WEBINAR:
Utkast til ny adekvansbeslutning for USA

Thea Rølsåsen
22.03.23

Hva skal jeg snakke om?

- Hva er en adekvansbeslutning?
- Kort om forhistorien, hvordan havnet vi egentlig her?
- Hva inneholder utkastet til adekvansbeslutning, herunder Bidens presidentordre?
- Hva skjer fremover? – veien videre og mulige utfall.

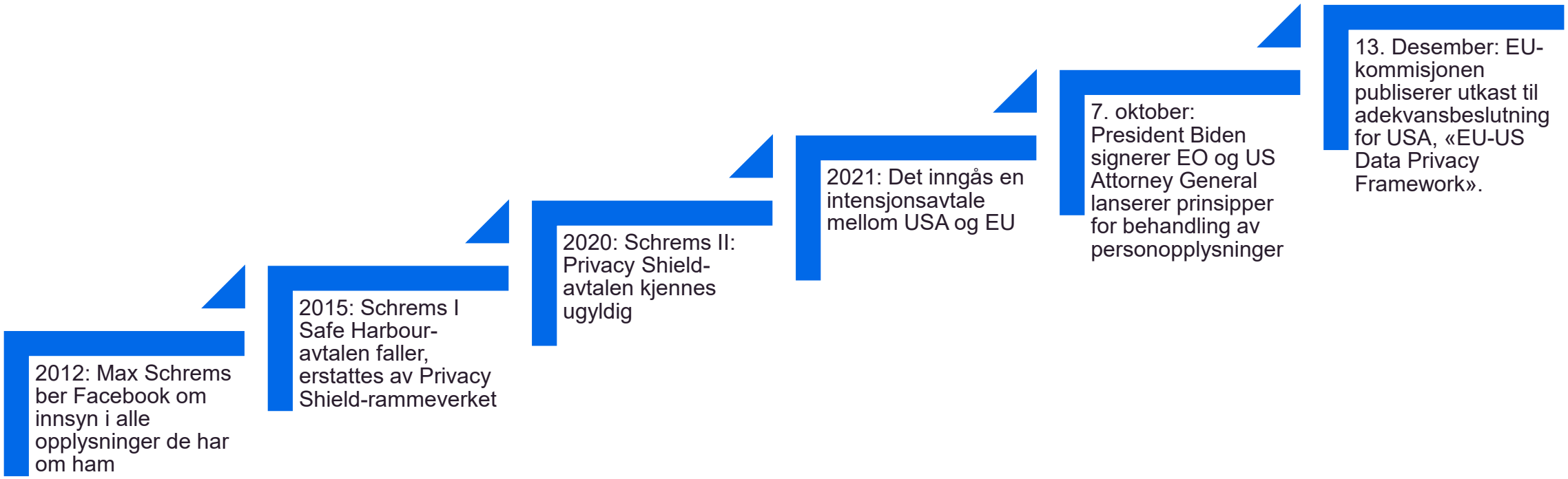
NORMEN

Hva er en adekvansbeslutning?

- EU-kommisjonen kan beslutte at et område utenfor EU/EØS har regler som ivaretar personvernet på en tilsvarende måte som land i EU/EØS. Disse beslutningene kalles adekvansbeslutninger og er hjemlet i personvernforordningen artikkel 45.

- Hvis EU-kommisjonen har fattet en slik beslutning, kan man overføre personopplysninger til området. Overføringsgrunnlag (rettslig grunnlag for overføring etter GDPR art. 46) eller godkjenning fra Datatilsynet er da ikke nødvendig. Overføringen vil være sammenlignbar med overføringer mellom land innenfor EØS.

Hva har skjedd så langt i denne historien?



NORMEN

EU-US Data Privacy Framework i et nøtteskall

- Legger til rette for fri dataflyt mellom EU og amerikanske selskaper
- Sertifiseringsordning
- Bindende garantier som skal begrense tilgangen til data for amerikanske etterretningsmyndigheter til det som er «nødvendig og proporsjonalt».
- En ny to-trinns klageadgang for ikke-amerikanske borgere rettet mot amerikanske etterretningsmyndigheter
- Overvåkning- og revisjonsmekanismer

NORMEN

EU-US Data Privacy Framework

Endringer i amerikansk lovgivning

Andre retningslinjer for behandling av personopplysninger

Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities

Prinsipper for behandling av personopplysninger

Regler for sertifisering, rettsmidler mot amerikanske selskaper, osv.

NORMEN

Sertifisering

- Under EU-US Data Privacy Framework baserer seg på et selv-sertifiseringssystem som krever:
  - Tilslutning til to sett med personvernprinsipper
  - Man må kunne etterforskeres av enten The Federal Trade Commision (FTC) eller The US Department of Transportation (DoT).
  - Resertifiserig hvert år
  - At virksomheten er behandlingsansvarlig eller databehandler.

- Unntak for opplysninger som er samlet inn for publisering, journalistiske formål eller tidligere publisert materiale hentet fra mediearkiver. Dette må ha annet overføringsgrunnlag, for eksempel Standard Contractual Clauses (SCC).

EU-US Data Privacy Framework

Endringer i amerikansk lovgivning

Andre retningslinjer for behandling av personopplysninger

Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities

Prinsipper for behandling av personopplysninger

Regler for sertifisering, rettsmidler mot amerikanske selskaper, osv.

NORMEN

Så, hva står det egentlig i denne presidentorderen?

Omfang

- Orderen omhandler såkalte «Signals Intelligence Activities». Det er ikke defininert i orderen, men NSA omtaler det slik: «SIGINT (signals intelligence) is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems that provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.»

- Kort sagt: innhenting av informasjon og data fra elektroniske systemer til bruk for etterretningsformål mot utenlandske personer, stater og organisasjoner.

Kort oppsummert:

Garantier

- Prinsipper for autorisering av innhenting og innhenting av data
- Beskriver 12 legitime formål for innhenting av data
- Gjør det forbudt å innhente data til enkelte formål
- Etablerer rutiner for kontrollere at data ikke innhentes for ugyldige formål og at det foretas vurderinger av konsekvensene for personvernet og andre sivile rettigheter. Det skal vurderes om innhentningen er nødvendig for oppnå formålet, og om innhenting disproposjonalt påvirker personvernet. Det skal videre vurderes om mindre ingripende metoder kan brukes
- Regler om bulk-innsamling
- Behandling av personopplysninger

Rettsmiddel

- Etablerer en klageadgang og en ny «domstol»: The Data protection Review Court.

Prinsipper for autorisering og innhenting av data

1. SIGINT skal være autorisert i lov eller i executive order/presidentordre, og skal gjennomføres i samsvar med den amerikanske grunnloven (legalitetsprinsippet).

2. SIGINT skal underlegges sikkerhetstiltak som skal sikre at personvern og sivile rettigheter står sentralt ved planlegging og gjennomføring av etterretningsaktiviteter.

Dette innebærer at SIGINT bare skal gjennomføres i den grad det er proporsjonalt med målene som søkes oppnådd. Det skal søkes å oppnå balanse mellom viktigheten av målet (the intelligence priority) og innvirkningen på personvern og andre rettigheter.

- Man skal vurdere om målene kan oppnås med mindre inngripende midler, jf. (i) (A)
- Innhentingen skal være så målrettet som mulig, og det skal om nødvendig innføres tiltak, jf (i)(B). Tiltakene skal vurderes opp mot:
  - Varighet
  - Antatt nytte
  - Konsekvenser for den enkelte
  - Hvor sensitive dataene er

12 legitime formål for innhenting av data

- Forstå eller vurdere kapabiliteter, intensjoner eller aktiviteter i fremmede stater
- Forstå eller vurdere kapabiliteter, intensjoner eller aktiviteter i fremmede organisasjoner, inkl. terrororganisasjoner
- Forstå eller vurdere kapabiliteter transnasjonale trusler som påvirker den globale sikkerheten
- Beskytte mot utenlandske militære aktiviteter og ferdigheter
- Beskytte mot terrorisme, gisseltaking, og at enkeltpersoner holdes i fangenskap
- Beskytte mot spionasje, sabotasje og henrettelser
- Beskyttelse mot masseødeleggelsesvåpen
- Beskyttelse mot cybersikkerhetstrusler
- Beskytte amerikansk personell
- Beskyttelse mot transnasjonal kriminalitet
- Beskytte integriteten til valgsystemer, valg og politiske prosesser, samt fysisk og elektronisk infrastruktur
- Andre aktiviteter som støtter disse legitime formålene.

Forbudte formål

- Aktiviteter som undertrykker eller begrenser kritikk eller ytringsfrihet (for både individer og medier)
- Aktiviteter som undertrykker eller begrenser legitime personverninteresser
- Aktiviteter som undertrykker eller begrenser retten til advokat
- Diskriminering på bakgrunn av etnisitet, rase, kjønn, kjønnsidentitet, seksuell legning eller religion.

Rutiner for innhenting

- Det skal sikres at det gjennomføres vurderinger på rett nivå for å sikre at de ønskene målene:

A) Dekkes av en eller flere at de legitime formålene
B) Ikke er innrettet eller forventet å stride mot de forbudte formålene, og
C) Ikke besluttes før det er gjort vurderinger av innvirkningen på personvernet og andre sivile rettigheter.

Det er flere retningslinjer for hvilke roller som kan godkjenne/autorisere innhenting.

Regler om bulk-innsamling

- Utgangspunkt: Målrettet innsamling skal prioriteres, MEN:

- Bulk-innsamling kan autoriseres dersom det er nødvendig og målene ikke kan oppnås ved målrettet innhenting.
- Det skal innføres tiltak for å sikre at innhentingen begrenses så mye som mulig.
- Bulk-innsamling kan kun benyttes for disse seks formålene:
  - Beskytte mot terrorisme, gisseltaking, og at enkeltpersoner holdes i fangenskap
  - Beskytte mot spionasje, sabotasje og henrettelser
  - Beskyttelse mot masseødeleggelsesvåpen
  - Beskyttelse mot cybersikkerhetstrusler
  - Beskytte amerikansk personell
  - Beskyttelse mot transnasjonal kriminalitet

Behandling av innhentede personopplysninger

- Plikt til å minimere spredning/formidling og oppbevaringstiden
  - Data om ikke-amerikanske borgere skal kun videreformidles dersom det inneholder opplysninger som nevnt i EO 12333 (f.eks: informasjon som er nødvending for å redde gisler eller at man er tilknyttet et terrornettverk).
  - Det skal gjøres konkrete vurderinger om hvem som eventuelt skal få tilgang til informasjonen, og virkningene av at opplesninger deles med andre myndigheter.

- Det er retningslinjer knyttet til tilgangsstyring, sikker lagring, datakvalitet (objektivitet) og, avvikshåndtering og dokumentasjon.

Klageadgang og en ny «domstol»: The Data protection Review Court.

- Klageadgang via en totrinnsrakett:

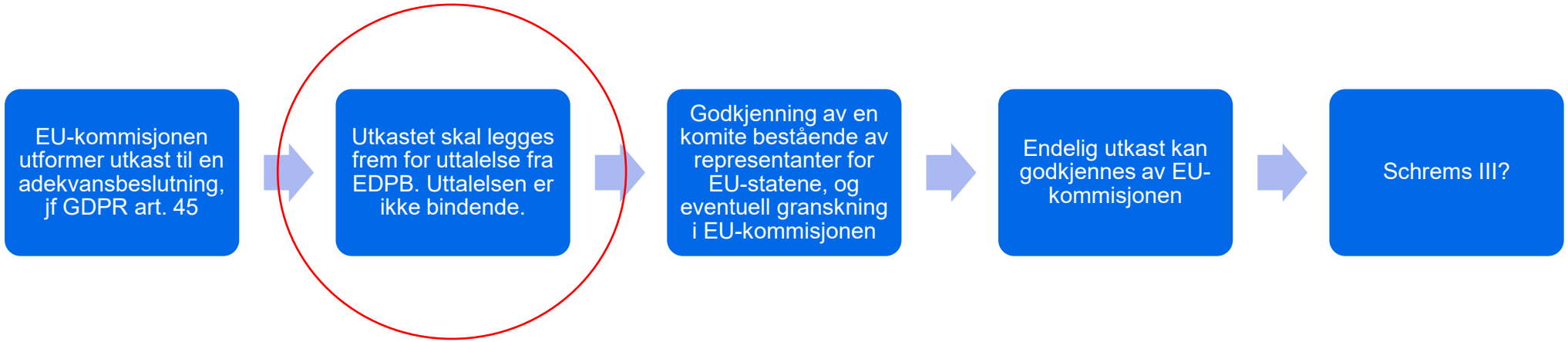
1. The Director of National Intelligence's Civil Liberties Protecion Officer
   - Erstatter klageadgangen til «The Ombudsperson» i Privacy Shield
   - Vil motta og behandle klager fra enkeltpersoner «submitted via an appropriate public authority in a qualifying state». Dersom brudd på amerikansk lov blir funnet, sendes saken videre til ytterligere kontrollprosesser tjenestevei, og kan påklages den registrerte til steg 2.
   - Klager skal ikke informeres om vedkommende var et mål for etterretningsaktivitet.

Klageadgang og en ny «domstol»: The Data protection Review Court.

1. The Data Protection Review Court
   - De dømmer ikke, men kan påpeke eventuelle brudd og kan for eksempel kreve at data slettes.
   - Klager får oppnevnt en egen advokat som argumenterer på deres vegne, men er ikke representert selv.
   - Klager skal ikke informeres om vedkommende var et mål for etterretningsaktivitet og retten skal i alle tilfelles svare «*The review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation*."»

- Fremstår som en form for internkontroll, og ikke en faktisk klageadgang for den registrerte.

Veien videre



- NOYB (Max Schrems) påpeker:

"Certain amendments, such as the introduction of the proportionality principle or the establishment of a Court, sound promising - but on closer examination, it becomes obvious that the Executive Order oversells and underperforms when it comes to the protection of non-US persons. It seems obvious that any EU "adequacy decision" that is based on Executive Order 14086 will likely not satisfy the CJEU. This would mean that the third deal between the US Government and the European Commission may fail."

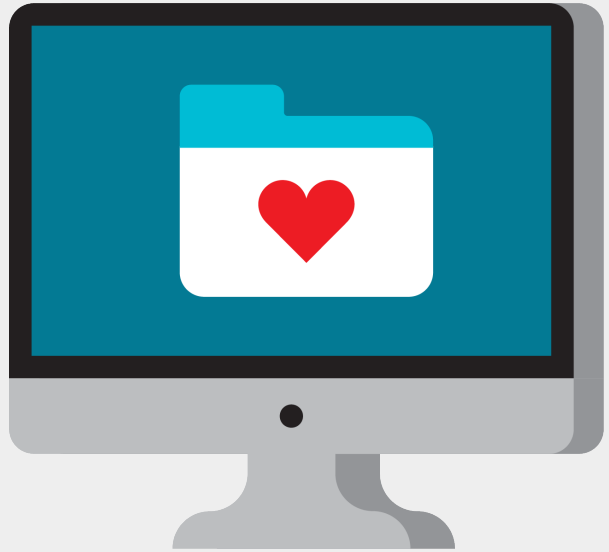
“Today’s draft decision is the outcome of more than one year of intense negotiations with the US that I led together with my US counterpart Secretary of Commerce Raimondo. Over the past months, we assessed the US legal framework provided by the Executive Order as regards the protection of personal data. We are now confident to move to the next step of the adoption procedure. Our analysis has showed that strong safeguards are now in place in the U.S. to allow the safe transfers of personal data between the two sides of the Altlantic. The future Framework will help protect the citizens’ privacy, while providing legal certainty for businesses.”

- Didier Reynders, Commissioner for Justice - 13/12/2022

Spørsmål fra den digitale salen

Ta gjerne kontakt om du har innspill til Normens veiledningsmateriell!

- Hva trenger du?
- Hva mangler?
- Hva kan oppdatert veiledningsmateriell bidra med?



sikkerhetsnormen@ehelse.no

Hvordan holde deg oppdatert på alt som skjer?!?

Forside > Normen

Normen

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.

NORMEN