

BIG TECH SOM BITRÄDE

Eller: kan ni inte bara göra som jag säger?!

Av Joakim Söderberg på noyb

Förkortningar

- PuA - Personuppgiftsansvarig
- PuB – Personuppgiftsbiträde
- PuB avtal – Personuppgiftsbiträdesavtal
- EDPS – Europeiska datatillsynsmannen
- EUD – EU domstolen

Frågor vi ska behandla

- Var går gränsen mellan PuA och PuB?
- Varför är det viktigt att säkerställa huruvida en leverantör är PuA eller PuB?
- Vad säger dataskyddsmyndigheterna om Big Tech som biträde?
 - Datatilsynet DK
 - Österreichisches Datenschutzbehörde
 - EDPS
- Hur bedömer jag om min leverantör är PuA eller PuB?

PuA eller PuB?

- PuA – Bestämmer „ändamål och medel“ med en personuppgiftsbehandling
 - Vad händer om någon bestämmer ändamål men inte medel?
 - Medel men inte ändamål?
- Förtydligande från EUD mål C-683/21 rörande PuA:
 - Inflytande för egna syften med konsekvens:
 - Att man deltar i „determination of“ ändamål och medel

Varför ska vi bry oss?

- Mina antaganden kring GDPR
 - Vi är alla privatpersoner
 - Som privatpersoner vill vi ha rättigheter
 - Lagen ger oss rättigheter
 - Att andra följer lagen är något vi vill
 - Därför ska vi också följa lagen

Varför ska vi bry oss?

- Mina antaganden kring GDPR
 - Alla jobbar för en PuA
 - Vi är lojala mot vår arbetsgivare
 - Genom regelbrott riskerar arbetsgivaren böter
 - Vi är lojala genom att se till att minimera risken
 - Vi är lojala genom att följa lagen

Varför ska vi bry oss?

- Mina antaganden kring GDPR
 - Alla behandlar data på jobbet
 - Vi behöver veta hur data behandlas för att ha kontroll
 - Brist på kontroll leder till brist av vetande
 - Våra leverantörer behandlar data åt oss
 - Vi behöver ha koll på våra leverantörer för att bibehålla kontroll

Varför ska vi bry oss?

- GDPR har 99 Artiklar
 - PuA ansvar under 50
 - PuB ansvar under 5
- PuA ansvar för principer, laglighet, rättigheter och säkerhet
- PuB ansvar för säkerhet

Varför ska vi bry oss?

- PuA har ansvar för allt oavsett om de kan leva upp till kraven eller ej.
- Genom att välja „fel“ PuB blir regelefterlevnad svår till omöjlig.
 - Risk för böter
 - Risk för att individer går rättslösa
 - Risk att tappa kontroll

Hur det började (Danmark)



Datatilsynet nedlægger behandlingsforbud i Chromebook-sag

Dato: 14-07-2022

Afgørelse

Offentlige myndigheder

Alvorlig kritik

Forbud

Suspension

Anmeldt brud på persondatasikkerheden

Børn

Behandlingssikkerhed

Overførsel til tredjelande

Risikovurdering og konsekvensanalyse

Grundlæggende principper

I en sag om brug af Chromebooks i Helsingør Kommune udtaler Datatilsynet alvorlig kritik og nedlægger forbud mod overførsel til tredjelande og mod brugen af Google Workspace.

Journalnummer: 2020-431-0061

Fortsättningen



Ny afgørelse

Datatilsynet fastholder forbud i Chromebook-sag

Dato: 18-08-2022



Nyhed

I en meget omtalt sag om brug af Google Workspace i Helsingør Kommune har Datatilsynet nu forholdt sig til det materiale, kommunen senest har leveret. På den baggrund fastholder Datatilsynet det forbud, der blev nedlagt i juli.

Konstruktivt møde om Chromebooks

Dato: 19-08-2022

Nyhed

I dag mødtes Datatilsynet med bl.a. KL og Helsingør Kommune for sammen at lægge en plan for en lovgivning af kommunens brug af Chromebooks.

Chromebooks: Datatilsynet suspenderer forbud og giver påbud om lovliggørelse

Dato: 08-09-2022

Afgørelse

Offentlige myndigheder

Påbud

Anmeldt brud på persondatasikkerheden

Børn

Grundlæggende principper

Overførsel til tredjelande

Risikovurdering og konsekvensanalyse

Behandlingssikkerhed

I sagen om brug af Google Workspace i Helsingør Kommune har Datatilsynet nu suspenderet det gældende forbud, men har samtidig givet påbud om lovliggørelse af brugen. Et tilsvarende påbud er givet til Aarhus Kommune.

Journalnummer: 2020-431-0061

Yderligere materiale udsætter afgørelse om Chromebooks

Dato: 13-12-2022

Nyhed

For at få et mere fyldestgørende materiale har Datatilsynet givet kommunerne udsættelse i sagen om brug af Google Workspace i skolerne.

Datatilsynet giver påbud i Chromebook-sag

Dato: 30-01-2024

Afgørelse

Offentlige myndigheder

Påbud

Anmeldt brud på persondatasikkerheden

Børn

Databehandler

Risikovurdering og konsekvensanalyse

Grundlæggende principper

Behandlingsgrundlag

I sagen om brug af Google Workspace i folkeskolerne vurderer Datatilsynet, at der ikke er hjemmel til videregivelse af personoplysninger til Google til alle de formål, der videregives til i dag. Derfor giver Datatilsynet nu et påbud til kommunerne om at bringe behandlingen i overensstemmelse med reglerne og anviser forskellige måder, det kan gøres på.

Journalnummer: 2023-431-0001

Slutsatsen

Datatilsynet giver 51 kommuner alvorlig kritik i Chromebook-sag

Dato: 29-01-2026

Afgørelse

Offentlige myndigheder

Alvorlig kritik

Anmeldt brud på persondatasikkerheden

Behandlingssikkerhed

Børn

Grundlæggende principper

Databehandler

Datatilsynet udtaler alvorlig kritik og advarer samtidig kommunerne i forhold til, hvordan de gør brug af Googles produkter i folkeskolen.

Journalnummer: 2025-431-0053.

<https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/jan/datatilsynet-giver-51-kommuner-alvorlig-kritik-i-chromebook-sag>

Myndigheternas syn (Danmark)

- „Datatilsynet udtaler alvorlig kritik“
 - för inställningarna i programmen
 - Användning av underbiträden utanför EU

- Slutsats:

Det är bra att veta vad man gör på jobbet och vilka som gör det

Myndigheternas syn (Danmark)

- „Datatilsynet udtaler alvorlig kritik“ (och varnar)
 - för inställningarna i programmen (som troligen är olagliga)
 - Användning av underbiträden utanför EU (som troligen är olagligt)
- Slutsats:

Efter fyra år blev det en tummetott.

Myndigheternas syn (EU)



https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf

EDPS INVESTIGATION INTO USE OF MICROSOFT 365 BY THE EUROPEAN COMMISSION (Case 2021-0518)

Decision
(8 March 2024)

Myndigheternas syn (EU)

- Finn fem (tre gånger flera egentligen) fel!
 - Ändamålsbegränsning!
 - Tredjelandsoverföringar!
 - Olovlig datadelning!
- 180 sidor lång diss.

Myndigheternas syn (EU)

- Ändamålsbegränsning
 - PuA visste inte vad som hände eller varför
 - Brist på specifikation kring data som MS behandlade
 - Brist på tydlig instruktion till MS
 - Brist i att MS behandlade mer än vad instruktionen tillät
 - Nya syften lirade inte med originalsyftena
 - Plus specialbrott som bara är applicerbart för EU-organ (Artikel 9 EU-GDPR)

Myndigheternas syn (EU)

- Tredjelandsöverföringar
 - Ingen instruktion vad som skulle skickas till vem
 - Inget som säkerställde skyddsnivå i mottagarlandet
 - Skrivit på Standardavtalsklausuler utan att kartlägga överföringarna först
 - Plus specialregel som inte finns i vanliga GDPR:
 - Artikel 47 EU-GDPR

Myndigheternas syn (EU)

- Olovlig datadelning!
 - Bristfällig instruktion att dela data till underbiträden!
 - Brist i säkerställandet av säkerhet i mottagarlanden!
 - Ergo också brott mot principen om säkerhet och konfidentialitet!

Myndigheternas syn (EU)

- Order om att fixa allt ovan
- Och en reprimand
- Samt filosoferande över om Microsoft egentligen kanske är PuA

Myndigheternas syn (EU)

- Den 11 July 2025 förklarar sig EDPS nöjda:

Based on the substantially changed situation demonstrated by the Commission, I conclude that the Commission now complies with the provisions of Regulation (EU) 2018/1725 found to be infringed in the EDPS Decision of 8 March 2024. Therefore, I consider the infringements established in that Decision as remedied, and I hereby close the enforcement proceedings in case 2021-0518.

https://www.edps.europa.eu/system/files/2025-07/25-07-11_letter-to-commission_2021-0518_en.pdf

Myndigheternas syn (EU)

- Den 11 July 2025 förklarar sig EDPS nöjda, men:
 - Inga ändringar i PuB-avtal, rörande kategorier av personuppgifter.

<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

- Bara tillägg i lista på underbiträden.

<https://servicetrust.microsoft.com/DocumentPage/f84b7858-4ee2-4bff-bf99-9bf44241efda>

- EU-kommissionens speciallösning löser inget för kreti och pleti.

Myndigheternas syn (Österrike)

- Datenschutzbehörde
 - Konstaterar att Microsoft är PuA (alltså inte PuB)
 - Förbjuder Microsoft att ladda upp cookies i barnens datorer
- Slutsats:
Microsofts PuB-avtal duger inte

Är min leverantör PuA eller PuB?

- Svaret är enkelt: har du kontroll över vad de gör och varför?
 - Ja – De är PuB
 - Nej – De är PuA

Bonusslides!!!

Bonusslides!

- Kan man använda Microsoft som PuB när man kör Azure?
 - Säkerhetstransparens
 - Möjlighet till revision
 - Tredjelandsoverföringar
 - Kontroll över instruktion
 - Är Microsoft PuA eller PuB?

Säkerhetstransparens

Logs/records: Please give us access to the event logs mentioned in Appendix A, the data restoration logs and a complete record of security breaches under 2024 and remedial efforts taken on account of these breaches.	If a security breach impacts a customer, we notify the customer privately and partner with them confidentially to remediate. Thus, you would have access to information on a security breach only if there is a security breach affecting your tenant(s). Azure provides customers a variety of logging capabilities, which are outlined at Azure security logging and auditing Microsoft Learn.
Personnel: We would like a list of personnel that have access to our data, their job description and rationale regarding their access, as well as a complete inventory of assets used to store our data.	We will not provide a list of personnel or data bearing assets. Please see above regarding the just-in-time and just-enough access policy that limits our personnel's access to Customer Data.

Från Microsofts svar vid leverantörsgranskning

Säkerhetstransparens

- Vid behandling av personuppgifter ska följande gälla:
 1. f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).
 2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (ansvarsskyldighet).

Säkerhetstransparens

Öppen fråga:

- Hur visar jag som PuA att jag jobbar säkert om jag inte vet var min kunddata finns eller vem som har tillgång till den?

Möjlighet till revision

- **Audit Fees.** We present auditing fees for accommodating your audit. We only present fees for the consumed time of subject matter experts devoted to preparing for your audit and submitting to it. There are no fees for mundane activities such as document preparation, but in the case your audit test plan involves a particular Microsoft specialist to attend at a particular location we will present travel expenses as additional fees. (e.g., a US-based Azure compliance specialist must meet you at a Netherlands datacentre facility for a physical site inspection and other audit assurance work). Sometimes after discussions customers only require simple assurance information (e.g., additional transparency into how Microsoft manages certain privacy risks in service operations), and we realize we can provide that without presenting any fees. If Microsoft facility attendance is a requirement, then this is rarely the case. Our fees are based on our consulting fee basis for senior technology architects which is USD \$500, or local market equivalents, or a pre-negotiated professional services fee table if one exists with the customer. Most customer audits attract fees in the range of USD \$20,000 - \$80,000 but it depends on the assurance controls scope, the test plan, and the number of Azure services in scope.

Från Microsofts svar vid leverantörsgranskning

Möjlighet till revision

- Kostnad 200 000kr – 800 000kr för en revision av Microsoft som PuA.
- Lagen säger (Artikel 28.3.h)
 - Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Möjlighet till revision

Öppen fråga:

- Bidrar man till revision genom när man gör revisionen ohemult dyr?

Bonusfråga:

- Kan man ens ta betalt för något man har en laglig skyldighet att bistå med?

Tredjelandsoverføringar

Källa:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/personnel-loc/m365-personnel-location?view=o365-worldwide>

Contract Staff Personnel Locations			
Argentina	Egypt	Japan	Serbia
Armenia	El Salvador	Korea	Singapore
Australia	Finland	Malaysia	South Africa
Austria	France	Mexico	Spain
Belgium	Georgia	Netherlands	Sweden
Bolivia	Germany	New Zealand	Switzerland
Brazil	Ghana	Norway	Taiwan
Bulgaria	Guatemala	Panama	Trinidad and Tobago
Canada	Honduras	Paraguay	Türkiye
China	Hong Kong SAR	Peru	United Kingdom
Costa Rica	Hungary	Philippines	United States
Czech Republic	India	Poland	Uruguay
Denmark	Ireland	Portugal	
Dominican Republic	Italy	Qatar	
Ecuador	Jamaica	Romania	

Tredjelandsoverföringar

- Lagen säger följande (Artikel 44):

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att **den personuppgiftsansvarige och personuppgiftsbiträdet**, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

TredjELandsöverföringar

- PuA måste säkerställa att alla mottagarländer är säkra
 - Dvs: tredjELandsbedömningar (Transfer Impact Assessments) behöver göras för alla potentiella mottagarländer.

Tredjelandsoverføringer

- Överföringer till tredjeland är enbart OK om det är på instruktion:
 - Artikel 28(3)(a): personuppgiftsbiträdet får endast „behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation“

Tredjelandsoverföringar

- PuB får inte bestämma vem de skickar uppgifter till
 - Dvs: Microsofts får inte föra över uppgifter enligt sitt avtal utan instruktion.

Tredjelandsoverföringar

Öppen fråga:

- Är ni villiga att göra TIAs för 30 olika länder när ni köper en molntjänst?

Öppen fråga:

- Har någon här faktiskt instruerat Microsoft att föra över uppgifter till Guatemala?

Kontroll över instruktion

We've reviewed the documents and answers you've provided and must conclude the following based on our understanding of the concept of controller; the person determining the purpose and means of processing:

1. Without full transparency regarding the means; that is to say the who, the where and the what; we can't control the means of processing.
2. Without an actual instruction to process personal data, written as an instruction to process personal data, we can't control the purpose.

Our conclusion based on this and the information, or rather lack thereof in your response leads us to conclude that our relationship can not be considered a Controller-Processor relationship. If you are of a different opinion, you are more than welcome to produce evidence for this opinion.

If you agree with our assessment you would have to assume liability as a controller. Either in a joint controllership, the details of which we would have to discuss, or as an independent controller bound by the purpose limitation principle.

Kontroll över instruktion

We respectfully disagree with your conclusion on Microsoft's role in providing Azure to our enterprise and public-sector customers. Those customers across the EU and beyond are controllers choosing the services Microsoft provides them as a processor acting on their behalf in accordance with the Microsoft Products and Services Data Protection Addendum. That DPA makes clear that the customer's agreement with Microsoft, product documentation and the customer's own use and configuration of the services constitute the instructions to Microsoft to process personal data. Microsoft is neither a controller nor a joint controller in providing services to our customers under the DPA.

Kontroll över instruktion

Datakategorier: Personuppgifterna som ingår i e-post, dokument och andra data i elektronisk form i samband med produkterna och tjänsterna. Microsoft bekräftar att Kunden beroende på Kundens användning av produkterna och tjänsterna kan välja att i personuppgifterna inkludera personuppgifter från någon av följande kategorier:

Ca 20 kategorier av personuppgifter listade, och avslutas med:

- Andra personuppgifter som anges i Artikel 4 i GDPR.

Kontroll över instruktion

Microsoft skriver instruktionen till sin kund, och lämnar instruktionen öppen.

Kontroll över instruktion

Kunden ger Microsoft tillåtelse

- att skapa sammanställda, icke-personliga uppgifter från data som innehåller pseudonymiserade identifierare (såsom användningsloggar som innehåller unika, pseudonymiserade identifierare)
- att beräkna statistik som avser Kunddata eller data i Professionella tjänster

Microsoft ger kunden instruktion, ovan ett exempel.

Kontroll över instruktion

Öppen fråga:

- Har du kontroll över personuppgiftsbehandlingen om din leverantör är den som intruerar dig?

Är Microsoft PuA eller PuB?

Öppna frågor:

- Vem har inflytande över behandlingen?
- Vilken del har kund inflytande över och vad styr Microsoft?

Min slutsats:

Man kan bara ha kontroll över sin data om man vet var den finns och vem som har tillgång till den.

Om ens leverantör gör revision omöjlig, ska man välja en annan leverantör.

Om leverantören skickar uppgifter till tredje land utan att du ber dem att göra det, så har leverantören olämplig.

Om leverantören skriver sin egen instruktion så har du inte instruerat dem.

Min slutsats:

En sån leverantör är alltid PuA.

Genom att anlita dem tappar du kontroll.

Tack för mig!

Joakim Söderberg

Kontakt – js@noyb.eu