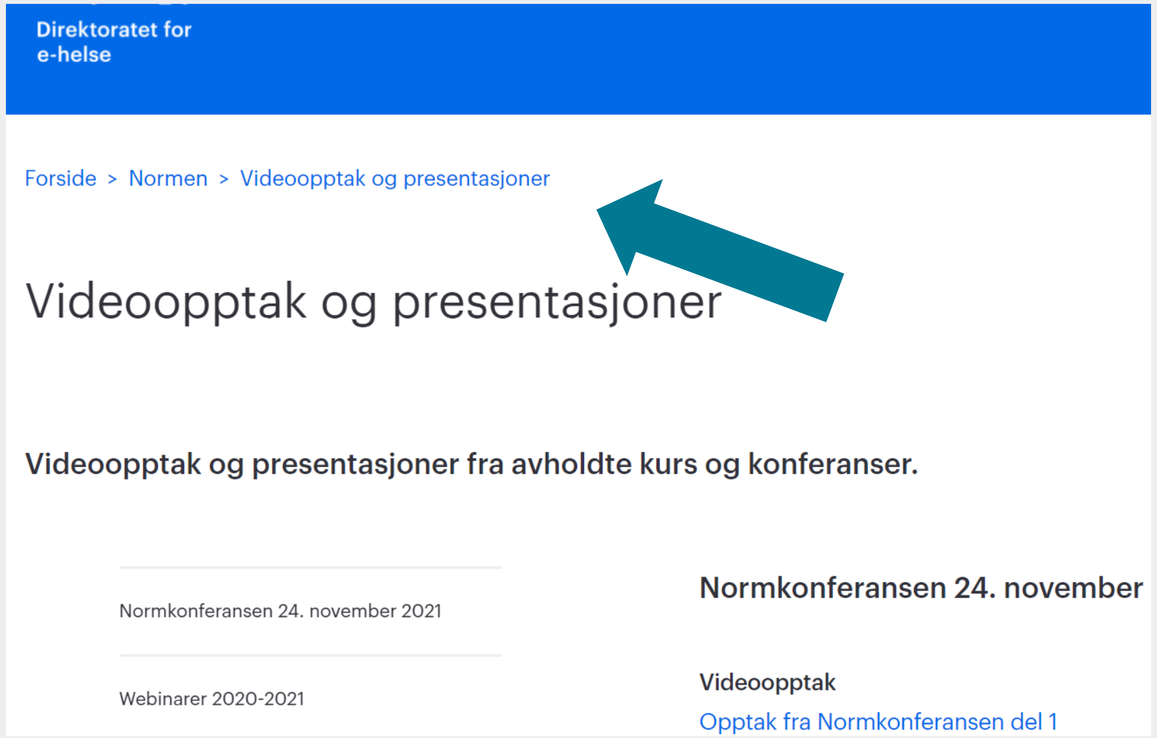
Ny adekvansvurdering for USA - hva nå?

11.10.23

Thea Gulbranson
Seniorrådgiver, avdeling informasjonssikkerhet

Kjøreregler

- Vi setter mikrofonene deres på «mute» fra start
- Det foretas opptak av dette webinaret
- Vi legger ut opptak og presentasjoner på normen.no



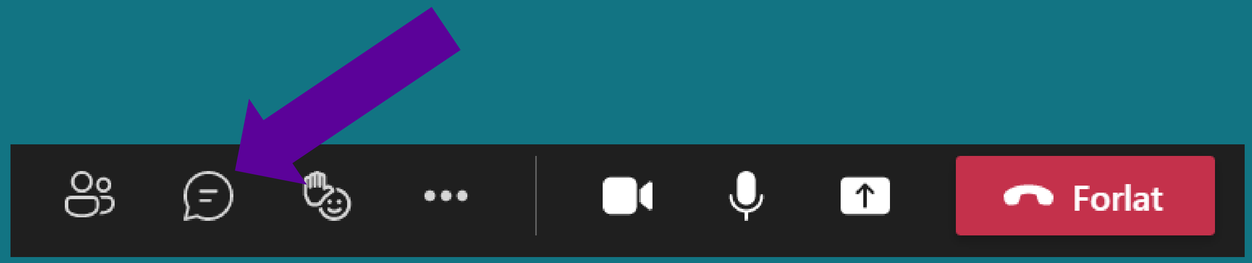
NORMEN

Spørsmål og kommentarer underveis

- Bruk chatfunksjonen når som helst under webinaret til spørsmål eller kommentarer

- Vi svarer på spørsmål enten i plenum og/eller i chat

- Hvis du har spørsmål som ikke blir besvart under webinaret eller innspill du ønsker å komme med i etterkant, send oss en epost til sikkerhetsnormen@ehelse.no



NORMEN

Bli med på våre andre arrangementer!

18. Oktober	Updates on the EU cybersecurity policy framework related to health
1. November	Vil du lære mer om god passordhåndtering?
14. desember	Intro til Normen, heldagskurs

Følg med på normen.no, sosiale medier og Normens nyhetsbrev!

Påmelding: ehelse.no/arrangementer

NORMEN

Normkonferansen

NOV | 21-22 | 2023

The Qube, Gardermoen

SKANN MEG

Bli med på kurs på Pre-Normkonferansen

Program for Normkonferansen

Agenda

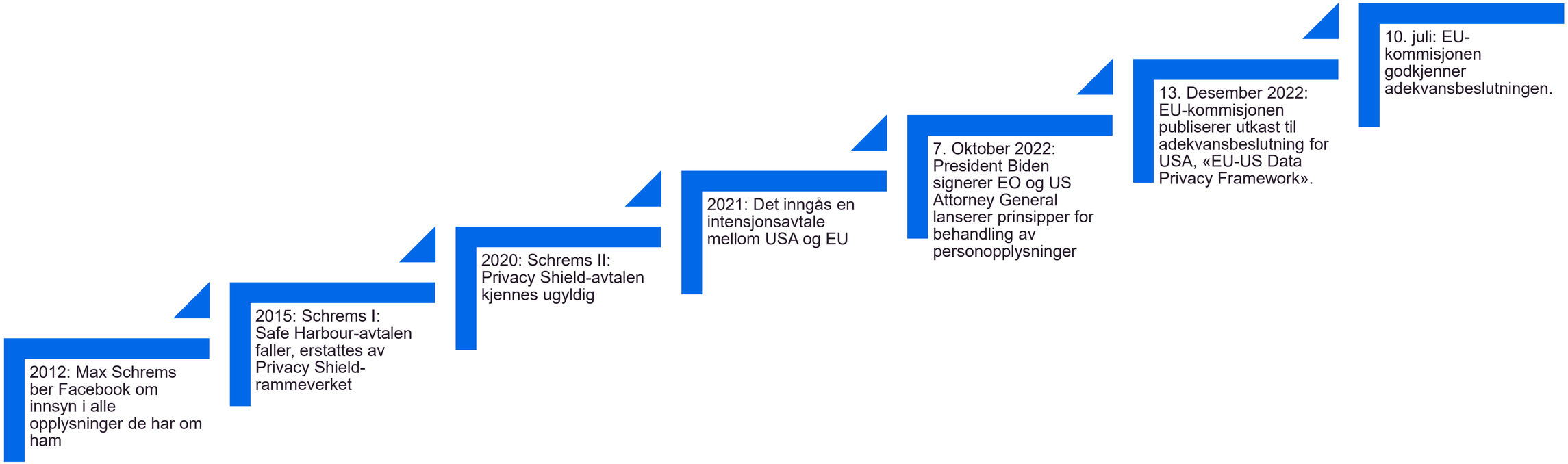
- Hva er en adekvansvurdering? Hvilke overordnede virkninger har det?
- Kort Schrems-tidslinje
- Er alt bra nå?
  - Hva gjør man hvis man vil overføre data til USA? Hva bør man tenke på?
  - Muligheter og problemer – FISA, EO osv.
  - Reaksjoner på adekvansbeslutningen – hva skjer fremover og hva er risikoen for virksomhetene?
    - Hva er kritikken mot beslutningen?

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 EU/EØS.

Hva har skjedd så langt i denne historien?



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

Hvilke problemstillinger beslutningen løser og ikke løser

- Beslutningen løser:
  - USA «friskmeldes» som tredjeland. Personopplysninger kan overføres fritt dersom man har overføringsgrunnlag.

- Beslutningen løser ikke:
  - Leverandørenes avtalevilkår, for eksempel bruk av personopplysninger til egne formål.
  - Dataansvarliges øvrige plikter etter personvernforordningen.
  - Virksomhetene må fremdeles vurdere hvorvidt skytjenester er egnet for den enkelte behandling av personopplysninger.

Hva er egentlig forskjellen mellom overføringsgrunnlagene (art 45 og 46)?

- Utgangspunkt: De ensidige endringene i amerikansk lovgivning gjelder uansett.

EDPB presiserer: «…all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used.»

Hva må til for å benytte adekvansvurderingen som overføringsgrunnlag?

- EU-US Data Privacy Framework baserer seg på et selv-sertifiseringssystem som krever:
  - Tilslutning til personvernprinsippene som er nevnt i beslutningen
  - Man må kunne etterforskeres av enten The Federal Trade Commision (FTC) eller The US Department of Transportation (DoT).
  - Re-sertifisering hvert år.
  - At virksomheten er behandlingsansvarlig eller databehandler.

  - OBS: Også underleverandører må være sertifisere.

- Virksomheten må befinne seg i EU/EØS, gjelder ikke for virksomheter som befinner seg utenfor EU/EØS, jf. GDPR art. 3(2).

- Virksomheten må oppfylle andre plikter etter personvernforordningen, for eksempel ha behandlingsgrunnlag og inngå databehandleravtale.

DATA PRIVACY FRAMEWORK
PROGRAM

Search

Home | Self-Certify | Data Privacy Framework List | Audiences | About

ACTIVE | INACTIVE

Search

Advanced Search

23andMe, Inc.
South San Francisco,California
Active

Framework
EU-U.S. Data Privacy Framework
Swiss-U.S. Data Privacy Framework
UK Extension to the EU-U.S. Data Privacy Framework

Covered Data
Non-HR

Questions or Complaints

247Digitize LLC
Chicago,Illinois
Active

Framework
EU-U.S. Data Privacy Framework
Swiss-U.S. Data Privacy Framework

Covered Data
Non-HR

Questions or Complaints

250Mils
Carlsbad,California
Active

Framework
EU-U.S. Data Privacy Framework

Covered Data
Non-HR

Questions or Complaints

2nd Watch
Liberty Lake,Washington
Active

Framework
EU-U.S. Data Privacy Framework
Swiss-U.S. Data Privacy Framework

Covered Data
HR
Non-HR

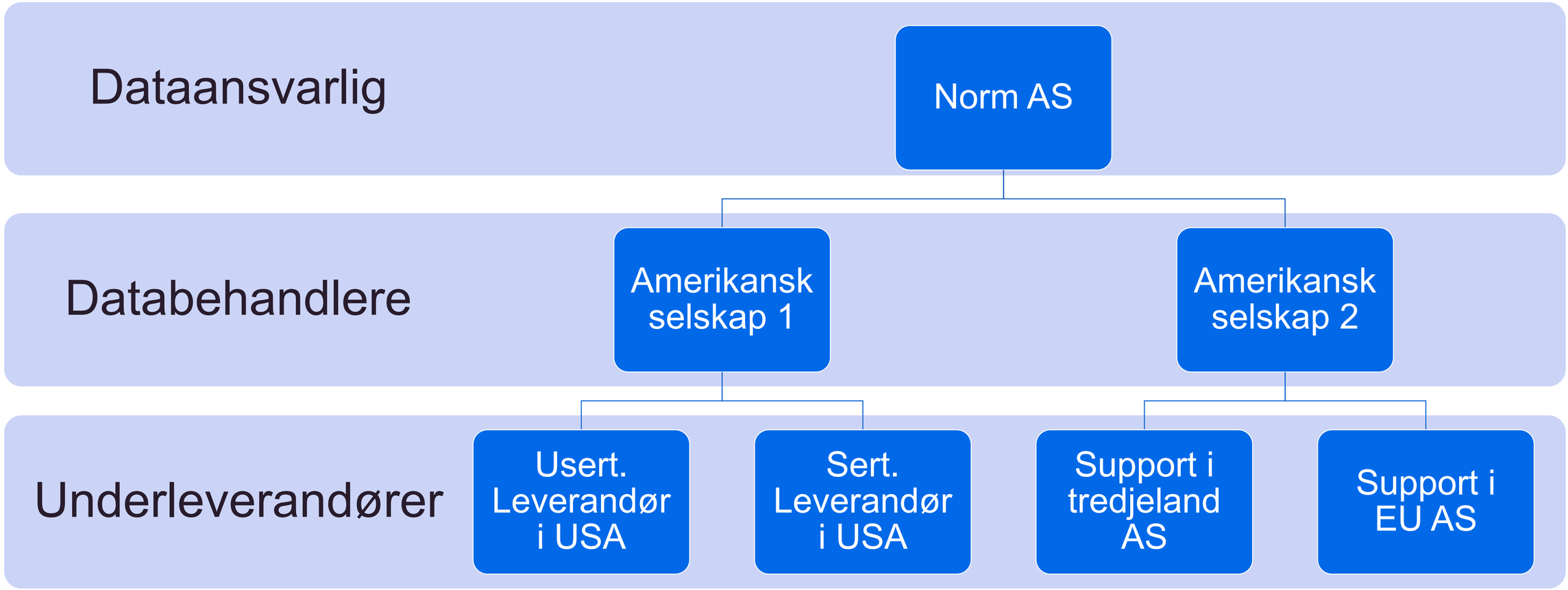
Questions or Complaints

Overføring til selskaper som ikke er sertifiserte under DPF

- Det er kun sertifiserte virksomheter som kan få overført personopplysninger under DPF, jf. art 45.
- Dersom virksomheten ikke er sertifisert, må man bruke et av overføringsgrunnlagene i art. 46, for eksempel SCC.
- Dersom overføringsgrunnlaget følger av art 46, må virksomheten sørge for:
  - Tilstrekkelige sikkerhetstiltak for personopplysningene
  - Oppfyllelse av de registrertes rettigheter
- EDPB presiserer: «…all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used.»

  Det er derfor ikke nødvendig med «ytterligere tiltak», jf. Schrems II.

Men, hva hvis selskap X ikke er sertifisert, da?



Det gjenstår fremdeles risiko

- Adekvansvurderingen kommer til å bli utfordret rettslig. Må vurdere fremtidig rettslig risiko dersom overføring baseres på adekvansbeslutningen.
  - Momenter som kan angripes er:
    - Manglende reell domstolskontroll/rettsmidler for de registrerte, jf. EU-charteret.
    - Usikkerhet om det er lik forståelse av nødvendighet og proporsjonalitet
    - Etterretningslovene/EO har fremdeles vide formål.
    - FISA 702 er ikke endret.
- Endringer i amerikansk lovgivning, for eksempel presidentorderen.
- NOYB (Max Schrems) argumenterer for at DPF i realiteten er en kopi av Privacy Shield som innebærer ingen reell endring.

Spørsmål fra den digitale salen

Direktoratet for e-helse

Takk for meg!