PRIVACY COMPANY

Onderwijs en Big Tech

Nationale Privacy Conferentie 24 januari 2024

Wie gebruikt er geen Big Tech?

- Steek je hand op als jij of je kind tenminste 1 keer per week Microsoft Office of Gmail gebruikt.
- Laat je hand zakken als je géén Facebook, WhatsApp of Instagram account hebt.
- Laat je hand zakken als jouw organisatie of school een duidelijke exit strategie heeft als Microsoft de prijzen met 25% verhoogt.

Nederlandse universiteiten koploper in cloudgebruik

NOS Nieuws • Maandag 17 oktober, 10:05

'Driekwart Nederlandse studentendata opgeslagen bij Amerikaanse techbedrijven'

- Tobias Fiebig van het Duitse Max Planck instituut heeft wereldwijd DNS verkeer van universiteiten onderzocht op verkeer naar cloud storage, Zoom en online leersystemen.
- Nederlandse universiteiten zijn al voor de pandemie massaal de cloud ingegaan: gebruik van Zoom is enorm toegenomen sinds Covid.

Tobias Fiebig

Tobias Fiebig

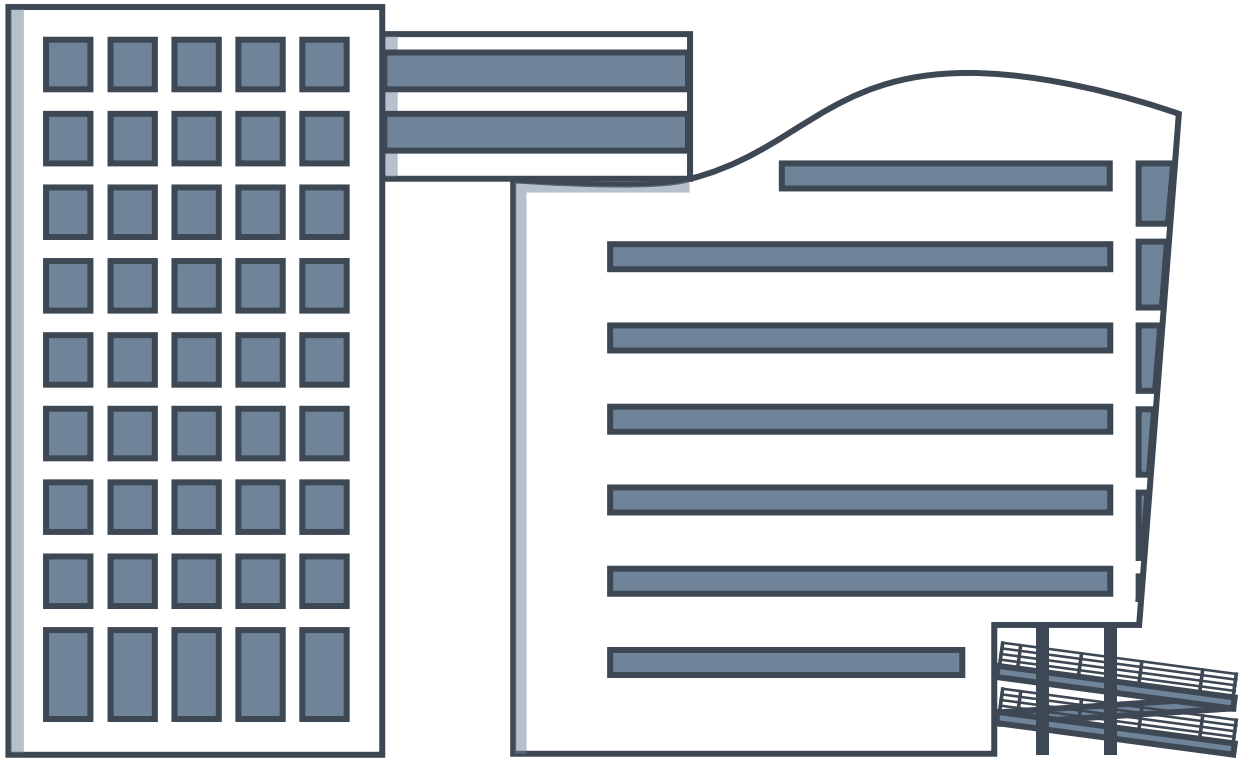
Dr.-Ing. Tobias Fiebig

Address: *Max-Planck-Institut für Informatik*
Saarland Informatics Campus
Campus E1 4
66123 Saarbrücken

Standort: E1 4 - 519
Telefon: +49 681 9325 3527
Fax: +49 681 9325 5719
E-mail : Get email via email

https://doing-stupid-things.as59645.net/research/ clouds/ measurement/2022/10/20/heads-in-the-cloud.html

Wat is Privacy Company en wie ben ik?



- Opgericht in 2014
- Team van 30+ veelzijdige professionals
- Gericht op praktische oplossingen
- Advies, training, privacy management tooling, FG diensten, ePrivacy en informatiebeveiliging

Uitgevoerde DPIA's op BigTech

Microsoft Intune

salesforce

SAP

facebook

Microsoft Office 2016

Windows 10 Enterprise

Azure

aws

Microsoft Edge

IBM Cloud

Meta

Google Workspace

BlackBerry

ORACLE CLOUD

zoom

Publicaties op slmmicrosoftrijk.nl en surf.nl zoek op: DPIA

Rijksoverheid heeft standaardmodel voor DPIA

- De AP heeft 17 criteria gepubliceerd wanneer je een DPIA moet uitvoeren.
- De EDPB hanteert 9 criteria: je moet een DPIA doen als je aan 2 criteria voldoet.
- Privacy Company heeft voor de Privacy Adviseur Rijk een pre-scan DPIA gemaakt. Dat is een openbare checklist wanneer moet je een DPIA moet uitvoeren.

https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

DPIA aanpak Privacy Company: juridisch en technisch

Analyse raamwerk contracten

vaak veel verschillende documenten

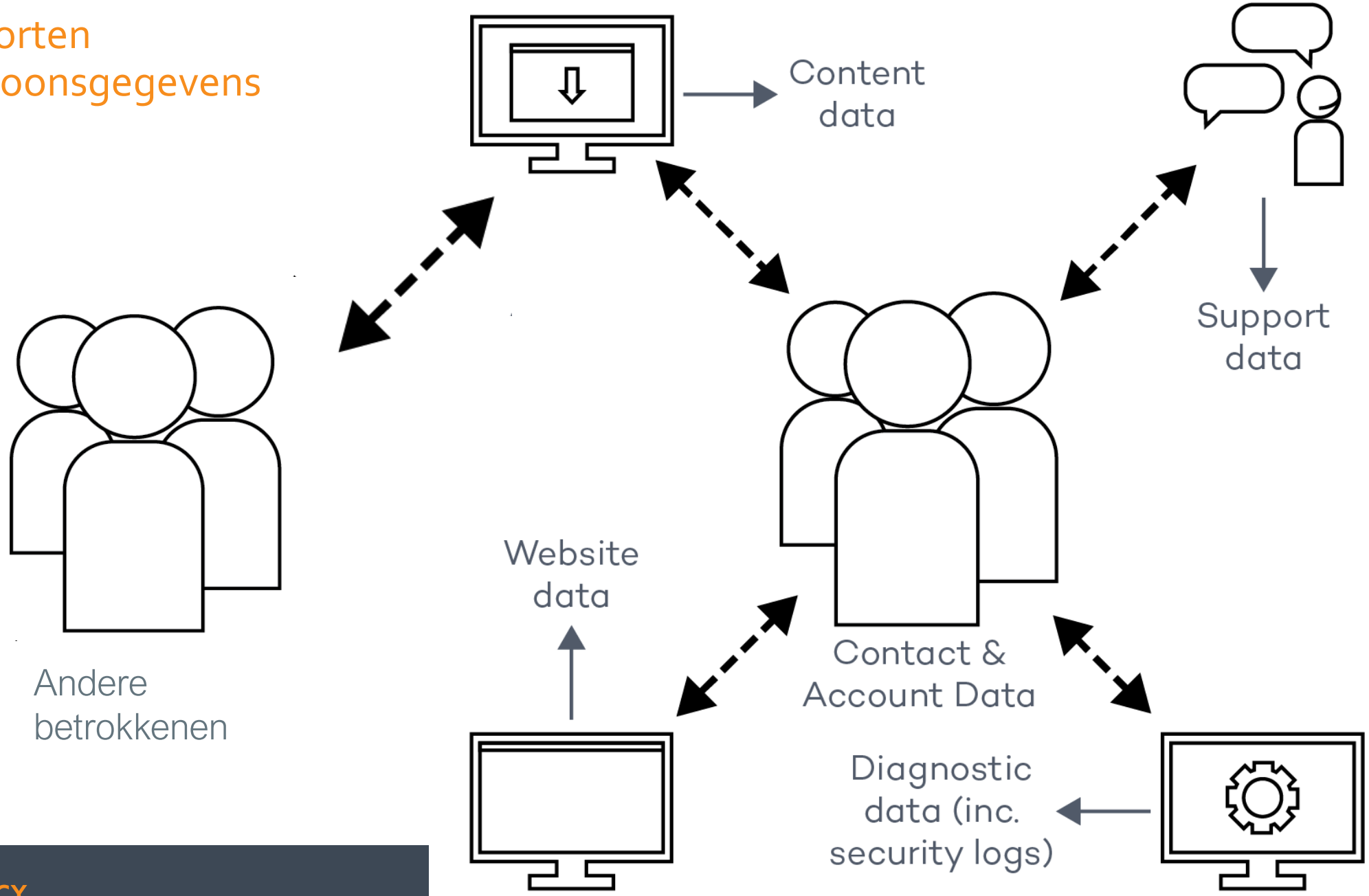
DPIA als handhavingsinstrument

- Formele AVG-handhaving bij de Ierse Data Protection Commissioner (DPC).
- Maar klanten van Big Tech kunnen ook zelf de AVG gereedschapskist inzetten om de privacynaleving te vergroten!
- Denk aan: recht van inzage, medewerkingsplicht van verwerkers, omgekeerde bewijslast voor verantwoordelijken dat ze aan de wet voldoen, èn het uitvoeren van een DPIA.
- SURF, SIVON en SLM Microsoft, Google en Amazon Web Services Rijk hebben samen paraplu DPIA's laten uitvoeren.
- Door de resultaten in het Engels te publiceren, is duidelijker dat hoge risico's voor de hele EU-markt gelden.

Hoofdvragen DPIA's op cloudproviders

1. Welke soorten persoonsgegevens verwerkt de leverancier?
2. Zijn de verwerkingen voldoende transparant?
3. Gedraagt de leverancier zich voor alle gegevens als verwerker?
4. Wat zijn de doelen van de verwerkingen?
5. Kan de beheerder de verwerkingen beperken (dataminimalisatie)?
6. Hebben de verantwoordelijke organisaties een effectief auditrecht?
7. Wat zijn de risico's van doorgifte naar *derde* landen?
8. Hoe lang bewaart de leverancier de diagnostische gegevens?

5 soorten persoonsgegevens



Onderzoeksmethoden bij cloudproviders

Privacyrisico's (fysiek, materieel en immaterieel)

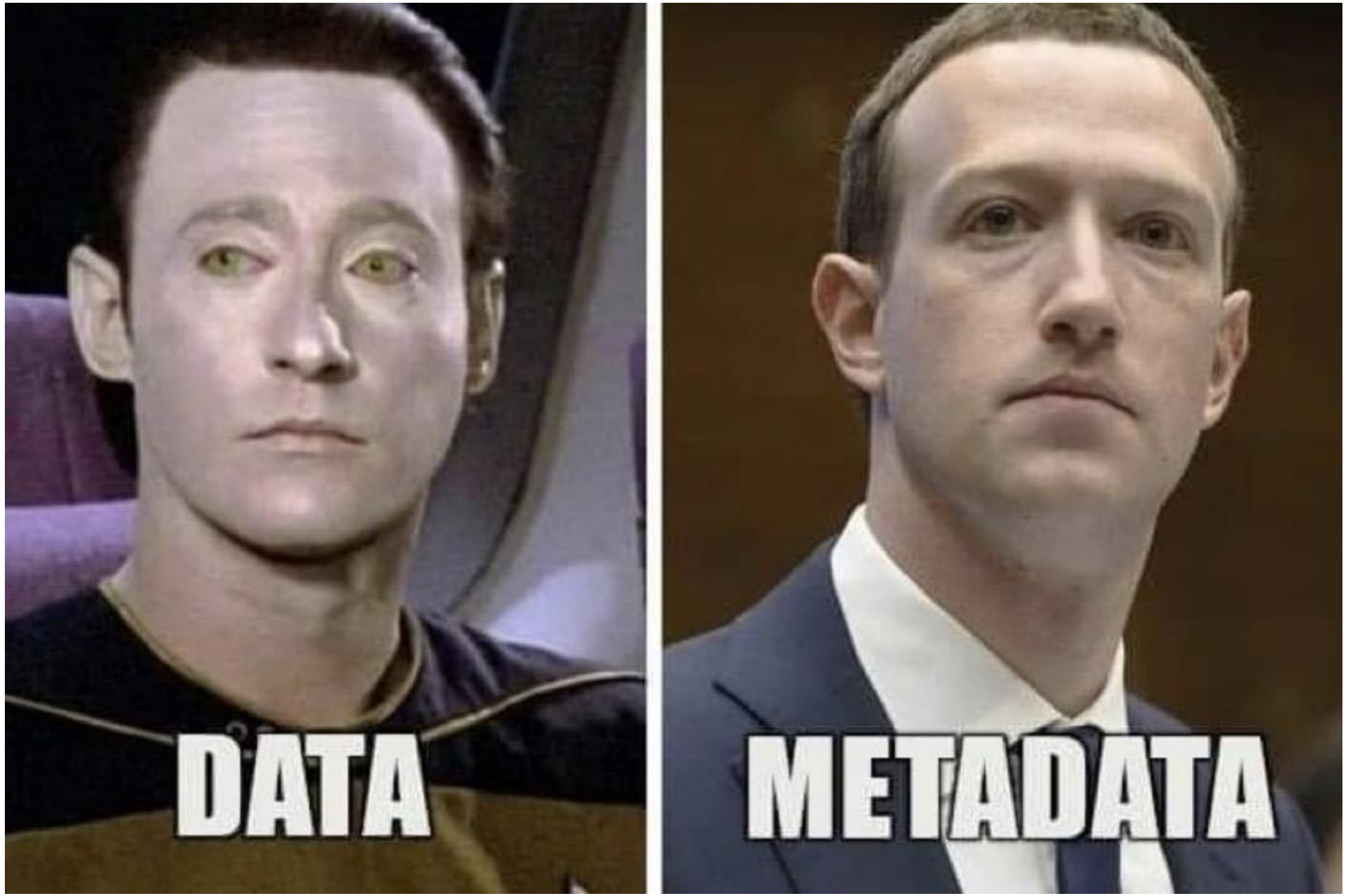
- Je kunt je rechten niet uitoefenen (privacy, vrijheid van meningsuiting, etc.)
- Je kunt niet bij bepaalde diensten of kansen
- Verlies van controle over het gebruik van de Persoonsgegevens
- Discriminatie
- Identiteitsdiefstal of fraude
- Financieel verlies
- Reputatieschade (voor de persoon!)
- Lichamelijke schade/letsel
- Verlies aan vertrouwelijkheid
- Heridentificatie van pseudonieme gegevens
- Elk ander betekenisvol economisch of sociaal nadeel

Hoe bepaal je of een risico hoog is? Kans x impact

Ernst van de gevolgen voor de betrokkene(n)	Ernstige gevolgen	Laag risico	Hoog risico	Hoog risico
	Enige negatieve gevolgen	Laag risico	Medium risico	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

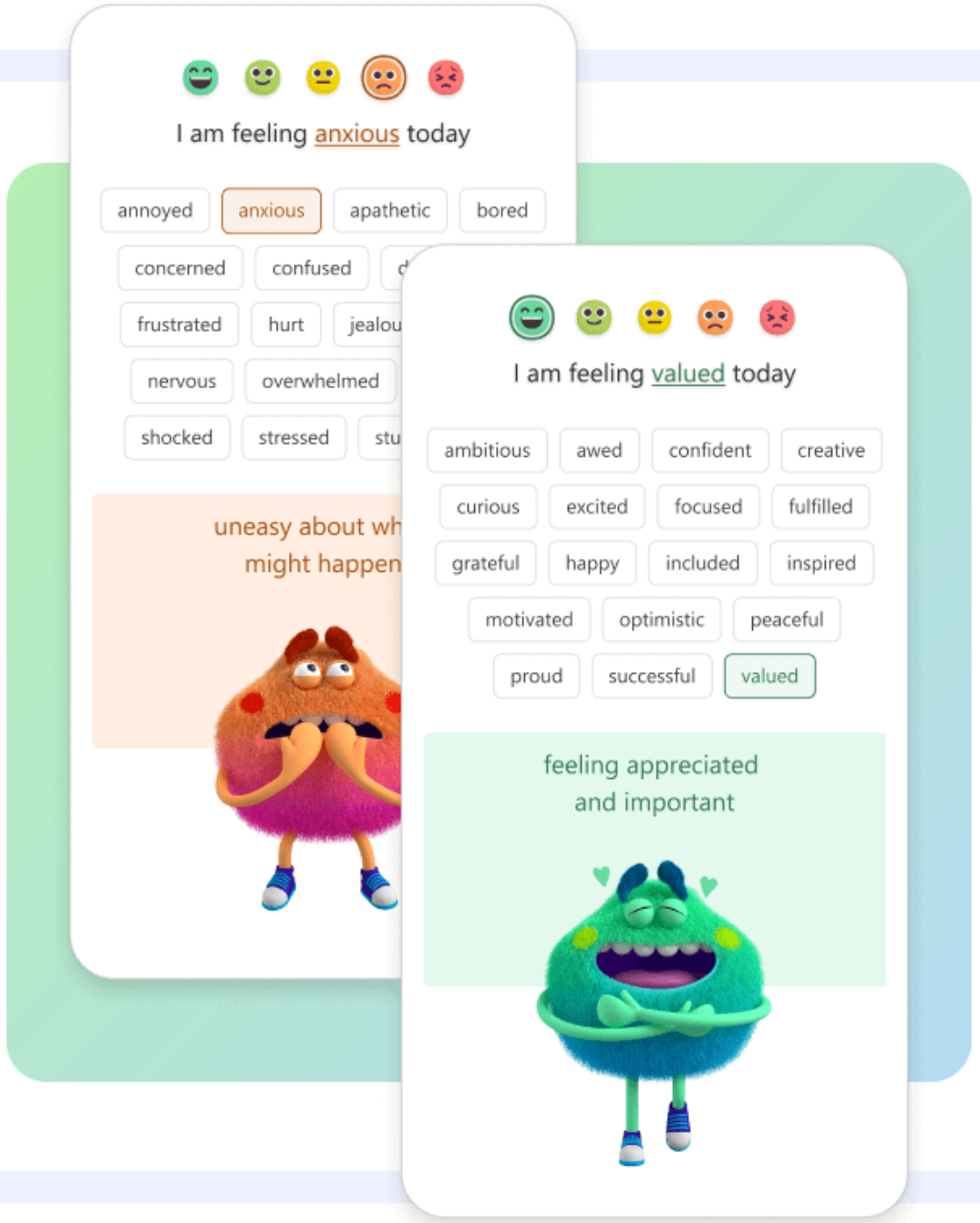
Terugkerende hoge risico's

- Gebrek aan transparantie, vooral over de diagnostische en website gegevens.
- De cloud provider treedt voor de meeste persoonsgegevens op als verantwoordelijke, en niet als verwerker.
- Daardoor: gebrek aan doelbinding, geen afspraken gezamenlijke verantwoordelijkheid en gebrek aan grondslag. Dit zorgt voor hoge risico's op verlies aan controle over de gegevens omdat ze 'verder' verwerkt kunnen worden voor commerciële doelen.
- Geen volledige inzage in reactie op inzageverzoek van betrokkene.
- Kans op toegang tot onversleutelde gegevens door niet-Europese opsporings- en inlichtingendiensten.
- Daarnaast risico's in de eigen organisatie als logs en analytic tools gebruikt kunnen worden als personeelsvolgsysteem.


DATA
METADATA

Waarom zijn de metadata zo belangrijk?

- Voorbeeld: Microsoft Analytics
- Microsoft weet veel over jou en je dagelijkse gedrag als je met Microsoft 365 werkt.
- Microsoft maakt ongevraagd veel analytics hoe efficiënt je werkt, maar ook, hoe je je voelt.
- Met de nieuwe 'Expressions' krijgt Microsoft nog meer zicht op je emoties.



Risico's van *Sphere transgression* (Landjepik)

- De Radboud filosofe Tamar Sharon doet onderzoek naar de machtsgreep van Big Tech naar andere maatschappelijke domeinen.
- Bijvoorbeeld opsporing, onderwijs en wetenschappen, beoordelingen en examineringen, werving en selectie, medische sector en psychologie

Resultaten onderhandelingen met cloudproviders

- Strakke verwerkersovereenkomsten voor alle soorten persoonsgegevens.
- Beperkte uitzondering voor gegevens die de cloudprovider wel moet verwerken voor eigen bedrijfsvoering.
- Strikte doelbinding als verwerker: de dienst leveren, up-to-date en storingsvrij houden, inclusief support, en de gegevens beveiligen.
- Bouw van inzagemachines, en tooling zodat eindgebruikers zelf de telemetriegegevens kunnen bekijken.
- Uitgebreide publieke documentatie over de verschillende soorten verwerkte Persoonsgegevens.
- Afspraken doorgezet in de contracten met alle subverwerkers.
- Auditrecht: trust but verify.
- Verhuizing van de meeste verwerkingen naar een Europese cloud.

Afspraken over beperkte verwerkingen eigen doelen

- De provider mag beperkte persoonsgegevens van de klant verwerken als zelfstandige verantwoordelijke wanneer dat strikt noodzakelijk is voor de eigen gerechtvaardigde bedrijfsdoeleinden.
- Voorbeelden: om rekeningen te sturen, om fraude te bestrijden, om contact te leggen met inkopers, etc.
- Voor analytische doelen, zoals capaciteitsmanagement, mag de provider alleen gepseudonimiseerde en op hoog niveau geaggregeerde gegevens verwerken.
- De provider is uiteindelijk ook zelfstandig verantwoordelijk voor verstrekkingen aan opsporingsdiensten, als hij 1) de vordering niet mag doorsturen naar zijn klant, 2) de klant ook niet mag informeren en 3) de vordering niet kan weigeren via een juridische procedure. Een Amerikaanse provider overtreedt de AVG bij verstrekking aan een Amerikaanse dienst zonder MLAT.

Resultaten DPIA's op Microsoft, Google en Zoom

The New York Times

How the Netherlands Is Taming Big Tech

Dutch privacy negotiators have spurred major changes at Google, Microsoft and Zoom, using a landmark European data protection law as a lever.

Februari 2019: Microsoft kondigt wereldwijde verbeteringen in Office aan

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 20 december 2018

Onderwerp Reactie op berichtgeving in de media ov
door Microsoft.

De heer Öztürk (DENK) heeft tijdens regeling van w
november gesproken over berichtgeving in de medi
opslag door Microsoft[1].

Naar aanleiding van zijn verzoek deel ik u, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, het volgende mede.

De minister van Binnenlandse Zaken en Koninkrijksrelaties bevordert vanuit de

Microsoft CEO Satya Nadella | Stephen Brashear/Getty Images

Microsoft to update Office Pro Plus after Dutch ministry questions privacy

The Netherlands' justice ministry was concerned popular programs were sending diagnostic data from Europe to the US without adequate user controls.

By **DANIEL LIPPMAN** | 2/8/19, 7:30 AM CET | Updated 2/8/19, 5:03 PM CET

Januari 2020: wereldwijde nieuwe Online Service Terms en Data Processing Addendum

Microsoft's new Office 365 terms: 'We won't use your data for advertising or profiling'

US businesses can thank privacy-conscious Europeans for improvements in Microsoft's Online Services Terms.

Microsoft | Microsoft 365 Products Resources Support Buy now All Microsoft Search

January 8, 2020

Updated Microsoft Online Services Terms are available to our customers around the world

By The Microsoft 365 Marketing Team

Jan 2024: Microsoft verwerkt alle gegevens in de EU

Microsoft | EU Policy Blog About Us Policy Issues Tech Fit 4 Europe Podcast

Answering Europe's Call: Storing and Processing EU Data in the EU

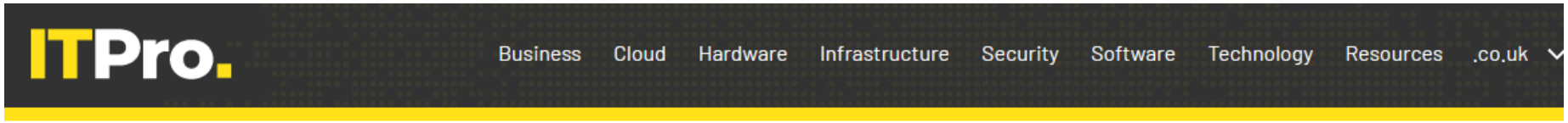
May 6, 2021 | Brad Smith - President and Chief Legal Officer

First, we are going beyond customer data and are further expanding our local storage and processing commitments to now **include *all* personal data within the boundary**. Through significant investments and

Microsoft Cloud enables customers to keep all personal data within European Data Boundary

Jan 11, 2024 | Julie Brill - Corporate Vice President and Chief Privacy Officer

Google DPIA in het nieuws



NEWS Home > Business > Policy & Legislation > Data Protection

Google r… protecti…

Privacy Compa…

by: Keumars Afifi-Sabet

DutchNews.nl

Housing | Best of the Web | Donate

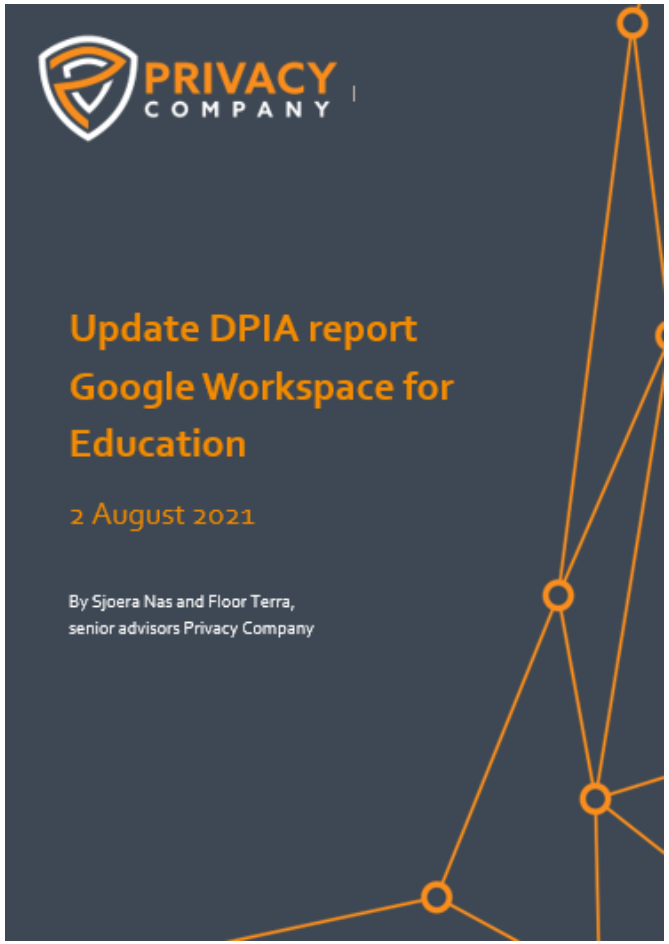
…ety | Sport | Education | Health | Intern

Google addresses customer data protection, security in Workspace

Google has also introduced new Workspace features as we continue to work from home.

Google Workspace verbeteringen onderhandeld door SURF en SIVON

- Na eerste DPIA met 8 hoge risico's en 3 lage risico's AP om hulp gevraagd (voorafgaande consultatie)
- Advies AP aan scholen: stop ermee voor september 2021
- Resultaat publieke druk: Google treedt op als verwerker voor de diagnostische data, verwerking voor 3 ipv 33 doelen
- Google gaat veel meer documentatie publiceren
- Organisaties moeten zelf nog wel heel veel maatregelen nemen om de hoge risico’s te mitigeren



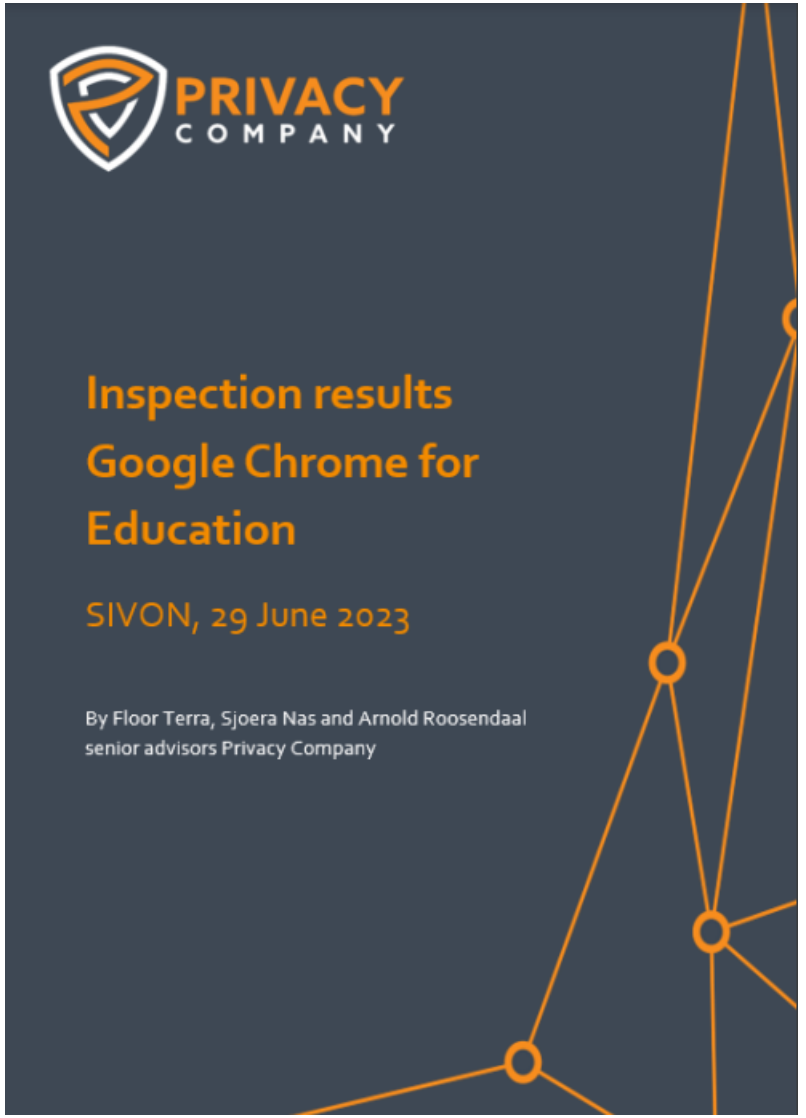
Voortgangsrapport Workspace juli 2023

- Google heeft de beloofde verbetermaatregelen getroffen, inclusief meer documentatie, en meer inzage via een Diagnostic Information Tool.
- Als scholen ook zelf de aanbevolen maatregelen treffen, zijn er géén hoge risico's meer.
- Belangrijkste maatregelen: koop een betaalde versie van Workspace, kies de instelling voor het funderend onderwijs (K-12) en zet de Additional Services uit (YouTube, Maps, etc.)

https://sivon.nl/wp-content/uploads/2023/07/20230724-clean-Workspace-for-Education.pdf

Onderzoeksrapport Chrome juli 2023

- Google biedt sinds augustus 2023 een verwerkersversie van de Chrome browser en het Chrome OS op Chromebooks aan voor het NL onderwijs.
- Als scholen de aanbevolen maatregelen treffen, zijn er géén hoge risico's meer.
- Belangrijkste maatregelen: zet de toegang tot de Optional Services uit, zoals de Chrome webstore en Google Play.



https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf

Binnenkort: risico's doorgifte in DTIA en extra bevindingen

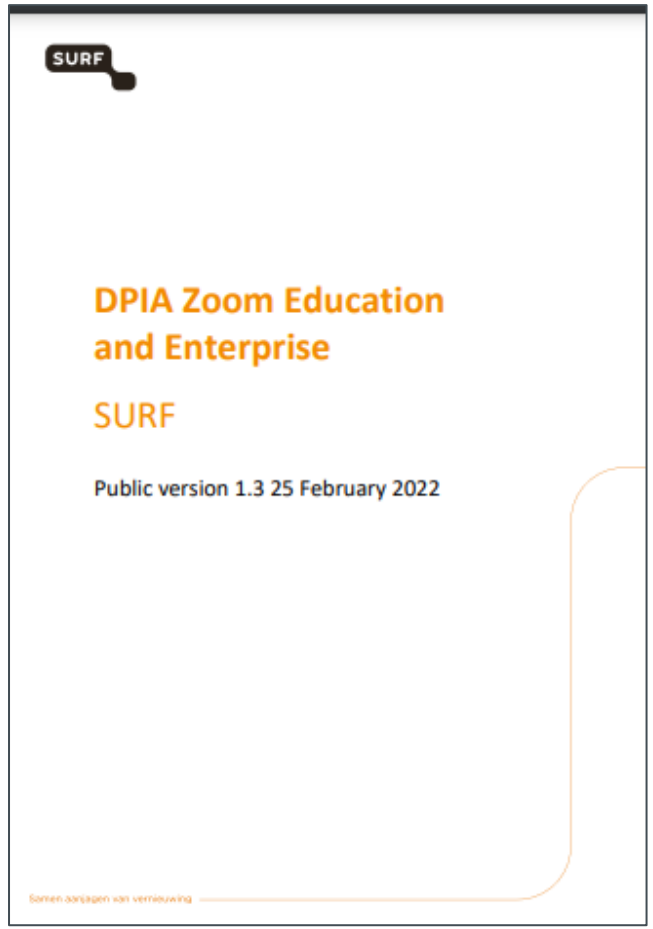
- Doorgifte naar de VS is niet meer problematisch voor Big Tech die zich heeft aangesloten bij het nieuwe dataverdrag tussen de EU en de VS.
- Maar de meeste Big Tech verwerken gegevens in wereldwijde datacentra, met wereldwijde toegang tot de gegevens door beheerders en helpdeskers.
- Daarom hebben SURF en SIVON ook een DTIA laten uitvoeren op de risico's van onrechtmatige toegang door overheidsdiensten in zogenaamde 'derde landen', een *Data Transfer Impact Asssesment.*
- Tijdens de verificatie-onderzoeken kwamen nieuwe risico's aan het licht. Deze zijn besproken met Google.
- OCW heeft de landsadvocaat om advies gevraagd over het rapport van extra bevindingen en de DTIA.

Zoom verbeterde verwerkersovereenkomst (maart 2022)

- Zoom treedt op als verwerker voor alle soorten persoonsgegevens voor alle EU-klanten.
- Doelbinding: (1) de dienst leveren en verbeteren, (2) de dienst up-to-date houden, en (3) veilig.
- Verbod op profilering, marktonderzoek, gerichte advertenties en data analytics. Verbod op sneaky toestemmingsvragen aan eindgebruikers. Verbod op 'aanbevelingen'/'tips' voor diensten of producten die de klant niet gekocht heeft of gebruikt.
- Zoom beschermt ook consumenten die deelnemen aan Zoom van Universiteit of school.

Zoom verbeterde verwerkersovereenkomst

- Effectieve audit rechten voor universiteiten en overheidsinstellingen.
- Ècht anonimiseren volgens richtlijnen WP29/EDPB.
- Publieke documentatie van telemetrie en service generated server logs.
- Versleuteling met eigen sleutels (End to End Encryptie).
- Zoom bouwt Data Viewer Tool voor inzage in de telemetrie.



https://www.privacycompany.eu/blogpost-nl/nieuwe-dpia-voor-surf-en-rijk-op-zoom-alle-hoge-risicos-opgelost

Binnenkort: verificatierapport Zoom

- SURF en Privacy Company hebben bijna maandelijks overleg met Zoom over de voortgang van de beloofde verbetermaatregelen en oplossen van lage risico's.
- Binnenkort verschijnt update rapport
- DTIA niet nodig: Zoom verwerkt alle persoonsgegevens binnen de EU

Gewijzigde algemene voorwaarden voor gratis diensten Zoom hebben geen gevolg voor het Nederlandse (en Europese) onderwijs

21 augustus 2023 - Zoom heeft in maart van dit jaar haar wereldwijd geldende algemene voorwaarden voor consumenten aangepast (voor de gratis diensten). In die gewijzigde voorwaarden staat dat Zoom het recht heeft om -in de toekomst- gegevens van klanten te analyseren met AI. Deze wijzigingen hebben geen negatieve gevolgen voor Europese betalende klanten van Zoom en in het bijzonder de Nederlandse onderwijsinstellingen die gebruik maken van de door SURF onderhandelde verwerkersovereenkomst.

Conclusies

- Gebruik de AVG schatkist om je leveranciers te dwingen netter om te gaan met persoonsgegevens.
- Neem DPIA's serieus. Doe technisch onderzoek en maak werk van de subsidiariteitstoets: zijn er echt geen andere privacyvriendelijkere leveranciers?
- Zet pilots op met open source alternatieven.
- Pas op met het gebruik van gratis AI-diensten: werk samen om goed onderzoek te doen naar de mensenrechten- en klimaatimpact.

Illustration Bert Knot from the Eisinga Planetarium, **CC BY-SA 2.0**

Vragen?

Sjoera.nas@privacycompany.nl
https://www.linkedin.com/in/sjoera/

www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
Den Haag