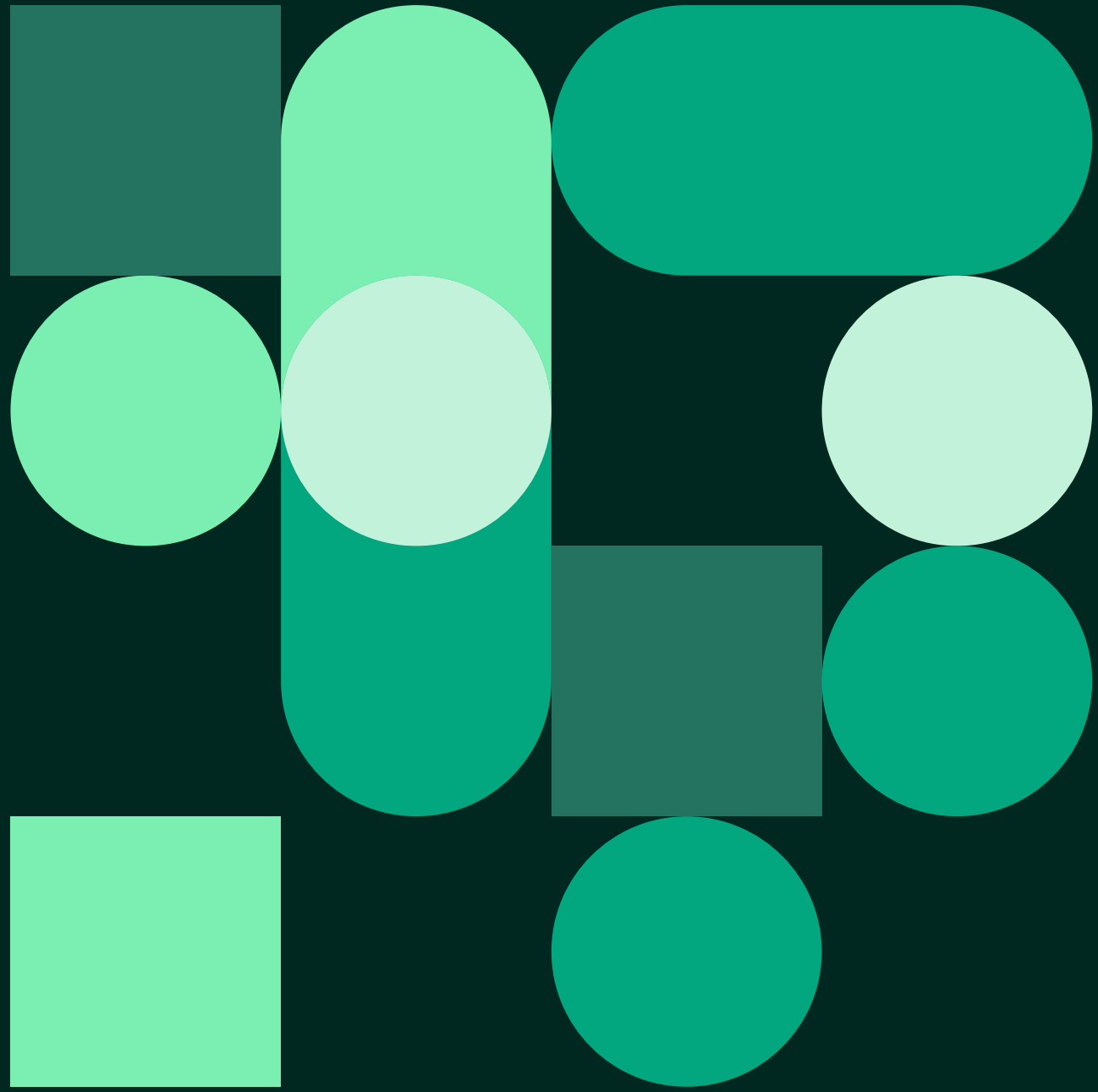
Norsk helsenett

PVO-samling Normen

Gardermoen

20.11.2023



Pre-Normkonferansen - PVO-samling

- Velkommen til samling - Aasta Margrethe Hetland og Marit Larsen Haarr (NHN)
- Nytt fra Datatilsynet - Camilla Nervik og Fredrik Christensen
- *Matpause* - 1710 - 1740
- Regulatorisk veiledningstjeneste kunstig intelligens (KI) - Kathrine Olsgard, Hdir
- Ny veileder for personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter - Ane Hessen Hjelle og Marie Strand Schildmann (E-helse)
- *Pause* - 1820 - 1830
- Ny adekvansvurdering for USA - hva nå? Marit Larsen Haarr
- *Pause* 1850 - 1900
- Samtale: Utfordringer i PVO’s dagligliv

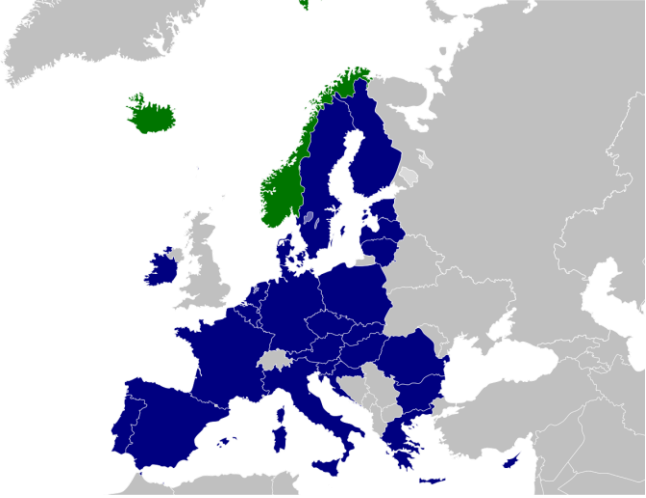
Norsk helsenett

Skytjenester og personvern post Schrems II

Oktober 2023

Hva er problemet?

- Skyleverandører bruker ofte datasenter og folk som ikke er i EU/EØS
- GDPR gjelder ikke der



Vurderinger

- SCC 2021
  - Lovlighet
  - Beskyttelse mot etterretning

Schrems

Ansvarlighet ved valg av databehandler

Informasjonssikkerhet

En sommergave

EU-Kommisjonens adekvansbeslutning for USA

10.7.2023

Datatilsynet

Hva leter du etter?

MENY

Aktuelle nyheter 2023

Nye regler for overføring av personopplysninger til USA

EU har vedtatt nye regler som gjør det enkelt å overføre personopplysninger til USA. Reglene trer i kraft umiddelbart.

Man kan overføre personopplysninger fritt innad i EØS, mens det som hovedregel er forbudt å overføre personopplysninger ut av EØS. Det finnes imidlertid noen unntak fra hovedregelen, og ett av dem er at EU-kommisjonen kan «godkjenne» enkeltland gjennom såkalte adekvansbeslutninger. 10. juli fikk USA en slik *adekvansbeslutning* som innebærer at hvis en amerikansk virksomhet står på lista over godkjente virksomheter (dataprivacyframework.gov), kan det overføres personopplysninger til den som om det var en europeisk virksomhet.

Virksomhetene må fortsatt følge de andre reglene i *personvernforordningen*, for eksempel ha behandlingsgrunnlag

Kontaktperson

Tobias Judin

seksjonssjef, internasjonal seksjon

Kontor: +47 22 39 69 47

E-post: tobias@datatilsynet.no

Publisert: 10.07.2023

Adekvansbeslutningen

- EU-kommisjonen kan beslutte at en stat sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger.

- Slike adekvansbeslutninger kan bare overprøves av EU-domstolen, ikke av tilsynsmyndighetene.

- 10.7.2023 besluttet Kommisjonen at USA gir slik beskyttelse for organisasjoner som står på Data Privacy Framework-lista.

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

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

(Text with EEA relevance)

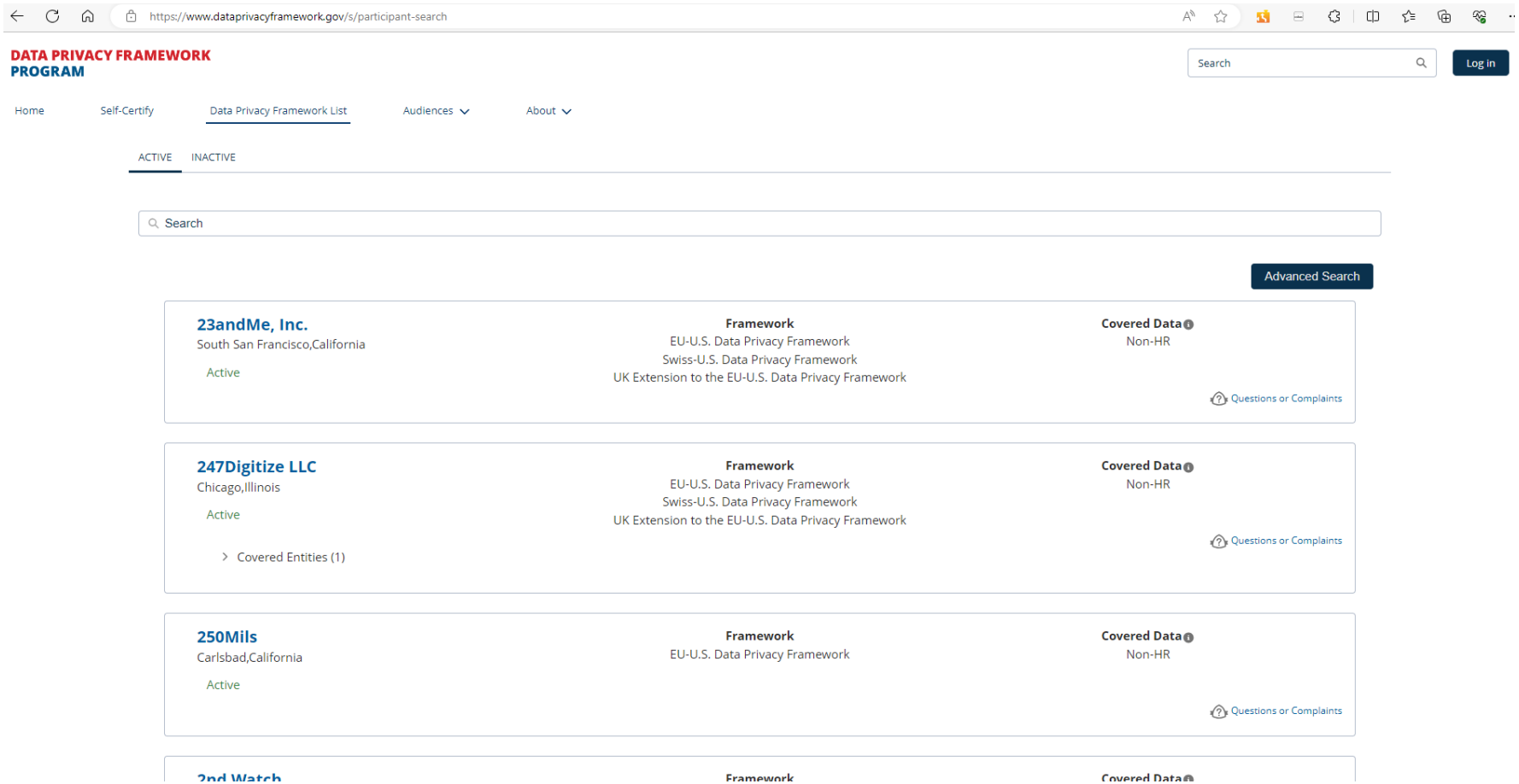
THE EUROPEAN COMMISSION,

HAS ADOPTED THIS DECISION:

Article 1

For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.

Data Privacy Framework List



Hva må til for å benytte adekvansvurderingen som overføringsgrunnlag?

- Mottaker i USA må stå på listen til Data Privacy Framework
  - Selvsertifisering
  - Underlegger seg tilsyn
  - Resertifisering hvert år

  - Skiller på typer av data:
    - «HR-data» er opplysninger om egne ansatte (nåværende og tidligere) som behandles i et arbeidsgiverforhold.
    - «Non-HR-data» er alle andre personopplysninger

- Eksportøren må befinne seg i EU/EØS

- (Virksomheten må selvsagt også oppfylle andre plikter etter personvernforordningen, for eksempel ha behandlingsgrunnlag og inngå databehandleravtale)

“…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.”

- Amerikansk lov ikke lenger problematisk

- Ikke nødvendig med «ytterligere tiltak»

European Data Protection Board

Hva er endret siden Schrems II?

- Felleserklæring i mars 2022 fra EU og USA om å adressere manglene påpekt av EU-domstolen i Schrems II-dommen av juli 2020

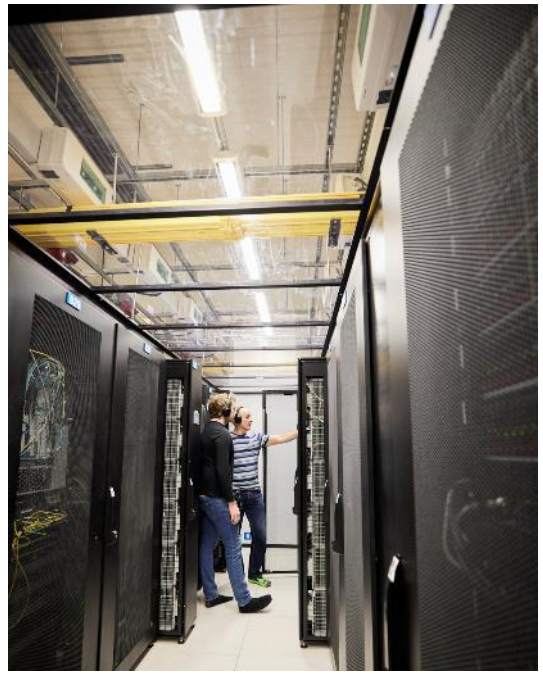
- Endringer i amerikansk rett oktober 2022 - juli 2023
  - EO 14086 – presidentordre om etterretningstjenestens virke (beslutning 7.10.22, erklæring om implementering 3.7.2023; direktivet erstatter PPD-28), bl.a.:
    - Krav til at nødvendighet og proporsjonalitet i signaletterretningen
    - Innfører klagerett for personer fra kvalifiserte land, domstolsliknende organ.
      - EØS-landene er utpekt som kvalifiserte land (generaladvokatens utpeking 10.7.2023)
  - **Endringene skal imøtekomme domstolens kritikk i Schrems II**

- Data Privacy Framework etablert, juli 2023
  - Selvsertifiseringsregime (selvdeklarasjonsregime) for virksomheter, med årlig resertifisering, underlagt tilsyn. Erstatter den tidligere Privacy Shield-ordningen.
  - **Selve ordningen ble ikke utfordret i Schrems II, det var spørsmålet om det var et tilsvarende personvernnivå i USA (adekvans) som var avgjørende. Domstolen sa nei til det, og da falt også ordningen bort.**

Norsk helsenett

Er det tut og kjør nå?
Ja – og nei….

Betydning for NHN



- Typisk situasjon
  - Behandling og lagring i Europa med europeisk databehandler (ev. med amerikansk eier)
    - Tidvis med mulighet for 24/7-support fra tredjeland
    - Spørsmål om amerikansk etterretning kan få tilgang
- Konsekvens av adekvansbeslutningen:
  - Amerikansk etterretningsregelverk anses ikke hindre «essentially equivalent» personvernbeskyttelse, derved er amerikansk eierskap eller support ikke problematisk
- Utenfor USA:
  - Support fra **andre** stater, eks. India, må **vurderes konkret**, inkl. om **tilleggstiltak** trengs, jf. Schrems II og EDPBs veiledning

Intern informasjon i NHN og Hdir (oktober 2023)

- **Veileder**: Overføring av personopplysninger til tredjeland
  - inkludert USA

- **Mal for vurdering** og dokumentasjon av overføringsgrunnlag etter GDPR kapittel V

- **Spørsmål til leverandører** (norsk og engelsk versjon)

«Nå for tiden har jeg inntrykk av at personopplysningene mine driver med mer reisevirksomhet enn meg.»

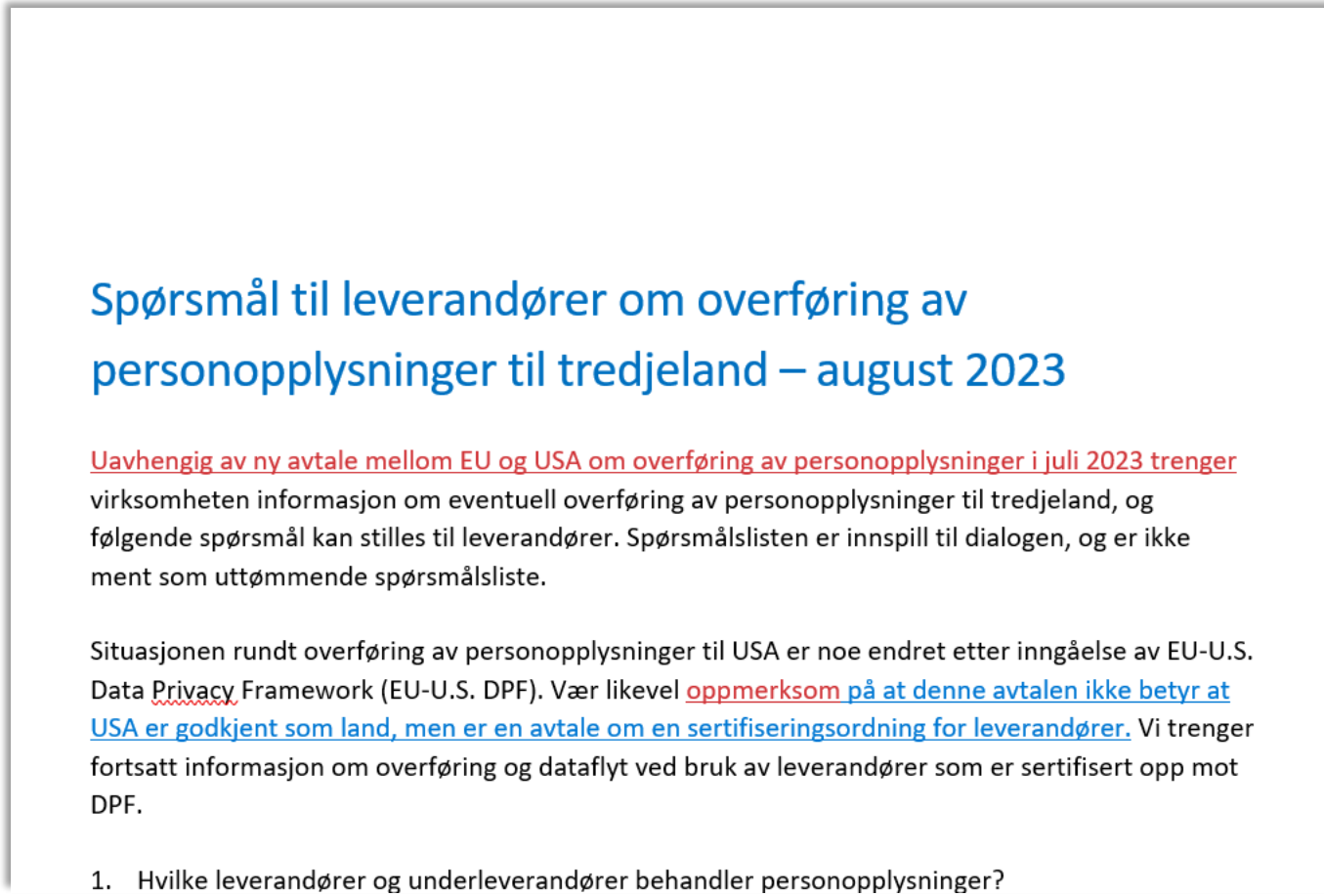
Hva må du gjøre når du vil overføre til USA?

Undersøk om den amerikanske virksomheten vi vil overføre til deltar i DPF

1. **Slå opp i listen over deltakende virksomheter**: Participant Search (dataprivacyframework.gov).
   - Viktig at det er det samme navnet på den virksomheten som vi inngår databehandleravtale med som er registrert i DPF
2. **Også underleverandører som mottar personopplysninger må være sertifisert.**
   - Undersøk verdikjeden og hvilke selskaper som inngår ved å se på databehandleravtalen eller personvernerklæring: *Spørsmål til leverandører* kan benyttes.
3. Enkelte selskap har tatt forbehold i avtalene om at det kan bli aktuelt å overføre personopplysninger til USA selv om de er etablert og primært skal behandle personopplysninger innenfor EØS. I slike tilfeller må også **datterselskaper i USA være sertifiserte**. Eksempler på dette er bl.a. Google, AWS og Microsoft.
4. **Undersøk hva slags type personopplysninger denne virksomheten sertifiserer seg for**, siden mottaker må være sertifisert for riktig type opplysninger. Det kan være HR-data eller Non-HR-data.
   - «HR-data» er opplysninger om egne (nåværende og tidligere) ansatte som behandles i et arbeidsgiverforhold. «Non-HR-data» er alle andre personopplysninger.
4. **Undersøk om informasjon om sertifiseringen er tatt inn i databehandleravtalen eller personvernerklæringen** for mottakende virksomhet i USA (skal være gjort innen 17. oktober 2023). Avtalen eller personvernerklæringen skal i tillegg ha en mekanisme for å løse tvister om behandlingen.
5. **Sertifisering gjelder bare for ett år av gangen**.
   - Legg inn i kalender/årshjul en kontroll av når sertifisering utløper, og om den fornyes for det kommende året.
6. **Dokumenter** som oversikt over håndtering av personopplysninger/ behandlingsprotokoll, personvernerklæring, databehandleravtaler mv. må **oppdateres med informasjon om at DPF benyttes som overføringsgrunnlag**
7. Hvis du er databehandler må du **følge opp at dataansvarlige har akseptert overføring** i tråd med inngått databehandleravtale.

Hva ber vi leverandørene om nå?

- Fortsetter å be om informasjon om
  - Leverandørkjeder
  - Dataflyt
  - Også for USA
- På vegne av både NHN og kunder:
  - Legge til rette for å vite, vurdere og ta ansvar
- Fordi….



Spørsmål til leverandører om overføring av personopplysninger til tredjeland – august 2023

Uavhengig av ny avtale mellom EU og USA om overføring av personopplysninger i juli 2023 trenger virksomheten informasjon om eventuell overføring av personopplysninger til tredjeland, og følgende spørsmål kan stilles til leverandører. Spørsmålslisten er innspill til dialogen, og er ikke ment som uttømmende spørsmålsliste.

Situasjonen rundt overføring av personopplysninger til USA er noe endret etter inngåelse av EU-U.S. Data Privacy Framework (EU-U.S. DPF). Vær likevel oppmerksom på at denne avtalen ikke betyr at USA er godkjent som land, men er en avtale om en sertifiseringsordning for leverandører. Vi trenger fortsatt informasjon om overføring og dataflyt ved bruk av leverandører som er sertifisert opp mot DPF.

1. Hvilke leverandører og underleverandører behandler personopplysninger?

Max Schrems har ting på gang

- *«Avtalen er ikke bedre enn den som ble ugyldig ved Schrems-II dommen»*

Blir ordningen stående?

Philippe Latombe hadde ting på gang

- *«Den nye avtalen strider mot EUs pakt om grunnleggende rettigheter»*
- *«Ikke tilstrekkelige garantier for respekten for privatlivet»*

- Ba om midlertidig suspendering av DPF
- Utfordret lovligheten i avtaleteksten

- Ble avvist (prosessuelt)

DPF gjelder

- inntil noe annet skjer…

7 Vil de nye reglene bli utfordret i EU-domstolen?

Mest sannsynlig vil de det. Det er imidlertid vanskelig å spå hva utfallet av en slik rettsak eventuelt vil bli.

På én side mener flere at de nye reglene adresserer bekymringene til EU-domstolen. Dessuten har den sikkerhetspolitiske situasjonen i verden forandret seg siden Schrems II-dommen. Flere peker på at europeiske overvåkningslover også kan være problematiske og at man bør prioritere å se på disse først. På den annen side mener flere at de nye løsningene ikke er gode nok. Flere mener også at det er andre utfordringer med amerikansk etterretning som EU-domstolen ikke har uttalt seg om før, men som den bør ta stilling til.

Det er med andre ord en *risiko* for at de nye reglene vil bli opphevet, og at det i så fall vil bli vanskelig å overføre personopplysninger til USA igjen. Vi vet ikke om denne risikoen vil slå til, men det er viktig å ha et bevisst forhold til den.

Pre-Normkonferansen - PVO-samling

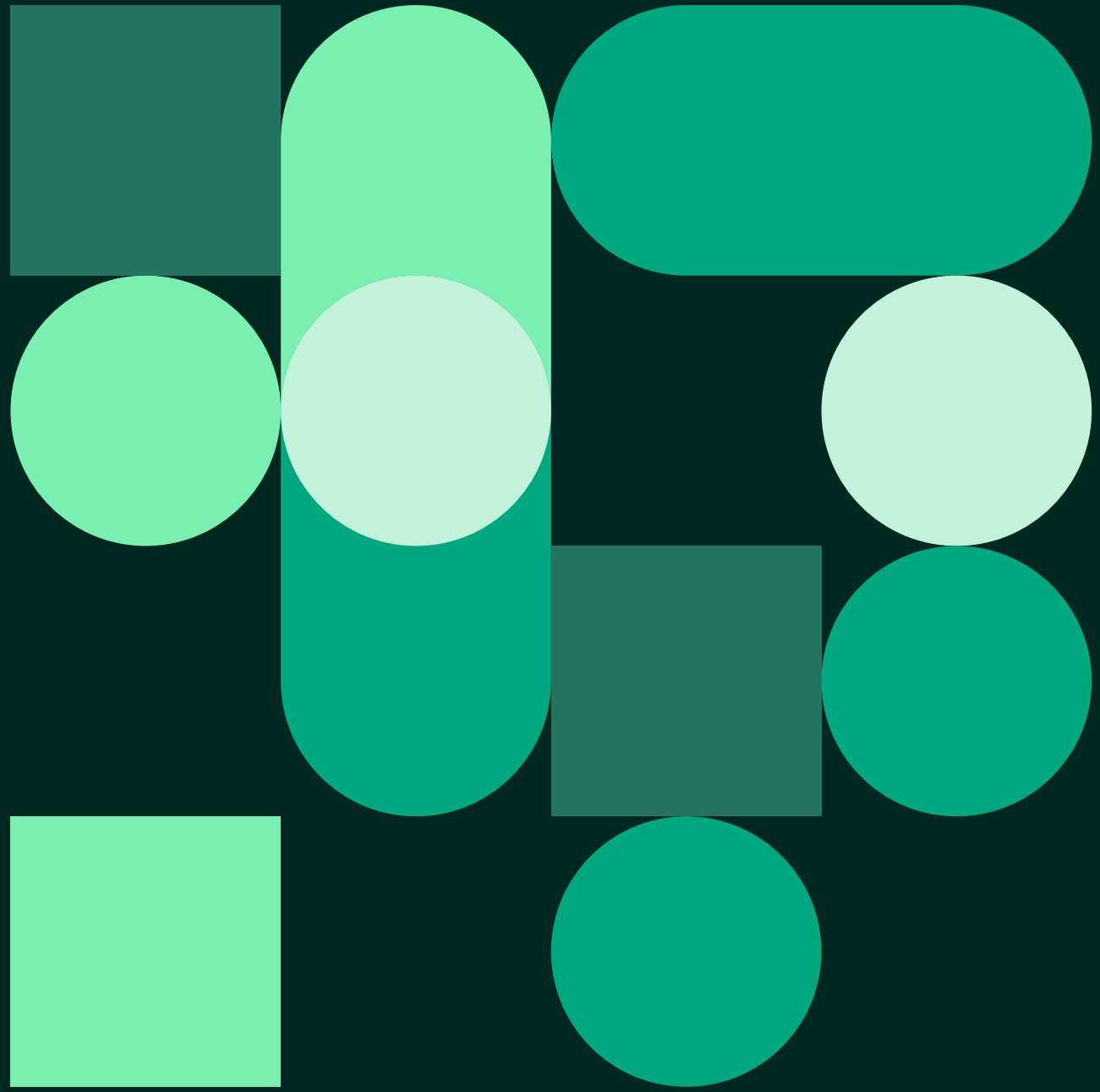
- Velkommen til samling - Aasta Margrethe Hetland og Marit Larsen Haarr (NHN)
- Nytt fra Datatilsynet - Camilla Nervik og Fredrik Christensen
- *Matpause* - 1710 - 1740
- Regulatorisk veiledningstjeneste kunstig intelligens (KI) - Kathrine Olsgard, Hdir
- Ny veileder for personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter - Ane Hessen Hjelle og Marie Strand Schildmann (E-helse)
- *Pause* - 1820 - 1830
- Ny adekvansvurdering for USA - hva nå? Marit Larsen Haarr
- *Pause* 1850 - 1900
- Samtale: Utfordringer i PVO’s dagligliv

Norsk helsenett

Hvem er jeg som PVO?

PVO-samling 2023

Marit Larsen Haarr



PVF artikkel 37, nr. 5

«Personvernombudet skal utpekes på grunnlag av **faglige** kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt **evne** til å utføre oppgavene nevnt i artikkel 39.»

Det viktigste?

Jeg er en endringsleder

Oppgavene

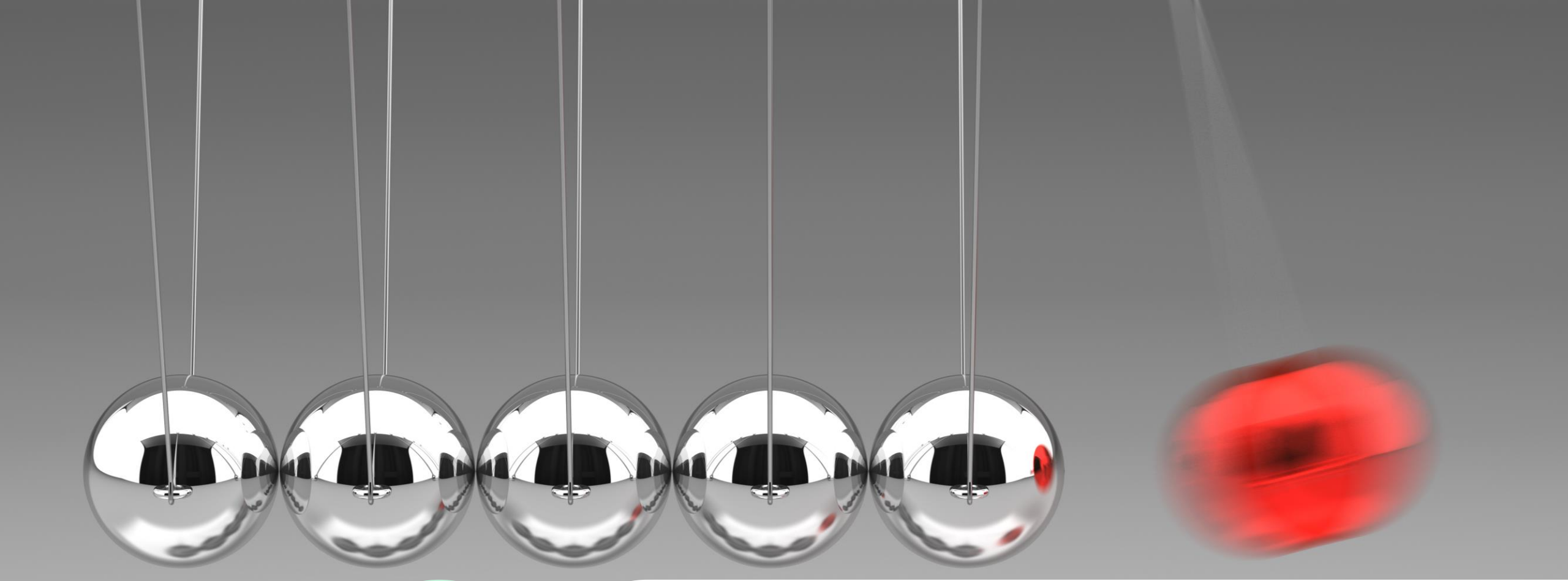
- Mine oppgaver: Opplæring, veiledning - og kontroll
  - Regelverk
  - Styringssystem

- Mine kollegers oppgaver: å etterleve og skape godt personvern i de tjenestene vi leverer

– og visjonene: HVORFOR? HVA?

KJEDEREAKSJON

- Skape engasjement for mennesker og rettigheter – hos oss
- – og tillit fra dem det gjelder til oss når vi forvalter deres mest intime hemmeligheter



Vi kan ikke dytte endring

Meg som virkemiddel

- Speil, speil på veggen der…