Konsekvensanalyse for Google Chromebooks og G-Suite for Education

Helsingør Kommune

August 2022

Konsekvensanalyse

Den dataansvarlige
Helsingør Kommune
Stengade 59
3000 Helsingør
CVR-nr.: 64502018

Emne for konsekvensanalyse
Google Chromebooks og G-Suite for Education

Dato
August 2022

Indholdsfortegnelse

Behov for udarbejdelse af konsekvensanalyse

Helsingør Kommune sendte den 10. november 2021 til Datatilsynet kommunens risikovurderinger for anvendelsen af Google Chromebooks og G-Suite for Education (Google Workspace for Education) (herefter samlet benævnt "**Tjenesterne**"). Samtidig tilkendegav Helsingør Kommune i samme ombæring over for Datatilsynet, at Helsingør Kommune ikke anvender Google Workspaces Tillægstjenester og på denne baggrund var det Helsingør Kommunes vurdering, at Helsingør Kommune ikke var forpligtet til at udarbejde en konsekvensanalyse vedrørende databeskyttelse.

I Datatilsynets afgørelse af 14. juli 2022 erklærer Datatilsynet sig imidlertid uenig i Helsingør Kommunes vurdering. I afgørelsen nedlægger Datatilsynet således et generelt forbud mod Helsingør Kommunes behandling af personoplysninger via Tjenesterne, indtil Helsingør Kommune har udarbejdet en konsekvensanalyse for behandlingen af personoplysninger som foreskrevet og afgrænset i Datatilsynets afgørelse afsnit 4.2 og 4.3.

Formålet med nærværende konsekvensanalyse og den dertilhørende dokumentation vedlagt som bilag, er dermed at udarbejde de krævede konsekvensanalyser som forudsætning for at få ophævet Datatilsynets forbud.

Overordnede konklusioner

Denne Data Protection Impact Assesmment (”DPIA” eller ”konsekvensanalyse”) identificerer den risiko, der er for de registrerede, når Helsingør Kommune anvender Tjenesterne.

Risikoen tager udgangspunkt i de risici, Datatilsynet beskriver i sin afgørelse af 14. juli 2022:

1. *"Datatilsynet finder, at Helsingør Kommunes risikovurdering ikke til fulde dokumenterer de risikoscenarier, som kan opstå som følge af databehandlerkonstruktionen og de foretagne systemvalg. Det gælder særligt, (i) hvordan de anvendte enheder og programmer reelt håndterer de indsamlede personoplysninger, samt (ii) hvordan Helsingør Kommune kontrollerer Googles adgang til personoplysningerne, herunder særligt ved ordinær brug af Google Chromebooks styresystem og Google Workspaces interaktion med Googles backend i forhold til de muligheder for adskillelse af personoplysninger, som skal ske i henhold til databehandleraftен.*

Det er Datatilsynets opfattelse, at gennemførelse af en konkret risikovurdering og konsekvensanalyse – inden udlevering af it-udstyr til elever og behandling af elevernes oplysninger – er en forudsætning for at kunne etablere og opretholde et passende sikkerhedsniveau. Det skyldes, at et passende sikkerhedsniveau skal ses i lyset af de risici, herunder konsekvenser, som behandlingen af elevernes personoplysninger kan have for de pågældende. Datatilsynet bemærker, at flere af ovennævnte manglende iagttagelser af databeskyttelsesreglerne kunne have være undgået, hvis Helsingør Kommune havde vurderet risiciene ved behandlingen og truffet passende foranstaltninger i lyset af disse risici."

2. *"Datatilsynet har imidlertid lagt til grund, at Helsingør Kommune ved sin vurdering af denne risiko alene anser risikoen for, at databehandleren handler i strid med databehandleraftalen som hypotetisk frem for decideret påregnelig.*

Datatilsynet finder, at Helsingør Kommune – i sin vurdering af denne risiko – ikke har dokumenteret, at Helsingør Kommune i denne situation benytter en databehandler, der kan stille de fornødne garantier for, at vedkommende vil opfylde kravene i databeskyttelsesforordningen, jf. forordningens artikel 24, jf. artikel 28, stk. 1.

Datatilsynet har lagt særlig vægt på, at der ville være tale om et indgribende rettighedstab for de registrerede, hvis den omhandlede risiko materialiserede sig, og at kommunen i sin risikovurdering ikke har anført reelt afhjælpende tekniske eller organisatoriske foranstaltninger med henblik på at mitigere denne risiko. Det er herunder Datatilsynet opfattelse, at Helsingør Kommunes henvisning til, at kommunen har tillid til, at leverandøren generelt overholder aftalen, ikke udgør en fornøden nedbringelse af denne risiko."

Helsingør Kommune har for at imødekomme de af Datatilsynet rejste spørgsmål foretaget følgende:

- Der er vedlagt dokumentation for, at kommunen har valgt indstillinger, der sikrer, at kommunen alene anvender Kernetjenester, jf. bilag 2. Disse indstillinger indebærer, at Google alene har en rolle som databehandler, og at Google alene må handle inden for kommunens instruks og dermed ikke lovligt kan varetage egne formål.
- Der er indhentet dokumentation i form af uafhængige tredjepartserklæringer for, at Google som databehandler ikke varetager egne formål, jf bilag 3. Denne dokumentation sikrer, at en uafhængig tredjepart har revideret Googles behandling af personoplysninger som databehandler, og derved at Google som databehandler handler inden for den givne instruks, og at Google ikke varetager egne formål i strid med databehandleraftalen.
- Denne konsekvensanalyse giver et overblik over de undersøgelser og overvejelser, som kommunen har foretaget i anledning af de rejste spørgsmål, samt vurderer, om behandlingen på baggrund af ovenstående indebærer en høj risiko.

På baggrund af foretagne foranstaltninger er det kommunens vurdering, at Helsingør Kommune har begrænset risikoen for de registreredes rettigheder til et acceptabelt niveau.

Indledning

Indledning

En konsekvensanalyse vedrørende databeskyttelse vurderer konsekvenser for fysiske personers privatliv, rettigheder og frihedsrettigheder som følge af behandling af personoplysninger. Konsekvensanalysen hjælper med at identificere og begrænse den risiko, der for de registrerede er forbundet med en given behandlingsaktivitet.

Denne konsekvensanalyse er udformet med henblik på at opfylde de krav, som databeskyttelsesforordningen stiller til indholdet af en konsekvensanalyse vedrørende databeskyttelse. Konsekvensanalysens tager endvidere udgangspunkt i den tidligere Artikel-29 Gruppes vejledning om "Data Protection Impact Assessment" (DPIA, på dansk: "risikovurdering og konsekvensanalyse"), som er anerkendt af Det Europæiske Databeskyttelsesråd (EDPB) henhold til forordning (EU) 2016/679", samt Datatilsynets og Justitsministeriets vejledning om Konsekvensanalyse fra marts 2018.

Denne konsekvensanalyse er udarbejdet for at beskrive de behandlinger og risici, som er relaterer sig til Helsingør Kommunes brug af Tjenesterne i forhold til:

1. Hvordan de anvendte enheder og programmer i Tjenesterne reelt håndterer de indsamlede personoplysninger, samt hvordan Helsingør Kommune kontrollerer Googles adgang til personoplysningerne, herunder særligt ved ordinær brug af Google Chromebooks styresystem og Google Workspaces interaktion med Googles backend i forhold til de muligheder for adskillelse af personoplysninger, som skal ske i henhold til databehandleraften.

2. Hvordan Helsingør Kommune kan sikre, at der er de fornødne garantier for, at Google vil opfylde kravene i databeskyttelsesforordningen, jf. forordningens artikel 24, jf. artikel 28, stk. 1, og dermed ikke behandle personoplysningerne til utilsigtede formål.

I konsekvensanalysen beskriver Helsingør Kommune endvidere de mitigerende foranstaltninger, Helsingør Kommune har truffet for at imødekomme disse risici.

Beskrivelse af behandlingen

Beskrivelse af behandlingsaktiviteterne

1. Behandlingernes karakter, omfang, sammenhæng og formål

Til brug for undervisningen, anvendes en digital læringsplatform baseret på Google Chromebooks med Workspace for Education Standard. Platformen muliggør deling af dokumenter mellem elever og lærere og gør det generelt muligt at samarbejde i klassen og på tværs af klasser.

Oplysninger indeholdt i Tjenesterne relaterer sig til elever og lærere.

Der behandles som udgangspunkt hverken følsomme oplysninger, CPR-numre eller oplysninger om strafbare forhold relateret til eleverne eller lærerne via systemerne. Det kan dog ikke udelukkes, at disse oplysninger kan indgå i e-mails fra lærerne eller via andet materiale, og der er også givet instruktion til lærerne, som skal forebygge dette. Dette må derfor anses som særdeles usædvanligt og utilsigtet.

Der er tale om personoplysninger relateret til elever, der generelt nyder en særlig beskyttelse i henhold til databeskyttelsesreglerne, da elever i den undervisningspligtige alder anses for en sårbar gruppe af personer henset til elevernes alder.

Helsingør Kommune arbejder målrettet med at forberede børn og unge til fremtidens samfund og arbejdsmarked som led i kommunens løsning af opgaver med at tilbyde undervisning. Alle klassetrin arbejder dagligt med it som en integreret del af undervisningen i alle fag for at understøtte den faglige læring i fagene og elevernes digitale færdigheder, hvilket understreger nødvendigheden af behandlingen.

For at sikre skolerne og eleverne en fremadrettet bæredygtig model for it-understøttet undervisning har kommunen valgt Tjenesterne som kommunens undervisningsplatform.

2. Personoplysninger, modtagere og det tidsrum, personoplysningerne opbevares i

Der behandles følgende typer af personoplysninger, på følgende måde, for at løse undervisningsopgaven.

- *Personoplysninger* Navn, Unilogin, klasse, mailadresse (brugernavn, unilogin + domæne), skole, materiale produceret, mails afsendt og billeder (profilbilleder eller i materiale).
- *Modtagere* Internt: Lærere, administratorer, elever. Eksternt: Wizkids og Google som databehandler
- *Tidsrum for opbevaring* Data opbevares indtil en elev enten skifter kommune – eller tre måneder efter eleven går ud efter endt skolegang (celle J9 i risikoanalysen).

3. Systematisk beskrivelse af behandlingsaktiviteten

KL beskriver den generelle behandlingsaktivitet for skoleområdet således:

"Behandling af personoplysninger sker med henblik på tilrettelæggelse af skoleåret herunder elevvurderinger, trivselsmålinger, erstatningskrav fra elever og eleverklæringer.

Der behandles desuden personoplysninger i forbindelse med skolebestyrelser, herunder medlemmer og vederlag til medlemmer og rådgivende organer, herunder elevråd, forældreråd og pædagogiske råd"

Yderligere:
Til brug for undervisningen, anvendes en digital læringsplatform baseret på Google Chromebooks med Workspace for Education Standard – Tjenesterne. Platformen muliggør deling af dokumenter mellem elever og lærere og gør det generelt muligt at samarbejde i klassen og på tværs af klasser.

Fra ”vugge til grav” kan dette systematisk fremstilles således:

1. Behandling af fysisk maskine

    a. Indkøb af fysisk maskine/Chromebook
    b. Udlevering til elev/forældre
    c. Tilbagelevering fra elev/forældre
    d. Genudlevering (efter powerwash)/destruktion

2. Kontooprettelse og –administration af kommunens overordnede Googlekonto

    a. Oprettelse og konfiguration af konto (fx hvor opbevares data)
    b. Udvælgelse af faciliteter (kun core)
    c. Backup
    d. Logning af aktiviteter (elever, lærere og admins)

3. Brugeradministration og systemovervågning

    a. Oprettelse af klasser (automatisk via TEA)
    b. Oprettelse af elever (automatisk via TEA)
    c. Oprettelse af aliasser for navnebeskyttede elever (manuelt. Indtil da er de i venteposition).
    d. Rapportering af elever og læreres brug af GWfES
    e. Når elev forlader Helsingør Kommune folkeskole, registreres det i TEA og elevens data slettes efter 3 måneder (automatisk)

4. Lærer-aktiviteter

    a. Oprettelse og opbevaring af lektieplaner, opgaver, spørgeskemaer (Classroom, Drev)
    b. Evaluering af opgaver (Classroom, Drev)
    c. Chat (Hangouts, Meet)

5. Elev-aktiviteter

    a. Oprettelse og opbevaring af opgaver (Drev), læsning af lektieplan
    b. Skrive og aflevere opgave og læse evaluering
    c. Chat (Hangouts, Meet)

4. **De aktiver, som personoplysningerne er afhængige af (hardware, software, netværk, personer, papir, papirforsendelseskanaler), identificeres.**

- Chromebook (browser er ”klient” for cloudløsning)
- Workspace for Education Standard (opsat som datacenter Europa) (del af cloudløsning)
- Googles datacenter (del af cloudløsning)
- Skolenetværk
- Admins (kommunens it-skolesupportere)
- Wizkids
- Skolesekretærer (TEA elevadministrationsplatform, aliasser)
- Lærere
- Elever

Risici og mitigerende for-anstaltninger

Vurdering af risici og beskrivelse af foranstaltninger, der imødegår disse

Den udarbejdede risikovurdering er vedlagt som **bilag 1** til denne konsekvensanalyse under rækkerne ”privacy by design” og ”brug af data til utilsigtede formål”. Dokumentationen for de implementerede mitigerende foranstaltninger er vedlagt som **bilag 2 og 3**.

Lovlighed og de registrere-des rettigheder

Behandlingernes lovlighed

I dette afsnit indgår vurdering af, om behandlingsaktiviteterne er nødvendige og lovlige. Endvidere beskrives foranstaltninger, der bidrager til de registreredes rettigheder.

1. Baggrund

Det fremgår af Datatilsynets afgørelse af 14. juli 2022, at kommunen ikke i tilstrækkelig grad har sikret Googles rolle som databehandler i forhold til Googles adgang til personoplysningerne, herunder særligt ved ordinær brug af Google Chromebooks styresystem og Google Workspaces interaktion med Googles backend, samt at kommunen ikke har tilvejebragt de fornødne garantier for, at Google vil opfylde kravene i databeskyttelsesforordningen, jf. forordningens artikel 24, jf. artikel 28, stk. 1.

Det er kommunens vurdering, at de foranstaltninger, der er beskrevet i den i oktober 2021 udarbejdede risikovurdering, sædvanligvis vil være tilstrækkelige til at dokumentere, at Google alene agerer som databehandler og i overensstemmelse med denne rolle.

Det bemærkes, at kommunen ikke i øvrigt er bekendt med praksis fra Datatilsynet, som i andre tilfælde stiller krav om en tilsvarende dokumentation i forhold til brugen af en databehandler, som ikke har en "forhistorie" med at agere uden for rammerne af databehandlerrollen.

I Datatilsynets afgørelse af 14. juli 2022 er dette kritiske standpunkt over for Google som databehandler, så vidt kommunen kan vurdere, ikke er nærmere underbygget. Datatilsynet har imidlertid mundtligt efter afgørelsen henvist til, at praksis fra Holland sår tvivl om, hvorvidt Google behandler personoplysninger fra Tjenesterne på undervisningsområdet til egne, kommercielle formål, som er uvedkommende og usaglige i forhold til brugen af Tjenesterne på dette område.

Kommunen har derfor som led i arbejdet med denne konsekvensanalyse også tilvejebragt oplysninger om, hvilke kritikpunkter der har været mod Google i den hollandske sag[1]. Det drejer sig nærmere om følgende overordnede spørgsmål pr. februar-marts 2021:

- Manglende formålsbegrænsning af Customer Data
- Manglende formålsbegrænsning af Diagnostic Data
- Manglende gennemsigtighed i forhold til Customer Data
- Manglende gennemsigtighed i forhold til Diagnostic Data
- Manglende hjemmel for Google til at behandle personoplysninger som dataansvarlig
- Manglende kontrol over den måde, Google behandler personoplysninger på
- Manglende kontrol med behandlingen af personoplysninger hos Googles underleverandører
- Manglende mulighed for de registrerende til at få indsigt

Kommunen forstår den hollandske DPIA således, at disse spørgsmål i det væsentlige drejer sig om udfordringer knyttet til, at Google helt eller delvist var dataansvarlig, at Google krævede ret til at behandle personoplysninger som databehandler som led i sine ydelser til formål, som var vanskeligt forenelig med Tjenesterne, og at behandlingen af bl.a. cookie- og telemetrioplysninger indebar en behandling, som var ikke-gennemsigtig.

[1] Se DPIA Google G Suite Enterprise, Data protection impact assessment on the processing of personal data on 3 platforms with the Chrome browser and as installed apps, Version 1 – for consultation with the Dutch DPA, 9 July 2020, with update on 12 February 2021, udarbejdet af Ministry of Justice and Security Strategic Vendor Management Microsoft (DPIA).

Kommunen har i bilag 4 for fuldstændighedens skyld vurderet en række problemstillinger, der blev rejst i den hollandske sag. Denne gennemgang viser, at disse problemstillinger har meget begrænset relevans i forhold til Helsingør Kommunes brug af Tjenesterne, da roller og opsætning er afgørende forskellig. En væsentlig årsag hertil er bl.a., at kommunen alene benytter Kernetjenesterne, og at Google derfor alene har en rolle som databehandler og dermed alene behandler personoplysninger til kommunens formål. Google har entydigt i denne sag (bl.a. i databehandleraftalen og den vedlagte dokumentation i bilag 2 og 3) vedkendt sig denne rolle med de begrænsninger, der følger heraf.

Disse problemstillinger er således ikke relevante i denne sag, fordi Google i denne sag alene agerer som databehandler og ikke behandler personoplysninger til egne formål eller kræver adgang til at behandle personoplysninger til mere generelle formål, som ikke er afgrænset til kommunens interesse i behandlingen.

Kommunen har derfor valgt at fokusere de mitigerende foranstaltninger på at dokumentere, at Google alene er databehandler og alene behandler personoplysninger som databehandler til de formål, som følger af kommunens instruks, når Google behandler personoplysninger som databehandler for kommunen.

En mere skematisk gennemgang af de potentielle problemstillinger angivet i den Hollandske afgørelse og dertilhørende DPIA med dertilhørende angivelse af, hvordan Helsingør Kommune har mitigeret disse problemstillinger, er angivet som **bilag 4** til denne konsekvensanalyse.

Disse mitigerende foranstaltninger er følgende:

- Der er vedlagt dokumentation for, at kommunen har valgt indstillinger, der sikrer, at kommunen alene anvender Kernetjenester, jf. bilag 2. Disse indstillinger indebærer, at Google alene har en rolle som databehandler, og at Google alene må handle inden for kommunens instruks og dermed ikke lovligt kan varetage egne formål.
- Der er indhentet dokumentation i form af uafhængige tredjepartserklæringer for, at Google som databehandler, ikke varetager egne formål, jf bilag 3. Denne dokumentation sikrer, at en uafhængig tredjepart har revideret Googles behandling af personoplysninger som databehandler, og derved at Google som databehandler handler inden for den givne instruks, og at Google ikke varetager egne formål i strid med databehandleraftalen.
- Denne konsekvensanalyse giver et overblik over de undersøgelser og overvejelser, som kommunen har foretaget i anledning af de rejste spørgsmål, samt vurderer, om behandlingen på baggrund af ovenstående indebærer en høj risiko.

Det fremgår af risikovurderingen, at behandlingen i forhold til de registreredes rettigheder og frihedsrettigheder med disse mitigerende foranstaltninger har en mellemrisiko, som kommunen kan acceptere. Det bemærkes i den forbindelse, at risikoen scores til 8, som er den laveste score i kategorien for mellemrisiko. Det bemærkes endvidere, at den primære grund til, at risikoen ikke er lavere, er, at der er tale om behandling af oplysninger om skoleelever i den undervisningspligtige alder, og at børn nyder en særlig beskyttelse i de databeskyttelsesretlige regler. Risikoen for skoleelever er herved mitigeret til et acceptabelt niveau.

Det er således samlet set kommunens vurdering, at de to identificerede risici i Datatilsynets afgørelse er mitigeret til at passende, acceptabelt niveau.

2. Grundbetingelser og lovlig behandling

For at kunne behandle personoplysninger i Tjenesterne som led i løsningen af den lovbestemte undervisningsopgave skal kommunen have et juridisk grundlag for behandling af personoplysninger.

Selvom det følger af folkeskoleloven, at kommunen skal tilbyde undervisning til børn i den undervisningspligtige alder – og behandling af personoplysninger er en forudsætning herfor – er det kommunens vurdering, at folkeskoleloven ikke alene udgør hjemlen for denne behandling end det egentlige hjemmelsgrundlag.

Som ovenfor beskrevet behandles der i Tjenesterne som udgangspunkt alene almindelige ikke-fortrolige personoplysninger. Fortrolige eller følsomme oplysninger vil således forventeligt ikke blive behandlet, og hvis det sker, er det usædvanligt, usystematisk og utilsigtet. Denne konsekvensanalyse fokuserer derfor på den tilsigtede behandling af almindelige personoplysninger.

Denne tilsigtede behandling sker til løsning af opgaver i samfundets interesse og som led i offentlig myndighedsudøvelse, som kommunen er pålagt (undervisningsforpligtelsen). Det indebærer, at databeskyttelsesforordningens artikel 6, stk. 1, litra e, udgør behandlingsgrundlaget for behandlingen af personoplysninger i Tjenesterne.

Datatilsynet har i forhold til principperne for behandling af personoplysninger anført, at kommunen ikke har påvist, at behandlingen er lovlig, rimelig og gennemsigtig. Dette skyldes ifølge afgørelsen, at kommunen

- Ikke har inkluderet de risikoscenarier, som kan opstå som følge af databehandlerkonstruktionen og de foretagne systemvalg i sin risikovurdering
- Ikke har foretaget tilstrækkelig afprøvning af omfang og virkemåde af den valgte hardware og benyttede software
- Ikke kan dokumentere, hvordan kommunen kontrollerer Googles adgang til personoplysningerne, herunder særligt ved ordinær brug af Google Chromebooks styresystem og Google Workspaces interaktion med Googles backend i forhold til de muligheder for adskillelse af personoplysninger, som kan ske i henhold til databehandleraften

Som ovenfor anført er der nærmere redegjort for, hvorfor disse problemstillinger har begrænset relevans i denne sag. Som også anført, har kommunen endvidere vedlagt dokumentation, som nærmere beskriver, hvorfor Google efter kommunens vurdering ikke har en realistisk mulighed for at udviske grænsen mellem sin rolle som databehandler og Googles egne formål, som adskiller sig fra at levere ydelser til kommunen, jf. bilag 2 og 3.

Kommunen forstår gældende ret således, at kontraktuelle forpligtelser også kan udgøre mitigerende foranstaltninger. Kommunen vil derfor endvidere for god ordens skyld også henvise til databehandleraftalen med Google[2] , hvor følgende er anført:

"5.2 Scope of Processing.
5.2.1 Customer's Instructions. Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide, secure, and monitor the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement (including this Data Processing Amendment); and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment (collectively, the "Instructions").
5.2.2 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by European Law.
5.2.3 Instruction Notifications. Google will immediately notify Customer if, in Google's opinion: (a) European Law prohibits Google from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Google is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. This Section does not reduce either party's rights and obligations elsewhere in the Agreement.

[2] Data Processing Amendment to Google Workspace and/or Complementary Product Agreement, July 7, 2022.

5.3. Additional Products. If Google at its option makes any Additional Products available to Customer in accordance with the Additional Product Terms, and if Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services."

Som tidligere beskrevet anvender kommunen ikke Tillægstjenesterne, og databehandleraftalen er således meget klar i forhold til, at Google alene har en rolle som databehandler, og at Google alene kan behandle personoplysninger til kommunens formål.

Den samlede mængde af mitigerende foranstaltninger i form af databehandleraftalen med Google, kommunens indstillinger m.v., jf. bilag 2, Googles supplerende dokumentation, jf. bilag 3, og vurderingen af relevansen af den hollandske sag, Datatilsynet har henvist til, jf. bilag 4, indebærer, at der efter kommunens vurdering er tilstrækkelig dokumentation til, at kommunen har påvist, at behandlingen er lovlig, rimelig og gennemsigtig.

Kommunen bemærker i den forbindelse endvidere, at denne dokumentation ikke skal vurderes i et tomrum. Det forhold, at Tjenesterne utvivlsomt er omfattet af databeskyttelsesforordningens anvendelsesområde og Datatilsynets kompetence, de aftalte forpligtelser for Google i kraft af databehandleraftalen og kommunens instruks og Googles dokumentation for, at Google lever op til disse forpligtelser, sammenholdt med en mere generel aftaleretlig forpligtelse for Google over for kommunen fører samlet til, at Google ved at behandle oplysninger i strid hermed ville udsætte sig for en meget stor risiko for bøder og erstatningskrav.

Ud over princippet om lovlig behandling vil kommunen også særligt henvise til princippet om dataminimering. I risikovurderingen er dette behandlet som et særskilt spørgsmål i række 11, og det er kommunens vurdering, at også dette princip overholdes.

3. De registreredes rettigheder

Kommunen har udarbejdet privatlivspolitikker og procedurer, som bidrager til at sikre de registreredes rettigheder. Kommunen oplyser således de registrerede om behandlingen. Kommunen vil udover information i privatlivspolitikken på hjemmesiden fremsende fornyet oplysningsbrev til medarbejderne.

Kommunen har endvidere procedurer for håndtering af indsigtsanmodninger samt anmodninger fra de registrerede om berigtigelse og sletning m.v. Procedurerne sikrer, at kommunen besvarer en anmodning fra en registreret uden unødig forsinkelse og senest efter en måned, medmindre anmodningen er kompliceret, hvorefter svarfristen vil kunne forlænges med yderligere to måneder.

Særligt i forhold til håndteringen af anmodninger fra de registrerede er kommunens procedurer understøttet af databehandleraftalen med Google, hvor følgende er anført:

"9.2 Data Subject Requests.
9.2.1 Responsibility for Requests. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Google's Data Subject Request Assistance. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:
a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance."

Det er på denne baggrund kommunens vurdering, at brugen af Tjenesterne vil kunne sikre de registreredes rettigheder.

Monitorering, opdatering, de registreredes synspunkter og forelæggelse for DPO

Monitorering og opdatering

Konsekvensanalysen gennemgås mindst en gang om året, og gennemgås i øvrigt, hvis det vurderes ud fra en risikobaseret tilgang, at der kan være ændringer af betydning vedrørende de omfattede behandlingsaktiviteter.

De registreredes synspunkter

Som led i konsekvensanalysen skal den dataansvarlige, hvis det relevant, indhente de registreredes eller deres repræsentanters synspunkter. Disse synspunkter kan indhentes ved hjælp af forskellige midler afhængigt af situationen. Det er op til den dataansvarlige at vælge, hvordan dette skal foregå. Der kan fx anvendes fokusgrupper, spørgeskemaer, forelæggelse for medarbejdernes repræsentanter eller høring af en relevant organisation.

Hvis den dataansvarliges endelige afgørelse afviger fra de registreredes synspunkter, skal myndighedens eller virksomhedens begrundelse for at gå videre eller ikke beskrives.

Denne konsekvensanalyse er netop baseret på en klage fra en forælder og Datatilsynet afgørelser. Helsingør Kommune har dermed ikke på baggrund af en faglig vurdering fundet det relevante at inddrage yderligere synspunkter fra de registrerede eller deres repræsentanter.

Forelæggelse for DPO

Denne konsekvensanalyse har været forelagt for kommunens DPO, Bech-Bruun, i august 2022.

Bilag 1 – Risikovurderinger

Dette bilag 1 udgør den reviderede risikovurdering i vedhæftede mappe på grundlag af Datatilsynets afgørelse.

Bilag 2 – Dokumentation for indstillinger

Dette bilag 2 viser kommunens indstillinger for at mitigere risikoen for de registrerede i vedhæftede mappe. Den samlede dokumentation udgøres af flere hundrede screenshots. Kommunen har imidlertid på grund af antallet alene vedhæftet screenshots for én skole for at illustrere disse indstillinger, men hvis Datatilsynet ønsker at modtage alle disse screenshots, sender kommunen gerne dette.

Bilag 3 – Dokumentation for at Google som databehandler ikke varetager egne formål

1. ISO 27001-certificering

   Google er ISO 27001-certificeret[3]. Denne certificering af Google som organisation indebærer et krav om, at Google efterlever gældende lovgivning og krav. Det drejer sig bl.a. om følgende

   • *Afsnit 4.2* Forståelse for interessenters behov og forventninger, hvor det af litra b fremgår, at organisationen skal fastlægge interessenters krav, som er relevante for informationssikkerhed. Kommunen lægger til, at dette også omhandler krav i forbindelse med indgåede kontrakter, jf. nærmere nedenfor.
   • *Anneks A: A5.1* Retningslinjer for styring af informationssikkerhed, hvoraf det fremgår, at formål er *"at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter"*.
   • *Anneks A: A18.1* Overensstemmelse med lov- og kontraktuelle krav, hvoraf det fremgår, at formålet er *"at forhindre [organisationens] overtrædelse af lov-, myndigheds- eller kontraktskrav i relation til informationssikkerhed og andre sikkerhedskrav"*.

   De nævnte krav skal efterleves for at opfylde betingelserne for at opnå certificering.

2. Googles supplerende garantier og oplysninger, som er indsat nedenfor:

Customer Questions	Google Responses
1) Can Google guarantee that Google does not, when it acts as data processor for Helsingør Kommune, process Customer Data or other personal data for which Helsingør Kommune is data controller for marketing purposes?	Our customers' data is theirs, not Google's. Google only processes Customer Data in accordance with the contracts with customers, and specifically commits in the Google Workspace for Education Terms of Service that Google does not process Customer Data for its own purposes, including for advertising purposes. Google's commitment to process Customer Data only in accordance with customer contracts and for no other purpose is also subject to audit by an independent third party auditor (currently, EY). For example, Google's latest SOC 2 report describes various tests performed by EY regarding the Control 22 description "*The organization only processes customer data in accordance with the applicable data processing terms and does not process customer data for any other purpose*", with no deviations being noted. Please see our response to question 6 for further instructions on how to download our SOC 2 report and other compliance-related resources. For users in primary and secondary schools, Google does not use any user personal information (or any information associated with a Google Workspace for Education Account) to target advertising, whether in Google Workspace Core Services (such as Gmail or Calendar), Chrome Education Upgrade, or

[3] Der henvises nærmere til Google Cloud: Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.1) af 19.8.2019, https://workspace.google.com/terms/10292019/dpa_terms.html, Anneks A: A18.1.

	other Google services accessed while using a Google Workspace for Education account.
2) Can Google confirm that when the settings in Google Workspace and Google Chromebooks are set to make sure that only Core Services are used and available and that Additional Service are disabled, then Google will only process personal data as data processor and not for other purposes than the ones instructed by Helsingør Kommune?	When Additional Services are disabled and only Workspace Core Services are used: • Google processes Customer Personal Data as a processor and only under your instructions. As mentioned in our response to question 1, we do not process Customer Data (including Customer Personal Data) for our own purposes (including advertising purposes), and this commitment is subject to audit by our independent third party auditor. • Google processes Service Data as a controller for limited purposes in accordance with our Google Cloud Privacy Notice. As per our Notice, Service Data is the personal information we collect or generate during our provision and administration of the Google Workspace services, excluding Customer Data. We have provided more information about the purposes for which we process Service Data in our response to question 3 below.
3) Does Google as data processor process Diagnostic Data, including telemetry, cookies, etc. for other purposes than the one instructed by Helsingør Kommune?	If "Diagnostic Data" (as described in your question) contains personal data, then that is classified as "Service Data" when it has been collected or generated through the Workspace Core Services. Google may process this Service Data as a controller for the limited purposes described in section "Why we process data" of the Google Cloud Privacy Notice.
4) When Google provides online technical support, can such support be initiated by Google on its own initiative, or will it only be initiated on request by Helsingør Kommune?	We understand "online technical support" to refer to our Technical Support Services for Google Workspace. As explained in our Google Workspace Subprocessors URL, Technical Support Services are "customer-initiated", and would not be initiated by Google since, by their nature, Technical Support Services are dependent on a request from a customer. This article describes how your administrator can contact Google directly for support.
5) Will it in the near future be possible as a general Google feature to opt out of online technical support from unsecure third countries?	First, we would like to clarify that each Subprocessor we engage goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy. We provide the same contract commitments for all Subprocessors in Section 11 of our Data Processing Amendment. As noted in our response to question 4, we understand "online technical support" to refer to our Technical Support Services for Google Workspace.

	Google continues to heavily invest on features to offer enhanced geo-location control over data. At the moment, to be able to offer 24/7 Technical Support Services as part of the 'follow the sun' support model, these services may be provided from locations outside the EU/EEA. However, as stated in our Google Workspace Subprocessors URL: • each Third Party Subprocessor providing Technical Support Services "only has access to Customer Data if Customer explicitly elects to share Customer Data in the course of a support case (e.g. screenshots)". • Google Group Subprocessors providing Technical Support Services "may require limited, authorized access to Customer Data to respond to Customer-initiated requests". Our customers can rely on our Standard Contractual Clauses (as well as our supplementary measures) as a legal mechanism to meet their compliance needs with regards to the transfer of Customer Personal Data (i.e. the personal data comprised in Customer Data) outside the EU.
6) If possible, Helsingør Kommune will appreciate any documentation, including documentation from third parties such as audits, etc., to support the answers provided above.	**Compliance Resources** Our Compliance Reports Manager provides you with easy, on-demand access to critical compliance resources. Please go to https://cloud.google.com/security/compliance/compliance-reports-manager/ and sign-in with your Google Workspace account to see all the resources available to you. You may specifically want to review our: • ISO certification (27001, 27017, 27018, 27701) • SOC 1, 2 and 3 audit reports As indicated above, we are also gathering other talking points and resources that may be useful to support your Data Protection Impact Assessment. We will share these with you early next week. **Other Useful Resources** Chromebooks 1. ChromeOS 1-Pager 2. ChromeOS (ISO 27001, 27017/18, SOC1) • Chrome Enterprise Upgrade • Chrome Education Upgrade • Chrome Nonprofit Upgrade • Chromebook Enterprise Our Guide on how to customize and implement Google Workspace (including Privacy best practices) 1. Google Workspace for EDU data protection implementation guide

	Data Processing Terms & Customer Data Processing Commitments 2.Google Workspace Service-Specific Terms 3. Data Processing Amendment to Google Workspace and/or Complementary Product Agreement 4. Google's adherence to the EU GDPR Code of Conduct Service Data 5. Google Cloud Privacy Notice 6. Google's commitment on processing of Service Data Data Transfers and Schrems II ruling 7. Transfer Impact Assessment: How to Assess the Risk of Cloud EEA-U.S.Data Transfers Using European Data Protection Board's Recommendations (dokumentet er udeladt, da dokumentet i sin helhed, af Google anses som fortroligt.) 8. Google Cloud's implementation of the New EU Standard Contractual Clauses 9. Safeguards for international data transfers with Google Cloud 10. Reaffirming Google Cloud's commitments to EU businesses in light of the EDPB's Recommendations 11. Google Cloud welcomes EU's new Standard Contractual Clauses for cross-border data transfers Additional Privacy Resources 12. Privacy Resource Center 13. Google Transparency Report 14. Enhancing our privacy commitments to customers (blog post 2020)

3. Tredjepartserklæringer, jf. vedhæftede mappe.

Bilag 4 – Skematisk gennemgang af problemstillinger og implementerede mitigerende foranstaltninger

Manglende formålsbegrænsning for kundedata	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Google ønsker ikke udtrykkeligt at udelukke den videre behandling af Helsingør kommunes personoplysninger i rollen som selvstændig dataansvarlig med det formål at afsløre ulovlig aktivitet uden først at indhente forudgående skriftlig godkendelse fra Kunden. Google leverer ikke kontrolelementer til at tilsidesætte eller undgå scanning, filtrering eller anden analyse af spam og malware, hvor det er kommercielt, teknisk og rimeligt muligt.	Google er alene databehandler, da kommunen kun bruger Kernetjenester, og Google er således ikke dataansvarlig. Denne problemstilling er ikke relevant. (Dette er bl.a. bekræftet af databehandleraftalen og af ISO 27001-certificeringen.) Eleverne har ikke adgang til e-mailfunktionen. En kontrol af lærernes brug af e-mail er slået til, herunder at vedhæftede filer ikke er skadelige, og at indkommende e-mails med vedhæftninger åbnes i en sandkasse. Denne problemstilling er ikke relevant.
Google behandler personoplysninger som selvstændig dataansvarlig med henblik på markedsføring, profilering, dataanalyser og markedsundersøgelser.	Risikoen er mitigeret, da Google kontraktuelt har forpligtet sig til ikke at behandle oplysninger til disse formål, da kommunen alene anvender Kernetjenester, jf. databehandleraftalens pkt. 5.
Der er risiko for, at maskinel indlæring til forbedring af indholdet af stave- og grammatikdata ikke er begrænset til Helsingør Kommunes eget domæne	Kommunen er dataansvarlig, dvs. behandling af tekster m.v. sker til kommunens formål. Herudover er metadatarapporteringer slået fra, så Google har adgang til identificerbare personoplysninger i forbindelse med maskinel læring.
Når Google anonymiserer oplysninger og efterfølgende anvender disse, er anonymiseringen ikke tilstrækkelig.	Google har oplyst, at anonymiseringen sker som foreskrevet i WP29-vejledningen.
Manglende formålsbegrænsning for diagnostiske data	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Google behandler diagnosticeringsdata (herunder telemetridata), supportdata, feedbackdata og alle indstillinger/konfigurationer valgt af Enterprise-kunder til en lang række egne formål.	Diagnosticeringsdata og feedback er slået fra som dokumenteret i bilag 2.

Google følger ikke de anbefalede foranstaltninger til at inkludere Chrome Enterprise i G Suite Enterprise-tilbuddet eller inkludere separat Chrome-browser med "databehandler" på Android-enheder og Chromebooks (hvor det ikke er realistisk at installere en anden browser).	Google er alene databehandler, da kommunen kun bruger Kernetjenester, og Google er således ikke dataansvarlig. Denne problemstilling er ikke relevant. (Dette er bl.a. bekræftet af databehandleraftaler og ISO 27001-certificeringen.)
Intet juridisk grundlag for Google	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Google ønsker ikke at blive databehandler for diagnostiske data, supportdata og feedbackdata.	Google er databehandler, og diagnosticeringsdata og feedback er slået fra som dokumenteret i bilag 2.
Med hensyn til det juridiske grundlag for indsamling af cookie- og telemetridata fra slutbrugerenheder oplyser Google, at Google anvender cookies og lignende teknologier, der er nødvendige for, at tjenesterne kan fungere.	Diagnosticeringsdata og feedback er slået fra som dokumenteret i bilag 2. Herudover er Google alene databehandler, og det juridiske grundlag er derfor fastlagt af kommunen.
Standardindstillinger for beskyttelse af personoplysninger, som ikke fremmer integriteten	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Det er ikke muligt at ændre Googles standardindstillinger, hvorved Helsingør Kommune ikke kan beskytte personoplysningerne via privacy by default.	Kommunens valg af indstillinger fremmer privacy by design som dokumenteret i risikovurderingen og den vedlagte dokumentation for indstillinger, og kommunen finder de foreliggende muligheder for indstillinger i Tjenesterne tilstrækkelige, jf. bilag 1 og 2.
Manglende kontrol underdatabehandlere	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Det er ikke muligt at kontrollere Googles underdatabehandlere via audits eller tilsvarende.	Google er databehandler for Helsingør Kommune i denne sag, og kommunen fører tilsyn med Google som databehandler og i fornødent omfang med underdatabehandlere svarende til de interne procedurer herfor. Kommunen finder samlet, at databehandleraftalen giver tilstrækkelig mulighed herfor.
Manglende indsigt i personoplysninger	
Potentielle problemstillinger	**Hvordan har Helsingør Kommune mitigeret risikoen?**
Der er risiko for, at Google ikke giver den nødvendige adgang til de personoplysninger, der er indeholdt i telemetri- og cookiedata.	Diagnosticeringsdata og feedback er slået fra som dokumenteret i bilag 2. Herudover er Google alene databehandler, og det juridiske grundlag er derfor fastlagt af kommunen. Det bemærkes i øvrigt, at Google i databehandleraftalen har forpligtet sig til at bistå med at besvare indsigtsanmodninger.