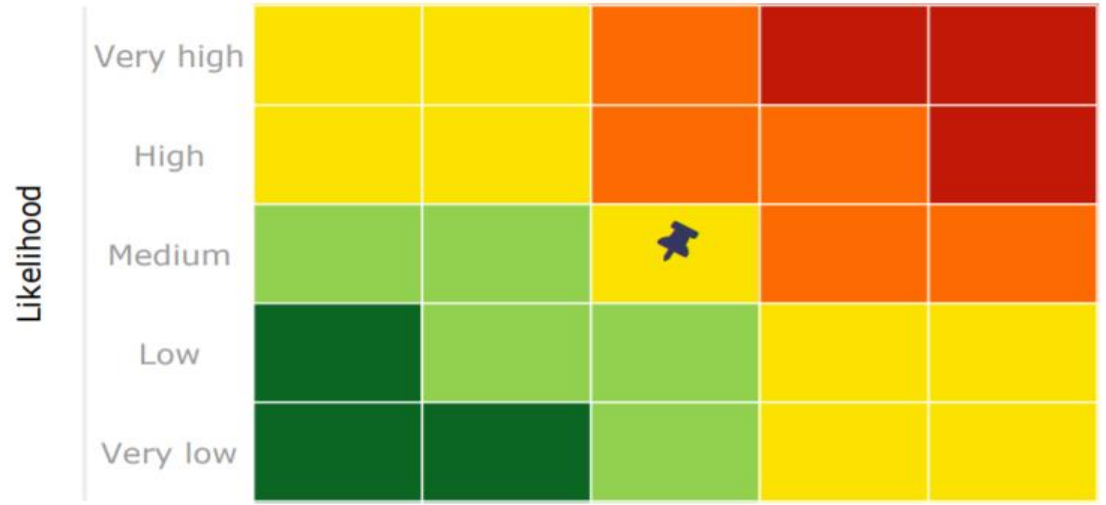
- Persondata overføres ved anvendelse af end-to-end kryptering, hvormed modtagerlandets myndigheder ikke kan få adgang under overførslen

- Persondata splittes op i flere separate dele før de overføres og behandles dermed ved flere separate databehandlere etableret i forskellige jurisdiktioner. Det indebærer, at de enkelte registrerede ikke kan identificeres i forbindelse med databehandlingen i de enkelte jurisdiktioner

assessment of the Receiving Organization's processing of personal data.

5.2 Confidentiality

In the heat map below, the Organization has assessed the overall risk to the confidentiality of the transferred personal data subject to this TIA. The risk assessment is based on a score of the potential negative consequences for the data subjects if the confidentiality to the personal data is breached and on a score of the likelihood of the confidentiality being breached. When assessing the likelihood, the Organization has taken into account the known factors and threats along with the Organization's implemented security measures. The transfer itself and the third country subject to this TIA is not covered by the risks assessment below as the assessment of the adequacy of the security measures in this respect will be assessed below under "Supplementary measures". The risk assessment is therefore conducted to give a full picture of the circumstances surrounding the transfer.



SIRIUS advokater

LEGALTECH:

- LegalTech sørger for at stille de rigtige spørgsmål, så man ikke overser noget
- Du bliver hjulpet igennem processen og tvunget til at tage stilling – skal ske i dialog med rette interessenter/eksperter
- Der genereres fuldtekstdokumenter, som kan anvendes som dokumentation
- Fuldtekstdelene i systemet er generiske, og vil i høj grad gælde for alle overførsler der opfylder den generelle ramme (eksempelvis overførsel til USA). D
- Det vil derfor være de konkrete spørgsmål/svar sammenholdt med den generiske tekst, der indebærer dokumentationen for den konkrete vurdering
- Systemet følger op med årshjul og reminders, så man bliver holdt i ørerne
- Vi bruger det selv og bistår gerne andre hermed, da det letter arbejdet en hel del
- Kræver det er logisk og ”omfavner bredt”