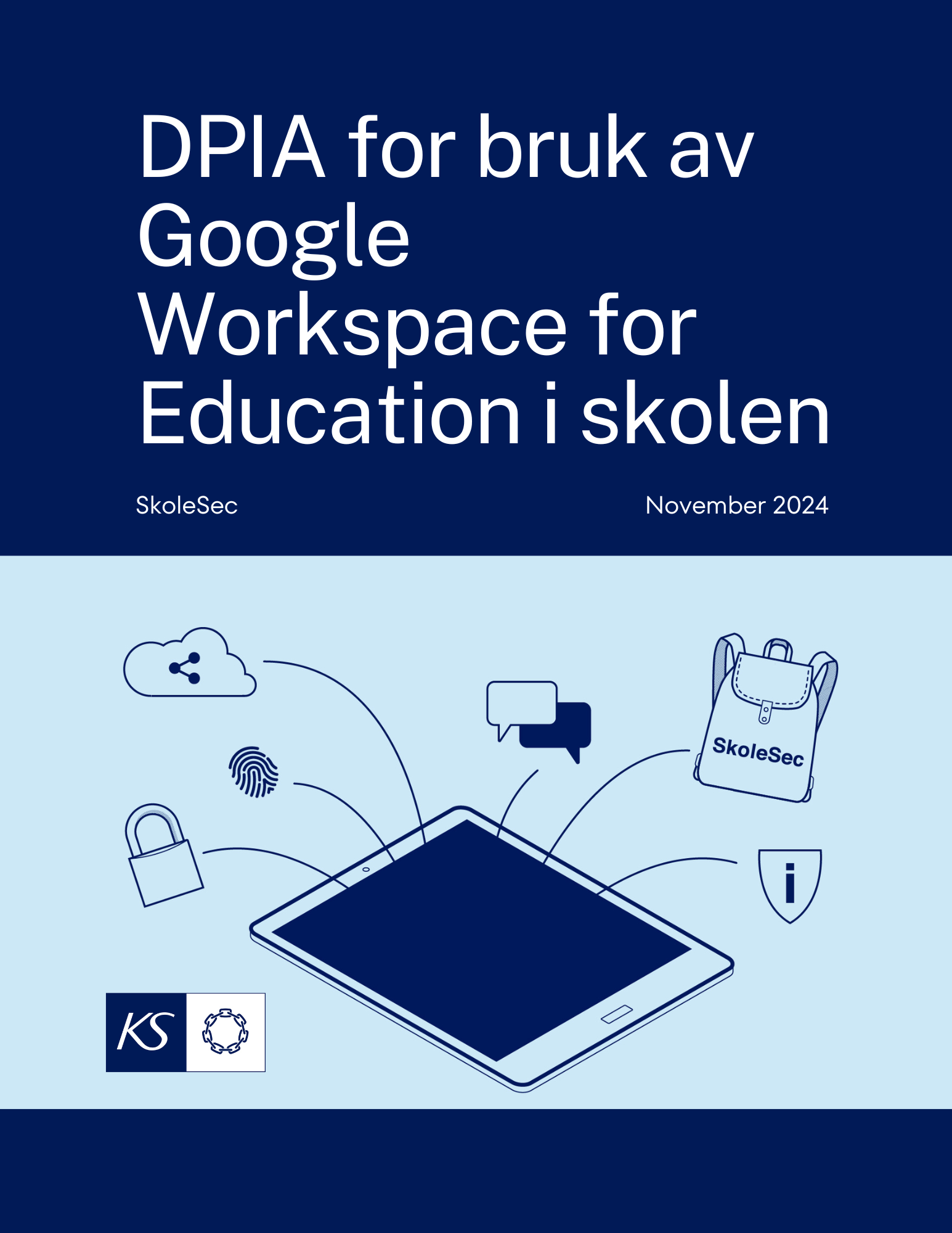
****

|  |  |  |  |
| --- | --- | --- | --- |
| Versjonslogg | | | |
| Versjon | Dato | Endring | Forfatter |
| 1.0 | November 2024 |  | KS, SkoleSec ved Ida Thorsrud |
|  |  |  |  |

Innholdsfortegnelse

[Hvilke tjenester i Google Workspace for Education bør brukes? 4](#_Toc185244647)

[Oversikt over tjenestene som vurderes 6](#_Toc185244648)

[Kort beskrivelse av Google Workspace for Education 6](#_Toc185244649)

[Roller og ansvar 7](#_Toc185244650)

[Utgangspunktet for hvem som er behandlingsansvarlig og hvem som er databehandler 7](#_Toc185244651)

[Behandlingsgrunnlaget til skoleeier legger føringer for hvilke digitale tjenester som kan tas i bruk i skolen 8](#_Toc185244652)

[Om Google er behandlingsansvarlig avhenger av hvilke personopplysninger det er snakk om, hvilke tjenester som brukes og hvordan 8](#_Toc185244653)

[Behandlingsaktiviteter, personopplysninger og behandlingsgrunnlag for den enkelte behandlingen 10](#_Toc185244654)

[Skoleeiers behandling av personopplysninger 10](#_Toc185244655)

[Kategorisering av personopplysninger som skoleeier behandler i Google Workspace for Education 10](#_Toc185244656)

[Behandlingsaktiviteter 11](#_Toc185244657)

[Googles behandling av personopplysninger 11](#_Toc185244658)

[Customer personal data 11](#_Toc185244659)

[Service data 11](#_Toc185244660)

[Skoleeiers formål for bruk av personopplysninger i Google Workspace for Education 12](#_Toc185244661)

[1. Fremme læring og kunne utøve tilpasset opplæring og variert undervisning 12](#_Toc185244662)

[2. Oppfylle skolens aktivitetsplikt for å følge opp skolemiljøsaker 13](#_Toc185244663)

[3. Beskytte tjenesten, avdekke misbruk og ulovlig aktivitet 13](#_Toc185244664)

[4. Oppfylle krav til lovpålagt utlevering av personopplysninger 13](#_Toc185244665)

[Personvernprinsippene 15](#_Toc185244666)

[Er kravet til lovlighet, rettferdighet og åpenhet ivaretatt? 15](#_Toc185244667)

[Er kravet til formålsbegrensning oppfylt? 16](#_Toc185244668)

[Er kravet til dataminimering ivaretatt? 17](#_Toc185244669)

[Er kravet til riktigheten av opplysningene ivaretatt? 18](#_Toc185244670)

[Er kravet til lagringsbegrensning ivaretatt? 18](#_Toc185244671)

[Er kravet til integritet og konfidensialitet ivaretatt? 18](#_Toc185244672)

[De registrertes rettigheter og friheter 19](#_Toc185244673)

[Hvordan ivaretas de registrertes rett til informasjon? 19](#_Toc185244674)

[Hvordan ivaretas de registrertes rett til innsyn? 19](#_Toc185244675)

[Hvordan ivaretas de registrertes rett til retting? 20](#_Toc185244676)

[Hvordan ivaretas de registrertes rett til sletting? 20](#_Toc185244677)

[Hvordan ivaretas de registrertes rett til å protestere? 20](#_Toc185244678)

[Hvordan ivaretas de registrertes rett til begrensing? 21](#_Toc185244679)

[Hvordan ivaretas de registrertes rett til dataportabilitet? 21](#_Toc185244680)

[Hvordan ivaretas de registrertes rett til å ikke være gjenstand for automatiserte avgjørelser? 21](#_Toc185244681)

[Oppsummering av nødvendig og forholdsmessig 21](#_Toc185244682)

[Kvalitativ metode 22](#_Toc185244683)

[De registrertes synspunkter 23](#_Toc185244684)

[Oppsummering av de registrertes synspunkter og anbefalinger 23](#_Toc185244685)

[Anbefaling fra personvernombudet 23](#_Toc185244686)

[Beslutning av leder med ansvar for personvern 24](#_Toc185244687)

[Beskrivelse av hva ledelsens har lagt vek på i sin beslutning: 24](#_Toc185244688)

[Vedlegg 1: Begrunnelse for anbefalte tjenester 25](#_Toc185244689)

[Vedlegg 2: Vurdering av om Googles behandling av personopplysninger til egne formål er kompatibelt med skoleeiers opprinnelige formål i opplæringsloven 29](#_Toc185244694)

[Vedlegg 3: Oversikt over avtaler som regulerer Google Workspace for Education, ChromeOS og Chrome nettleser 32](#_Toc185244695)

[Vedlegg 4: Illustrasjon av anbefalingene 34](#_Toc185244700)

Anbefalinger i DPIAen

# Hvilke tjenester i Google Workspace for Education bør brukes?

Når det gjelder bruk av Google Workspace for Education, er vår vurdering at norske skoleeiere kan fortsette å bruke følgende tjenester:

1. Google Workspace for Education (kjernetjenester og AppSheet) når skoleeier har godtatt tilleggsavtalen «Service Data Addendum» [[1]](#footnote-2)
2. Chrome nettleser når skoleeier har skrudd på «Data Processor Mode» (DPM)[[2]](#footnote-3) og bruker dette på en administrert Chromebook[[3]](#footnote-4)
3. «Essential Services»[[4]](#footnote-5) i ChromeOS når skoleeier har skrudd på «Data Processor Mode» (DPM)[[5]](#footnote-6) og bruker dette på en administrert Chromebook[[6]](#footnote-7)

DPIA-prosjektet anbefaler skoleeier å ikke bruker følgende Google-tjenester:

1. Tilleggstjenestene i Google Workspace for Education[[7]](#footnote-8)
2. Chrome nettleser når Data Processor Mode ikke er skrudd på[[8]](#footnote-9)
3. Chrome nettleser når det brukes på en ikke-administrert Chromebook
4. «Optional services» i ChromeOS[[9]](#footnote-10)

Se vedlegg 1 for begrunnelse til anbefalte tjenester. Se vedlegg 4 for en illustrasjon av anbefalingene.

|  |
| --- |
| Kommunen er skoleeier og behandlingsansvarlig for hvordan elever, lærere og andre ansattes personopplysninger behandles. I denne DPIAen kommer vi med flere anbefalinger som behandlingsansvarlig kan velge å følge eller ikke.  Anbefalingen om tilleggstjenestene som beskrevet ovenfor, er en av dem. Dersom behandlingsansvarlig velger å fortsatt bruke tilleggstjenestene, har vi skrevet en artikkel om tiltak skoleeier bør vurdere å iverksette.[[10]](#footnote-11) |

Del 1 Systematisk beskrivelse av behandlingsaktiviteter

# Oversikt over tjenestene som vurderes[[11]](#footnote-12)

Denne DPIAen omfatter behandling av personopplysninger i følgende Google-tjenester:

* Kjernetjenestene i Google Workspace for Education
* Tilleggstjenestene Google Søk og Assistent og YouTube
* Chrome nettleser når nettleseren brukes med en Google Workspace for Education-konto
* ChromeOS (operativsystemet på en Chromebook)

Et bilde som inneholder tekst, skjermbilde, diagram

Automatisk generert beskrivelse

Figur 1 Oversikt over tjenestene som vurderes i denne DPIAen

## Kort beskrivelse av Google Workspace for Education

Google er et kommersielt selskap som først og fremst er kjent for søkemotoren «Google», og en rekke tjenester som er rettet mot forbrukere.[[12]](#footnote-13) Google har også utviklet og tilpasset noen av disse tjenestene for utdanningssektoren i en kontorpakke kalt «Google Workspace for Education». Selv om noen av disse tjenestene har samme navn som tjenester som finnes på forbrukermarkedet, er tjenestene som er en del av «Google Workspace for Education» forskjellig fra Googles forbrukertjenester.

Google Workspace for Education er en skybasert plattform (SaaS)[[13]](#footnote-14) fra Google Cloud som tilbyr en rekke verktøy og tjenester for utdanningsinstitusjoner. Google Workspace for Education retter seg mot skoleeiere og har en forretningsmodell som er forskjellig fra de forbrukertjenestene Google er kjent for. Dette beskrives nærmere under overskriften Roller og ansvar nedenfor.

Google Workspace for Education består av «kjernetjenester» og en tjenester som kategoriseres som «andre tjenester» (AppSheet). [[14]](#footnote-15) Skoleeiere kan som kunder også legge andre Google-tjenester til i Google Workspace for Education, ofte kalt «tilleggstjenester».[[15]](#footnote-16)

* + - * 1. Kjernetjenester

Kjernetjenestene er de tjenestene som er «grunnpakka» til Google Workspace for Education. Det er tjenester som alle har tilgang til. Kommunen kan velge hvilke av disse tjenestene som elever og lærere skal ha tilgang til.[[16]](#footnote-17)

I utgangspunktet er kommunen behandlingsansvarlig for behandlingen av personopplysninger[[17]](#footnote-18) som skjer i Google Workspace for Education, mens Google er databehandler.[[18]](#footnote-19)

* + - * 1. Andre tjenester

Blant tjenestene i Google Workspace for Education er tjenesten «AppSheet» ikke definert som en kjernetjeneste, men som «other services».[[19]](#footnote-20) Dette er en web-basert plattform.

* + - * 1. Tilleggstjenester

Tilleggstjenester, er tjenester som kommunen selv må skru på. De kan koste ekstra og kommunen må ta et aktivt valg om å bruke dem før de kan tas i bruk. De er også tilpasset utdanningssektoren, men Google, i tillegg til skoleeier, er behandlingsansvarlig for den behandling av personopplysninger som skjer i tilleggstjenestene.

YouTube og Google Søk og Assistent Google er de to tilleggstjenestene som vi har vurdert i denne DPIAen, men Google er behandlingsansvarlig for alle tilleggstjenestene. Anbefalingene våre om disse tilleggstjenestene kan derfor brukes på øvrige tilleggstjenester.

* + - * 1. Chrome-tjenester

Denne DPIAen tar også for seg er nettleseren Chrome og ChromeOS som er operativsystemet på en Chromebook. Disse produktene er ikke en del av Google Workspace for Education, men de passer bra sammen med de øvrige Google-tjenestene. Dette er tjenester vi har kalt «Chrome-tjenester», og Google er i utgangspunktet behandlingsansvarlig for behandlingen av personopplysninger som skjer nettleseren Chrome og ChromeOS.[[20]](#footnote-21)

# Roller og ansvar

## Utgangspunktet for hvem som er behandlingsansvarlig og hvem som er databehandler

Det er skoleeier[[21]](#footnote-22) som er behandlingsansvarlig når elevers personopplysninger behandles i skolen. Dette betyr at det er skoleeier som har ansvaret for at elevers personvern og de rettighetene som fremgår av personvernforordningen ivaretas.[[22]](#footnote-23) En behandlingsansvarlig er også den som bestemmer hvorfor personopplysningene behandles (formålet med behandlingen) og hvordan gjennom å velge de digitale verktøyene som skal brukes for å oppnå formålet.

Den leverandøren som leverer digitale tjenester til skoleeier, er i utgangspunktet databehandler. En databehandler er den som behandler personopplysninger *på vegne av* en behandlingsansvarlig. Dette innebærer at databehandler ikke kan bruke personopplysningene til andre formål enn det som behandlingsansvarlig har instruert om. Denne instruksen kalles en «databehandleravtale».

## Behandlingsgrunnlaget til skoleeier legger føringer for hvilke digitale tjenester som kan tas i bruk i skolen

Skoleeier som behandlingsansvarlig må ha hjemmel i lov (et behandlingsgrunnlag) for å kunne behandle elevers personopplysninger. Behandlingsgrunnlaget setter rammer for hva skoleeier kan gjøre med elevers personopplysninger. For eksempel kan ikke skoleeier behandle elevers personopplysninger til andre formål enn de som fremgår av opplæringsloven.

Dette setter begrensninger for tjenester skoleeier kan kjøpe av Google når Google er behandlingsansvarlig.

For norske skoleeiere er det primære behandlingsgrunnlaget GDPR artikkel 6(1) bokstav e),[[23]](#footnote-24) mens de ulike bestemmelsene i opplæringsloven er det supplerende behandlingsgrunnlaget.[[24]](#footnote-25)

## Om Google er behandlingsansvarlig avhenger av hvilke personopplysninger det er snakk om, hvilke tjenester som brukes og hvordan

Spørsmålet om når Google er behandlingsansvarlig og når de er databehandler, må besvares både ut ifra hvilke personopplysninger det er snakk om («Customer personal data»[[25]](#footnote-26) eller «Service data»[[26]](#footnote-27)), hvilke tjenester som brukes[[27]](#footnote-28) og også på hvilken type operativsystem man bruker tjenestene på.[[28]](#footnote-29)

«Customer personal data» (også kalt «kundedata») er all informasjon som lastes opp, lagres, sendes eller mottas i Google-tjenestene. Dette er f.eks. teksten i oppgaven en elev leverer inn til læreren, den skriftlige tilbakemeldingen som eleven får fra læreren, eller meldinger som elevene sender til hverandre via Chat. Forenklet kan vi si at dette er «innholdsdata», dette i motsetning til «metadata».

«Service data» (også kalt tjenestedata) er informasjon som Google samler inn eller som genereres som en del av bruk, levering og administrering av tjenesten. Litt upresist kan vi si at dette er metadata. Dette er upresist fordi «service data» slik det er definert i brukervilkårene til Google, også inkluderer opplysninger som ikke er metadata, f.eks. informasjon som nødvendig ifbm fakturering eller brukeroppfølging (support tickets).

Metadata kalles gjerne også diagnostiske data. Dette er data som viser hvordan en elev eller lærer bruker Google Workspace for Education. Disse dataene er indirekte identifiserbare personopplysninger. Det betyr at dette er personopplysninger, siden det er mulig for Google å identifisere enkeltindivider. Dog er ikke formålet å identifisere den enkelte eleven eller læreren som bruker Google Workspace for Education. Formålet er å få informasjon om hvordan brukermassen generelt bruker tjenestene.

Dette betyr at skoleeier må se på den enkelte avtalen som regulerer den konkrete tjenester man kjøper for å kunne vurdere roller og ansvar, altså når skoleeier er behandlingsansvarlig alene, når Google er databehandler og når Google også er behandlingsansvarlig.

Kort oppsummert kan roller og ansvar for Google Workspace for Education oppsummeres i tabellen nedenfor. Merk at vi har markert de det i rødt der Google har en rolle som ikke er i tråd med skoleeiers ansvar og rammene i opplæringsloven.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tjeneste** | **Behandlingsansvarlig** | | **Databehandler** | |
| *Customer personal data* | *Service Data* | *Customer personal data* | *Service Data* |
| Google Workspace for Education kjernetjenester *uten* Service Data Addendum | Skoleeier | Google[[29]](#footnote-30) | Google | N/A |
| Google Workspace for Education kjernetjenester *med* Service Data Addendum | Skoleeier | Skoleeier  Google (for the purposes set out in the Supplemental Google Cloud Privacy Notice)[[30]](#footnote-31) | Google | Google |
| YouTube (Google Workspace for Education tilleggstjeneste) | Google | Google | N/A | N/A |
| Google Søk og Assistent (Google Workspace for Education tilleggstjeneste) | Google | Google | N/A | N/A |
| ChromeOS og Chrome nettleser med Data Processor Mode på managed Chromebook (ChromeOS essential services) | Skoleeier | Skoleeier  Google (for «legitimate business purposes»)[[31]](#footnote-32) | Google | Google |
| ChromeOS og Chrome nettleser med Data Processor Mode på managed Chromebook (ChromeOS optional services) | Skoleeier  Google | Google | Google | N/A |
| ChromeOS og Chrome nettleser uten Data Processor Mode på managed Chromebook (ChromeOS) | Skoleeier  Google | Google | Google | N/A |

Tabell 1 Oversikt over behandlingsansvar og databehandleransvar[[32]](#footnote-33)

# Behandlingsaktiviteter, personopplysninger og behandlingsgrunnlag for den enkelte behandlingen

## Skoleeiers behandling av personopplysninger[[33]](#footnote-34)

I denne DPIAen har vi tatt utgangspunkt i hva, hvorfor og hvordan skoleeier behandler personopplysningene til elever og lærere, med hovedfokus på elever. Vi har laget en systematisk beskrivelse av behandlingsaktivitetene som foregår i skolen. Det betyr at vi har fokusert på selve aktivitetene, altså på hvordan personopplysningene behandles, og mindre på det systemet som brukes (her Google Workspace for Education). Imidlertid har systemets funksjonalitet også satt rammer for hvordan personopplysningene faktisk behandles.

Se forslaget til behandlingsprotokoll for Google Workspace for Education som legges ved denne DPIAen som et Excel-ark for en oversikt over hvilke personopplysninger som skoleeier behandler når Google Workspace for Education tas i bruk i skolen, og hva som er behandlingsgrunnlaget for den enkelte behandlingen.

### Kategorisering av personopplysninger som skoleeier behandler i Google Workspace for Education

* Identifiserende opplysninger: navn, e-postadresse, bilde, brukernavn, telefonnummer, adresse.
* Demografiske opplysninger: skole, klasse.
* Internettkommunikasjonsopplysninger: MAC-adresse, IP-adresse, informasjonskapsler (cookies), lokasjon.
* Aktiviteter: adferdsmønster, tider innlogget/utlogget, tidspunkt for levering, tidspunkt for arbeid med dokumenter, tidspunkt for chat med venner.
* Fritekst: løpende tekst, besvarelser, kommunikasjonsinnhold, særlige kategorier av personopplysninger.
  + - * 1. Behandling av særlig kategori av personopplysninger (fritekst)

I denne DPIAen har vi valgt å tydeliggjøre at det i skolen gjennom undervisning og aktiviteter i klasserommet skjer behandling av det som potensielt kan være særlig kategori av personopplysninger slik de er definert i GDPR artikkel nr. 9.[[34]](#footnote-35)

Særlige kategorier er tatt med i kategorien vi har valgt å kalle *fritekst*. Dette for å presisere at særlig kategori personopplysninger ikke behandles av skoleeier med formål om å behandle disse opplysningene i seg selv. Google Workspace for Education inneholder flere muligheter til å skrive fritekst, både når elever skriver og leverer oppgaver, og i kommunikasjon elev-elev og elev-lærer. I slike fritekstfelter og i denne typen kommunikasjonskanaler, vil den enkelte skrive opplysninger om seg selv og andre som er særlig kategori personopplysninger.

### Behandlingsaktiviteter

Vi har valgt å dele behandlingsprotokollen inn i ulike «kategorier» (grupperinger): pedagogisk, skoleadministrativt og IT-teknisk. Disse grupperingene gir en pekepinn på at behandlingsaktivitetene kan ha ulike formål og behandlingsgrunnlag.

Alle aktivitetene utgjør samlet skoleeiers behandlingsaktiviteter og tydeliggjør skoleeiers ansvar og hva som er leverandørens ansvar og handlingsrom for behandling av personopplysningene.

* + - * 1. Pedagogiske aktiviteter

Under pedagogiske aktiviteter dekkes aktiviteter som utdeling og innlevering av oppgaver, samskriving i dokument, kommunikasjon mellom lærer og elev og eksamen. Disse aktivitetene gjøres med «formål om å fremme læring og utøve tilpasset opplæring og variert undervisning». Behandlingsgrunnlaget er primært GDPR artikkel 6(1) bokstav e), jf. opplæringsloven § 25-1 (behandle personopplysninger til nødvendige formål), jf. §11-1 (tilpasset opplæring) og § 2-3 fjerde avsnitt (undervisning skal gis i tråd med læreplanen og legge til rette for en aktiv elev).

* + - * 1. Skoleadministrative aktiviteter

Skoleadministrative aktiviteter omfatter oppgaver som er relevante for skoleadministrasjonen. Det gjelder aktiviteter som avvikling av eksamen, undersøke skolemiljø-sak og hente ut data. Formålene og behandlingsgrunnlaget er litt ulikt avhengig av aktiviteten, men det handler om å følge opp uønskede hendelser, sikre datakvalitet og sikre et godt skolemiljø.

* + - * 1. IT-tekniske aktiviteter

Disse aktivitetene sikrer og følger opp bruken av tjenestene, administrerer verktøy og klienter, og gir tilganger og begrensninger for elever og ansatte. Også her kan formålet variere, men kan overordnet sies å være å sikre elever og ansattes bruk av tjenestene og tilby support og støtte. Derfor vil behandlingsgrunnlaget ofte være en rettslig forpliktelse (GDPR artikkel 6 nr. 1 bokstav c) hjemlet i GDPR artikkel 32(1) og eForvaltningsforskriften §15(2) (plikt til å ha egnede tiltak for å oppnå et godt sikkerhetsnivå).

## Googles behandling av personopplysninger

### Customer personal data

Når skoleeier bruker kjernetjenestene i Google Workspace for Education eller Chrome-tjenester med Data Processor Mode på en administrert Chromebook, er det skoleeier som alene er behandlingsansvarlig for «Customer personal data».[[35]](#footnote-36) Dette betyr at Google behandler disse personopplysningene på instruks fra skoleeier.

«Customer personal data» er all informasjon som lastes opp, lagres, sendes eller mottas i Google-tjenestene, som kan knyttes til en enkeltperson. Dette er f.eks. teksten i oppgaven en elev leverer inn til læreren, den skriftlige tilbakemeldingen som eleven får fra læreren, eller meldinger som elevene sender til hverandre via Chat. Dette er med andre ord personopplysninger. Forenklet kan vi si at dette er «innholdsdata», dette i motsetning til «metadata».[[36]](#footnote-37)

### Service data

«Service data» (også kalt tjenestedata) er personopplysninger som Google bruker til egne formål. Google er med andre ord behandlingsansvarlig for denne typen personopplysninger. Dette er:[[37]](#footnote-38)

* **Kontoopplysninger**: Opplysninger skoleeier må legge inn for å opprette brukerkontoer for bruker av Google Workspace for Education. For elever, lærer og ansatte i norsk skole, vil dette være personopplysningene brukernavn, navn, kontaktinformasjon (e-postadresse og evt mobilnummer) og evt stillingstitler.
* **Betalinger og transaksjoner i skyen**: Google lagrer informasjon om gebyrer, betalinger og faktureringsdetaljer. I denne DPIAen har vi ikke identifisert situasjoner hvor enkeltbrukere som har en skolekonto i Google Workspace for Education vil kunne foreta slike betalinger. Vi har derfor lagt til grunn at når denne kategorien tjenestedata inneholder personopplysninger, vil det være kontaktinformasjon til ansatte i kommunen som har ansvaret for fakturering eller står som kundekontakt.
* **Innstillinger og konfigurasjoner**: Google behandler opplysninger om innstillinger og konfigurasjoner for Google Workspace for Education. Dette er f.eks. de sikkerhetsinnstillingene som kommunen har skrudd på. Personopplysningene som behandles i denne forbindelse er først og fremst informasjon om hvilken administratorbruker som har gjort endringer i innstillingene.
* **Brukerens direkte kommunikasjon med Google via GWFE**: Hvis eleven, læreren eller den kommunalt ansatte som har en bruker i Google Workspace for Education sender henvendelser om teknisk støtte til Google via løsningen, tar Google var på denne korrespondansen. Dette er tilbakemeldinger direkte fra brukeren om f.eks. brukeropplevelsen eller forespørsler om teknisk støtte.
* **Personopplysninger om hvordan brukerne bruker Google Workspace for Education eller Chrome-tjenestene**:[[38]](#footnote-39) Google behandler personopplysninger om hvordan brukerne bruker løsningen. Dette er i stor grad «metadata». Metadata kalles gjerne også diagnostiske data. Det er informasjon som viser hvordan en elev, lærer eller kommunalt ansatt bruker Google Workspace for Education. Dette er opplysninger om programvarefeil, driftsstatus, ytelsesdata, og data fra enhetene GWFE brukes på som enhetsidentifikatorer og IP-adresser. Disse dataene er indirekte identifiserbare personopplysninger. Det betyr at dette er personopplysninger, siden det er mulig for Google å identifisere enkeltindivider. Formålet med Googles behandling er ikke å identifisere den enkelte eleven, læreren eller den ansatte som bruker Google Workspace for Education. Formålet er å levere tjenesten, gi anbefalinger for optimal bruk til skoleeier som kunde, levere og forbedre sikkerhet og tilgjengelighet i løsningen.[[39]](#footnote-40) For mer om formålet og om opplæringslovens rammer for å behandle metadata, se vedlegg 1 og 2.

# Skoleeiers formål for bruk av personopplysninger i Google Workspace for Education

Når skoleeier behandler personopplysninger i Google Workspace for Education, gjøres dette til flere ulike formål. Se det vedlagte forslaget til behandlingsprotokoll i Excel-format for en oversikt over skoleeiers formål og behandlingsaktiviteter. Disse formålene kan oppsummeres slik:

1. **Fremme læring og kunne utøve tilpasset opplæring og variert undervisning**
2. **Oppfylle skolens aktivitetsplikt for å følge opp skolemiljøsaker**
3. **Beskytte løsningen**[[40]](#footnote-41)**, avdekke misbruk og ulovlig aktivitet**
4. **Oppfylle krav til lovpålagt utlevering av personopplysninger**

## ****1. Fremme læring og kunne utøve tilpasset opplæring og variert undervisning****

**Hovedformålet med å ta i bruk Google Workspace for Education er å oppfylle elevenes rett til utdanning som bestemt i opplæringsloven. Formålet er generelt beskrevet slik:**

**«Fremme læring og kunne utøve tilpasset opplæring og variert undervisning».**

**Under dette hovedformålet finner vi en rekke underformål både knyttet til typiske skoleaktiviteter og funksjonalitet i Google Workspace for Education, men også supportformål som skal sikre at elver og lærer klarer å bruke løsningen:**

* **Sikre at elever har et digitalt verktøy som skal brukes til å oppnå læring. Dette innebærer å produsere elevarbeid, kunne levere oppgaver, får tilgang til filer og dokumenter, samarbeide med hverandre og få tilgang til eksamen.**
* **Sikre at lærere har et digitalt verktøy til hjelp i undervisningen skal brukes til å gi elevene opplæring. Dette innebærer å ha et verktøy for å dele undervisningsmateriell og oppgaver, samarbeide med hverandre og å kunne gi individuelle tilbakemelding til elevene basert på deres arbeid.**
* **Tilby hjelp og support til administratorer og brukere av Google Workspace for Education.**

## ****2. Oppfylle skolens aktivitetsplikt for å følge opp skolemiljøsaker****

**Skolen har en lovpålagt aktivitetsplikt som betyr at den ved mistanke om eller kjennskap til at en elev ikke har et trygt og godt skolemiljø, snarest skal undersøke saken. Når skoleeier bruker et verktøy som Google Workspace for Education hvor elver kan kommunisere med hverandre, blir dette en arena som er en del av skolemiljøet.**

**Det betyr at skoleeier vil måtte undersøke hva elever har gjort i Google Workspace for Education, for eksempel ved å se på kommunikasjon elevene imellom eller kommunikasjon i grupper. Denne aktiviteten vil kunne bli en del av en skolemiljøsak.**

## ****3. Beskytte tjenesten, avdekke misbruk og ulovlig aktivitet****

**Skoleeier behandler en rekke personopplysninger i Google Workspace for Education av sikkerhetshensyn. Det vil både si å ivareta prinsippene konfidensialitet, tilgjengelighet og integritet, men også å sørge for at misbruk av løsningen og ulovlig aktivitet oppdages og følges opp.**

**Dette formålet inkluderer flere underformål:**

* **Begrense at elever får tilgang til skadelig innhold på nett og bruken av skoleverktøy.**
* **Sikre elevens og lærnes bruk av utstyret og tjenester på internett ved at skoleeiers retningslinjer og sikkerhetspolicyer for administrert utstyr og skolekontoer blir implementert.**
* **Avdekke og følge opp phishing, spam, malware, virus, datainnbrudd, passord på avveie, hacking, DDoS-angrep og andre sikkerhetsrelaterte hendelser.**
* **Følge opp potensielt misbruk av tjenester.**
* **Avdekke erstatningsansvar ved tap av utstyr.**
* **Tilgangsstyring som sikrer at elever og lærere får nødvendige tilganger. Dette kan for eksempel innebære å sørge for at elever ikke får lærertilganger i Google Classroom.**
* **Identifisering av brukere for å ivareta integritetsprinsippet. Dette kan for eksempel innebære å sikre at rett bruker er identifisert eller identifisering slik at man vet hvem man samskriver og deler opplysninger med, eller hvem som deltar på klasseromsundervisning**
* **Avdekke juks og følge opp mistanke om juks under eksamen og andre prøver.**

## ****4. Oppfylle krav til lovpålagt utlevering av personopplysninger****

Skoleeier vil i noen tilfeller være pålagt å utlevere personopplysninger fra systemer som Google Workspace for Education til tredjeparter. Dette vil være lovpålagte utlevering, hvor det er spesielt viktig å kunne vise til et konkret behandlingsgrunnlag.[[41]](#footnote-42) Formålet med dette vil være å «oppfylle krav til lovpålagt utlevering av personopplysninger».

Den mest aktuelle utleveringsplikten for skoleeier er retten til innsyn. Den registrerte har rett til innsyn i egne personopplysninger etter GDPR artikkel 15, og skoleeier vil måtte oppfylle denne rettigheten når den registrerte ber om det.

Skoleeier vil i tillegg kunne pålegges å utlevere personopplysninger til politiet når det foreligger en beslutning fra retten etter reglene om ransaking i straffeprosessloven[[42]](#footnote-43) eller til riksrevisjonen i forbindelse med kontroll eller revisjon.[[43]](#footnote-44)

Del 2 Nødvendighet og proporsjonalitet

* + - * 1. Denne delen av DPIAen er en kvalitetssikring av om de valgene skoleeier har tatt ved bruken av Google Workspace for Education står i et rimelig forhold til formålene med behandlingen og om de oppfyller personvernprinsippene og den registrertes rettigheter. Delene som skoleeier må fylle ut selv er markert i gult.

## Personvernprinsippene

I dette avsnittet beskrives det hvordan skoleeiers behandling av personopplysninger i Google Workspace for Education ivaretar personvernprinsippene.

### Er kravet til lovlighet, rettferdighet og åpenhet ivaretatt? [[44]](#footnote-45)

#### Lovlighet (rettslig grunnlag)

Lovlighetsprinsippet handler først og fremst om at behandlingsansvarlig må ha et behandlingsgrunnlag eller et rettslig grunnlag for behandlingen av personopplysninger.

##### Kjernetjenestene

Skoleeier kan bruke plattformer som Google Workspace for Education med hjemmel i GDPR Artikkel 6(1)e).[[45]](#footnote-46) Dette fordi bruken av slike digitale plattformer er nødvendig for å utføre oppgaver i offentlighetens interesse eller utøve offentlig myndighet. Skoler har også en plikt til å gi elevene tilpasset opplæring for å sikre at alle får utnyttet og utviklet sine evner.[[46]](#footnote-47)

##### Tilleggstjenestene

Google er behandlingsansvarlig for tilleggstjenestene i Google Workspace for Education. Dette betyr at Google behandler personopplysninger til egne formål. Konkret behandler Google personopplysninger om hvordan elever, lærere og andre som bruker løsningene for å videreutvikle eksisterende og nye kommersielle tjenester. Opplæringsloven setter rammer for hva skoleeier, og i forlengelsen databehandlere som skoleeier kjøper tjenester av, kan bruke personopplysninger til. I et brev av 20.09.24 sier Kunnskapsdepartementet følgende:

*Departementet kan ikke se at skoleeier er pålagt noen plikter i opplæringsloven som innebærer at skoleeier har blitt gitt i oppgave å bidra til utvikling av private aktørers produkter, verken gjennom reglene om tilpasset opplæring eller gjennom øvrige bestemmelser i opplæringsloven. Etter departementets syn kan skoleeier da heller ikke dele elevenes personopplysninger med leverandører for dette formålet.*

Dette betyr at norske skoleeiere ikke har et behandlingsgrunnlag for å bruke tilleggstjenester i Google Workspace for Education, i og med at det innebærer å dele personoplpysninger med Google som så behandles til utvikling av en privat aktørs produkter og tjenester. Dette betyr videre at det å ta i bruk tilleggstjenestene i Google Workspace for Education ikke oppfyller kravet om lovlighet.

#### Åpenhet

Åpenhetsprinsippet sikter til at behandlingsansvarlig plikter å kjenne til *og* opplyse elever, foreldre og ansatte om hvordan behandlingen av personopplysninger skjer, av hvem og i hvilke roller.[[47]](#footnote-48)

Beskriv på hvilken måte skoleeier informerer elever, foresatte, lærere og andre ansatte om hvordan deres personopplysninger behandles i Google Workspace for Education.

Etter at denne DPIAen er fylt ut, personvernkonsekvenser er vurdert og kommunen har utarbeidet en behandlingsprotokoll, vil skoleeier ha en oversikt over hvilke personopplysninger som behandles og hvordan i Google Workspace for Education. Vi anbefaler deretter at skoleeier oppdaterer den informasjonen som gis, for eksempel i personvernerklæringen til kommunen eller på en egen informasjonsside på internett.[[48]](#footnote-49)

#### Rettferdig

At behandlingen skal være rettferdig, betyr at det må være en sammenheng mellom innsamlingen og bruken av personopplysninger, og at det skal fremstå rimelig for den registrerte.[[49]](#footnote-50)

##### Kjernetjenestene

Personopplysninger i skolen samles hovedsakelig inn for å gi den enkelte elev opplæring her og nå, eller for den ansatte til å kunne undervise og legge til rette for et godt skolemiljø, for eksempel ved oppgaveutdeling og oppgaveinnlevering. Behandling av personopplysninger for denne aktiviteten, som navn og klasse- og gruppetilhørighet, fremstår forutsigbar og rimelig for den det gjelder. Tilsvarende gjelder for ansatte som arbeider i skolen.

Behandling av «service data» som er metadata (data om data) som produseres når elever og ansatte bruker Google sine verktøy, kan oppleves mindre forutsigbart, gjerne fordi det er en mindre «synlig» aktivitet for det blotte øyet.

Det er DPIA-prosjektets vurdering at metadata som behandles til formål for å levere tjenesten, gi anbefalinger for optimal bruk til skoleeier som kunde, levere og forbedre sikkerhet og tilgjengelighet i løsningen. Dette gjelder særlig for formålene som er nødvendige for å levere tjenesten. Videre er det vår vurdering at de øvrige formålene er rimelige og forutsigbare i og med at formålene ivaretar de grunnleggende informasjonssikkerhetsprinsippene (konfidensialitet, integritet og tilgjengelig), og legger til rette for en trygg og effektiv bruk av løsningen for skoleeier. En sikker og tilgjengelig tjeneste vil f.eks. innebære å hindre at uvedkommende får tilgang til tjenesten, men også å skjerme elever fra skadelig innhold. Ofte er det naturlig og behov for at skoleeier delegerer en del av slike behandlinger til den som leverer tjenesten. Dette henger sammen med skoleeiers valgfrihet til å velge hvilket verktøy som er best egnet til å oppnå formålet om tilpasset undervisning.

Google tilbyr ulike avtaler eller «terms of service» for Google Workspace for Education som åpner for forskjellige løsninger for hvem som er behandlingsansvarlig for metadata. Det betyr at norske skoleeiere må velge de avtalene hvor de beholder behandlingsansvaret for metadata. Da kan ikke Google bruke personopplysninger til egne formål, med mindre de nye formålene er kompatible med behandlingsansvarliges egne formål (god opplæring i et godt miljø).

##### Tilleggstjenestene

På grunn av konklusjonen om tilleggstjenestene ovenfor, kan ikke kravet til rettferdighet sies å være oppfylt når det gjelder tilleggstjenestene.

### Er kravet til formålsbegrensning oppfylt?[[50]](#footnote-51)

##### Kjernetjenestene

Prinsippet om formålsbegrensning sikter til at personopplysninger skal «samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene».[[51]](#footnote-52)

Prosjektet har spesifikt beskrevet formålene for de enkelte behandlingsaktivitetene, se vedlagt behandlingsprotokoll. Disse formålene samsvarer med hovedformålet i opplæringsloven, som er å legge til rette for at barn og ungdommer får god opplæring i et godt miljø,[[52]](#footnote-53) og det grunnleggende kravet i læreplanen om digitale ferdigheter.[[53]](#footnote-54) For å kunne tilby digitale verktøy i opplæringen, må skoleeier også sørge for forsvarlig drift av sine datasystemer etter KIT-prinsippene (konfidensialitet, integritet og tilgjengelighet). Formålene er derfor berettiget ut ifra skoleeiers plikt til å oppfylle retten til grunnskoleopplæring.[[54]](#footnote-55)

Viderebehandling av personopplysninger kan ikke skje på en måte som er uforenlig med disse formålene.[[55]](#footnote-56) Som drøftet under kravet om rettferdighet ovenfor, har vi i prosjektet vurdert viderebehandling av metadata til formålene «Levering, tilgjengelighet og sikkerhet for tjenesten». Dette formålet vil ofte være naturlig å delegere til databehandler. Vi mener formålet er forenlig med skoleeiers plikt til å sikre forsvarlig drift av datasystemer (KIT-prinsippene).[[56]](#footnote-57)

Viderebehandling for «arkivformål i allmennhetenes interesse», som er i samsvar med GDPR artikkel 89 nr.1, er ikke uforenlig med opprinnelig formål.[[57]](#footnote-58) Skoleeier kan derfor arkivere og dokumentere personopplysninger i tråd med arkivloven og påfølgende forskrifter. Det påpekes at kontorstøtteløsning og skole-læringsplattform som Google Workspace for Education, ikke er et egnet arkivsystem.

##### Tilleggstjenestene

Kravet til formålsbegrensning vil ikke være ivaretatt for tilleggstjenestene, se vurderingen av lovlighet ovenfor.

### Er kravet til dataminimering ivaretatt?[[58]](#footnote-59)

##### Kjernetjenestene

Prinsippet om dataminimering innebærer at behandlingen skal «være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for». Med andre ord, betyr det at det ikke skal behandles flere personopplysninger enn nødvendig for å oppnå formålet. Det innebærer også en vurdering av om det kan behandles færre opplysninger, eller eventuelt sette inn tiltak for pseudonymisering eller anonymisering.[[59]](#footnote-60)

I skolesammenheng kan det være vanskelig å behandle få opplysninger om elever, så lenge formålet er knyttet til det pedagogiske. Med det sikter vi til at et av hovedformålene med opplæringen er at elever skal få «få utfalde skaparglede, engasjement og utforskartrong», jf. § 1-3 i opplæringsloven. Det betyr at elevene aktivt skal bidra i opplæringen selv (§10-6). Det er derfor ikke et mål for skoleeier å begrense data som elever og lærere lager/deler selv (innholdsdata), men heller å veilede elevene etter fag og tematikk som er fastsatt i læreplanen. Det betyr igjen, at mengden personopplysninger i innholdsdata kan kan bli stor (se vår utgreining av «Behandling av særlig kategori av personopplysninger (fritekst)» på s. 10). Personopplysninger som knytter seg til elevenes aktive deltakelse i opplæringen, må anses å ha en nær og naturlig sammenheng med formålet for behandlingen. Altså er opplysningene «adekvate» og «relevante», samtidig som elevene selv kan begrense hvilken informasjon de ønsker å gi fra seg.

Personopplysninger knyttet til brukerkonto (pålogging) har derimot mindre rom for hva som er «relevante» opplysninger å behandle. For brukerkonto vil opplysninger som identifiserer eleven og elevens klasse- og skoletilhørighet være de nødvendige personopplysningene for behandlingen.

For behandling av personopplysninger til IT-tekniske formål, som sikkerhet, gjøres for å ivareta krav om innebygget personvern og KIT konfidensialitet, integritet og tilgjengelig). Det vil for eksempel være nødvendig å behandle IP-adresse og lokasjon.

##### Tilleggstjenestene

Kravet til dataminimering vil ikke være ivaretatt for tilleggstjenestene, se vurderingen av lovlighet ovenfor.

### Er kravet til riktigheten av opplysningene ivaretatt?[[60]](#footnote-61)

Riktighetsprinsippet krever at personopplysninger skal være korrekte og holdes oppdatert. Skoleeier må derfor sørge for at personopplysninger i Google Workspace for Education er korrekte.

Personopplysninger holdes oppdaterte i Google Workspace for Education ved at informasjon om elever, lærere og andre brukere hentes fra skoleadministrative system. Ellers holdes personopplysningene oppdatert ved at flere av personopplysningene kommer direkte fra den registrerte. Dette gjelder for eksempel elevarbeid eller kommunikasjon brukerne imellom.

Her må skoleeier redegjøre for eventuelt andre tiltak.

### Er kravet til lagringsbegrensning ivaretatt?[[61]](#footnote-62)

Skoleeier må selv gjøre en vurdering av dokumentasjon- og arkivplikten i tråd med riksantikvarens forskrift § 7-28 avsnitt (3) Grunnskoleopplæring. For eksempel er «Underveisvurdering, inkl. halvårsvurdering med karakter» arkivverdig, og må arkiveres i et egnet arkiv- og dokumentasjonssystem. Normalt vil elever og ansattes brukerkonto (pålogging i GWFE via FEIDE-konto), deaktiveres og slettes innen et gitt tidsrom fra de slutter på skolen. Skoleeier må gjøre en konkret vurdering av hvor lenge det er nødvendig å bevare brukerkontoen.[[62]](#footnote-63)

### Er kravet til integritet og konfidensialitet ivaretatt?[[63]](#footnote-64)

Se redegjørelsene for hvordan integritet, konfidensialitet og andre krav til informasjonssikkerhet i den vedlagte oversikten over risikoscenarioer og i behandlingsprotokollen.

Her må skoleeier redegjøre for eventuelt andre tiltak.

Beskrivelser som kan gjøre denne redegjørelsen bedre:

* Teknisk rollestyring
* Organisatoriske tiltak som begrenset tilgangsstyring til tjenstlig behov
* Begrensninger skoleeier har innført I Google Workspace for Education f.eks. i chat-funksjonalitet
* Etablert rutiner som regulerer ekstern deling og samarbeid med eksterne
* Prosedyrer og krav til undersøkelse i skolemiljøsaker, inkludert elevers rett til kontradiksjon
* Varsling og rutiner for oppfølging når lærere ved en feiltakelse gir elever tilgang som lærere
* …

Husk at skoleeier både må fylle ut behandlingsprotokoll og redegjøre for hvilke tekniske og organisatoriske sikkerhetstiltak som er implementert, og ta stilling til risikoscenarioene i den vedlagte vurderingen (del 3 i denne DPIAen), samt beskrive andre risikoscenarioer som er relevante for skoleeier.

## De registrertes rettigheter og friheter

I dette avsnittet beskrives det hvordan skoleeiers behandling av personopplysninger i Google Workspace for Education ivaretar de registrertes rettigheter og friheter.

### Hvordan ivaretas de registrertes rett til informasjon?**[[64]](#footnote-65)**

Retten til informasjon innebærer at skoleeier plikter å informere elever og foresatte, lærere og andre ansatte som bruker Google Workspace for Education om hvordan personopplysningene deres behandles.

Behandling av personopplysninger, og særlig i systemer som leveres av store teknologiselskaper, er noe mange synes er vanskelig å forstå. Det gjelder både for innbyggere, men også for skoleeier. Som nevnt over har prosjektet opplevd at det har vært komplisert å sette seg inn i tjenesteporteføljen til Google. Skoleeier har likevel et ansvar for å sette seg inn i produktet som er kjøpt, og videreformidle informasjon om bruken til elever, foreldre og ansatte. I dette prosjektet har vi jobbet med å avklare juridiske spørsmål, vilkår, grensedragning mellom tjenestene til Google m.m., som vi mener vil hjelpe skoleeier til å forstå og forvalte Google Workspace for Education.

Skoleeier bør videre, som minimum, informere elever og foreldre om hvilke googleverktøy kommunen bruker, hvilke opplysninger om elever som behandles i tjenesten(e) og til hvilket formål, lagringstid og elevens rettigheter. Dette kan for eksempel gjøres i et eget informasjonsskriv eller på kommunens hjemmeside.

Her må skoleeier redegjøre for hvordan informasjon om Google Workspace for Education gis til elever og foresatte, lærere og andre ansatte som bruker løsningen.[[65]](#footnote-66)

### Hvordan ivaretas de registrertes rett til innsyn?**[[66]](#footnote-67)**

Retten til innsyn gir elever (og foresatte på vegne av elevene), lærere og andre ansatte, rett til innsyn i hvilke personopplysninger som behandles om dem i Google Workspace for Education.

Pålogging i Google Workspace for Education gjøres gjennom Feide-konto. Elever og ansatte kan logge inn på Feide sine sider å få innsyn i alle opplysninger som ligger i den digitale brukerkontoen.

Skolearbeid og vurderinger vil elever og ansatte få tilgang til via på sin egen PC eller Chromebook.

Google Workspace for Educationinneholder funksjonalitet som gjør det mulig for skoleeier å oppfylle retten til innsyn, både ved at den registrerte selv laster ned egne dokumenter, og at skoleeier åpner for at brukeren kan laste ned egne personopplysninger via løsningen Takeout.[[67]](#footnote-68),[[68]](#footnote-69)

Her må skoleeier redegjøre for hvordan elever og foresatte, lærere og andre ansatte skal gå frem for å få oppfylt sin rett til innsyn. Skoleeier bør ha et kontaktpunkt, gjerne på skolen og/eller sentralt, som kan kontaktes ved behov for å utøve retten til innsyn. Skoleeier må ta stilling til om elever som er ferdig med sin skolegang skal gis mulighet til å overføre egne dokumenter og filer fra sin skolekonto til en privat Google-konto.

### Hvordan ivaretas de registrertes rett til retting?[[69]](#footnote-70)

Registrerte har rett til å få rettet personopplysninger om seg selv som ikke er korrekte. Denne rettigheten må sees i sammenheng med personvernprinsippet riktighet som pålegger skoleeier å sikre at personopplysningene som behandles i Google Workspace for Education er korrekte og oppdaterte.

De fleste av personopplysninger som behandles i Google Workspace for Education, vil enten hentes fra skoleeiers skoleadministrative system, eller så er det personopplysninger som den registrerte har skapt selv (for eksempel elevarbeid eller kommunikasjon brukerne imellom). Det å gjennomføre retting på bakgrunn av en henvendelse fra den registrertes henvendelse vil derfor som regel ikke være aktuelt.

Her må skoleeier redegjøre for hvordan elever og foresatte, lærere og andre ansatte skal gå frem for å få oppfylt sin rett til retting. Skoleeier bør ha et kontaktpunkt, gjerne på skolen og/eller sentralt, som kan kontaktes ved behov for å utøve retten til retting. Dette kontaktpunktet kan være det samme som for øvrige slettehenvendelser fra registrerte hvis personopplysninger som kommunen behandler. Skoleeier må også informere brukerne av Google Workspace for Education hvordan de skal gå frem for å ivareta denne rettigheten.

### Hvordan ivaretas de registrertes rett til sletting?[[70]](#footnote-71)

Registrerte har rett til å få sine personopplysninger om seg slettet. Denne rettigheten må sees i sammenheng med skoleeiers plikt til lagringsbegrensning som pålegger skoleeier å slette personopplysninger fra Google Workspace for Education når formålet med behandlingen er oppfylt.

For personopplysninger som behandles i Google Workspace for Education, vil skoleeier ha behandlingsgrunnlag til å behandle den registrertes personopplysninger. Det å gjennomføre sletting på bakgrunn av en henvendelse fra den registrertes henvendelse vil derfor som regel ikke være aktuelt.

Her må skoleeier redegjøre for hvordan elever og foresatte, lærere og andre ansatte skal gå frem for å få oppfylt sin rett til sletting. Skoleeier bør ha et kontaktpunkt, gjerne på skolen og/eller sentralt, som kan kontaktes ved behov for å utøve retten til sletting. Dette kontaktpunktet kan være det samme som for øvrige slettehenvendelser fra registrerte hvis personopplysninger som kommunen behandler. Skoleeier må også informere brukerne av Google Workspace for Education hvordan de skal gå frem for å ivareta denne rettigheten.

Merk at retten til sletting ikke nødvendigvis innebærer at den registrerte har rett til å faktisk få personopplysningene sine slettet da skoleeier i utgangspunktet har behandlingsgrunnlag til å behandle personopplysninger om elever, lærere og andre ansatte i Google Workspace for Education.

### Hvordan ivaretas de registrertes rett til å protestere?[[71]](#footnote-72)

Retten til å protestere etter GDPR artikkel 21, gjør seg gjeldende på behandlingsaktiviteter i skolen som har behandlingsgrunnlag i GDPR artikkel 6(1) bokstav e) «offentlig myndighet eller oppgave i allmennhetens interesse» eller f) «berettiget interesse». De fleste behandlingsaktiviteter knyttet til pedagogiske formål er hjemlet i bokstav e), og eleven/foreldre vil derfor ha rett til å fremme en protest.

Den som fremmer en protest, må peke på grunner knyttet til sin særlige situasjon. Det må altså foreligge individuelle forhold hos den registrerte som tilsier at behandlingen skal stoppes.

Her må skoleeier redegjøre for hvordan skoleeier er forberedt på å ta imot og behandle protest-henvendelser. Dette er noe mange skoleeiere kan oppleve som vanskelig. Vi har derfor laget en veileder for retten til å protestere, som kan hjelpe kommunene å håndtere denne rettigheten på en god måte: [Veileder for retten til å protestere - KS](https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/veileder-for-retten-til-a-protestere/).

Både for retten til å protestere og for retten til begrensning, bør skoleeier ha et kontaktpunkt, gjerne på skolen og/eller sentralt, som elever, foresatte og ansatte kan kontaktes ved behov for å utøve egne rettigheter.

### Hvordan ivaretas de registrertes rett til begrensing?[[72]](#footnote-73)

Retten til begrensning er en rettighet som er aktuelt i forbindelse med retten til å protestere. Se redegjørelsen for ivaretagelse av retten til å protestere ovenfor.

### Hvordan ivaretas de registrertes rett til dataportabilitet?[[73]](#footnote-74)

Retten til dataportabilitet gjelder kun når behandlingsgrunnlaget er samtykke eller avtale. Behandlingsgrunnlaget for bruk av Google Workspace for Education er GDPR artikkel 6(1) bokstav e) «offentlig myndighet eller oppgave i allmennhetens interesse» med supplerende behandlingsgrunnlag i opplæringsloven. Vurdering av denne rettigheten er derfor ikke aktuelt.

### Hvordan ivaretas de registrertes rett til å ikke være gjenstand for automatiserte avgjørelser?[[74]](#footnote-75)

Kjernetjenestene i Google Workspace for Education inneholder ikke funksjonalitet som kan brukes til å fatte automatiserte avgjørelser. Vurdering av denne rettigheten er derfor ikke aktuelt.

## Oppsummering av nødvendig og forholdsmessig

Er behandlingen av personopplysninger den minst inngripende måten å oppnå formålet på?   
  
☐ Ja ☐ Nei

Begrunnelse:   
[Sett inn begrunnelse for avkrysningen over. Hvorfor er behandlingen den minst inngripende måten å oppnå formålet på? Hvorfor er behandlingen ikke den minst inngripende måten å oppnå formålet på? Husk å få frem hvilke endringer som kan gjøres som medfører at man kan oppnå formålet på en mindre inngripende måte, dersom det er tilfellet]

Del 3 Vurdering av personvernkonsekvenser og tiltak

Dette er den delen av DPIAen hvor skoleeier skal vurdere hvilke personvernkonsekvenser som foreligger ved behandlingen av personopplysninger. I denne DPIAen, er dette gjort i et eget Excel-ark som legges ved DPIAen. Se dette Excel-arket for vurdering av personvernkonsekvenser og tiltak.

Skoleeier må ta stilling til og vurdere de enkelte risikoscenarioene, og føye til nye som er aktuelle for skoleeier ut ifra lokale forhold.

# Kvalitativ metode

I denne DPIAen er det valgt en kvalitativ metode for vurdering av personvernkonsekvenser.

Tradisjonelle risikovurderingsmodeller, som forskjellige fler-faktormodeller som vurderer sannsynligheten for at et risikoscenario inntreffer og konsekvensene av dette, er ofte anvendt innen informasjonssikkerhet. Slike modeller være utilstrekkelige for personvernrisikovurderinger fordi de ikke tar nok hensyn til interne forhold som kan føre til brudd på etterlevelse av personvernprinsipper og den registrertes rettigheter. Årsakene til slike brudd kan nemlig i større grad skyldes interne forhold hos den behandlingsansvarlige, heller enn eksterne trusler.

For å håndtere disse utfordringene, er det som nevnt brukt en kvalitativ metode for vurdering av personvernkonsekvenser i denne DPIAen. Denne tilnærmingen bygger på faglig skjønn og kontekstuell forståelse, og vurderer risiko basert på følgende nivåer:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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. |

Del 4 Den registrertes mening og rådgivning fra personvernombudet

# De registrertes synspunkter

De registrertes synspunkter er innhentet I forbindelse med gjennomføring av denne DPIAen. Se rapportene om henholdsvis elevenes, lærernes og de foresattes mening om personvern i Google Workspace for Education for utfyllende informasjon om personvernbekymringene til de registrerte.[[75]](#footnote-76)

# Oppsummering av de registrertes synspunkter og anbefalinger

[Sett inn deltakernes anbefalinger. Husk å få frem om deltakerne mener at det foreligger en høy risiko eller ikke. Få også med om deltakerne mener at det er nødvendig å gjennomføre en forhåndsdrøftelse med Datatilsynet eller ikke på bakgrunn av deltakernes forståelse av risikobildet.]

# Anbefaling fra personvernombudet

[Sett inn ombudet sin kommentar til DPIAen]

Del 5 Ledelsens beslutning

# Beslutning av leder med ansvar for personvern

Ledelsens beslutning etter at personvernkonsekvensvurderingen er gjennomført er følgende:

Risikoen for de registrertes rettigheter og friheter er redusert til et akseptabelt nivå. Når tiltak er implementert kan behandlingen av personopplysninger gjennomføres.

Risikoen for de registrertes rettigheter og friheter er **ikke** redusert til et akseptabelt nivå. Behandlingen av personopplysninger kan **ikke** gjennomføres.

Risikoen for de registrertes rettigheter og friheter er **ikke** redusert til et akseptabelt nivå. Forhåndsdrøfting med Datatilsynet gjennomføres før ledelsentar en beslutning om behandling av personopplysninger.

# Beskrivelse av hva ledelsens har lagt vek på i sin beslutning:

[Sett inn ledelsen sin begrunnelse for valget tatt ovenfor]

|  |  |  |
| --- | --- | --- |
| Dato | Navn på beslutningstaker | Rolle |
|  |  |  |

# Vedlegg 1: Begrunnelse for anbefalte tjenester

***Merk at dette dokumentet beskriver tjenestene YouTube og Google Søk og Assistent som tjenester i Google Workspace for Education. YouTube og Google Søk eksisterer også som forbrukertjenester. Det vi sier i dette dokumentet beskriver ikke disse tjenestene som forbrukertjenester.***

## Skoleeier er behandlingsansvarlig og skal instruere leverandører om hvordan elevers personopplysninger skal behandles

Det er skoleeier[[76]](#footnote-77) som er behandlingsansvarlig når elevers personopplysninger behandles i skolen. Dette betyr at det er skoleeier som har ansvaret for at elevers personvern og de rettighetene som fremgår av personvernforordningen[[77]](#footnote-78) ivaretas. En behandlingsansvarlig er også den som bestemmer hvorfor personopplysningene behandles (formålet med behandlingen) og hvordan gjennom å velge de digitale verktøyene som skal brukes for å oppnå formålet.

Den leverandøren som leverer digitale tjenester til skoleeier er databehandler. En databehandler er den som behandler personopplysninger *på vegne av* en behandlingsansvarlig. Dette innebærer at databehandler ikke kan bruke personopplysningene til andre formål enn det som behandlingsansvarlig har instruert om. Denne instruksen kalles en «databehandleravtale».

Et bilde som inneholder tekst, skjermbilde, diagram, Font

Automatisk generert beskrivelse

*Figur 1 Googles rolle som databehandler og behandlingsansvarlig setter rammene for de tjenestene som skoleeier anbefales a bruke (innenfor det grønne) og de tjenestene som ikke anbefales (innenfor det røde)*

En del av behandlingsansvaret er å sikre at det ikke inngås avtaler med databehandlere som behandler personopplysninger til «egne formål». Sagt på en annen måte, må den behandlingsansvarlige forsikre seg om at databehandler bare behandler personopplysninger i tråd med instruks og avtale. Hvis databehandler behandler personopplysninger til egne formål, endrer de status fra databehandler til behandlingsansvarlig. I så fall vil databehandler (som nå er behandlingsansvarlig) bestemme selv hva den skal bruke personopplysningene til. Dette er problematisk når det er snakk om elevers personopplysninger, da situasjonen kan sammenlignes med å «selge» elevers personopplysninger til leverandøren.

Flere store leverandører forhandler ikke egne databehandleravtaler med kundene sine, men bruker standardavtaler. Dette gjelder også Google. I avtaleverket som ligger til grunn for Google Workspace for Education, har Google beskrevet at de er behandlingsansvarlige for tilleggstjenestene. Dette er en rollefordeling som ikke er forenlig med skoleeiers behandlingsansvar.

## Behandlingsgrunnlaget til skoleeier legger føringer for hvilke digitale tjenester som kan tas i bruk i skolen

Skoleeier som behandlingsansvarlig må ha hjemmel i lov (et behandlingsgrunnlag) for å kunne behandle elevers personopplysninger. For norske skoleeiere er behandlingsgrunnlaget de ulike bestemmelsene i opplæringsloven. Behandlingsgrunnlaget setter rammer for hva skoleeier kan gjøre med elevers personopplysninger. For eksempel kan ikke skoleeier behandle elevers personopplysninger til andre formål enn de som fremgår av opplæringsloven.

Dette setter begrensninger for hvilke personopplysninger skoleeier kan dele med leverandører som Google for Googles viderebruk av elevers personopplysninger til egne formål.

## Opplæringsloven setter tydelige rammer for hva elevers personopplysninger (inkludert metadata) kan brukes til

Selv om Google er databehandler for kjernetjenestene i Google Workspace for Education,[[78]](#footnote-79) og for Chrome nettleser når den brukes på en administrert Chromebook (ChromeOS), er Google likevel alltid behandlingsansvarlig for metadata.[[79]](#footnote-80)

Metadata er informasjon om informasjon, det vil si om hvordan elever og lærere bruker Google Workspace for Education. Dette er for eksempel informasjon om det trådløse nettverket en elev har koblet Chromebooken sin til, hvilket tidspunkt eleven logget inn i Google Classroom eller hvilken versjon av Chrome-nettleseren eleven bruker. Metadata kalles ofte også for diagnostiske data eller telemetri.

Metadata skiller seg fra innholdsdata. Innholdsdata er for eksempel teksten i en oppgave en student leverer til læreren, den skriftlige tilbakemeldingen studenten mottar fra læreren, eller meldinger som studentene sender til hverandre i løsningen.

Metadata er indirekte identifiserbare personopplysninger. Det er mulig for Google å identifisere den enkelte eleven, selv om identifikasjon ikke er formålet med Googles behandling av disse personopplysningene.[[80]](#footnote-81)

De aller fleste leverandører bruker denne typen personopplysninger (metadata) fra kundene sine til egne formål i større eller mindre grad. Google er ikke alene om dette. Denne problemstillingen er også kjernen i den danske Chromebook-saken der det danske datatilsynet forbød Helsingør å bruke Google Workspace for Education i 2022. I denne saken kom det danske datatilsynet til at den danske opplæringsloven åpnet for at personopplysninger i Google Workspace for Education kunne behandles til formålet:

*Levering, tilgjengelighet og sikkerhet for tjenesten*

Mens følgende formål lå utenfor den danske opplæringsloven:

* *Videreutvikling av den spesifikke tjenesten som skoleeier har kjøpt*
* *Videreutvikling av andre og nye produkter fra leverandører*

Spørsmålet om leverandørens adgang til å bruke personopplysninger om elever til egne formål har lenge vært uavklart. I september 2024 kom Kunnskapsdepartementet med en avklaring om at opplæringsloven ikke åpner for at elevers personopplysninger kan brukes til utvikling av private aktørers produkter. Kunnskapsdepartementet understreker at dette betyr at skoleeier heller ikke kan dele elevenes personopplysninger med leverandører for dette formålet. Konkret sier Kunnskapsdepartementet:[[81]](#footnote-82)

*Departementet kan ikke se at skoleeier er pålagt noen plikter i opplæringsloven som innebærer at skoleeier har blitt gitt i oppgave å bidra til utvikling av private aktørers produkter, verken gjennom reglene om tilpasset opplæring eller gjennom øvrige bestemmelser i opplæringsloven. Etter departementets syn kan skoleeier da heller ikke dele elevenes personopplysninger med leverandører for dette formålet.*

Dette betyr at det er svært begrenset hvilke formål opplæringsloven åpner for at en leverandør kan behandle elevdata til. Det er vår vurdering at den norske opplæringsloven åpner for at Google og andre leverandører kan bruke personopplysninger om elever til følgende formål:[[82]](#footnote-83)

*Levering, tilgjengelighet og sikkerhet for tjenesten, herunder videreutvikling av sikkerhet og tilgjengelighet i tjenesten.*[[83]](#footnote-84)

Videre vil opplæringsloven ikke åpne for at Google eller andre leverandører kan behandle personopplysninger om elever til følgende formål:

1. Videreutvikling av den spesifikke tjenesten som skoleeier har kjøpt
2. Videreutvikling av andre og nye produkter fra leverandører

## Hva er de sannsynlige og største risikoene og konsekvensene for elevene (i praksis) om skolene fortsatt bruker Google Søk og Assistent og YouTube?

Hvis skoleeier fortsetter å bruke tilleggstjenester som Google Søk og assistent og YouTube, er det en risiko for at skoleeier utleverer elevers personopplysninger til en kommersiell aktør som så bruker personopplysningene til formål som ikke er i tråd med (formålene i) opplæringsloven. Kunnskapsdepartementets uttalelse fra september 2024 har gjort dette enda tydeligere enn før.

Google er behandlingsansvarlig for alle personopplysninger som behandles i tilleggstjenestene. Det betyr at Google kan behandle personopplysninger om elever til egne formål. Dette innebærer en personvernrisiko for elevene i form av mulig viderebehandling av deres personopplysninger på en måte som ikke er forenlig med opplæringsloven. Det innebærer også en etterlevelsesrisiko for skoleeier ved at skoleeier ikke ivaretar sitt behandlingsansvar.

Google har iverksatt flere tiltak for å begrense hvilke personopplysninger som selskapet samler inn om elever.[[84]](#footnote-85) Imidlertid samler Google fortsatt inn personopplysninger om elever når de bruker tilleggstjenester fra en skolekonto, og bruker dem til egne formål.

# Vedlegg 2: Vurdering av om Googles behandling av personopplysninger til egne formål er kompatibelt med skoleeiers opprinnelige formål i opplæringsloven

Skoleeier kan behandle personopplysninger når det er nødvendig for å utføre oppgaver etter opplæringsloven, jf. opplæringsloven § 25-1.

Kunnskapsdepartementet har tidligere konkludert med at det ikke finnes noen konkret rettslig forpliktelse i opplæringsloven om å ta i bruk Google Workspace for Education, eller lignende programvare i skolen.[[85]](#footnote-86)

Skoleeier har imidlertid en rettslig forpliktelse til å oppfylle retten til grunnskoleopplæring og videregående opplæring, jf. opplæringsloven (2023) §§ 28-1 og 28-2. Det følger videre av forskrift om overordnede mål og prinsipper i skolen (Overordnet del – verdier og prinsipper for grunnopplæringen) punkt 2.3 at digitale ferdigheter er definert som en av de fem grunnleggende ferdighetene, og at skolen skal legge til rette for og støtte elevenes utvikling av de fem grunnleggende ferdighetene gjennom hele opplæringsløpet.

Departementet mener det er de forpliktelsene som kan utledes til en rettslig forpliktelse for skoleeier til å ta i bruk løsninger som Google Workspace for Education.

Behandlingsgrunnlaget for å bruke systemer som Google Workspace for Education er dermed GDPR artikkel 6(1) bokstav e), jf. opplæringsloven § 25-1, jf. §§ 28-1 og 28-2 lest i sammenheng med kravet om digitale ferdigheter, jf. forskrift om overordnede mål og prinsipper i skolen (Overordnet del – verdier og prinsipper for grunnopplæringen) punkt 2.3.

Det er med andre ord opplæringsloven med forskrift som hjemler bruken av løsninger som Google Workspace for Education. Det betyr at elevers, læreres og andre ansattes personopplysninger kan brukes til formål som er nødvendig for å levere tjenesten. Google behandler elevers personopplysninger for å levere tjenesten. Vi har i denne DPIAen formulert dette formålet slik: «Levering, tilgjengelighet og sikkerhet for tjenesten».

I Google Workspace for Education (kjernetjenester og AppSheet) viderebehandler Google elevers personopplysninger for «å videreutvikle sikkerhet og tilgjengelighet i tjenesten».[[86]](#footnote-87) I Chrome nettleser og i ChromeOS «Essential services» med Data Processor Mode, behandler Google elevers personopplysninger for «forbedring og optimalisering av ytelse og kjernefunksjonalitet i tilknytning til effektiviteten av tilgjengelighet, personvern, sikkerhet og IT-infrastruktur for tjenestene»[[87]](#footnote-88)

*Spørsmålet blir om dette formålet er kompatibelt med det opprinnelige formålet om å levere tjenesten.*

For å gjøre denne kompatibilietsvurderingen, har vi brukt veilederen til det norske Datatilsynet om om formålsbegrensningsprinsippet[[88]](#footnote-89)

1. **Finnes det en naturlig kobling mellom det opprinnelige formålet og det nye formålet?**

Det opprinnelige formålet med å behandle personopplysningene er å bruke Google Workspace for Education som et verktøy for å oppfylle kravene i opplæringsloven, spesielt knyttet til kravet om å utvikle elevenes digitale ferdigheter. Det nye formålet er å behandle elevers personopplysninger i form av «service data», for å videreutvikle sikkerhet og tilgjengelighet i tjenesten.

Det er en naturlig sammenheng mellom disse formålene, da forbedring av sikkerhet i tjenesten og oppetid (tilgjengelighet) er forutsetninger for å kunne levere løsningen. Google Workspace for Education er en SaaS-tjeneste (Software as a Service), og i denne typen tjenester er det nødvendig med kontinuerlig videreutvikling av sikkerhet og tilgjengelighet for å møte teknologiske endringer, håndtere nye sikkerhetstrusler og sikre at tjenesten er stabil og pålitelig for brukerne.

Dette taler for at behandling av personopplysninger for å forbedre tjenesten innenfor områdene «sikkerhet» og «tilgjengelighet» er kompatibelt med det opprinnelige formålet. I og med at forbedring av tjenesten er en forutsetning for å kunne levere en trygg og effektiv læringsplattform, kan dette anses som en forlengelse av det opprinnelige formålet og dermed være i samsvar med prinsippet om formålsbegrensning.

1. **I hvilken sammenheng er personopplysninger for det opprinnelige formål samlet inn?**

Personopplysningene er samlet inn for å kunne bruke Google Workspace for Education. Dette i en utdanningskontekst, hvor elever, lærere og andre ansatte bruker Google Workspace for Education som en del av undervisnings- og læringsprosessen. Personopplysningene er innhentet for å muliggjøre kommunikasjon, samarbeid og tilgang til læringsressurser, i tråd med skolens forpliktelser til å utvikle digitale ferdigheter hos elevene.

1. **Hvilket forhold har behandlingsansvarlig til den registrerte? Er den registrerte en del av en særlig sårbar gruppe eller har et avhengighetsforhold til behandlingsansvarlig?**

De registrerte er i all hovedsak elever i skolen, det vil si mindreårige, og utgjør således en sårbar gruppe i GDPRs forstand. Alder er med andre ord en av grunnene til at det foreligger et asymmetrisk maktforhold mellom den registrerte og den behandlingsansvarlige.

Det forsterker dette asymmetriske makt-forholdet at elevene ikke har noe valg i hvorvidt personopplysningene deres skal behandles i Google Workspace for Education eller ikke. Dette er et valg som den enkelte skoleeier (kommune) tar på deres vegne.

Dette gjør at skoleeier må være ekstra oppmerksom for å sikre at elevers personopplysninger behandles på en måte som ivaretar deres personvern.

1. **Er det nye formålet og behandling av personopplysninger fra databehandler side forutsigbart for den registrerte?**

Som nevnt ovenfor under spørsmål 1, er det en naturlig sammenheng mellom formålet «videreutvikle sikkerhet og tilgjengelighet i tjenesten» og det opprinnelige formålet personopplysningene ble brukt til. For skoleeier som behandlingsansvarlig og profesjonell kunde av diverse digitale tjenester, er det forutsigbart at personopplysninger brukes til dette formålet. Dette er nok ikke like åpenbart for de registrerte (her elever og lærere som bruker Google Workspace for Education).

Det blir derfor viktig at dette kommuniseres tydelig til de registrerte, f.eks. gjennom personvernerklæringen til kommunen og informasjon fra skolen, slik at elevene og deres foresatte er informert om hvordan personopplysningene blir brukt. Transparens er en forutsetning for å sikre at behandlingen er forutsigbar og i tråd med de registrertes rimelige forventninger.

1. **Er det snakk om særlige kategorier personopplysninger?**

Det er ikke snakk om særlig kategori personopplysninger.[[89]](#footnote-90)

1. **Innebærer den nye behandlingen av personopplysninger særskilt risiko for den registrerte?**

Det vurderes at den nye behandlingen ikke innebærer særskilt risiko for den registrerte. Dette fordi det nye formålet er så nært knyttet til det opprinnelige formålet, og behandlingen skjer innenfor samme kontekst og med tilsvarende sikkerhetstiltak, innebærer den nye behandlingen ikke en særskilt risiko for den registrerte.

1. **Er det mulig å iverksette særlige beskyttelsestiltak eller nødvendige garantier for å ivareta den registrertes personvern, for eksempel ved bruk av pseudonymisering?**

Det er mulig og nødvendig å implementere beskyttelsestiltak for å ivareta personvernet. I dette tilfellet er det iverksatt tiltak ved at det samles inn indirekte identifiserbare personopplysninger. Selv om dataene ikke er direkte pseudonymisert, reduserer innhenting av indirekte identifiserbare opplysninger risikoen for at enkeltpersoner kan identifiseres direkte.

Google har dessuten implementert ulike former for kryptering i kjernetjenestene, noe som også er med på å ivareta den registrertes personvern (nærmere bestemt konfidensialitet).[[90]](#footnote-91)

**Konklusjon**

Denne vurderingen viser at behandling av personopplysninger om elevers aktivitetsdata i form av metadata («service data») for å sikre sikkerhet og tilgjengelighet i Google Workspace for Education (kjernetjenester og AppSheet), samt i Chrome nettleser og i ChromeOS «Essential services» med Data Processor Mode, er kompatibelt med formålet «videreutvikle sikkerhet og tilgjengelighet i tjenesten».

Dette fordi det er en naturlig sammenheng mellom det opprinnelige formålet om å levere tjenesten og det nye formålet om å forbedre sikkerhet og tilgjengelighet. Denne viderebehandlingen er nødvendig for å tilby en stabil og trygg læringsplattform.

# Vedlegg 3: Oversikt over avtaler som regulerer Google Workspace for Education, ChromeOS og Chrome nettleser

# **Google Workspace for Education kjernetjenester (core services) og AppSheet**

1. Google Workspace for Education Privacy Notice: <https://workspace.google.com/intl/no/terms/education_privacy/>
2. Google Workspace for Education Terms of Service​: <https://workspace.google.com/terms/education_terms/>
3. Google Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum/>
4. Google Cloud Privacy Notice: <https://cloud.google.com/terms/cloud-privacy-notice>
5. Cloud Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum/>
6. Valgfrie avtaler vi anbefaler at du signerer:
   * Google Workspace for Education Service Data Addendum: <https://workspace.google.com/terms/service-data-addendum/>

Når skoleeier har signert dette dokumentet, vil personvernerklæringen bli dette dokumentet: Supplemental Google Cloud Privacy Notice: <https://cloud.google.com/terms/cloud-privacy-notice-supplement>

# **Google Workspace for Education tilleggstjenester (additional services)**

YouTube

* Workspace for Eduaction Privacy Policy: <https://workspace.google.com/intl/no/terms/education_privacy/>
* Google Privacy Policy: <https://policies.google.com/privacy?hl=no>

Google Search and Assist

* Google Privacy Policy: <https://policies.google.com/privacy?hl=no>

# **Andre tjenester vi har vurdert**

ChromeOS og Chrome bowser (på en administrert Chromebook med Data Processor Mode)

* (Engelsk) ChromeOS Data Processor Mode Agreement: <https://www.google.com/chrome/dpchromeos/eu/index.html>
* (Norsk) Avtale om databehandlermodus for ChromeOS: <https://www.google.com/chrome/dpchromeos/eu/no/index.html>

# Hva må du vite fra de forskjellige avtalene

**Google Workspace for Education Privacy Notice** (Personvernerklæring) angir hvilke personopplysninger som samles inn i kjernetjenestene. I tillegg gjøres det rede for hvilke personopplysninger som samles inn. Samtidig gjøres det grundigere rede for hvilke data og hvordan dataen behandler i personvernerklæringen til Google Cloud (Google Cloud Privacy Notice).

Google deler inn personopplysninger i «Customer personal data» og «Service data». «Customer personal data» er personopplysninger som lastes opp i Google Workspace for Education, som lagres, sendes eller mottas gjennom kjernetjenestene av eleven eller skolen. For eksempel: elevers brukernavn, passord, elevers adresse, telefonnummer, profilbilde osv. Det er med andre ord kunden som direkte oppgir disse opplysningen til Google.

«Service data» defineres som informasjon Google samler inn når elever bruker kjernetjenestene. Eksempler på dette er kontoinformasjon, elevaktivitet, kommunikasjon og samhandling med folk, detaljer om bruken av tjenesten, posisjonsdata, innstillinger, apper, nettlesere og enheter eleven bruker osv. Tjenestedata er også informasjon som er nødvendig for Google å lagre for å kunne sende skoleeier faktura for lisensen til Google Workspace for Education «billing information» og informasjon som den enkelte brukeren i forbindelse med en brukerstøttehenvendelse («support ticket»).

Merk at «billing information» og personopplysninger som behandles i forbindelse med «support tickets», er opplysninger som også oppgis av skoleeier som kunde av Google, men dette er data som defineres som «Service data», ikke «Customer personal data».

**Google Cloud Privacy Notice** (personvernerklæring) gir informasjon om hvilke personopplysninger Google samler inn som tjenestedata, hvem den deles med og formålet med innsamlingen.

Google deler som hovedregel ikke tjenestedata med tredjeparter. Google deler imidlertid disse personopplysninger med underleverandører, med skolens administrator (med samtykke fra elev eller foresatt), når du bruker tredjepartstjenester gjennom f.eks. Google Marketplace, for ekstern behandling til Googles samarbeidspartnere og andre tredjeparter i tråd med googles instrukser og i tråd med Googles personvernregler.

Formålet med innsamlingen av tjenestedata er å tilby Cloud-tjenestene, komme med anbefalinger om mer effektiv bruk av Cloud-tjenester, tilby og forbedre andre tjenester som Google eller tredjeparter tilbyr, teknisk support, beskytte brukere og Google fra sikkerhetsbrudd og svindel og etterleve juridiske forpliktelser.

Ifølge denne avtalen er Google behandlingsansvarlig for tjenestedata.

Ifølge **Google Cloud processing Amendment** er kunden behandlingsansvarlig for kundedata.

Hvis kunden ønsker å være behandlingsansvarlig for tjenestedata i tillegg til kundedata, kan kunden skrive under **Google Workspace for Education Service Data Addendum.** Da gjelder i tillegg **Supplemental Google Cloud Privacy Notice.**

Konsekvensen blir dermed at vilkårene i **Google Cloud Privacy Notice** fortsatt gjelder bortsett fra der **Supplemental Google Cloud Notice** er annerledes. Dette er hovedsakelig under formålene for behandlingen.

Hovedforskjellen mellom **Google Cloud Privacy Notice** og **Supplemental Google Cloud Notice** er at skoleeier også er behandlingsansvarlig for tjenestedata «for the purposes of providing the service». I tillegg er Google behandlingsansvarlig for en del av kan bruke personopplysningene til egne formål som beskrevet i Supplemental Google Cloud Privacy Notice.

# Vedlegg 4: Illustrasjon av anbefalingene

Figur 2 Illustrasjon av anbefalinger når skoleeier bruker en administrert Chromebook

Et bilde som inneholder tekst, skjermbilde, Operativsystem, Dataikon

Automatisk generert beskrivelse

Figur 3 Illustrasjon av anbefalinger når skoleeier bruker en ikke-administrert Chromebook

Et bilde som inneholder tekst, skjermbilde, diagram, Operativsystem

Automatisk generert beskrivelse

Figur 4 Anbefaling når skoleeier bruker en PC som ikke er en Chromebook

Et bilde som inneholder tekst, skjermbilde, diagram, design

Automatisk generert beskrivelse



1. Service Data Addendum <https://support.google.com/a/answer/13865350?hl=en> [↑](#footnote-ref-2)
2. Bruk av DPM forutsetter at Chrome nettleser brukes på en administrert Chromebook [↑](#footnote-ref-3)
3. En Chromebook er en type PC som produseres av Google og som bruker operativsystemet ChromeOS [↑](#footnote-ref-4)
4. ChromeOS Data Processor Mode Agreement, punkt 2.1 til 2.6 (under overskrift 1 «Data Processing Terms») og 13 «Definisjoner» <https://www.google.com/chrome/dpchromeos/eu/index.html> [↑](#footnote-ref-5)
5. Bruk av DPM forutsetter at Chrome nettleser brukes på en administrert Chromebook [↑](#footnote-ref-6)
6. En Chromebook er en type PC som produseres av Google og som bruker operativsystemet ChromeOS [↑](#footnote-ref-7)
7. Bakgrunnen for denne anbefalingen er at Google er behandlingsansvarlig for alle personopplysninger som behandles i tilleggstjenestene. Det nasjonale DPIA-prosjektet har vurdert tilleggstjenestene YouTube og Google Søk og Assistent. Imidlertid er Google behandlingsansvarlig for øvrige tilleggstjenester, så denne anbefalingen gjelder for alle tilleggstjenestene, også for de som ikke eksplisitt er vurdert av det nasjonale DPIA-prosjektet.

   <https://support.google.com/a/answer/181865#zippy=%2Cturn-services-on-or-off-for-users%2Cadditional-services-with-an-individual-on-or-off-control> [↑](#footnote-ref-8)
8. Bruk av DPM forutsetter at Chrome nettleser brukes på en administrert Chromebook [↑](#footnote-ref-9)
9. Bakgrunnen for denne anbefalingen er at Google er behandlingsansvarlig for den behandlingen av personopplysninger (både kundedata og service data) som skjer i «optional services», se punkt 1.8 «Optional Services» i ChromeOS Data Processor Mode Agreement (<https://www.google.com/chrome/dpchromeos/eu/index.html>) [↑](#footnote-ref-10)
10. <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/nasjonal-dpia-for-google/bruk-av-tilleggstjenestene-i-google-workspace-for-education/> [↑](#footnote-ref-11)
11. <https://workspace.google.com/intl/en/terms/user_features/> [↑](#footnote-ref-12)
12. For eksempel YouTube, Gmail, Chrome nettleser, Google Maps, Google Translate og Google Calender. [↑](#footnote-ref-13)
13. SaaS, eller Software as a Service, er en modell hvor programvare leveres over internett. Brukere får tilgang til applikasjoner via nettlesere, uten behov for lokal installasjon. Tjenestene hostes i skyen og tilbys ofte på abonnementsbasis. [↑](#footnote-ref-14)
14. Google Workspace for Education Privacy Notice, Intruduction

    (<https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-intro>) [↑](#footnote-ref-15)
15. Service summary for Google Workspace Services (Core services and Other services) (<https://workspace.google.com/terms/user_features/>) [↑](#footnote-ref-16)
16. <https://support.google.com/a/answer/182442?hl=en> [↑](#footnote-ref-17)
17. Nærmere bestemt “kundedata” eller “customer personal data”. Google er behandlingsansvarlig for personopplysningene som også er “service data” og som behandles i kjernetjenestene i Google Workspace for Education. [↑](#footnote-ref-18)
18. Mer persist sagt er kommunen behandlingsansvarlig for “kundedata” i Google Workspace for Education, og Google er databehandler for “kundedata”. For nærmere om dette, se nedenfor under “Googles behandling av personopplysninger”. [↑](#footnote-ref-19)
19. <https://workspace.google.com/intl/en/terms/user_features/> [↑](#footnote-ref-20)
20. Google har rullet ut Data Processor Mode for nettleseren Chrome på en administrert Chromebook (ChromeOS) i Norge våren 2024. Ved å sku på Data Processor Mode for Chrome-produktene, blir skoleeier behandlingsansvarlig alene, og Google blir databehandler. Dette er en funksjonalitet som må skrus på. For nærmere om dette, se nedenfor under “Googles behandling av personopplysninger”. [↑](#footnote-ref-21)
21. Kommunen er skoleeier for offentlig skoler på grunnskolenivå, fylkeskommunen for videregående skoler og øverste ledelse for privatskoler [↑](#footnote-ref-22)
22. General Data Protection Regulation (GDPR) er inkorporert i norsk rett gjennom personopplysningsloven. [↑](#footnote-ref-23)
23. For veiledning om dette valget av primært behandlingsgrunnlag for norske skoleeiere, se prosjektets veiledning om dette publisert på KS.no: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/behandlingsgrunnlag-for-google-workspace-for-education/> [↑](#footnote-ref-24)
24. For forslag til de forskjellige supplerende behandlingsgrunnlagene, se prosjektets forslag til behandlingsprotokoll publisert på KS.no: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/forslag-til-behandlingsprotokoll-for-kjernetjenestene-i-google-workspace-for-education/> [↑](#footnote-ref-25)
25. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-26)
26. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-27)
27. Kjernetjenester, tilleggstjenester eller andre produkter som Chrome nettleser eller operativsystemet ChromeOS [↑](#footnote-ref-28)
28. ChromeOS på Chromebook eller andre operativsystem som Windows på en PC [↑](#footnote-ref-29)
29. <https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info> [↑](#footnote-ref-30)
30. <https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info> og <https://cloud.google.com/terms/cloud-privacy-notice-supplement> [↑](#footnote-ref-31)
31. <https://www.google.com/chrome/dpchromeos/eu/index.html> [↑](#footnote-ref-32)
32. Verifisert i møte med Google 11.03.24 og i e-post sendt 11.03.24 [↑](#footnote-ref-33)
33. Den fulle listen finnes i egen fane i behandlingsprotokollen (se vedlegg X). Dette er en oversikt over alle personopplysninger i løsningen, ikke for hvert enkelt formål, og er ikke knyttet til hvorvidt en behandlingsansvarlig eller en databehandler behandler dem. [↑](#footnote-ref-34)
34. «Personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap», «genetiske opplysninger og biometriske opplysninger» og «helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering» [↑](#footnote-ref-35)
35. Se Tabell 1 Oversikt over behandlingsansvar og databehandleransvar [↑](#footnote-ref-36)
36. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-37)
37. <https://cloud.google.com/terms/cloud-privacy-notice> [↑](#footnote-ref-38)
38. Service data er tilsvarende definert I Chrome-tjenestene (<https://support.google.com/chrome/a/answer/14316192?hl=en-IN&visit_id=638699548975939322-390431313&rd=1>) [↑](#footnote-ref-39)
39. Se formålsbeskrivelsene i Google Cloud Privacy Notice (<https://cloud.google.com/terms/cloud-privacy-notice>). [↑](#footnote-ref-40)
40. Med løsningen mener vi kjernetjenestene og AppSheet i Google Workspace for Education, ChromeOS og Chrome nettleser med Data Processor Mode på en administrert Chromebook [↑](#footnote-ref-41)
41. Se forslag til behandlingsprotokoll for Google Workspace for Education: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/forslag-til-behandlingsprotokoll-for-kjernetjenestene-i-google-workspace-for-education?trk=public_post_comment-text> [↑](#footnote-ref-42)
42. Straffeprosessloven kapittel 15 [↑](#footnote-ref-43)
43. Riksrevisjonsloven § 12 [↑](#footnote-ref-44)
44. GDPR artikkel 5 nr. 1 bokstav a [↑](#footnote-ref-45)
45. [Kunnskapsdepartementet har i brev av 19. juni 2024 adressert til KS at dette er det treffende behandlingsgrunnlaget](https://www.ks.no/contentassets/c3c0b09667ad41e3a0eee2f6bdebe9e9/Svar-pa-henvendelse-om-behandlingsgrunnlag-for-bruk-av-digitale-leringsplattformer.pdf). [↑](#footnote-ref-46)
46. Opplæringsloven § 1-1 og § 11-1 [↑](#footnote-ref-47)
47. Som påpekt av det Danske Datatilsynet i Chromebook-saken 10.juli 2024 (J.nr. 2023-431-0001) [↑](#footnote-ref-48)
48. Se eksempel fra Bergen kommune om hvordan skoleeier kan informere om broken av Google Workspace for Education i skolen: <http://193.161.171.199/innbyggerhjelpen/barnehage-og-skole/grunnskole/grunnskoleopplaring/googleverktoy-i-bergensskolen> [↑](#footnote-ref-49)
49. Jf. Juridika sin lovkommentar til GDPR artikkel 5 [↑](#footnote-ref-50)
50. GDPR artikkel 5 nr. 1 bokstav b [↑](#footnote-ref-51)
51. GDPR artikkel 5 nr. 1 b. [↑](#footnote-ref-52)
52. Opplæringsloven §1-1 [↑](#footnote-ref-53)
53. Rammeverk for grunnleggende ferdigheter, [2.1 Digitale ferdigheter som grunnleggende ferdighet](https://www.udir.no/laring-og-trivsel/rammeverk/rammeverk-for-grunnleggende-ferdigheter/2.1-digitale-ferdigheter/)  [↑](#footnote-ref-54)
54. Opplæringsloven § 28-1 [↑](#footnote-ref-55)
55. GDPR artikkel 6 nr. 4 [↑](#footnote-ref-56)
56. Se Vedlegg 2: Vurdering av om Googles behandling av personopplysninger til egne formål i kjernetjenestene er kompatibelt med skoleeiers opprinnelige formål i opplæringsloven [↑](#footnote-ref-57)
57. GDPR artikkel 5 nr. 1 b. [↑](#footnote-ref-58)
58. GDPR artikkel 5 nr. 1 bokstav c [↑](#footnote-ref-59)
59. Juridkas lovkommentar til GDPR artikkel 5 [↑](#footnote-ref-60)
60. GDPR artikkel 5 nr. bokstav d [↑](#footnote-ref-61)
61. GDPR artikkel 5 nr. 1 bokstav e [↑](#footnote-ref-62)
62. Google bruker i tillegg opp til 180 dager før data garantert er slettet fra alle systemer, jf. REFERANSE [↑](#footnote-ref-63)
63. GDPR artikkel 5 nr. 1 bokstav f [↑](#footnote-ref-64)
64. GDPR artikkel 13-14 [↑](#footnote-ref-65)
65. Se forslag fra Bergen kommune (<https://www.bergen.kommune.no/innbyggerhjelpen/barnehage-og-skole/grunnskole/grunnskoleopplaring/googleverktoy-i-bergensskolen>), Stavanger kommune (<https://www.stavanger.kommune.no/barnehage-og-skole/skole/ikt-i-stavangerskolen/personvern-i-stavangerskolen/>) og Lillesand kommune (<https://sites.google.com/lillesandskolen.no/lillesandskolen-digital/hjem>) for forslag til hvordan dette kan gjøres. [↑](#footnote-ref-66)
66. GDPR artikkel 15 [↑](#footnote-ref-67)
67. <https://services.google.com/fh/files/misc/gsuite_dsr_customer_guide.pdf> [↑](#footnote-ref-68)
68. <https://support.google.com/a/answer/6396995?hl=en> [↑](#footnote-ref-69)
69. GDPR artikkel 16 [↑](#footnote-ref-70)
70. GDPR artikkel 17 [↑](#footnote-ref-71)
71. GDPR artikkel 21 [↑](#footnote-ref-72)
72. GDPR artikkel 18 [↑](#footnote-ref-73)
73. GDPR artikkel 20 [↑](#footnote-ref-74)
74. GDPR artikkel 22 [↑](#footnote-ref-75)
75. <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/innhenting-av-den-registrertes-mening/> [↑](#footnote-ref-76)
76. Kommunen er skoleeier for offentlig skoler på grunnskolenivå, fylkeskommunen for videregående skoler og og øverste ledelse for privatskoler [↑](#footnote-ref-77)
77. General Data Protection Regulation (GDPR) inkorporert i norsk rett gjennom personopplysningsloven [↑](#footnote-ref-78)
78. Helt presist er Google databehandler for «Customer personal data» i kjernetjenestene og for Chrome-tjenester som brukes med Data Processor Mode på en administrert Chromebook. Se DPIAens hoveddokument under overskriftene «Roller og ansvar» og «Googles behandling av personopplysninger» for en detaljert beskrivelse av hvilket ansvar og hvilke roller Google har for behandlingen av personopplysninger, herunder hva «Customer personal data» konkret er. [↑](#footnote-ref-79)
79. Helt presist er Google behandlingsansvarlig for «Service data», og det inkluderer mer enn bare «metadata». For en nærmere beskrivelse av hva som er service data, se DPIAens hoveddokument under overskriften «Service data». I dette notatet brukes vi imidlertid betegnelsen «metadata», da det er Googles behandling av elevers aktivitetsdata som er utfordrende for norske skoleeieres forpliktelser etter opplæringsloven. [↑](#footnote-ref-80)
80. Formålene fremgår av Google Workspace for Education Privacy Notice: <https://workspace.google.com/intl/no/terms/education_privacy/#privacy-police-revamp-your-info> [↑](#footnote-ref-81)
81. Brev fra Kunnskapsdepartementet til KS av 20. September 2024 [↑](#footnote-ref-82)
82. For vår vurdering, se Vedlegg 2: Vurdering av om Googles behandling av personopplysninger til egne formål er kompatibelt med skoleeiers opprinnelige formål i opplæringsloven [↑](#footnote-ref-83)
83. «Security, reliability and availability of the service» [↑](#footnote-ref-84)
84. Brukere under 18 år som bruker Google Workspace for Education [↑](#footnote-ref-85)
85. Brev adressert til KS fra Kunnskapsdepartementet av 19. Juli 2024 <https://www.ks.no/contentassets/c3c0b09667ad41e3a0eee2f6bdebe9e9/Svar-pa-henvendelse-om-behandlingsgrunnlag-for-bruk-av-digitale-leringsplattformer.pdf> [↑](#footnote-ref-86)
86. “Service data is used to deliver and maintain the services that schools and students use, as well as to improve the security and reliability of these services.”, jf. Google Workspace for Education Privacy Notice [↑](#footnote-ref-87)
87. ChromeOS Data Processor Mode Agreement, punkt 13 «Definitions», «Legitimate Business Purposes (ii)» <https://www.google.com/chrome/dpchromeos/eu/no/index.html> [↑](#footnote-ref-88)
88. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/> [↑](#footnote-ref-89)
89. Personopplysninger om hvordan brukerne bruker Google Workspace for Education: Google behandler personopplysninger om hvordan brukerne bruker løsningen. Dette er i stor grad «metadata». Metadata kalles gjerne også diagnostiske data. Det er informasjon som viser hvordan en elev, lærer eller kommunalt ansatt bruker Google Workspace for Education. Dette er opplysninger om programvarefeil, driftsstatus, ytelsesdata, og data fra enhetene GWFE brukes på som enhetsidentifikatorer og IP-adresser. Disse dataene er indirekte identifiserbare personopplysninger. Det betyr at dette er personopplysninger, siden det er mulig for Google å identifisere enkeltindivider. Formålet med Googles behandling er ikke å identifisere den enkelte eleven, læreren eller den ansatte som bruker Google Workspace for Education. Formålet er å forbedre sikkerhet og tilgjengelighet i løsningen, jf. <https://cloud.google.com/terms/cloud-privacy-notice> [↑](#footnote-ref-90)
90. <https://workspaceupdates.googleblog.com/2023/06/improvements-for-client-side-encryption.html> [↑](#footnote-ref-91)