

**05 oktober**  
Suikerunieterrein  
Groningen



# Bloei Digitaal 2023

Sjoera Nas - Privacy en BigTech

# Agenda

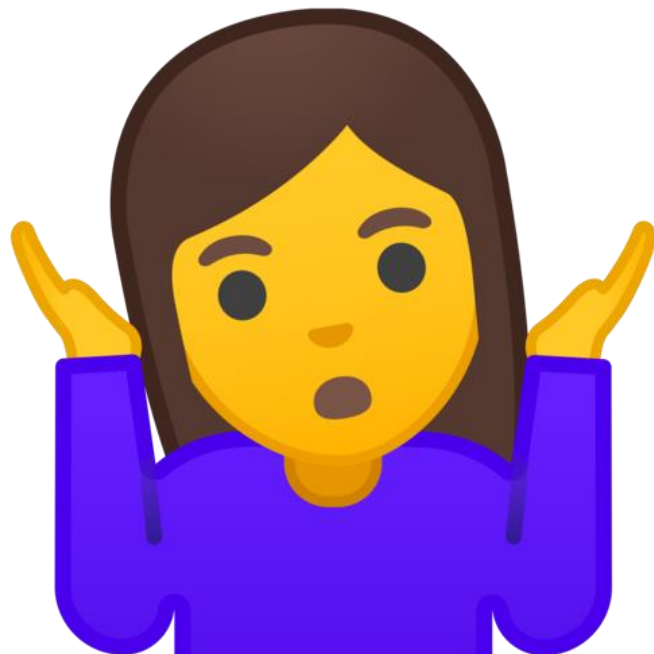
- Waarom is privacy belangrijk?
- Wat is een DPIA, en hoe doe je dat op clouddiensten?
- Resultaten onderhandelingen met cloudproviders door universiteiten en Rijk

## Waarom is het erg als je privacy geschonden wordt?

Ik doe toch  
niets illegaals?



Ik heb toch niets  
te verbergen?

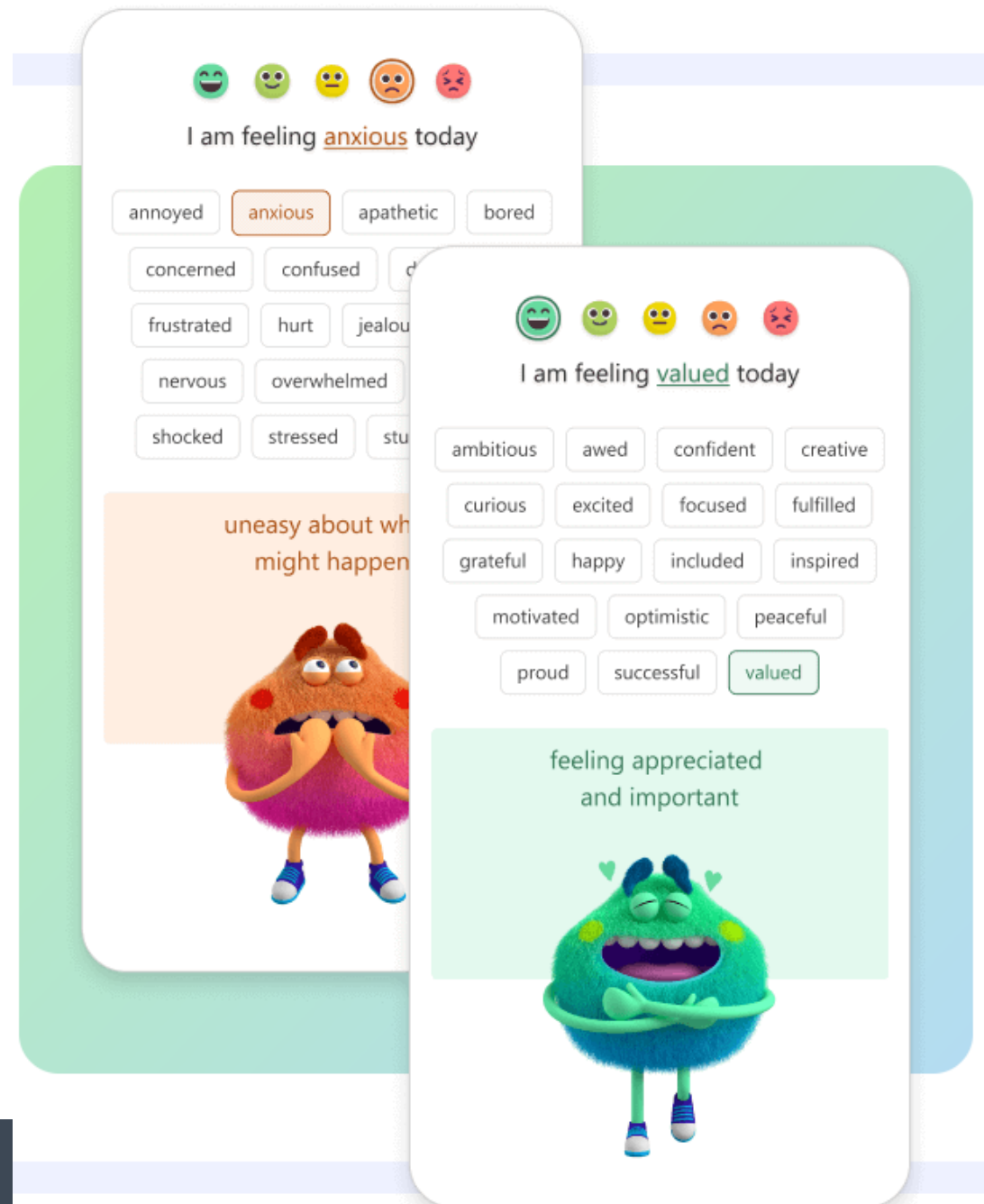


Ik doe toch  
niets fout?



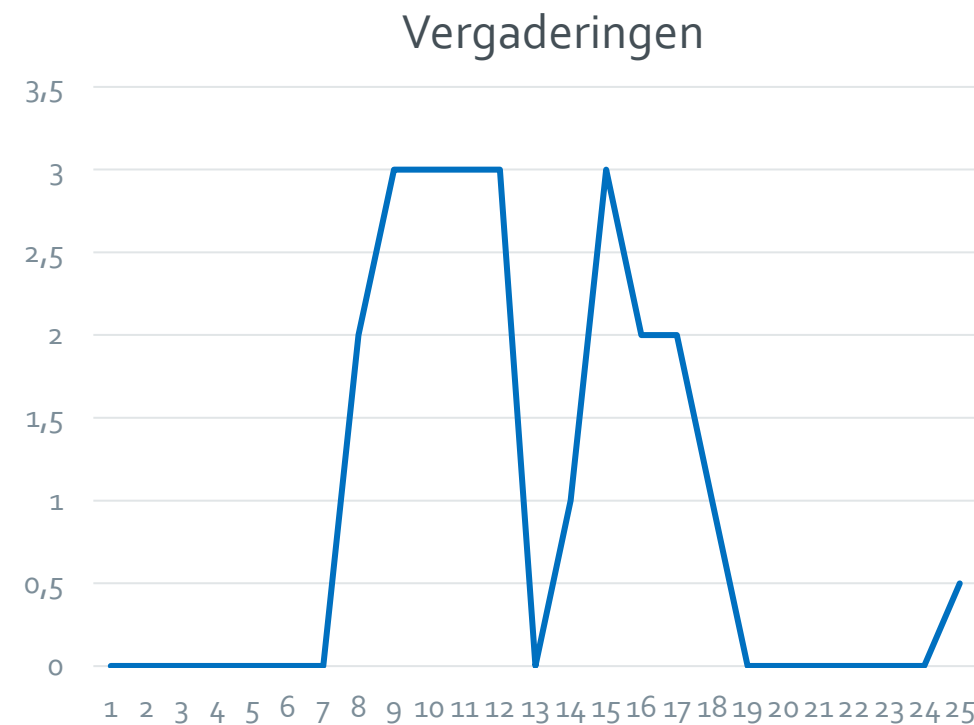
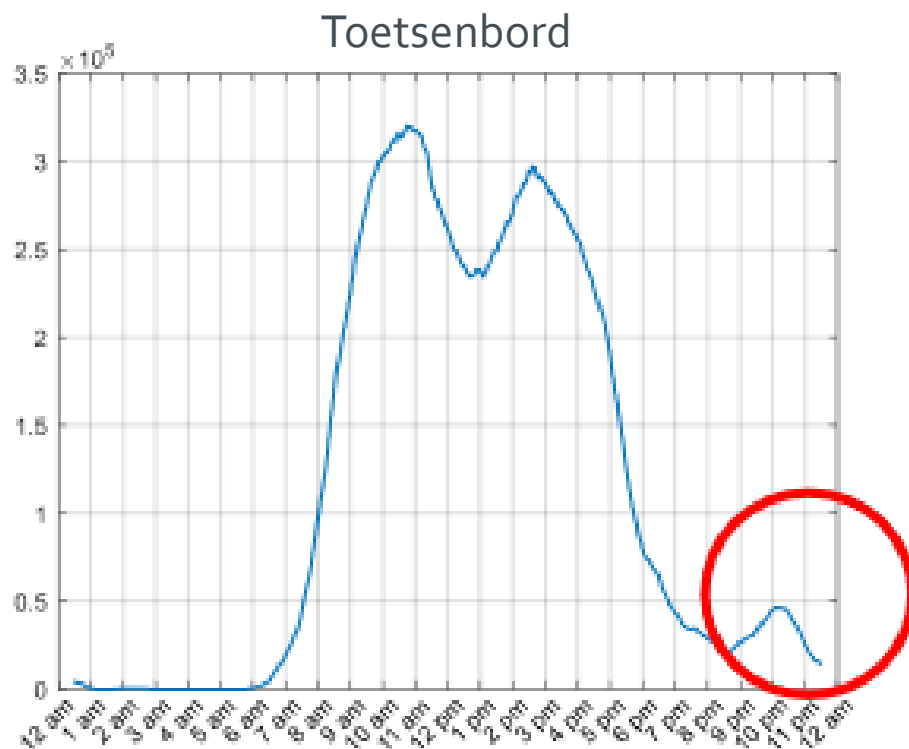
## Clouddiensten en analytics

- Steek je hand op als je niet werkt met Microsoft Office en/of Windows.
- Clouddiensten weten heel veel over jou en je dagelijkse gedrag.
- Ze maken ongevraagd heel veel analytics hoe efficiënt je werkt, maar ook, hoe je je voelt...

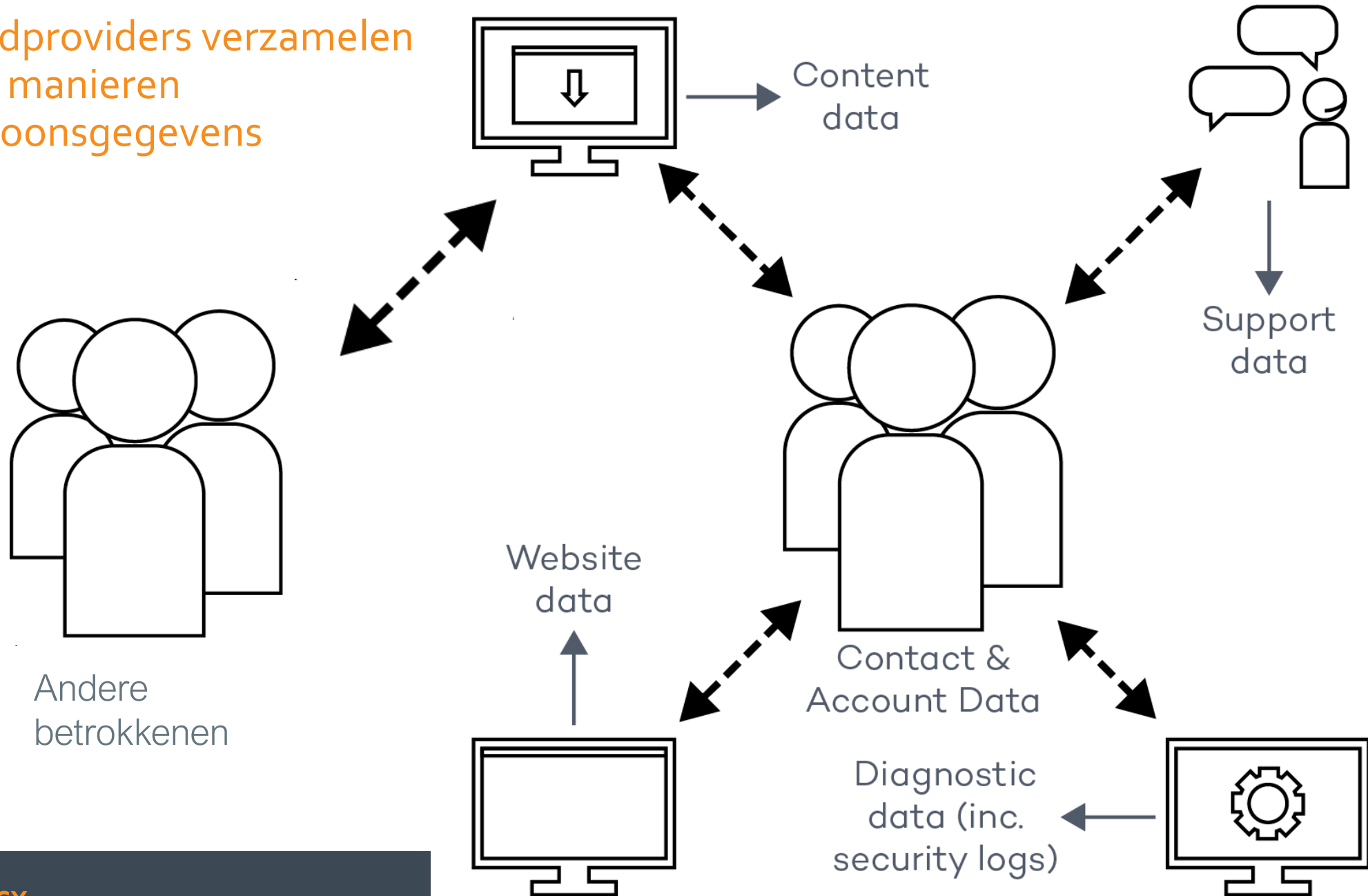


## Jouw privacy als werknemer

- Uit de analytics kunnen Microsoft èn jouw manager allerlei conclusies trekken. Maar wie is de productiefste werknemer?



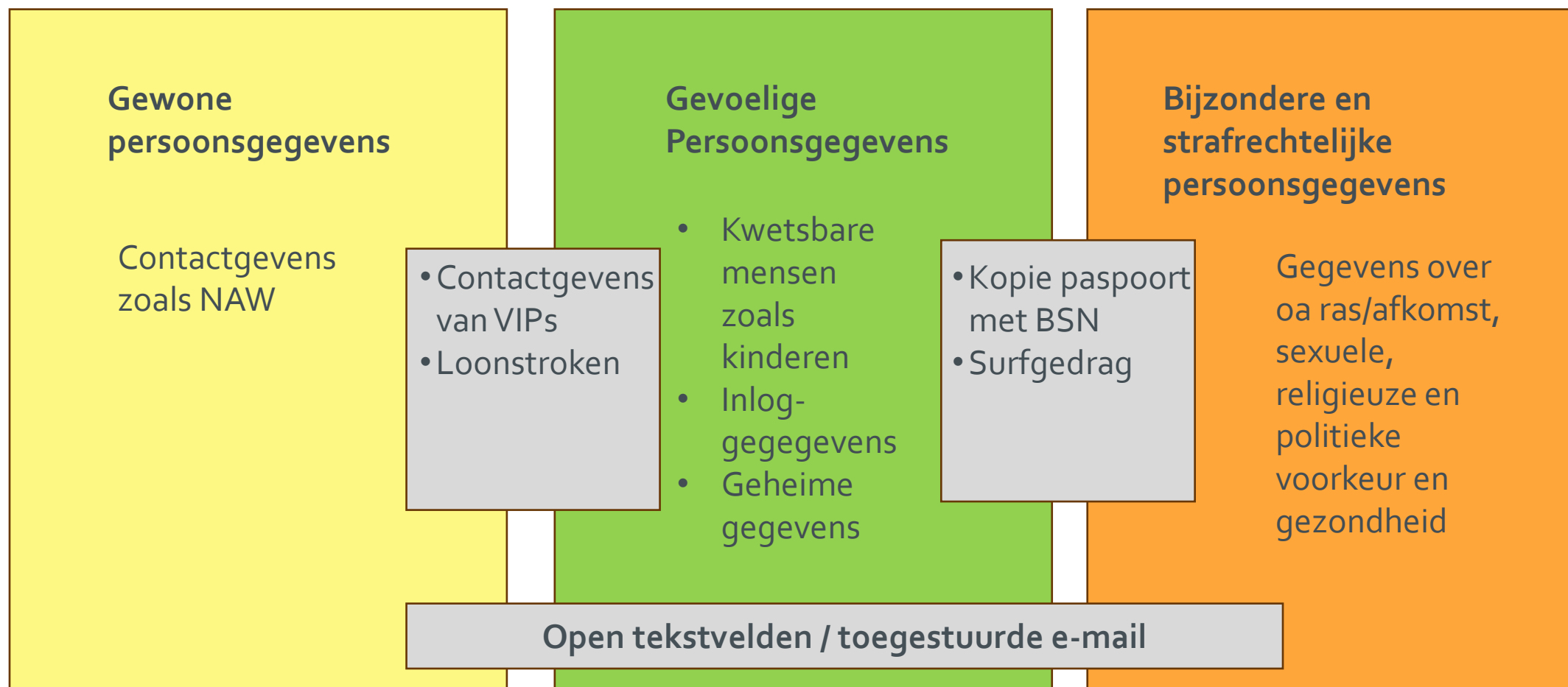
cloudproviders verzamelen op 5 manieren persoonsgegevens



## Wat weet Big Tech over jou als werknemer?

- De gegevens die jij zelf actief mailt/uploadt/deelt, dan wel gegevens die bv HR over jou uploadt: de Content Data
- Je accountnaam, wachtwoord, e-mailadres, je functie en je autorisaties, en eventueel een pasfoto: Account Data
- Gegevens over je gebruik van de dienst: Diagnostic Data, inclusief tijdstip van in- en uitloggen, hoe vaak je bv de spellingscorrectie of vertaling gebruikt, een aparte informatiestroom vanuit je apparaat over je handelingen, registraties in security logs of je spam of malware ontvangt
- Cookies bij het gebruik van een browser app, maar ook, als je systeembeheerder bent, gebruik van de beheerders console
- Als jij, of een systeembeheerder een hulpverzoek hebt ingediend met gegevens van of over jou, bijvoorbeeld in een crash dump

## Gewone, gevoelige en bijzondere persoonsgegevens







# Google Fired 80 Employees Over Data Misuse

NSA hackt Belgische cyberprof

# Former Twitter Employee Convicted of Spying for Saudi Arabia

Vooral VIP's lopen een risico, de medische dossier van de Haagse DAIWIE, ut

# Microsoft confirms it was breached by hacker group

Maar ook werknemers met toegang tot gevoelige persoonsgegevens kwetsbaar winst belu

# Gegevens van Belastingdienst zijn goudmijn voor criminelen

Amerikaanse geneime dienst NSA en zijn Britse tegenhanger GCHQ. Zo staat in de oktoberkrant van De Standaard

voor een 35-gram

# Veel onderzoeken Privacy Company voor het Rijk, voor de universiteiten en voor de scholen

- Een DPIA is een Data Protection Impact Assessment, een onderzoek of de verwerking van persoonsgegevens leidt tot privacyrisico's.
- Het Rijk heeft een eigen model, de Model DPIA Rijksdienst.
- DPIA met hoge privacyrisico's vormt het startpunt voor onderhandelingen met Big Tech.



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

## Rapportagemodel DPIA Rijksdienst


Versie	2.0
Contact	5.1.2.e 5.1.2.e
Datum	3 mei 2022
Status	Definitief

# DPIA's op BigTech



<https://slmmicrosoftrijk.nl/downloads-dpias/>

## DPIA aanpak Privacy Company: juridisch en technisch



The large print  
giveth, but the  
small print taketh  
away.



**Analyse raamwerk contracten**  
vaak veel verschillende documenten

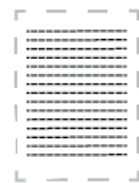


# Techniek: verschillende soorten gegevens

## Kantooractiviteiten werknemer



Content



Functioneel



Diagnostisch

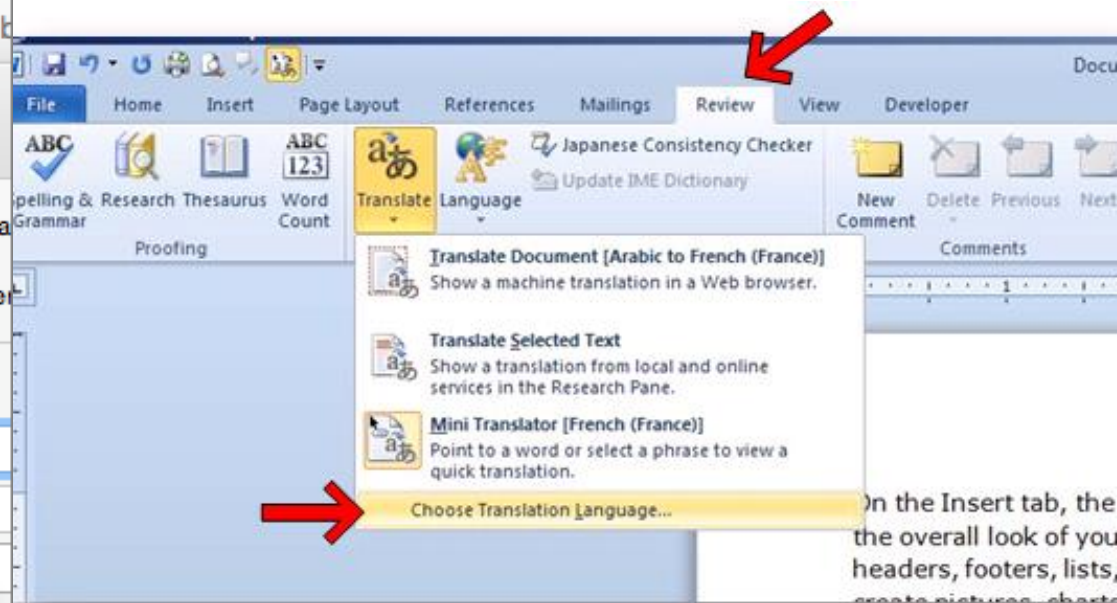
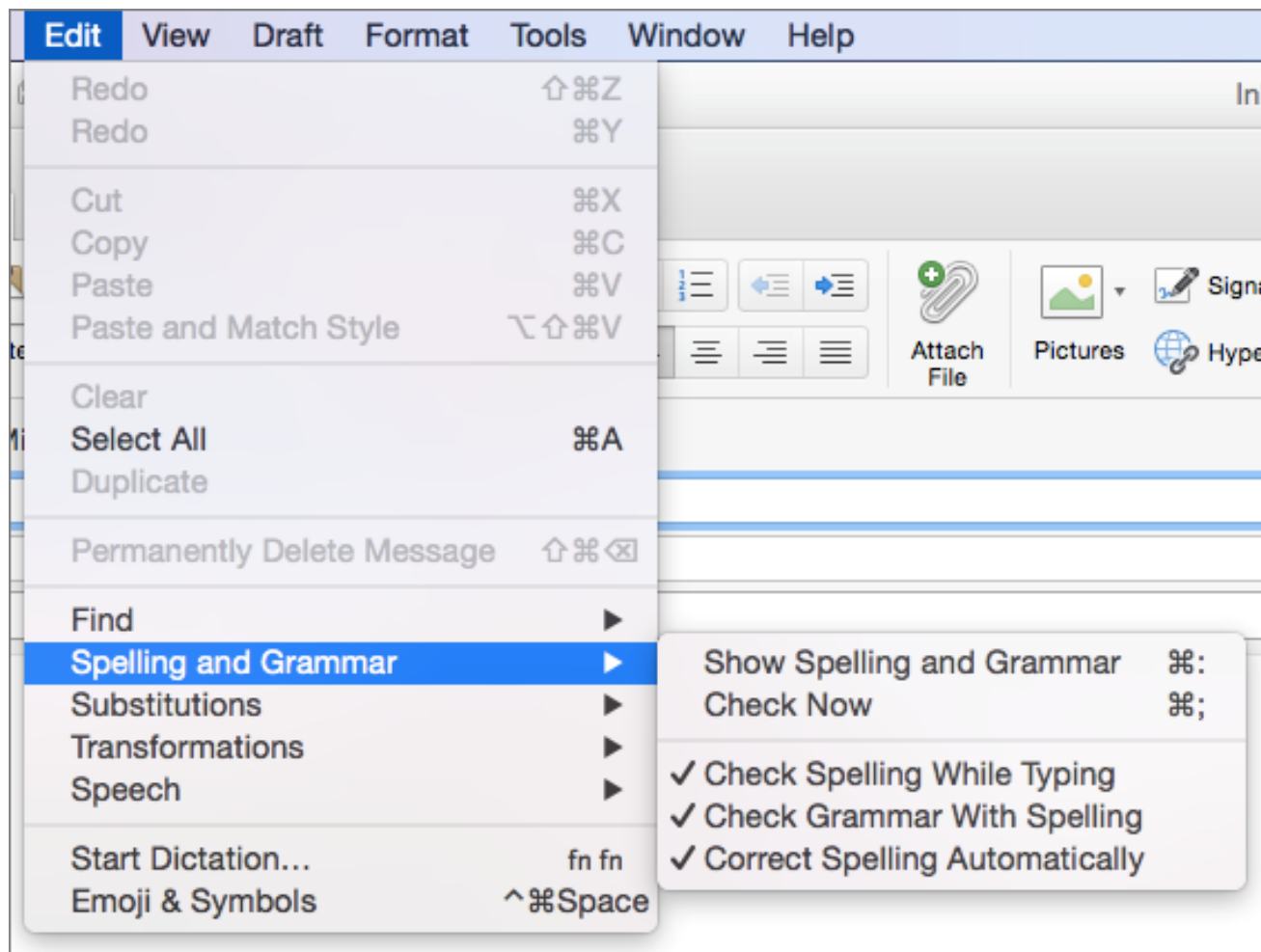


**DATA**



**METADATA**

# 2018: Ophief over Word spellingchecker en vertaaldiensten in de cloud





## Dataproductierisico'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 (nummers worden namen)
- 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 bij cloud providers

- 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 datalek bij de cloud provider of bewuste verstrekking aan overheidsdiensten
- Daarnaast risico's in de eigen organisatie als die de logs en analytics inzet als personeelsvolgsysteem.

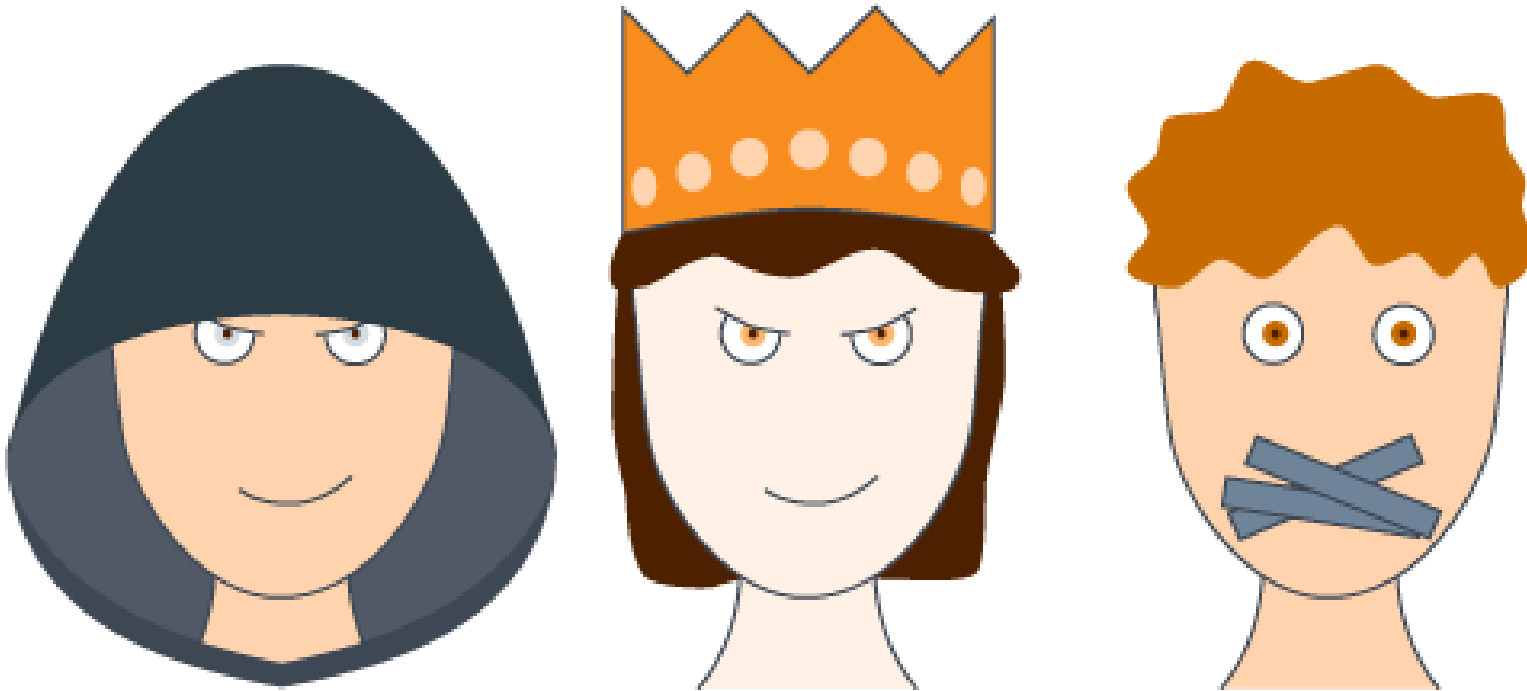
# Terugkerend probleem: de cloud provider als verantwoordelijke



## Terugkerende hoge risico's bij cloud providers

- 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 datalek bij de cloud provider of bewuste verstrekking aan overheidsdiensten
- Daarnaast risico's in de eigen organisatie als logs en analytic tools gebruikt kunnen worden als personeelsvolgsysteem.

## Drie risico's onrechtmatige toegang tot gegevens bij cloudprovider



## Resultaten onderhandelingen Rijk en universiteiten met cloudproviders

- Strakke verwerkersovereenkomsten voor alle 5 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 diagnostische gegevens kunnen bekijken
- Uitgebreide publieke documentatie over de verschillende soorten verwerkte persoonsgegevens
- Afspraken doorgezet in de contracten met alle subverwerkers
- Auditrecht: trust but verify
- Onrechtmatige toegang: verhuizing van de meeste verwerkingen naar Europese cloud

SURF is de ICT inkoopcoöperatie van de Nederlandse universiteiten en hogescholen.  
[www.surf.nl](http://www.surf.nl)

# 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 over  
door Microsoft.

De heer Öztürk (DENK) heeft tijdens regeling van w  
november gesproken over berichtgeving in de medi  
opslag door Microsoft<sup>1</sup>.

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 365

Products

Resources

Support

Buy now

January 8, 2020

## Updated Microsoft Online Services available to our customers around

By The Microsoft 365 Marketing Team

Share

Today, we published the updated [Microsoft Online Services Terms](#) with the changes

As Julie Brill, Microsoft's Corporate Vice President for Privacy and Regulatory Affairs, [commercial cloud customers](#), these changes provide our customers with more transparency on data processing in the Microsoft cloud, and increase Microsoft's data protection responsibilities for a subset of data processing that we engage in when we provide commercial cloud services. As of today, the updated terms are available to all our commercial customers—public sector and private sector, large enterprises, and small and medium businesses—globally.



MUST READ DIGITAL TRANSFORMATION PROJECTS ARE A NIGHTMARE. HERE'S HOW TO GET THEM ON TRACK

### 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.



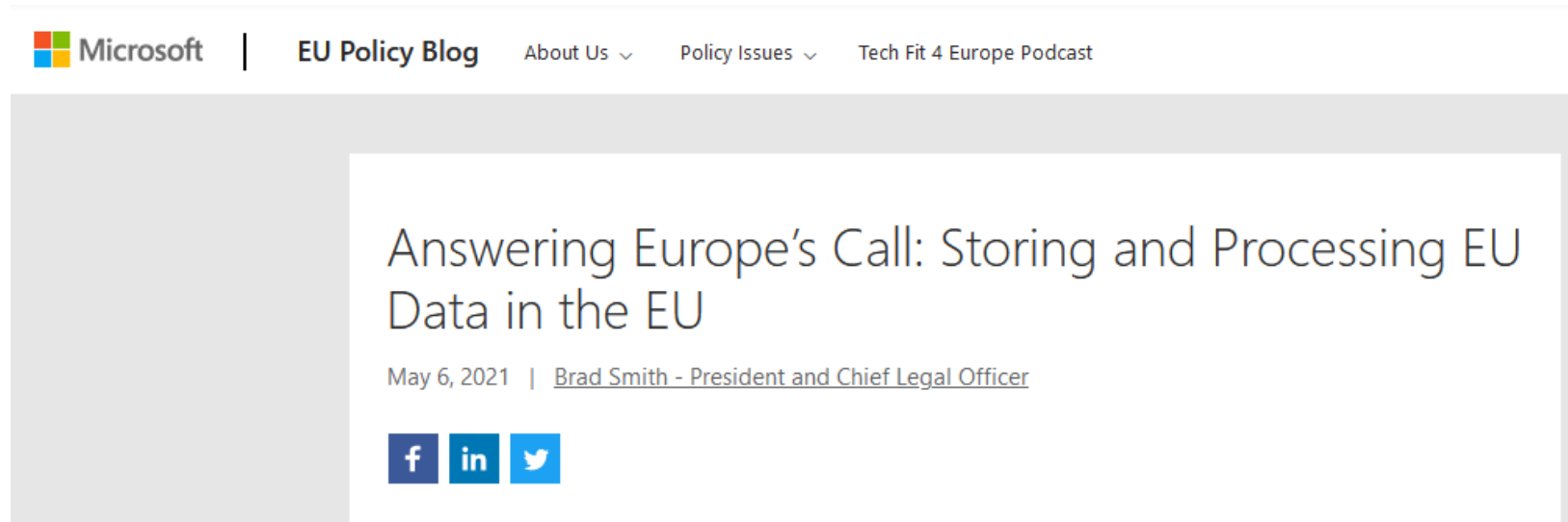
By Liam Tung | January 9, 2020 -- 13:22 GMT (05:22 PST) | Topic: CXO



[/transparency for our](#)



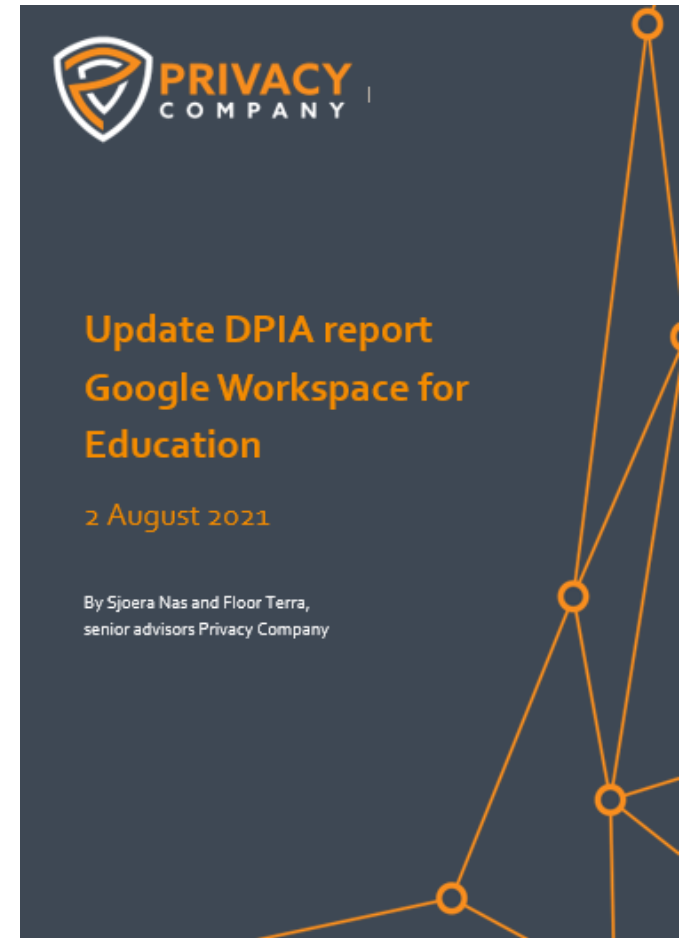
# Mei 2021: Microsoft belooft alle gegevens eind 2022 in de EU te verwerken



Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the EU. This commitment will apply across all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365. We are beginning work immediately on this added step, and we will complete by the end of next year the implementation of all engineering work needed to execute on it. We're calling this plan the EU Data Boundary for the Microsoft Cloud.

## Google verbeteringen onderhandeld door de universiteiten

- Google treedt op als verwerker voor de diagnostische data, verwerking voor 3 ipv 33 doelen
- Google gaat veel meer documentatie publiceren
- Google wordt ook verwerker voor de Chrome browser en het Chrome OS op Chromebooks, uiterlijk september 2023
- Organisaties moeten zelf nog wel heel veel maatregelen nemen om de hoge risico's te mitigeren



# 33 doelen Google's algemene privacyverklaring

- 1. Providing our service**
- 2. Help users share content** by suggesting recipients from their contacts.
- 3. Maintaining the service by tracking outages**
- 4. Troubleshooting user reported issues**
- 5. Make improvements to the services**, for example *understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services*. This purpose is also described in a slightly different way later in the Privacy Policy as: *"Understanding how people use our services to ensure and improve the performance of our services"*
- 6. Develop new products and features** that are useful for our users
- 7. Provide recommendations** For example, *Security Checkup provides security tips adapted to how you use Google products*
- 8. Provide personalised content**, for example based on information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like
- 9. Customizing our services** to provide you with a better user experience, provide customised search results
- 10. Providing advertising** which keeps many of our services free (and when ads are personalized, we ask for your consent)
- 11. Show personalized ads** based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google.
- 12. Share information that personally identifies you with advertisers**, such as your name or email, only if you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.
- 13. Create analytical data** to
- 14. Optimize product design**, For example, we analyze data about your visits to our sites to do things like optimize product design
15. Enable advertisers to **combine information with Google Analytics**, When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.
- 16. Use data for measurement**, for example data about the ads you interact with to help advertisers understand the performance of their ad campaigns.
- 17. Communicate with you to interact with you directly**. For example, we may send you a notification if we detect suspicious activity,
- 18. Inform you about upcoming changes or improvements to our services.**
- 19. Marketing** to inform users about our services
- 20. Provide support if you contact Google**, to help solve any issues you might be facing.
- 21. Improve the safety of our services**. This includes detecting, preventing, and responding to fraud, security risks, and technical issues that could harm Google, our users, or the public.
- 22. Detect abuse** such as spam, malware, and illegal content by analyzing your content
- 23. Protecting against harm to the rights, property or safety of Google, our users, or the public** as required or permitted by law, including [also slightly differently defined as: "Fulfilling obligations to our partners like developers and rights holders AND Enforcing legal claims, including investigation of potential violations of applicable Terms of Service"]
- 24. Disclosing information to government authorities** Also slightly differently defined as: "To respond to legal process or an enforceable governmental request."
- 25. Improve the reliability of our services**. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services.
- 26. Use algorithms to recognize patterns in data**. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.
- 27. Combining information among all services and across devices to improve Google's services and the ads delivered by Google**, For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.
- 28. Help other users identify you**, If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo.
- 29. Use cookies for many purposes**. We use them, for example, to remember your safe search preferences, to make the ads you see more relevant to you, to count how many visitors we receive to a page, to help you sign up for our services, to protect your data, or to remember your ad settings.
- 30. To allow specific partners to collect information from your browser or device** for advertising and measurement purposes using their own cookies or similar technologies
- 31. Performing research**, Performing research that improves our services for our users and benefits the public
- 32. When necessary for legitimate business or legal purposes** such as security, fraud and abuse prevention, or financial record-keeping.
- 33. Other purposes not covered in this Privacy Policy**, we'll ask for your consent, for example,
  - Collect your voice and audio activity for speech recognition.
  - Use Location History if you want traffic predictions for your daily commute
  - Use YouTube Watch History to get better video suggestions.
  - if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant.
  - Process your payment information when you buy extra storage for Google Drive.

# Additional purposes Chrome OS and browser

- Store websurfing data in your Google Account by turning on Sync.
- Send standard log information to all sites you visit, including your IP address and data from cookies.
- **Use cookies** to deliver the services, **personalize ads** and analyze traffic.
- Intercepting man in the middle types of suspicious activity.
- Prerendering the sites you visit
- **Share the location from mobile devices with Google if you use Google Search,** or with third parties if the user consents, and send the following information:
  - The Wi-Fi routers closest to you;
  - Cell IDs of the cell towers closest to you;
  - The strength of your Wi-Fi or cell signal;
  - The IP address that is currently assigned to your device.
- Send information to Google to check for updates, get connectivity status, estimate the number of active users.
- Send URLs of some pages you visit to Google *when your security is at risk*.
- Storing all queries in Google Search in your Google Account.
- **Predict the word(s) a users wants to search for, even before hitting enter in the Search engine,** based on the individuals browsing history and what other people are looking for.
- Sending limited anonymous information about web forms to **improve Autofill**.
- Process payment information and share with Google Pay.
- Customize your language based on the languages of sites you visit.
- **Send usage statistics** and crash reports to Google.
- **Share aggregated, non personally identifiable information publicly and with partners – like publishers, advertisers or web developers.**
- **Send a unique Adobe Flash identifier** to content partners and websites that use Adobe Flash Access
- Provide access to Additional Services such as Google Translate
- **Install three kinds of unique identifiers** and use these for:
  - Installation tracking
  - Tracking of promotional campaigns
  - Field trials

# Dutch education IT crisis averted as Google agrees to 'major privacy improvements'

'Google has agreed to become more transparent' - over optimistic?

Tim Anderson

Wed 11 Aug 2021 // 07:01 U

14 



Google has agreed to "major privacy improvements" following a threat to ban the use of Google Workspace in education by the Dutch Data Protection Authority (DPA).

In March, Privacy Company concluded that eight out of 10 high privacy risks in Google's productivity suite, Workspace, remained. The Dutch educational institutions then asked the Dutch DPA for advice. At the **end of May** the DPA warned schools and universities to stop using Google Workspace for Education before the start of the new school year.

Now, after what Privacy Company, a data consultancy employed by Dutch education IT cooperatives, **called** Google's "intense negotiations with

## Zoom verbeteringen

Treedt op als verwerker voor alle soorten persoonsgegevens voor alle EU-klienten

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 verbeteringen

Effectieve audit rechten voor universiteiten en overheidsinstellingen

Ècht anonimiseren volgens richtlijnen EDPB (alle EU privacytoezichthouders)

Publieke documentatie van telemetrie en service generated server logs

Versleuteling met eigen sleutels (End to End Encryptie)

Zoom heeft ook een Data Viewer Tool gebouwd voor inzage in de telemetrie

# Resultaten onderhandelingen met 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.



overheid via Microsoft data in handen krijgt zeer klein. Experts denken dat het kritische privacy-oordeel alsnog flinke impact kan hebben.

set of privacy measures Redmond has agreed to with the Dutch government.





## Actualiteiten

- Er zijn en komen naast de Algemene Verordening Gegevensverwerking (AVG, in het Engels: GDPR) heel veel nieuwe Europese wetten die de macht van BigTech inperken.
- Van de AI-verordening tot de Data Act, Digital Governance Act, Digital Services Act, Digital Markets Act en Cyber Resilience Act. Bijvoorbeeld met een verbod op reclame gericht op kinderen, plicht om toegang te geven tot metadata, een verplichting om gegevens ter beschikking te stellen aan wetenschappelijke onderzoekers en minimaal 5 jaar security updates op slimme apparaten.
- Nederlands cloudbeleid en privacyversterking in de digitale Agenda (staatssecretaris Van Huffelen)
- De mededingingstoezichthouders gaan zich ook met privacy bemoeien: BigTech mag zijn monopoliepositie niet misbruiken om toestemming af te dwingen.

# Nieuw besluit Europese Commissie: data zijn veilig in de VS

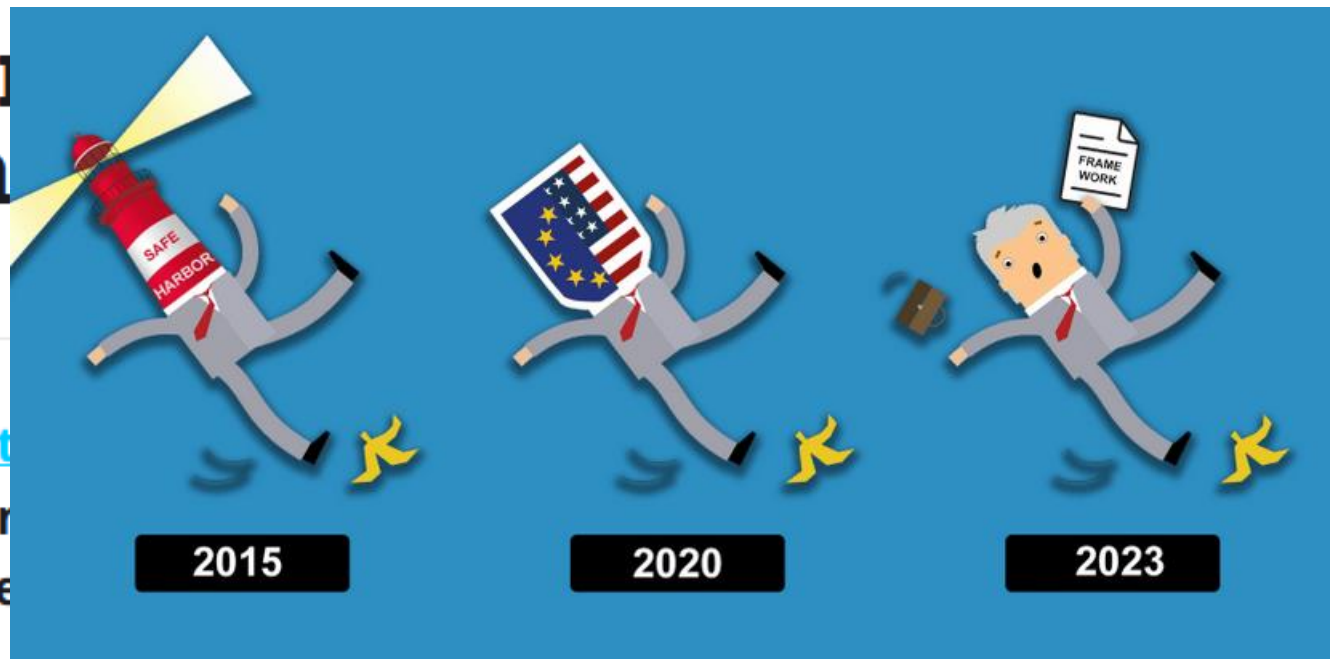
DECEMBER 28, 2004

www.time.com AOL Keyword: TIME

## EU en VS sluiten p weer naar Amerika

🕒 10 juli - 16:00 Laatste update: 16:38

De [Europese Unie](#) en de [Verenigde Staten](#) overdracht van data van Europeanen persoonsgegevens van de EU naar de



Illustratie website NOYB.eu



## Conclusies en take aways 1/3

Iedereen is verantwoordelijk voor privacybescherming. Niet alleen de privacy officer, maar ook:

- de afdeling inkoop om goede privacyvoorwaarden op te leggen
- de ICT-afdeling om de meest privacyvriendelijke instellingen te kiezen
- de OR om je te beschermen tegen personeelsvolgsystemen
- Iedere medewerker voor het tijdig opruimen van e-mails, Teams en intranet



## Conclusies en take aways 2/3

- De Rijksoverheid publiceert allerlei paraplu-DPIA's en onderhandelt met vrijwel alle grote cloudproviders. Gebruik die onderzoeken en volg de aanbevelingen op voor privacyvriendelijke instellingen.
- Werk samen als gemeenten in de VNG bij het beoordelen van applicaties, voer gezamenlijke onderhandelingen over de privacyvoorwaarden.



[https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/Handleiding-privacyvriendelijke-instellingen-Microsoft-365-v1\\_o-Def.pdf](https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/Handleiding-privacyvriendelijke-instellingen-Microsoft-365-v1_o-Def.pdf)

## Conclusies en take aways 2/2

- Denk ook eens na over open source alternatieven.
- Gebruik je Google Analytics? Verdiep je in een Europees of niet-Amerikaans alternatief zoals Matomo of Plausible. De Radboud universiteit heeft een pilot gedaan, en geeft antwoord op bijna alle bezwaren van marketeers.



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

<https://nogadata.nl>

## Do It Yourself!

- Cloud providers reageren per definitie afwijzend op je vraag om aanpassingen, maar geef niet op, wees het kleine trimvlak dat het grote roer aanstuurt!



“Something hit me very hard once, thinking about what one little man could do. Think of the Queen Mary — the whole ship goes by and then comes the rudder. And there's a tiny thing at the edge of the rudder called a trimtab.

It's a miniature rudder. Just moving the little trim tab builds a low pressure that pulls the rudder around. Takes almost no effort at all. So I said that the little individual can be a trimtab. Society thinks it's going right by you, that it's left you altogether. But if you're doing dynamic things mentally, the fact is that you can just put your foot out like that and the whole big ship of state is going to go.

› I said, call me Trimtab.”



*Buckminster R. Fuller*



# Vragen?

[www.linkedin.com/in/sjoera](http://www.linkedin.com/in/sjoera)

[www.privacycompany.eu](http://www.privacycompany.eu)

[info@privacycompany.nl](mailto:info@privacycompany.nl)

070 – 820 96 90

Maanweg 174

Den Haag

