



Vil adekvansbeslutningen falle?

En veileder om hva overføringsgrunnlaget for overføringer av personopplysninger til USA bygger på, om det fortsatt bør være gyldig og om vi bør fortsette å overføre personopplysninger til USA.

FORORD

Den geopolitiske situasjonen i verden har endret seg mye og raskere enn det vi er vant med siden 2025. USA, en nær alliert, har truet vårt naboland Danmark med militærmakt, om de ikke får ta over Grønland.¹ Spørsmålet om Microsoft egentlig stengte e-postkontoen til en advokat hos den internasjonale straffedomstolen i Haag, har satt digital suverenitet på dagsordenen i Europa.^{2 3 4} NSM har i sin trusselvurdering for 2026 fremhevet «omfattende bruk av et fåtall utenlandske skytjenester» som en sikkerhetsrisiko.⁵ Mens amerikanske myndigheter flere ganger har kritisert EUs personvernregelverk for å være for strengt og unødvendig.^{6 7}

Overføringer av personopplysninger ut av EU/EØS har alltid vært et vanskelig spørsmål. Nå virker det i tillegg usikkert, selv om skoleeiere fortsatt har et gyldig overføringsgrunnlag i adekvansbeslutningen til EU-kommisjonen.

Denne veilederen er et forsøk på å forklare hva adekvansbeslutningen står og faller på. Hva EU-kommisjonen har vurdert og lagt vekt på når den har kommet til at personopplysninger som overføres til USA nyter tilsvarende personvernbeskyttelse som etter GDPR.

Hvis de forhold som adekvansbeslutningen hviler på endres eller faller bort, vil dette i tid skjedd før EU-kommisjonen trekker den tilbake eller EU-domstolen kjenner den ugyldig.

I den nasjonale DPIA-prosjektet for bruk av Microsoft 365 i skolen, ønsket vi å se på hva forutsetningene for adekvansbeslutningen er. Dette for å kunne gjøre oss opp en mening om når forholdene i USA har endret seg så mye at adekvansbeslutningen *burde* falle.

Nå har det skjedd. Adekvansbeslutningen *burde* falle.

Sommeren 2026 kom amerikansk høyesterett til at tilsynsorganet Federal Trade Commission (FTC), ikke er et selvstendig og uavhengig tilsynsorgan. Det er politisk underlagt presidenten.

¹ <https://www.tv2.no/nyheter/reuters-trump-vil-overta-gronland-i-denne-presidentperioden/18438608/>

² https://www.theregister.com/2026/02/18/microsoft_asks_uk_parliament_to_correct_record/

³ https://www.theregister.com/2025/10/31/international_criminal_court_ditches_office/?gl=1*q38rxt*ga*NzQxMDE3NzA4LjE3MDQ4MDY3MzY.*ga_JXW44Y23NM*czE3NzEwMDIwODYkbzI1NTEkZzEkdDE3NzEwMDIzODkkaQ5JGwwJGgw

⁴ Khan, en advokat hos den den internasjonale straffedomstolen i Haag (ICC) fikk sperret sin Microsoft e-postkonto i mai 2025. Saken sees i sammenheng med at han ble sanksjonert av amerikanske myndigheter for å ha utstedt en arrestordre på Israels statsminister på grunn av folkerettighetsbrudd i Gaza. Det har kommet motstridene rapporter på hvem som stengte kontoen hans, om det var Microsoft eller ICC, men ICC valgte i oktober 2025 å avslutte sin avtale med Microsoft til fordel for et kontorstøtteverktøy levert av Center for Digital Sovereignty (ZenDiS) på vegne av det tyske føderale innenriksdepartementet. Til tross for usikkerheten knyttet til faktiske forhold, har saken satt digital suverenitet på dagsordenen i Europa.

⁵ [https://nsm.no/getfile.php/1314962-](https://nsm.no/getfile.php/1314962-1770630853/NSM/Filer/Dokumenter/Rapporter/Risiko%202026.pdf)

[1770630853/NSM/Filer/Dokumenter/Rapporter/Risiko%202026.pdf](https://nsm.no/getfile.php/1314962-1770630853/NSM/Filer/Dokumenter/Rapporter/Risiko%202026.pdf)

⁶ <https://www.forbes.com/sites/siladityaray/2025/02/11/jd-vance-knocks-eus-regulation-of-us-tech-giants-america-cannot-accept-that/>

⁷ https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25/?utm_source=euractiv&utm_medium=newsletter&utm_content=INTRO&utm_term=0-0&utm_campaign=PRO_Tech

Dommen slo også fast at ingen tilsynsorgan i forvaltningen er uavhengige. Det betyr at en viktig forutsetning for adekvansbeslutningen har falt.

Bare så det er sagt: adekvansbeslutningen kan brukes som overføringsgrunnlag så lenge den er gyldig. Den kan *bare* bli kjent ugyldig av EU-domstolen eller trekkes tilbake av EU-kommisjonen. Inntil det faktisk skjer, kan du som skoleeier og behandlingsansvarlig bruke den som grunnlag for å overføre personopplysninger til USA. Nærmere bestemt til virksomheter i USA som har sertifisert seg etter rammeverket «Data Privacy Framework».

Men det kan være lurt å forstå hvorfor dette overføringsgrunnlaget bør settes til side nå. Vi inviterer deg derfor til å lese denne veiledningen for å forstå hvorfor, og for å forberede seg på hva du kan gjøre.

28. september 2026

Hvordan vi har brukt generativ KI i denne veilederen

I førsteutkastet til denne veilederen, ble generativ KI (språkmodell fra SIKT) brukt til å utforme tekstforbedringsforslag til tre avsnitt.

I redigeringsfasen brukte vi ikke generativ KI til å generere eller forbedre teksten.

Den endelige teksten du leser i denne veilederen, er redigert i flere omganger, og er så forskjellig fra de første utkastene, at vi i det nasjonale DPIA-prosjektet er komfortable med å si at ingen tekst her er generert med generativ KI.

Versjonslogg			
Versjon	Dato	Endring	Forfatter
1.0	April 2026		KS, SkoleSec ved Ida Thorsrud og Saredo Osman
2.0	September 2026	Oppdatering av forord, punkt 4.2 (Garanti C – Uavhengige tilsyn) og Kapittel 5.	KS, SkoleSec ved Ida Thorsrud og Saredo Osman

1 INNHOLDSFORTEGNELSE

Forord.....	1
1 Innholdsfortegnelse.....	4
2 Bakgrunn.....	6
2.1 Adekvansbeslutninger åpner for overføringer.....	6
2.2 Hvorfor fikk vi et nytt overføringsgrunnlag for USA?.....	6
2.3 Fire grunnleggende garantier.....	7
3 Kommisjonens vurdering.....	8
3.1 Strafferett.....	8
3.2 Nasjonal sikkerhet.....	8
3.3 Personvernprinsippene i Data Privacy Framework.....	8
3.4 Tilsynsorgan.....	9
3.4.1 Department of Commerce (DoC).....	9
3.4.2 The Federal Trade Commission (FTC).....	9
3.4.3 Department of Transportation (DoT).....	9
3.5 Effektive rettsmidler.....	10
3.5.1 Nye klagemuligheter gjennom Civil Liberties Protection Officer og Data Protection Review Court.....	10
3.5.2 Gratis ordninger for tvisteløsning skal være tilgjengelig for EU/EØS-borgere.....	10
3.5.3 Klage gjennom Europeiske datatilsyn.....	10
3.5.4 Bindende voldgift.....	11
4 Kritikk mot Data Privacy Framework.....	12
4.1 Garanti A og B – Klare regler, nødvendighet og proporsjonalitet.....	12
4.1.1 I praksis er regelverket for sårbart.....	12
4.1.2 Har USA åpnet for overvåkning av seksuelle minoriteter?.....	13
4.2 Garanti C – Uavhengig tilsyn.....	14
4.2.1 EO 14215 utfordrer tilsynsorganenes uavhengighet.....	14
4.2.2 Manglende tverrpolitisk representasjon utfordrer FTCs uavhengighet.....	15
4.2.3 Privacy and Civil Liberties Oversight Board (PCLOB) er ikke beslutningsdyktig.....	15
4.2.4 Alle tilsynsorgan i den amerikanske forvaltningen er direkte underlagt politisk styring fra den amerikanske presidenten.....	16
4.3 Garanti D – Effektive rettsmidler.....	17
4.3.1 Ordningen er for sårbar.....	17
4.3.2 Ingen følger opp PCLOB.....	17

4.3.3	Ikke kjent hvordan den jevne borger skal kunne bruke de rettsmidlene de har til rådighet 17	
5	Hva nå?	19
5.1	Blir det Schrems III?	19
5.2	Hva kan du som skoleeier gjøre?	19
5.3	Du kan velge å se på alternativer til store amerikanske skyleverandører	20

2 BAKGRUNN

2.1 ADEKVANSBESLUTNINGER ÅPNER FOR OVERFØRINGER

Hvis du som behandlingsansvarlig skal overføre personopplysninger ut av EU/EØS, må du ha et overføringsgrunnlag. Forenklet kan vi si at hvis EU-kommisjonen har fastslått at et land utenfor EU/EØS har et «tilstrekkelig beskyttelsesnivå», vil det være et overføringsgrunnlag du kan bruke. Slike vurderinger fra EU-kommisjonen kalles en «adekvansvurdering» eller en «adekvansbeslutning».

Den 10. juli 2023 vedtok EU-kommisjonen en slik beslutning for USA. Du som behandlingsansvarlig kan overføre personopplysninger til amerikanske virksomheter som har selv-sertifisert seg under personvernrammeverket «Data Privacy Framework».⁸ Ordningen gjør det enklere å bruke amerikanske skytjenester, samtidig som personvernet ivaretas.

2.2 HVORFOR FIKK VI ET NYTT OVERFØRINGSGRUNNLAG FOR USA?

I Schrems-dommene⁹ ble de tidligere overføringsgrunnlagene for USA¹⁰ kjent ugyldige av EU-domstolen. Den siste Schrems II-dommen falt sommeren 2020. Da slo EU-domstolen fast at USAs beskyttelsesnivå ikke var tilstrekkelig for å ivareta personvernet. Dette skyldtes i all hovedsak tre ting:

1. Amerikanske overvåkingslover ga etterretningsmyndighetene for vide fullmakter til å samle inn og bruke personopplysninger,
2. det manglet uavhengig tilsyn med etterretningsmyndighetene for å hindre brudd på EU/EØS-borgeres personvern, og
3. EU/EØS-borgere hadde ikke reelle klagemuligheter til å klage dersom personvernet deres hadde blitt brutt.

Med Schrems II-dommen, ble alle overføringer til USA basert på adekvansvurderingen ugyldig over natta. Dette gjorde alle overføringer som hadde brukt dette grunnlaget ulovlige, noe som skapte stor usikkerhet.

Etter dette har EU og USA forhandlet fram flere endringer som skulle bedre personvernet til EU/EØS-borgere. I 2022 signerte daværende president Biden Executive Order¹¹ 14086 som blant annet innførte nye personvernbegrensninger for amerikansk etterretning og et nytt klageorgan.

Disse endringene ble sentrale for at EU-kommisjonen i den nye adekvansvurderingen konkluderte med at personopplysninger kan overføres til USA med tilsvarende personvernbeskyttelse som etter GDPR.

⁸ Sjekk om din leverandør er sertifisert her: <https://www.dataprivacyframework.gov/list>

⁹ Schrems I C-362/14 og Schrems II C-311/18

¹⁰ Safe Harbor og Privacy Shield

¹¹ Presidentordre

2.3 FIRE GRUNNLEGGENDE GARANTIER

For å vurdere om personvernet for EU/EØS-borgere er «tilsvarende» det vernet vi har etter GDPR når personopplysningene våre behandles i USA, må fire grunnleggende krav eller garantier være oppfylt:¹²

- **Garanti A:** Inngrep i personvernet (f.eks. myndigheters tilgang til personopplysninger), må være basert på klare og presise regler som er tilgjengelige for offentligheten.
- **Garanti B:** Inngrep må være nødvendige og forholdsmessige for å oppnå et legitimt formål.
- **Garanti C:** Det må eksistere et uavhengig tilsynsorgan som kan føre kontroll med etterretningstjenesten, myndighetenes overvåking og tilgang til data. Tilsynsmyndigheten skal sikre at regler følges og maktmisbruk avdekkes.
- **Garanti D:** EU/EØS-borgere må ha tilgang til effektive rettsmidler. Dette betyr at de må kunne få prøvd om deres personvernrettigheter har blitt krenket av myndighetene i tredjelandet sin overvåking. Dette i form av mulighet til å klage saken inn for et tilsynsorgan eller en domstol og eventuelt få kompensasjon eller stanse ulovlig overvåking.

Hvis du er en av dem som ser på de endringene som skjer i USA, og blir bekymret for om adekvansvurderingen fortsatt vil stå seg, må du se på disse fire garantiene. I denne veiledningen gjennomgår vi dem og ser på om de fortsatt står seg slik situasjonen i USA er i nå (mars 2026).

¹² [edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf](#)

3 KOMMISSJONENS VURDERING

Da EU-kommisjonen vurderte de fire grunnleggende garantiene opp mot amerikansk regelverk og praksis, så de særlig på tre ting:

- 1) Hvordan strafferetten i USA håndheves,
- 2) nasjonal sikkerhet (signaletterretning), og
- 3) hvordan personvernprinsippene i rammeverket Data Privacy Framework .

På bakgrunn av de endringene som vi har gjennomgått ovenfor, kom EU-kommisjonen til at personopplysninger som overføres til USA vil beskyttes med et tilsvarende personvern som det vi har etter GDPR. Dette så lenge personopplysningene overføres til en amerikansk virksomhet som er sertifisert etter Data Privacy Framework.

3.1 STRAFFERETT

Kommisjonen hadde få bemerkninger til hvordan strafferetten håndheves i USA. Dette fordi de strafferettslige garantiene i USA i stor grad samsvarer med det vi har i EU/EØS. Dette er garantier som at ingen skal dømmes uten hjemmel i lov eller at en som er tiltalt skal få vite hva hen er tiltalt for. Dette for å kunne komme opp med et forsvar (kontradiksjon).

3.2 NASJONAL SIKKERHET

I Schrems II ble amerikansk etterretning sin behandling av personopplysninger for nasjonale sikkerhetsformål kritisert. EU-kommisjonen brukte mye plass i adekvansvurderingen på å redegjøre for hvordan dette er forbedret i EO 14086.

Presidentordren innførte krav om at etterretning bare skal skje for spesifikke, legitime formål.¹³ Dette er endringer knyttet til klarhet og presisjon, nødvendighet og forholdsmessighet.

EO 14086 fastsetter for første gang klare og lovlige formål for amerikansk signaletterretning, som å bekjempe terrorisme, cybertrusler og fremmed etterretning, og forbyr overvåking for politisk, økonomisk eller diskriminerende formål.

3.3 PERSONVERNPRINSIPPENE I DATA PRIVACY FRAMEWORK

De amerikanske virksomhetene som sertifiserer seg under Data Privacy Framework¹⁴ må overholde personvernprinsipper som er veldig like de personvernprinsippene vi kjenner fra GDPR. Konkret plikter de å:

- gi (tilstrekkelig) informasjon

¹³ Se EO 14086 2(b)i om "Legitimate objectives"

¹⁴ Lista over virksomheter sertifisert etter Data Privacy Framework finnes her:
<https://www.dataprivacyframework.gov/list>

- innhente samtykke
- ta ansvar for videreoverføringer
- oppnå tilstrekkelig sikkerhet
- ivareta dataintegritet og formålsbegrensning
- gi den registrerte innsyn
- sørge for at de skal kunne motta klager fra den registrerte og at de har effektive klageordninger, håndhevelse og ansvar

Amerikanske firmaer som ønsker å følge forpliktelsene i Data Privacy Framework, selvsertifiserer seg.¹⁵

3.4 TILSYNSORGAN

Amerikanske myndigheter kontrollerer og håndhever at disse selskapene faktisk etterlever Data Privacy Framework gjennom flere organer:

3.4.1 Department of Commerce (DoC)

Department of Commerce har det overordnede administrative ansvaret for rammeverket. De forvalter sertifiseringsordningen, fører og publiserer listen over sertifiserte selskaper, og kontrollerer at virksomheter som søker om eller fornyer sertifisering faktisk oppfyller kravene i prinsippene.

DoC gjennomfører både forhåndskontroller ved sertifisering og løpende oppfølging gjennom stikkprøver, spørreskjemaer og undersøkelser ved mistanke om manglende etterlevelse. Dersom et selskap ikke samarbeider eller ikke retter opp brudd, kan det fjernes fra ordningen og miste retten til å motta personopplysninger fra EU på dette grunnlaget.

3.4.2 The Federal Trade Commission (FTC)

For de fleste kommersielle selskaper er det Federal Trade Commission som har ansvar for håndhevingen av Data Privacy Framework. The Federal Trade Commission har uavhengig etterforsknings- og sanksjonsmyndighet og kan gripe inn dersom et selskap bryter forpliktelsene sine under Data Privacy Framework eller gir uriktige opplysninger om deltakelse i ordningen. Brudd på prinsippene i Data Privacy Framework anses som villedende eller urimelig forretningspraksis etter amerikansk rett og kan føre til bindende pålegg og krav om endring av praksis, og i alvorlige tilfeller, økonomiske sanksjoner.

FTC følger også opp etterlevelse av slike vedtak over tid og kan reagere dersom et selskap ikke oppfyller de bindende påleggene.

3.4.3 Department of Transportation (DoT)

Det er Department of Transportation som har myndighet til å håndheve og kontrollere at flyselskaper, reisebyråer og andre selskaper som selger billetter etterlever Data Privacy Framework. Konkret kontrollerer de at personvernforpliktelsene etterleves. De kan fatte vedtak,

¹⁵ For oversikt over de amerikanske selskapene som til enhver tid har sertifisert seg etter Data Privacy Framework, se <https://www.dataprivacyframework.gov/list>

illegge sanksjoner og føre tilsyn med at pålegg faktisk etterleves. Også her kan manglende etterlevelse føre til formelle reaksjoner som er rettslig bindende.

3.5 EFFEKTIVE RETTSMIDLER

En annen ting som EU-kommisjonen vurderer i adekvansbeslutningen, er om EU/EØS-borger har tilgang på effektive rettsmidler. «Tilgang på effektive rettsmidler» betyr at EU/EØS-borgere skal ha en klagemulighet for å få sjekket at personvernrettighetene våre ikke er brutt. Dette ivaretas gjennom flere ordninger:

3.5.1 Nye klagemuligheter gjennom Civil Liberties Protection Officer og Data Protection Review Court

Adekvansbeslutningen beskriver hvordan EO 14086 etablerer en ny klageordning som EU/EØS-borgere kan bruke for å sjekke om amerikanske etterretningsmyndigheter bryter med deres personvern.

Klager fra europeiske borgere blir først vurdert av en «Civil Liberties Protection Officer» («CLPO») tilknyttet det amerikanske etterretningsorganet Office of the Director of National Intelligence (ODNI). CLPO skal påse at amerikanske etterretningsmyndigheters praksis ivaretar personvernet og andre grunnleggende rettigheter.

I tillegg har EO 14086 opprettet en uavhengig og upartisk personverndomstol kalt «Data Protection Review Court» («DPRC») som fungerer som andreinstans i saksgangen for en klage.

For at DPRC skal være en tilstrekkelig uavhengig prøvingsinstans, er det bestemt at dommerne skal være utenfor den amerikanske regjeringen, ha relevant erfaring innen personvern og nasjonal sikkerhet, og ha oppsigelsesvern. Videre har domstolen kompetanse til å vedta bindende avhjelpende tiltak.

Europeiske borgere som ønsker å klage, kan enten sende klage direkte til datatilsynet i det landet man bor, eller rette klagen direkte til den amerikanske virksomheten som behandler personopplysningene.

3.5.2 Gratis ordninger for tvisteløsning skal være tilgjengelig for EU/EØS-borgere

Amerikanske selskaper som er sertifisert etter Data Privacy Framework, plikter å tilby gratis ordninger for tvisteløsning for EU/EØS-borgere, enten gjennom uavhengige klageorganer i USA eller i EU. Det er gjerne eksterne selskaper som vil stå for denne typen tvisteløsning.

Twisteløsningsorganene vil ha myndighet til å undersøke klager, kreve retting eller sletting av personopplysninger og pålegge amerikanske selskap som bryter med forpliktelsene i Data Privacy Framework å iverksette tiltak. Dersom et selskap ikke følger avgjørelser fra tvisteløser, kan saken oversendes til amerikanske myndigheter for håndheving (Department of Commerce, the Federal Trade Commission eller Department of Transportation).

3.5.3 Klage gjennom Europeiske datatilsyn

Europeiske datatilsyn har også en rolle i håndhevingen av EU/EØS-borgeres personvernrettigheter i USA. Datatilsynene kan undersøke klager fra registrerte, gi råd og pålegg. Dersom et amerikansk

selskap ikke etterlever slik pålegg, kan saken bringes videre til amerikanske myndigheter for formell håndheving.

3.5.4 Bindende voldgift

Som en siste utvei har registrerte også tilgang til bindende voldgift dersom andre klagemekanismer ikke fører frem. Dette skal sikre at personvernrettighetene faktisk kan håndheves i praksis.

Voldgift er en prosess for å avgjøre en rettslig tvist hvis man ikke blir enige, og uten å ta saken til domstolen. Her vil registrerte kunne overlate vurderingen av om deres personvernrettigheter er brutt til en virksomhet som tilbyr voldgift.

4 KRITIKK MOT DATA PRIVACY FRAMEWORK

Selv om Data Privacy Framework ble etablert for å rette opp svakhetene fra tidligere ordninger, har rammeverket blitt kritisert. Det har skapt usikkerhet om hvor robust og varig rammeverket vil være. I tillegg har det siden 2025 skjedd flere endringer i USA som også kan være relevante for spørsmålet om adekvansbeslutningen vil eller bør bli ugyldiggjort.

I dette kapittelet gjennomgår vi denne kritikken. Vi vil også gjennomgå de endringene som har skjedd siden 2025 for å se om de har påvirket hvordan personvernet ivaretas i praksis.

Vi håper at dette vil hjelpe deg som er ansatt hos en skoleeier å vurdere hvordan dere som behandlingsansvarlige skal forholde dere til usikkerheten rundt å bruke adekvansbeslutningen som overføringsgrunnlag.

Vi har organisert dette under de fire grunnleggende garantiene som må være oppfylt for at USA kan sies å gi tilsvarende personvern som det vi har etter GDPR i EU/EØS.¹⁶

4.1 GARANTI A OG B – KLARE REGLER, NØDVENDIGHET OG PROPORSJONALITET

- **Garanti A:** Inngrep i personvernet (f.eks. myndigheters tilgang til personopplysninger), må være basert på klare og presise regler som er tilgjengelige for offentligheten.
- **Garanti B:** Inngrep må være nødvendige og forholdsmessige for å oppnå et legitimt formål.

4.1.1 I praksis er regelverket for sårbart

Executive Order 14086 har innført viktige begrensninger i hvordan amerikanske etterretningsorganer kan innhente og bruke personopplysninger. Den inneholder krav om at overvåkning må være nødvendighet og proporsjonal, og den skal forhindre vilkårlig masseinnsamling av personopplysninger.

Den amerikanske tolkningen av begrepene «nødvendighet» og «proporsjonalitet» er litt forskjellig fra den europeiske tolkningen. USA tillater fortsatt overvåking med bredt definerte mål hvor etterretningsorganene har tilgang til store datamengder fra personer som ikke er mål i seg selv.¹⁷ Fra et europeisk ståsted utfordrer dette kravet om målrettet og individuelt begrunnet overvåking.

¹⁶ Garanti A: Inngrep i personvernet (f.eks. myndigheters tilgang til personopplysninger), må være basert på klare og presise regler som er tilgjengelige for offentligheten.

Garanti B: Inngrep må være nødvendige og forholdsmessige for å oppnå et legitimt formål.

Garanti C: Det må eksistere et uavhengig tilsynsorgan som kan føre kontroll med etterretningstjenesten, myndighetenes overvåking og tilgang til data. Tilsynsmyndigheten skal sikre at regler følges og maktmisbruk avdekkes.

Garanti D: EU/EØS-borgere må ha tilgang til effektive rettsmidler. Dette betyr at de må kunne få prøvd om deres personvernrettigheter har blitt krenket av myndighetene i tredjelandet sin overvåking. Dette i form av mulighet til å klage saken inn for et tilsynsorgan eller en domstol og eventuelt få kompensasjon eller stanse ulovlig overvåking.

¹⁷ Dette reguleres etter FISA § 702

Selv om Executive Order 14086 på papiret oppfyller mye av Garanti A (klare regler) og Garanti B (nødvendighet og forholdsmessighet), gjenstår to hovedproblemer:

1. Manglende lovforankring: Tiltakene bygger kun på en presidentordre, ikke på lov, og kan endres med et pennestrøk av en ny president.
2. Begrenset transparens: Flere overvåkingsprogrammer er fortsatt hemmelige, og det finnes lite offentlig dokumentasjon om hvordan reglene faktisk håndheves.

Med andre ord: på papiret har USA et tydelig regelverk, men i praksis er vernet politisk sårbart og avhenger av hvordan hver administrasjon velger å følge opp prinsippene.

Selv om EO 14086 fortsatt gjelder og ikke har blitt trukket tilbake av Trump-administrasjonen, er det en risiko for at det vil skje. I en plan for omstrukturering av den amerikanske forvaltningen kalt «Project 2025» publisert i 2023 av tankesmia The Heritage Foundation, anbefales det at EO 14086 evalueres og at bestemmelser i den som hindrer etterretningsmyndighetene i å gjøre jobben sin fjernes.¹⁸ Trump-administrasjonen har per januar 2026 gjennomført flere av tiltakene i dokumentet,¹⁹ men ingen som er relevante for vurderingen av om adekvansbeslutningen fortsatt bør være gyldig.²⁰

4.1.2 Har USA åpnet for overvåkning av seksuelle minoriteter?

Det har skjedd noen endringer ved overvåkningspraksis som får direkte virkninger for adekvansbeslutningen. EU-kommisjonen la særlig vekt på at Executive Order 14086 «limits the grounds on which data can be collected as part of signals intelligence activities» blant annet ved at den «lists certain objectives that must never be pursued by signals intelligence activities». Dette betyr at presidentorden inneholder flere formål som overvåkning aldri skal brukes til. To av disse er:

- «for the purpose of burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;»
- «for the purpose of disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; or to afford a competitive advantage to U.S. companies».

¹⁸ Project 2025, The Heritage Foundation, s. 226: “The United States has never seriously pushed back against the EU; now is the time. An incoming President should ask for an immediate study of the implementation of Executive Order 14086 and suspend any provisions that unduly burden intelligence collection. At the same time, in negotiations with the Europeans, the United States should make clear that the continued sharing of intelligence with EU member states depends on successful resolution of this issue within the first two years of a President’s term. It is time for a real solution, not the 30 years of stopgaps imposed by Brussels.”

¹⁹ Dette ifølge to forskjellige «Project 2025-trackers»: <https://www.project2025.observer/en> og <https://progressivereform.org/tracking-trump-2/project-2025-executive-action-tracker/>.

²⁰ Det skal sies at ingen av trackerne inneholder evaluering av EO 14086 som et tiltak som spores, selv om det å oppheve presidentorden er en del av «Project 2025». Det betyr at trackerne ikke gir en fullstendig liste over alle tiltakene i «Project 2025» og at prosjektet inneholder langt flere tiltak enn det disse trackerne har oversikt over.

Det siste kulepunktet handler om at etterretningsorganene ikke skal kunne overvåke folk blant annet på grunn av kjønnsidentitet og seksuell orientering.

I februar 2025, ble det meldt i media at Departement of Homeland Security hadde gjort endringer i sine interne retningslinjer for etterretning ved å fjerne de bestemmelsene som tidligere uttrykkelig forbød overvåkning kun på grunnlag av seksuell orientering eller kjønnsidentitet.²¹ Senere ble det meldt at seksuell orientering var inntatt igjen,²² men per mars 2026 virker denne retningslinjen å ha blitt fjernet fra hjemmesidene til Department of Homeland Security.²³²⁴ Det er derfor uklart hva status er på dette i 2026.

Hvis DHS i praksis skulle drive etterretning basert på opplysninger om seksuell orientering og kjønnsidentitet, så ville dette være i strid med kravene som EO 14086 stiller til overvåkingen. I tillegg vil det være i strid med kravet til nødvendighet. Dette fordi det å tilhøre en seksuell minoritet i seg selv ikke er en god nok grunn til å overvåke noen av nasjonale sikkerhetshensyn. Dette vil også være et brudd på krav om forholdsmessighet da denne typen overvåkning vil være svært inngripende. Overvåkingen vil nok også være uforholdsmessig sett opp mot den sikkerhetsgevinsten som man ønsker å oppnå.

4.2 GARANTI C – UAVHENGIG TILSYN

- **Garanti C:** Det må eksistere et uavhengig tilsynsorgan som kan føre kontroll med etterretningstjenesten, myndighetenes overvåking og tilgang til data. Tilsynsmyndigheten skal sikre at regler følges og maktmisbruk avdekkes.

4.2.1 EO 14215 utfordrer tilsynsorganenes uavhengighet

En del av kritikken mot adekvansvurderingen har vært at de ulike tilsynsorganene som USA har innført, i praksis ikke er så uavhengige som de bør være.

Executive Order 14215 (heretter «EO 14215») ble utstedt av Trump 18. februar 2025 for å gi presidenten større makt over uavhengige statlige tilsyn. Dette inkluderer tilsynsorganet The Federal Trade Commission (FTC) som skal håndheve og etterprøve at amerikanske selskaper som er selvsertifisert etter DPF faktisk overholder prinsippene i dette rammeverket.

EO 14215 krever at alle føderale etater i USA må operere i henhold til presidentens og justisministerens lovtolkning og rapportere jevnlig til dem. Dette utfordrer FTCs uavhengighet.

²¹ <https://news.bgov.com/bloomberg-government-news/trumps-dhs-loosens-sexual-orientation-based-surveillance-policy>

²² <https://news.bgov.com/bloomberg-government-news/dhs-intelligence-unit-restores-sexual-orientation-protections>

²³ <https://www.dhs.gov/sites/default/files/2025-03/Office%20of%20Intelligence%20and%20Analysis%20Policy%20Manual-508.pdf>

²⁴ Department of Homeland Security, Office of Intelligence and Analysis, Policy Manual 2025, en tidligere versjon finnes her: <https://primarynewssource.org/wp-content/uploads/Office-of-Intelligence-and-Analysis-Policy-Manual-508.pdf>

4.2.2 Manglende tverrpolitisk representasjon utfordrer FTCs uavhengighet

EU-kommisjonen beskriver i adekvansbeslutningen at en del av The Federal Trade Commission sin uavhengighet, handler om at den består av representanter fra begge de største partiene i USA:

«The FTC may not have more than three Commissioners of the same political party and Commissioners may not, during their appointment, engage in any other business, vocation, or employment.»

FTC består av 5 medlemmer eller kommissærer («commissioners»). I mars 2025 sparket Trump de demokratiske medlemmene av FTC.²⁵ Disse har per mars 2026 ikke blitt erstattet, og FTC består nå utelukkende av to medlemmer fra det republikanske partiet.²⁶

Det er ikke første gang FTC bare har to medlemmer fra det samme partiet. Også under Biden hadde FTC bare to medlemmer i lengre perioder, den gangen demokrater.²⁷ FTC er operative uten å være fulltallige.

Det at tilsynsorganet over lengre perioder kun består av medlemmer fra ett av partiene, og mangler den tverrpolitiske representasjonen det er ment å ha, er imidlertid en svakhet som utfordrer dets uavhengighet.

4.2.3 Privacy and Civil Liberties Oversight Board (PCLOB) er ikke beslutningsdyktig

Et sentralt element i adekvansbeslutningen er at USA har et uavhengig tilsynsorgan, Privacy and Civil Liberties Oversight Board (PCLOB). Dette organet skal føre kontroll med etterretningsprogrammene og sikre at prinsippene om nødvendighet og forholdsmessighet faktisk etterleves.

I januar 2025 ble tre av PCLOBs fire medlemmer avsatt av den nye administrasjonen.²⁸ Ettersom styret må ha minst tre medlemmer for å være beslutningsdyktig, er PCLOB i praksis ikke operativt. Dette svekker PCLOB som uavhengig tilsyn rett og slett fordi organet ikke lenger fungerer.

Selv om amerikanske myndigheter har varslet at nye medlemmer vil bli utnevnt, og EU foreløpig ikke har suspendert DPF, er dagens situasjon en reell svakhet. Uten et velfungerende PCLOB finnes det ingen instans som systematisk kan overvåke amerikanske etterretningspraksiser på vegne av borgerne.

Det norske datatilsynet uttalte seg i februar 2025 at det at PCLOB ikke lenger er vedtaksdyktige, bare er et problem hvis det å få nye styremedlemmer «trekker ut i veldig lang tid».²⁹

Per januar 2026 har ikke PCLOB vært beslutningsdyktig på ett år. Det er ikke gitt noe offisiell informasjon fra EU-kommisjonen om eller når de vil gjøre noe med dette. Men uoffisielle uttalelser kan tyde på at EU-kommisjonen ikke vil handle før PCLOB har vært vedtaksudyktige i minst 18 måneder, det vil si tidligst sommeren 2026.

²⁵ <https://apnews.com/article/trump-ftc-firings-bedoya-slaughter-488bfe5419e48d5acbd95d3f9401404b>

²⁶ <https://www.ftc.gov/about-ftc/commissioners-staff/commissioners>

²⁷ <https://www.ebglaw.com/insights/publications/the-federal-trade-commission-moves-closer-to-a-full-complement-of-commissioners>

²⁸ <https://news.bloomberglaw.com/privacy-and-data-security/trump-terminates-trio-of-democrats-from-privacy-oversight-board>

²⁹ <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/informasjon-om-overforinger-til-usa/>

4.2.4 Alle tilsynsorgan i den amerikanske forvaltningen er direkte underlagt politisk styring fra den amerikanske presidenten

4.2.4.1 *Avskjed av personell fra tilsynsorganer som man tidligere trodde hadde stillingsvern*

I adekvansbeslutningen³⁰ fremhever EU-kommisjonen at the Federal Trade Commission (FTC) er et uavhengig og selvstendig organ. EU-kommisjonen beskrives i adekvansbeslutningen at:

«The FTC is an independent authority composed of five Commissioners, who are appointed by the President with the advice and consent of the Senate.»

Når det kommer til hvordan medlemmer av FTC utpekes, beskriver EU-kommisjonen det slik:

«Commissioners are appointed for a seven-year term and may only be removed by the President for inefficiency, neglect of duty, or malfeasance in office.»

Dette betyr at stillingsvernet som de politisk utvalgte medlemmene av FTC har, er en del av det som gjør FTC til et uavhengig og selvstendig tilsynsorgan. I amerikansk rett, har medlemmer av organer som FTC nytt et særlig stillingsvern lenge.³¹

Dette stillingsvernet har falt bort. I mars 2025 sa Trump opp de to demokratiske medlemmene i FTC.³² Et av medlemmene saksøkte Trump-administrasjonen for ulovlig oppsigelse. Dette fordi det finnes en egen lov som sier at disse medlemmene ikke kan sparkes, understøttet av 91 år med dommer som bekrefter at disse medlemmene har et særlig stillingsvern.

I juni 2026 kom Amerikansk Høyesterett til at dette stillingsvernet ikke eksisterer.³³ Dommen godkjente at den amerikanske presidenten kan sparke medlemmene i FTC. Begrunnelsen for dette er at alle organer i forvaltningen er direkte underlagt presidenten. Presidenten kan derfor sparke medlemmene av alle organer i forvaltningen, også de som har vært selvstendige.

Det er verdt å merke seg at denne høyesterettsdommen setter en lovbestemmelse fra 1914 om at presidenten kan bare avsette kommisjonærene i FTC "for inefficiency, neglect of duty, or malfeasance in office,"³⁴ samt en 91 år gammel Høyesterettsdom³⁵ som stadfester dette stillingsvernet, til side.

Dommen svekker både FTC, Department of Commerce og Department of Transportation sine roller som selvstendig og uavhengig tilsyn med Data Privacy Framework

4.2.4.2 *Det finnes ikke lenger uavhengige tilsynsorganer i amerikansk forvaltning*

Selv om denne dommen gjelder FTC, betyr den at det ikke lenger finnes selvstendige tilsynsorganer i amerikansk offentlig forvaltning. Dette betyr at heller ikke Department of Commerce eller

³⁰ Avsnitt 60

³¹ <https://apnews.com/article/humphreys-executor-supreme-court-trump-independent-agencies-8facfe6107fa94b28f391734d1620fe4>

³² <https://apnews.com/article/trump-ftc-firings-bedoya-slaughter-488bfe5419e48d5acbd95d3f9401404b>

³³ https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf

³⁴ 15 U.S.C. § 41 (<https://www.law.cornell.edu/uscode/text/15/41>)

³⁵ Humphrey's Executor v. United States (<https://tile.loc.gov/storage-services/service/l1/usrep/usrep295/usrep295602/usrep295602.pdf>)

Department of Transportation er selvstendige tilsynsorganer. De er alle underlagt politisk styring fra den amerikanske presidenten.

I personvernsammenheng er dette viktig fordi krav til «uavhengig tilsyn» (Garanti C) forutsetter at tilsynsorganer kan utøve kontroll uten politisk innblanding. I og med at FTC og de andre tilsynsorganene nevnt i adekvansbeslutningen kan instrueres av den amerikanske presidenten, reduseres troverdigheten til tilsynet med amerikanske selskaper.

Det finnes ikke lenger uavhengig tilsynsorgan i den amerikanske forvaltningen. Dette betyr at garanti C ikke er oppfylt.

4.3 GARANTI D – EFFEKTIVE RETTSMIDLER

- **Garanti D:** EU/EØS-borgere må ha tilgang til effektive rettsmidler. Dette betyr at de må kunne få prøvd om deres personvernrettigheter har blitt krenket av myndighetene i tredjelandet sin overvåking. Dette i form av mulighet til å klage saken inn for et tilsynsorgan eller en domstol og eventuelt få kompensasjon eller stanse ulovlig overvåking.

4.3.1 Ordningen er for sårbar

Etter Schrems II opprettet USA en ny klageordning for borgere i EU/EØS, gjennom Civil Liberties Protection Officer (CLPO) og Data Protection Review Court (DPRC). Denne ordningen gjør det mulig for EU-borgere å klage dersom de mener amerikanske myndigheter har behandlet data ulovlig.

DPRC er et klart fremskritt, men uavhengigheten er ikke fullt garantert. Dommerne oppnevnes av justisministeren, og ordningen er etablert gjennom presidentordre, ikke ved lov. Dermed kan en ny administrasjon endre eller svekke ordningen.

I tillegg får klageren ikke innsyn i bevis eller mulighet til å møte, men representeres av en utpekt spesialadvokat («special advocate» på engelsk). Ordningen gir dermed ikke samme grad av rettsikkerhet som europeiske domstoler.

4.3.2 Ingen følger opp PCLOB

Fraværet av et aktivt PCLOB svekker også denne mekanismen. Dette fordi PCLOB skulle kontrollere at DPRC faktisk fungerer uavhengig og følge opp DPRC sine avgjørelser.

4.3.3 Ikke kjent hvordan den jevne borger skal kunne bruke de rettsmidlene de har til rådighet

Som nevnt beskriver adekvansbeslutningen at det er etablert en ny klageordning som EU/EØS-borgere kan bruke for å sjekke om amerikanske etterretningsmyndigheter bryter med deres personvern. Borgerne kan sende klage via sitt lokale datatilsyn.

Det norske datatilsynet har lite tilgjengelig informasjon om klageordningene på sine nettsider.³⁶ Informasjonen beskriver ikke det som adekvansbeslutningen legger opp til: at klager skal gå gjennom nasjonale datatilsyn. Det å vite om at man som EU/EØS-borger har rett og mulighet til å klage på amerikansk etterretning, er en forutsetning for at denne rettigheten skal være reell.

³⁶ Det ligger litt informasjon om den enkeltes rettigheter på en nyhetssak om overføringer fra 2023. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/nye-regler-for-overforing-av-personopplysninger-til-usa/>

Det at det norske datatilsynet ikke har informasjon om at denne typen klager kan rettes til dem, taler for at dette er en rettighet som få vet om, og som derfor vil være vanskelig å oppfylle i praksis. Det tyder på at denne klageordningen kanskje ikke er et så effektivt rettsmiddel som det EU-kommisjonen legger til grunn i adekvansbeslutningen. Det er en klar svakhet.

5 HVA NÅ?

5.1 BLIR DET SCHREMS III?

Etter at denne amerikanske høyesterettsdommen kom sommeren 2026, har Max Schrems sendt et brev til EU-kommisjonen hvor han oppfordrer dem til å trekke tilbake adekvansbeslutningen siden en viktig forutsetning den hviler på nå er borte. I brevet har han også varslet rettslige skritt.³⁷

Det betyr at vi må belage oss på Schrems III. Sagt på en annen måte, det er ganske sannsynlig at adekvansbeslutningen vil falle. Men hvis EU-kommisjonen ikke trekker den tilbake, vil det ta tid. Schrems anslår at det vil ta 2-3 år.³⁸

5.2 HVA KAN DU SOM SKOLEEIER GJØRE?

Så hva kan du gjøre sånn helt konkret? Den kjedelige sannhet er at det ikke finnes et godt eller tilfredsstillende svar på det. Men anbefalingen vår fra den første versjonen av denne veiledningen står seg fortsatt om enn noe justert:

ANBEFALING

Ta et bevisst valg om hvordan du som skoleeier vil forholde deg til at grunnlaget som adekvansvurderingen bygger på har endret seg så mye at den bør bli satt til side.

Vi mener at det ikke lenger er lurt å vente til adekvansbeslutningen faktisk faller, selv om det er et alternativ siden den fortsatt er et gyldig overføringsgrunnlag på papiret. Det er nemlig flere ting du kan gjøre allerede nå for at jobben ikke skal bli så overveldende når den først faller:

1. Få oversikt over hvilke overføringer til USA som faktisk skjer og om de bygger på adekvansbeslutningen som overføringsgrunnlag

Da vet du hva som blir et problem du må jobbe med når adekvansbeslutningen faller.

2. Børst støv av den gamle tredjelandsvurderingen til USA for den må oppdateres

Har du ikke en? Begynn å tenke på hvordan du skal gjøre en. Ta gjerne inspirasjon fra den vi har gjort for Taiwan i Google-prosjektet.³⁹

3. Snakk med leverandørene dine om hvordan de har tenkt å løse dette

Det er ikke sikkert at de har noe godt svar, men ved å begynne samtalen allerede nå, gjør du det enklere for deg selv når adekvansbeslutningen faller.

³⁷ https://noyb.eu/sites/default/files/2026-06/Letter_noyb_EU-US_data_transfers.pdf

³⁸ <https://noyb.eu/en/us-supreme-court-just-blew-eu-us-data-transfers>

³⁹ <https://www.ks.no/fagomrader/digitalisering/skolesec/nasjonal-dpia-for-google/ressurser/tredjelandsvurderinger/>

5.3 DU KAN VELGE Å SE PÅ ALTERNATIVER TIL STORE AMERIKANSKE SKYLEVERANDØRER

Den amerikanske høyesterettsdommen Trump v. Slaughter er et brudd med en nesten 100 år gammel lov, og nesten like mange år med rettspraksis som har bekreftet at ansatte i FTC både har et stillingsvern, og at organet er et selvstendig tilsynsorgan. Det at amerikansk høyesterett har gått bort fra dette, er alvorlig. Det betyr at rettsikkerheten ikke er det vi trodde den var i USA. Det igjen kan gjøre at det er tid for å begynne å se seg om etter alternativer til amerikanske skyleverandører, slik som myndighetene andre steder i Europa allerede har startet med.⁴⁰ Det er dette som har blitt kalt en «Exit-strategi», «digital suverenitet», «digital handlefrihet» eller til og med «leverandøruavhengighet».

Vi tror det arbeidet starter med å i alle fall *begynne* å tenke på hva det betyr å ha leverandører som ikke overfører personopplysninger til USA. Det kan være at både digital suverenitet eller handlefrihet, økonomi (økte lisenskostnader) og personvern (usikkerheten knyttet til overføringsgrunnlaget) nå trekker i retning av at tiden er inne for å i alle fall *starte* å utforske alternativer.

Vi har tre konkrete anbefalinger hvis du ønsker å bli mer leverandøruavhengig:

1. Få en avgjørelse fra ledelsen, hvordan? Tenk langsiktig kostnad

Det å bli mer leverandøruavhengige må være forankret i ledelsen, typisk som en del av en egen sak eller mer langsiktig strategi. For de kommunene som har startet denne prosessen, har den viktigste motivasjonen vært å redusere kostnader over tid (f.eks. økning i lisenskostnader).

2. Bygg intern kompetanse

Det å bli mer leverandøruavhengige, krever en investering i intern kompetanse. Lag en plan og begynn p investere i de folka som dere allerede har.

3. Beskriv leverandøruavhengige løsninger i nye kravspesifikasjoner

En veldig kokret ting som kan gjøres, er å beskrive at de løsningene som skal anskaffes må være kontorstøtteverktøy-uavhengige. Dette betyr å lage kravspesifikasjoner som ikke tillater knytninger. Larvik kommune har brukt denne strategien.

En annen veldig konkret ting du kan gjøre, er å bli en del av DPIA-prosjektet. Vi jobber helt konkret med å få oversikt over de overføringene som skjer i M365. Ta kontakt med KS ved ida.thorsrud@ks.no hvis dette er noe du har tid og lyst til.

En exit-strategi vil ta tid. Poenget er å starte å planlegge for det selv om du ender opp med å ikke ta den i bruk.

⁴⁰ <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/france-phases-out-proprietary-operating-systems-workstations>, <https://cybernews.com/tech/schleswig-holstein-linux/>, <https://www.computerworld.com/article/4219743/swiss-authorities-want-to-replace-microsoft-365-with-open-source-software.html>

