«Det er nå barna går på skolen»

Nettverksmøte personvernombud

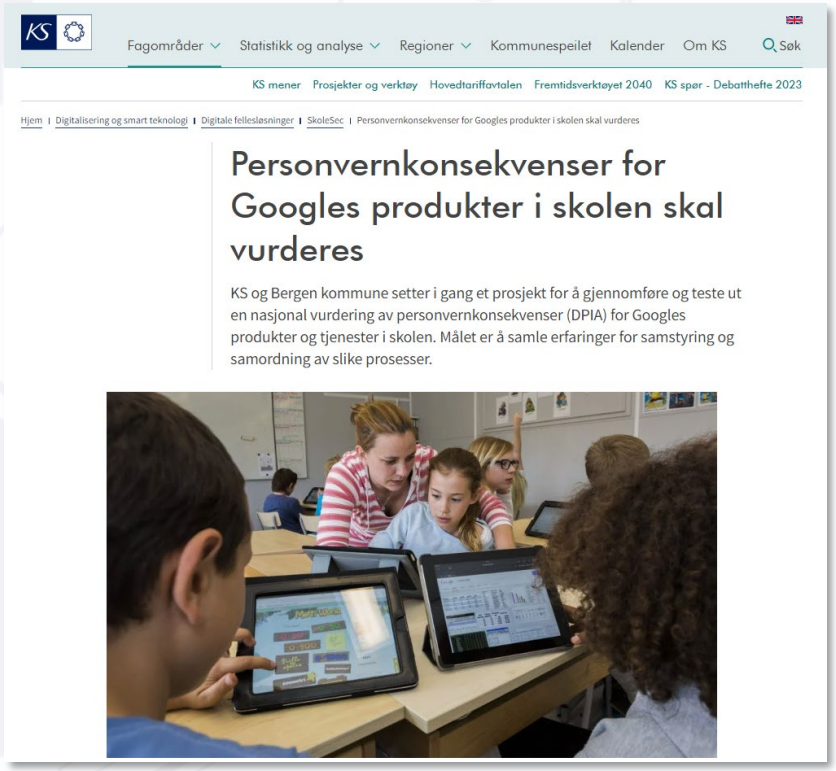
27. november 2023

Scann QR-koden for å lese mer

Nasjonal DPIA for Google

Bakgrunn

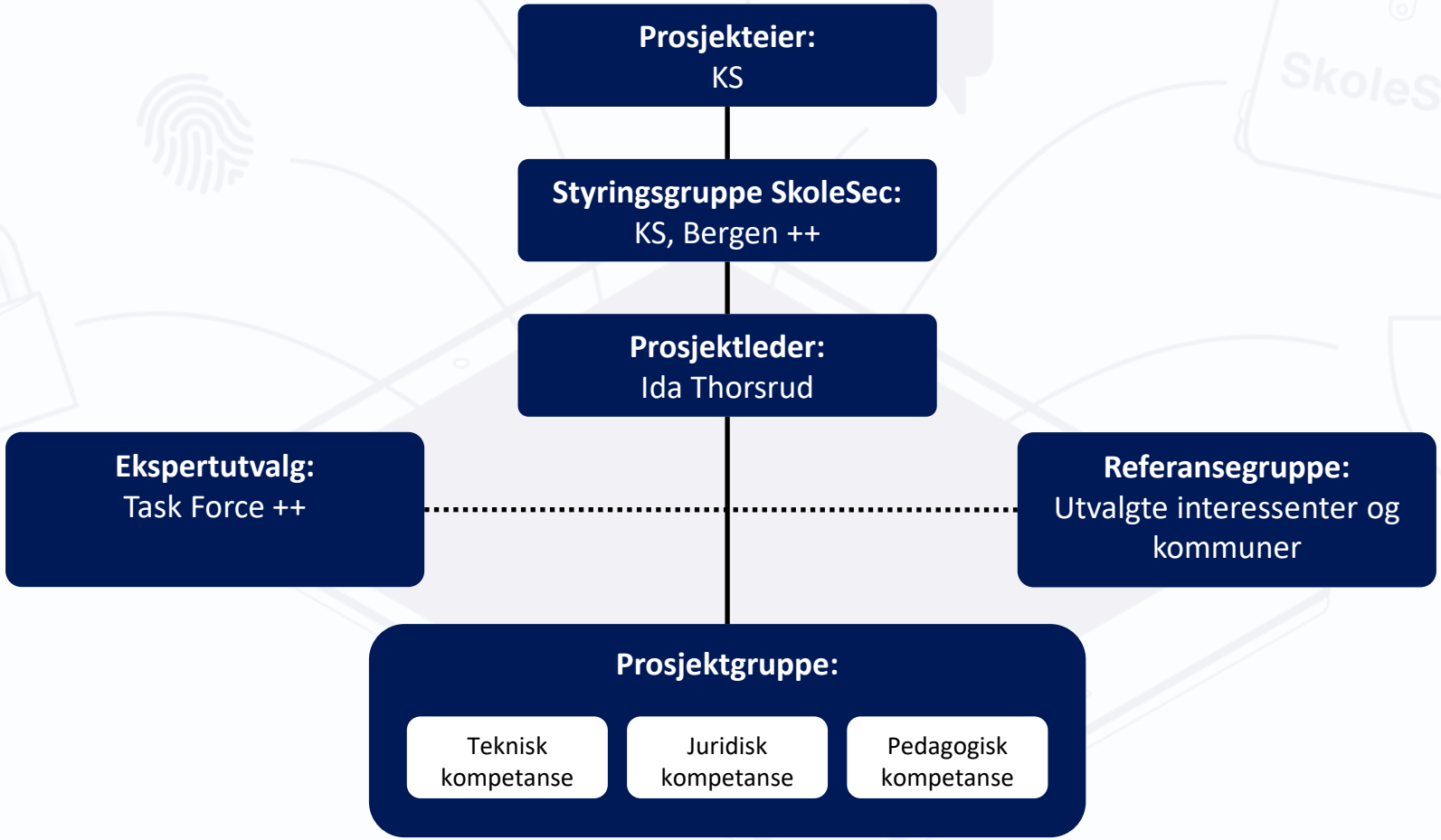
- Microsoft, Apple og Google er de store plattformleverandørene til norsk skole. 21% av elevene i norsk skole har egen Google Chromebook. I tillegg benytter flere skoleeiere Google sine tjenester på andre digitale enheter.
- Bergen kommune har foreslått at KS bidrar til å realisere en nasjonal DPIA for kommunene i Norge.



Overordnet mål

DPIAen skal være en mal for andre, tilsvarende vurderinger kan gjøres på nasjonalt nivå.

Prosjektorganisering



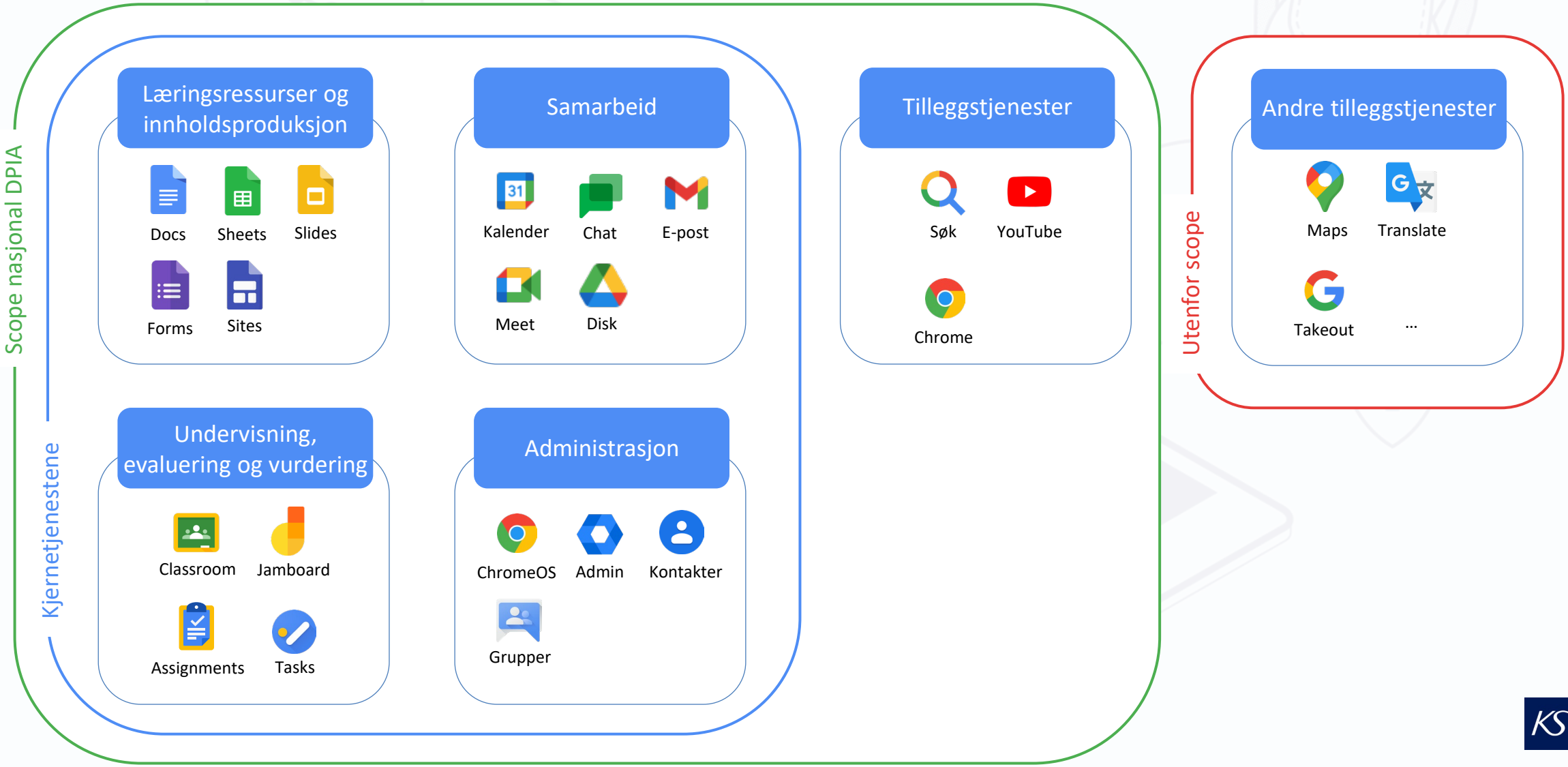
Scann QR-koden for å lese mer

Nasjonal DPIA for Google

Leveranser

Ref.	Hovedprodukt	Beskrivelse
A	Paraply-DPIA for Google sine tjenester	En generell vurdering av personvernkonsekvenser (art. 35 nr. 10) for Google sine tjenester i skolen («paraply»-DPIA). DPIA vil inneholde en vurdering av Google Workspace (kjernetjenester, enkelte tilleggstjenester og Features), Chromebook (hardware), Chrome OS (software), Chrome nettleser (software) og Google søk (online tjeneste).
B	Oversikt over problematiske lover utenfor EU/EØS	Prosjektet vil utarbeide en oversikt over de problematiske personvernlovene til landene utenfor EU/EØS som lagrer eller behandler personopplysninger på vegne av Google.
C	Steg-for-steg-veiviser	En steg-for-steg-veiviser som forklarer skoleeier hvordan en skal lese og forstå paraply-DPIA-en og oversikten over problematiske lover i tredjeland. Veiviseren forklarer også hvilke steg den enkelte skoleeier må gjøre for å vurdere restrisiko knyttet til eget bruksmønster.
D	Veiledning	En enkel veiledertjeneste som vil bistå skoleeier i å ta i bruk paraply-DPIA-en, oversikten over problematiske lover i tredjeland og steg-for-steg-veiviseren.
E	Evaluering/utredning av prosess for felles vurderinger	Erfaringene fra piloten dokumenteres og evalueres, da dette vil ha betraktelig overføringsverdi til en eventuell ny modell for samordning av slike prosesser og etablering av et sentralt støttesenter/forvaltningsorgan.

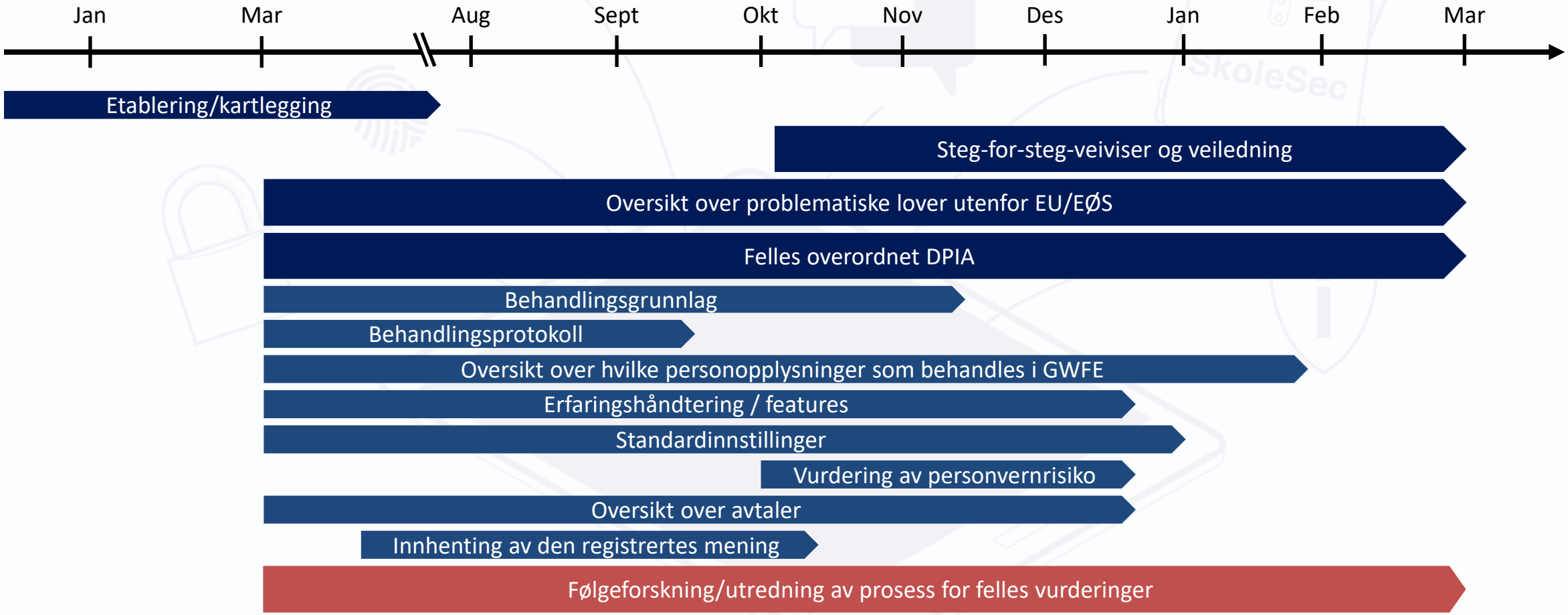
Google Workspace for Education?



Scann QR-koden for å lese mer

Nasjonal DPIA for Google

Prosjektplan



Leveranse A

Pilot for paraply-DPIA for Google sine tjenester

Felles overordnet DPIA

For bruk av Google Workspace for Education i skolen

GDPR artikkel 35

- Behandlingsgrunnlag
- Vurdering av personvernrisiko
- Beskrivelse av behandlingsaktiviteter
- Innhenting av den registrertes mening
- Standardinnstillinger
- Oversikt over avtaler

Leveranse B

Oversikt over problematiske lover utenfor EU/EØS

Her ønsker vi rådgivning fra Datatilsynet

Overføringer til tredjeland

Singapore, Taiwan og Chile (Fundamentals) og USA (øvrige lisenser)

GDPR kapittel V

Veiledning til adekvansvurderingen

- Bruk rammeverket som overføringsgrunnlag
- Forstå hva endringene i DPF er og forstå risiko for ny overprøving
- Vit hva du må gjøre hvis DPF blir ugyldiggjort

TIA / Helhetsvurderinger av tredjeland

- Singapore
- Taiwan
- Chile

Utfordringer

- Deling av dokumenter
- Vanskelige vurderinger
- Anbefaling om lisens / versjon

Leveranse C og D

Steg-for-steg veiviser og veiledning

Veiledning

Hva trenger kommunene for å gjøre DPIAen til sin egen? Og hvilke andre personvernspørsmål har de?

Behandlingsprotokoll

Behandlingsgrunnlag

Endringshåndtering

Prosess for tilpasning av DPIA

Avtalevilkår med Google

Retten til å protestere

Problemstillinger

Ting vi må ta stilling til i prosjektet

Her har vi fått rådgivning fra Datatilsynet

Det «primære» behandlingsgrunnlag

Alle er enige om kommunene har et supplerende behandlingsgrunnlag, men vi krangler om c) eller e)

GDPR artikkel 6

Vi skal ikke velge for dem

Utkast med begge begrunnelsene

Anbefalingen vår i veiledningen

Problemstillinger

Ting vi må ta stilling til i prosjektet

Retten til å protestere

Kommunene skjønner ikke hvordan denne skal oppfylles – vi vil lage en veiledning

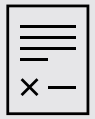
GDPR artikkel 21

Protest vs. klage vs. sletting?

«Tvingende berettigede grunner»

Brukerhistorier og eksempler

Steg for steg veiviser



Maler for hvordan svare

Juridisk artikkel

Problemstillinger

Ting vi må ta stilling til i prosjektet

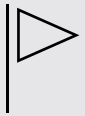
Her har vi fått rådgivning fra Datatilsynet

Behandlingsansvar og Googles behandling av personopplysninger til egne formål

Når er kommunen behandlingsansvarlig alene? Er den noen gang felles behandlingsansvarlig med Google?

GDPR artikkel 24, 26 og 28

Databehandler for kjernetjenestene



Med unntak av «service data»

Ikke felles behandlingsansvar?

Uklart ansvarsfordeling

Uklar begrunnelse

Problemet med tilleggstjenestene

Metode DPIA

	Risiko	Forklaring	Eksempel
🟢	Lav	Det er ikke et brudd på eller stor fare for at et prinsipp, en rettighet eller frihet blir brutt.	Behandlingen er basert på samtykke som lovlig grunnlag, men informasjonen gitt i forbindelse med samtykket har noe uklart språk, men det er mulig å forstå hva behandlingen innebærer. Det kan være noen registrerte misforstår behandlingen, men det utgjør ikke en stor risiko for brudd på informasjonsplikten eller for at samtykke ikke er gyldig inngått.
🟡	Middels	Det er en fare for at et prinsipp, en rettighet eller en frihet blir brutt eller ikke alltid overholdes.	Det kan være brudd på dataminimering dersom man har et fritekstfelt uten en hjelpetekst. Det vil da være sannsynlig at enkelte bruker fritekstfeltet til å avgi flere personopplysninger enn nødvendig.
🔴	Høy	Det er tydelig at det kan forekomme brudd på et prinsipp, en rettighet eller en frihet.	Man bruker et eldre skoleadministrativt system for behandlingen av personopplysninger hvor sletting ikke er mulig.

Eksempel risikoscenario – arbeidsversjon

«Risikotrigger» *Kan f.eks. være den enkelte behandlingsaktiviteten*	**Risikoscenario** *Beskrivelse av risiko - hva gjør at vi har å gjøre med en potensiell personvernkonsekvens?*	**Beskrivelse av personvernkonsekvenser** *Hvilke personvernkonsekvenser innebærer scenarioet?*	**Risikonivå** *Lav – Middels – Høy* 🟢 🟡 🔴	**Begrunnelse** *Redegjør for hvorfor vi har valgt risikonivået*
Endringer i Google Workspace for Education (GWFE).	Det kommer endringer I GWFE som skoleeier ikke får med seg. De aller fleste endringer handler om brukergrensesnitt. Noen av endringene får bivirkninger som er vanskelig å forutse, f.eks. at en endring innebærer at man skrur på en tilleggstjeneste som skoleeier ikke har en avtale med. Dette påvirker innstillingene og hvordan man har satt opp løsningen, noe kommunen må ha kontroll på. I enkelte og mer sjeldne tilfeller vil endringene utløse behov for nye vurderinger fordi man må ta stilling til om de også innebærer at skoleeier nå behandler nye personopplysninger som de f.eks. ikke har behandlingsgrunnlag for.	Utilsiktet bruk og økning av bruk av personopplysninger - du kan komme til å ta i bruk tjenester som ikke er dekket av databehandleravtalen din. Det kan gjøre at du ikke lever opp til alle krav i ansvarlighetsprinsippet (GDPR artikkel 5 nr. 2) om at du skal kunne demonstrere etterlevelse / ha kontroll på den behandlingen av personopplysninger du gjør. I mer sjeldne tilfeller kan konsekvensene bli at behandlingen er ikke hjemlet og det er derfor uklart om den er lovlig (har ikke behandlingsgrunnlag) og at man ikke har et formål med behandlingen. Dette vil også føre til at den registrertes tillit til behandlingsansvarlig reduseres.	Middels	Det kommer ofte endringer i GWFE, men de er ofte av mindre karakter. Dette betyr at det skal litt til for at en endring gjør at kommunen behandler personopplysninger ulovlig fordi man ikke har et behandlingsgrunnlag og derfor må gjøre nye interne vurderinger, endre DPIA, oppdatere behandlingsprotokoll etc.

Hvordan sikrer vi at det vi lager faktisk treffer kommunene?

Medlemmer i prosjektgruppen

Nyhetsbrev og LinkedIn Live

Publisering fortløpende

Rådgivning med Datatilsynet

Erfaringsdeling med andre

Behandlingsprotokoll for kjernetjenestene

Publisert utkast til behandlingsprotokoll

LinkedIn Live-presentasjon (se den her)

Hvordan fange opp endringer i GWFE?

Publisert veileder på endringshåndtering

LinkedIn Live 06.11 kl. 12.00-13.00 (se den her)

Hvilket primære behandlingsgrunnlag skal du bruke?

Utkast til begrunnelse for behandlingsgrunnlagene

LinkedIn Live 28.11 kl. 12.00-13.00

Hva er risikoen for at overføringsgrunnlaget til USA blir overprøvd?

LinkedIn Live 07.12 kl. 12.00-13.00

Vil du følge med på hva vi gjør i nasjonal DPIA-prosjektet fremover?

Meld deg på nyhetsbrevet vårt her!