Chromebook-sagen: Fem vigtige pointer om cloud-tjenester

I juli 2022 nedlagde Datatilsynet forbud mod overførsel til tredjelande samt brugen af de såkaldte Chromebooks og Google Workspace i Helsingør Kommune, og i august fastholdt tilsynet forbuddet. Sagen tog en overraskende drejning, da Datatilsynet i september suspenderede det gældende forbud og i stedet gav en frist for at lovliggøre brugen.

Sagen om Helsingør Kommune startede tilbage i 2019, da en forælder klagede til Datatilsynet over, at vedkommendes barn havde oprettet en YouTube-konto til brug i undervisningen. Skolen havde ikke spurgt eller informeret forælderen om oprettelsen af kontoen, som omfattede, at elevens navn, skolenavn og klasse blev offentliggjort, da eleven postede kommentarer på YouTube. Desuden var elevens loginoplysninger noteret på et stykke papir, som sad fast på låget til den bærbare computer. Det vil sige, at alle kunne logge ind på computeren og få information om eleven.

Kritik fra Datatilsynet

I september 2021 kritiserede Datatilsynet Helsingør Kommune for ikke at have udarbejdet en tilfredsstillende risikovurdering for brugen af Google Chromebooks og Google Workspace for Education. Kommunen blev pålagt at udarbejde en risikovurdering, og Datatilsynet oplyste desuden, at der skulle udarbejdes en databeskyttelsesretlig konsekvensanalyse. Datatilsynet gav alvorlig kritik for databehandlingen, som ikke var i overensstemmelse med databeskyttelsesreglerne. Desuden blev kommunen mindet om sin forpligtelse til at kontakte forældrene og sørge for at rette, anonymisere eller slette personoplysninger, hvis forældrene ikke selv kunne gøre det for deres børn.

I juli 2022 udstedte Datatilsynet et påbud til Helsingør Kommune om at indstille brugen af Google Chromebooks og Google Workspace, da Datatilsynet vurderede, at kommunens dokumentation ikke opfyldte kravene i GDPR. Datatilsynet konstaterede, at kommunen ikke havde vurderet nogle konkrete risici i forhold til databehandlerkonstruktionen, særligt snitfladen mellem dataansvaret hos kommunen og hos Google. Desuden fremgik det af kommunens databehandleraftale, at der kunne overføres oplysninger til tredjelande i supportsituationer uden det fornødne sikkerhedsniveau.

Datatilsynet meddelte, at påbuddet ville være gældende, indtil kommunen havde sikret, at behandlingsaktiviteterne opfyldte GDPR, og at den obligatoriske GDPR-dokumentation var på plads.

Kommunen fik frist til 3. august 2022 til at slette brugere og overføre data. Helsingør Kommune leverede herefter ny dokumentation til Datatilsynet, herunder en konsekvensanalyse.

Konsekvenser for undervisningen

Eleverne måtte starte skoleåret i begyndelsen af august uden Chromebooks, mens lærerne fortsat fik lov til at bruge computerne baseret på en beslutning fra kommunens kommunalbestyrelse. Lærerne skulle derfor undervise eleverne i klasserne på andre måder, fx med tavleundervisning, bøger, papir og blyant.

Datatilsynet fastholdt påbuddet senere i august 2022, men valgte i september 2022 at suspendere sit eget påbud og i stedet give et påbud om lovliggørelse af brugen. Årsagen til suspensionen var en smule overraskende, nemlig at kommunen nu havde erkendt de juridiske problemer og samarbejdede med Datatilsynet om at løse dem i henhold til en særlig procedure efter artikel 36 i GDPR. Vi afventer pt. Datatilsynets endelige vurdering af det materiale, som kommunerne og Google har sendt ind. Tilsynets afgørelse forventes inden jul.

Vigtige pointer om cloud-tjenester

Datatilsynets mange afgørelser i Chromebook-sagen inkluderer en overflod af vigtige takeaways om brug af cloud-tjenester. Vi lister fem af dem herunder.

1. Dokumentation af datastrømmen

Når en kommune (eller andre) leverer et komplekst system til brugere, fx elever, medarbejdere eller kunder, skal organisationen være særligt opmærksom på at dokumentere datastrømmene i, mellem og uden for de involverede systemer, for at sikre at kommunen kan indrette compliancearbejdet efter, hvilken enhed der er dataansvarlig og databehandler for hvilke oplysninger. Datatilsynet omtaler det som den involverede teknologistak, der i Chromebook-sagen var den bærbare computer som hardware, operativsystemet, applikationslaget og cloudlaget.

2. Det juridiske grundlag for behandlingen

Når datastrømme og dataansvar er afklaret, skal det undersøges, om kommunen videregiver personoplysninger til leverandøren. I så fald skal det vurderes, om en videregivelse kan ske med hjemmel i artikel 6, stk. 1, litra e, i GDPR, det vil sige behandling, som er nødvendig for udførelsen af en opgave udført i offentlighedens interesse eller under udøvelsen af offentlig myndighed overdraget til den dataansvarlige. I Chromebook-sagen fandt Datatilsynet, at Google ikke havde identificeret præcist, hvilke personoplysninger der blev videregivet, og at § 6, stk. 1, litra e, nok godt kunne anvendes til brug af værktøjer og systemer, der understøtter klasseundervisningen som fastsat i folkeskoleloven, men ikke til en videregivelse af elevoplysninger til Google.

3. Risikovurderinger efter GDPR artikel 32 om sikkerhed

Risikovurderinger skal dække alle kendte risikoscenarier, fx hvordan applikationerne behandler personoplysningerne, hvordan kommunen fører tilsyn med Googles adgang til personoplysninger i operativsystemet, og hvordan personoplysninger bliver adskilt i interaktionen mellem Google Workspace for Education og Googles backend (det vil sige, hvilke data der bliver delt og hvordan).

4. Risikovurderinger efter GDPR artikel 35 om konsekvensanalyser

En konsekvensanalyse skal udarbejdes, hvis der er en "iboende høj risiko" efter kriterierne i artikel 35 i GDPR. Det er der ifølge de allerede eksisterende vejledninger, når der er tale om "kompleks teknologi, oplysninger om børn og en omfattende mængde oplysninger". I juli 2022 understregede Datatilsynet, at konsekvensanalysen skal laves, selvom sandsynligheden for, at de risici, der kan indtræffe, er relativt lav. Det vil sige, at det skal revurderes, om der skal udarbejdes flere konsekvensanalyser.

5. Overførsel til tredjelande

Selvom oplysninger bliver opbevaret på datacentre inden for EU, vil support udført i tredjelande skulle undergives en analyse efter kapitel V i GDPR, og hvor det er relevant, skal man anvende EU-Kommissionens standardkontrakter og udarbejde en "transfer impact assessment" med vurdering af lovgivningen i tredjelandet.

Det kræver ressourcer at forberede en lovlig implementering af cloud-tjenester, og det er fristende at vælge højere behandlingssikkerhed, bedre funktionalitet og i visse tilfælde lavere priser over manglende overholdelse af kapitel V i GDPR om internationale overførsler. Men det er vigtigt at tilgodese begge hensyn, og at beslutningstagerne klædes ordentligt på, så de kan tage informerede og lovlige beslutninger. Samtidigt skal leverandører, der ikke kan levere lovlige løsninger, sorteres fra så tidligt som muligt i processen.

Det medfører massive omkostninger og kritiske afbrydelser af den daglige virksomhedsdrift at skulle rulle tilbage eller omdirigere cloud-beslutninger efter et påbud. I Cromebook-sagen viste det sig ved, at eleverne ikke kunne bruge deres bærbare computere i skolen. Det kunne lige så godt være, at en virksomhed ikke kunne betjene sine kunder, og at forretningen derfor reelt gik i stå.

Birgitte Toxværd
Partner, advokat
bit@horten.dk

Clara Øhrgaard
Advokatfuldmægtig
cld@horten.dk