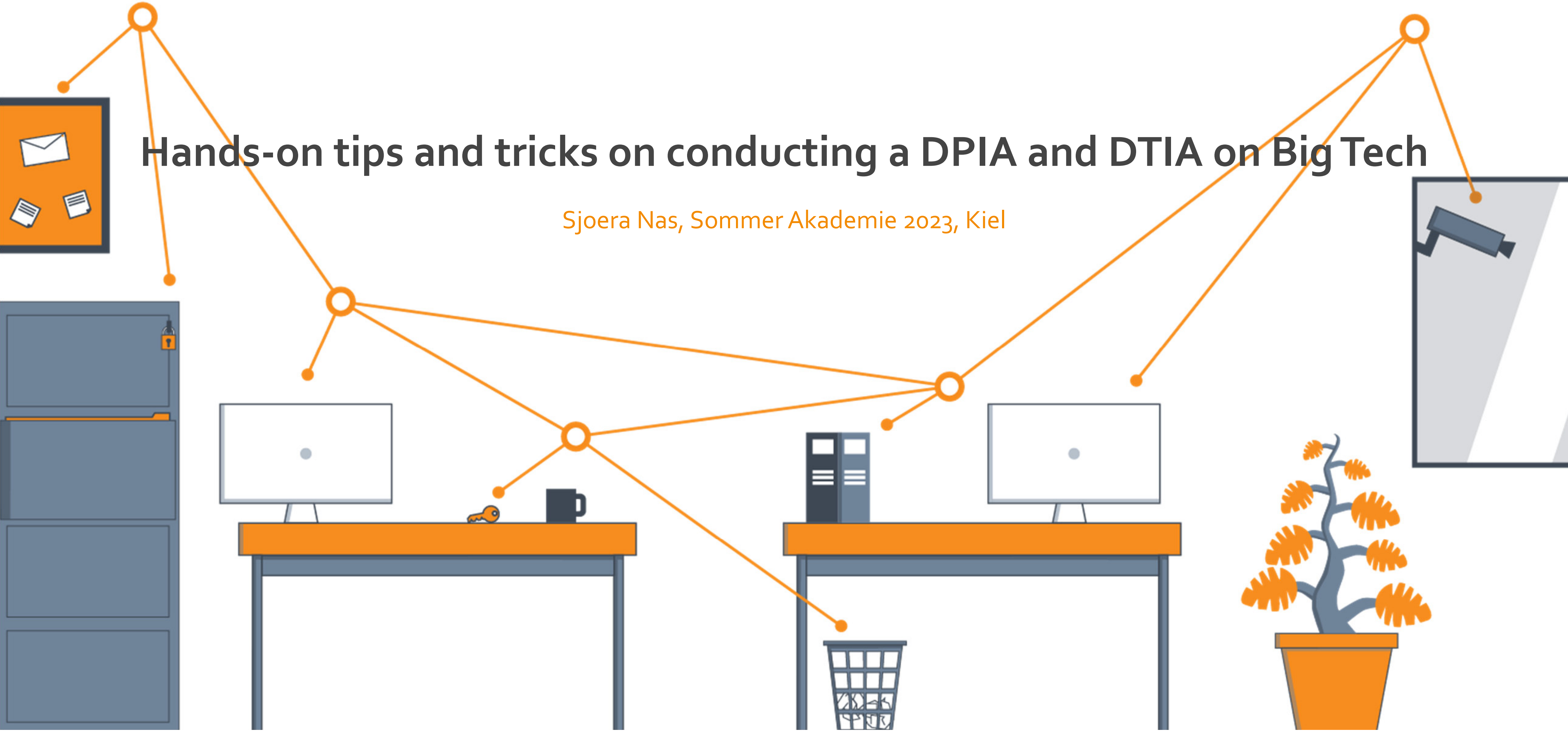
PRIVACY COMPANY

Hands-on tips and tricks on conducting a DPIA and DTIA on Big Tech

Sjoera Nas, Sommer Akademie 2023, Kiel



Experience with DPIAs (including work in progress)

facebook

Meta Quest

SAP®

Windows 11

Microsoft Intune

salesforce

Azure

Microsoft Office 2016

Windows 10 Enterprise

Microsoft 365

aws

Microsoft Edge

A fast and secure way to get things done on the web

IBM Cloud

BlackBerry

zoom

Google Workspace

chrome enterprise

ORACLE CLOUD

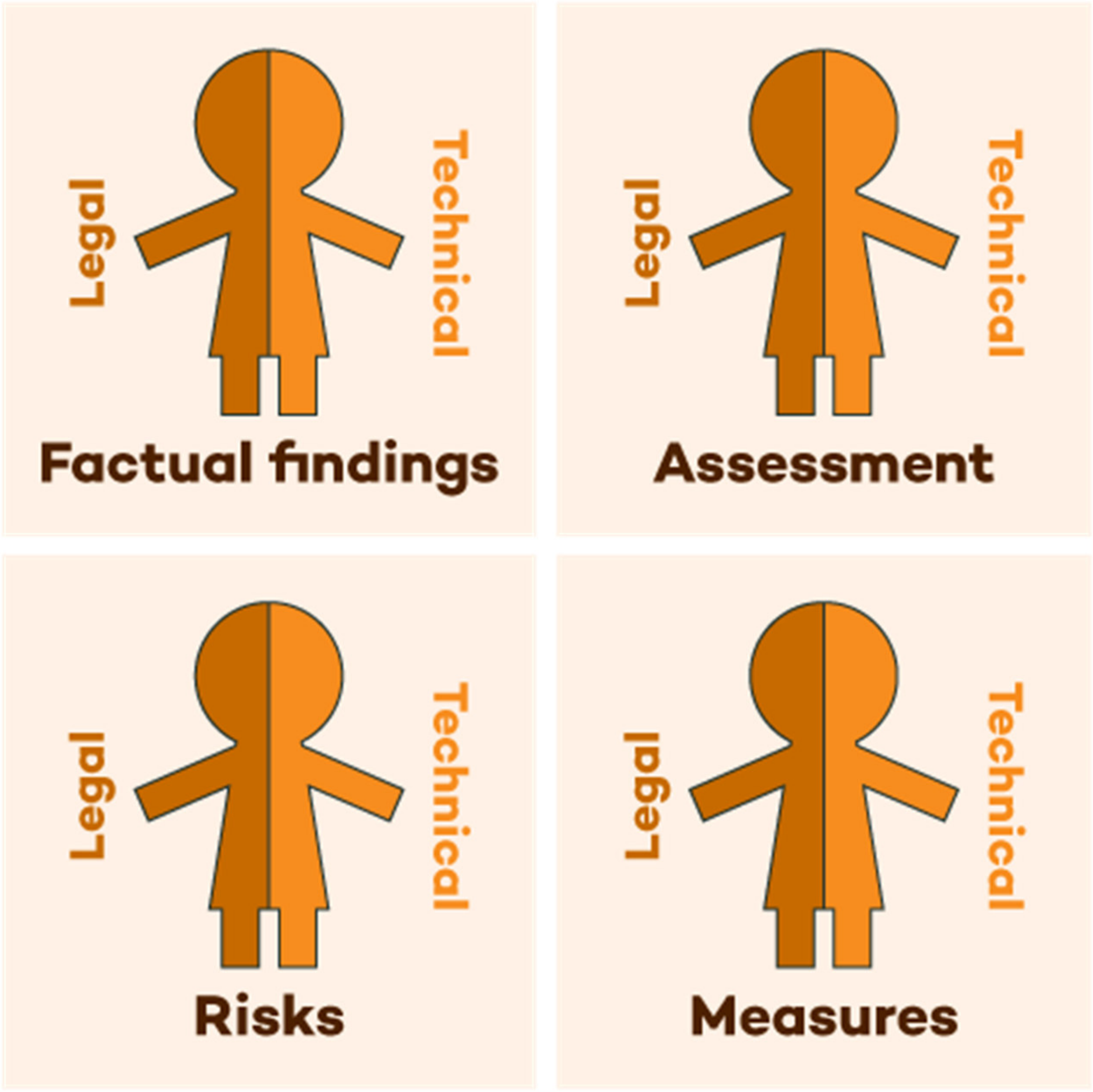
Outline

- Dutch government DPIA model
- Results DPIAs on Microsoft 365, Google Workspace, Chrome, Zoom, Facebook Pages and AWS
- Performing a DTIA
- Your questions

DPIA approach based on Dutch government DPIA model

https://www.avghelpdeskzorg.nl/documenten/publicaties/2022/03/15/model-dpia-rijksdienst-2022

DPIA in 4 parts



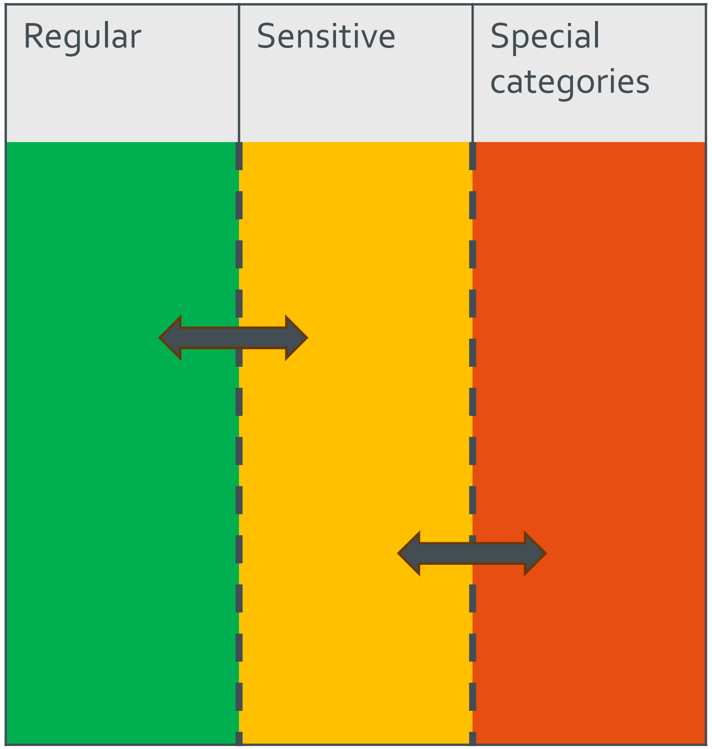
Impact depends on nature of data subject and nature of personal data

Unauthorised processing of sensitive data has a higher impact on data subjects.

Examples:

- Detailed location information over time (visiting religious institutions, hospitals, brothels, etc)
- Data relating to children
- Contents of communications including URLs
- 'Regular' personal data such as the home addresses of politicians and journalists or names and e-mail addresses of system administrators with responsibility for databases containing state secret data.
- In the Netherlands: financial data (salaries!)

3 categories of personal data


Regular
Sensitive
Special categories

How do you determine if a risk is high? Chance x impact

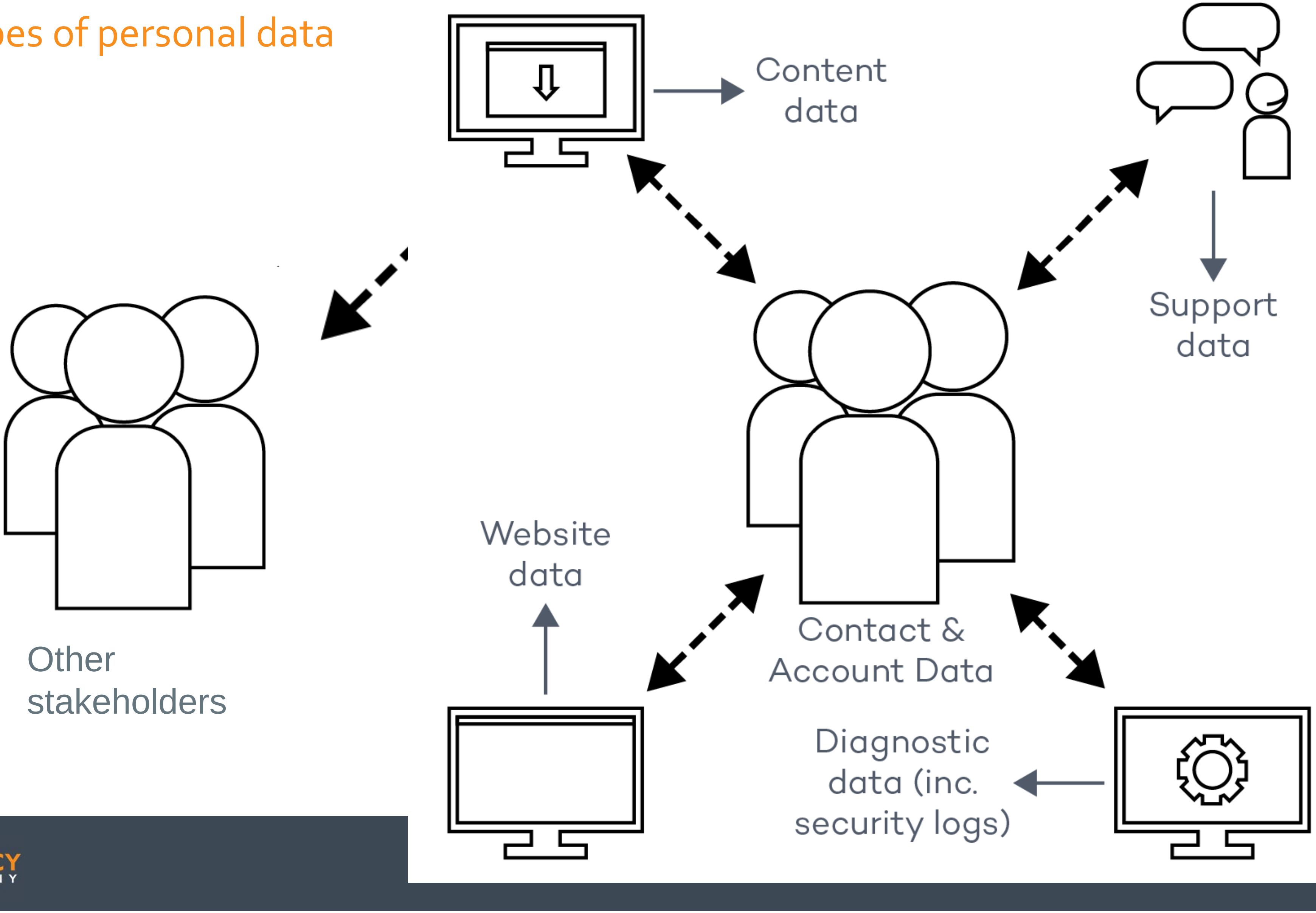
Severity of impact	Serious consequences	Low risk	High risk	High risk
	Some negative consequences	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Very small	Reasonable opportunity	More likely than not
		Probability (likelihood) of the risk occurring		

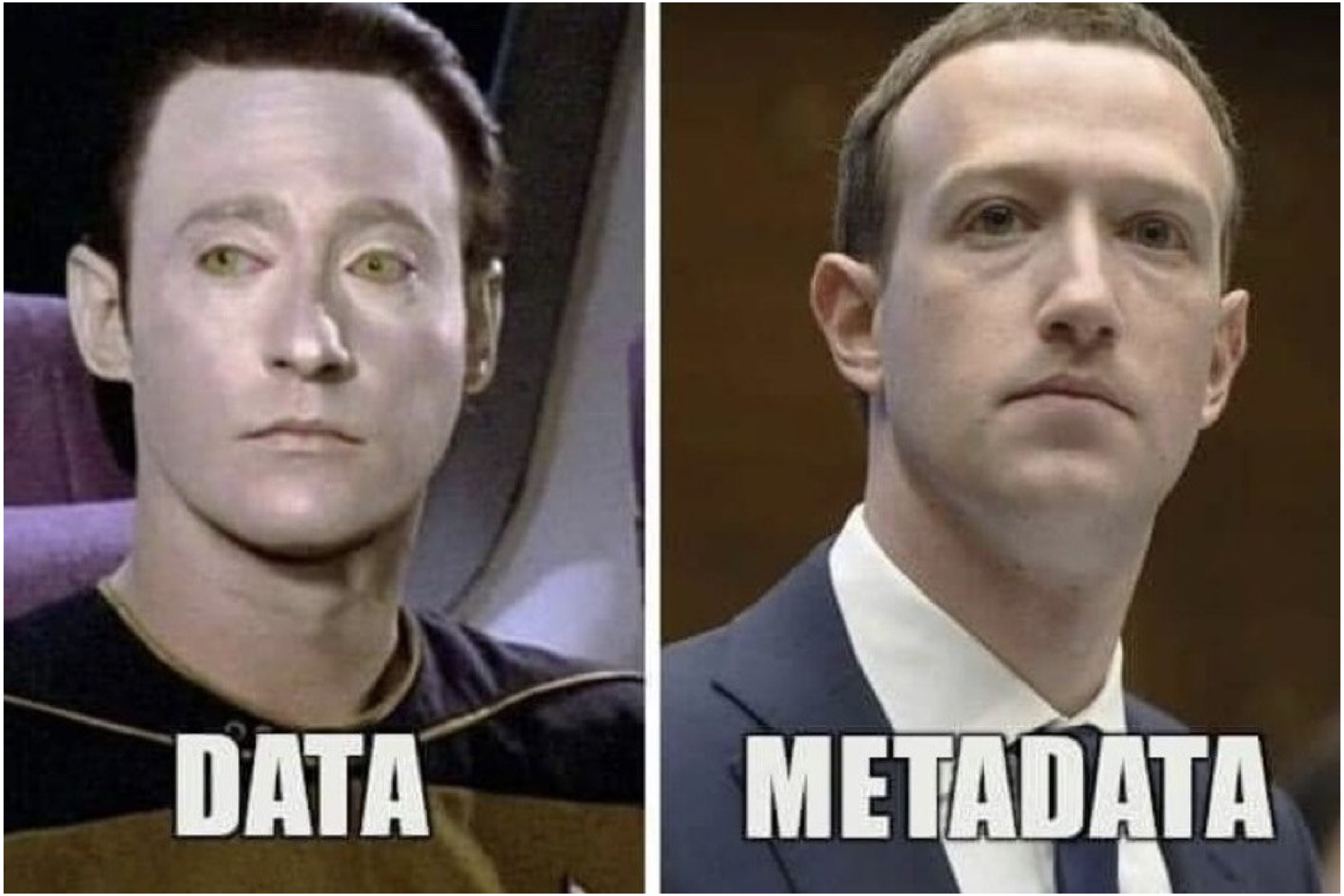
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

Key legal questions DPIA

1. Are the data personal data?
2. Is the data processing sufficiently transparent?
3. What are the purposes of the processing?
4. Can the admin minimise the data collection?
5. Does the provider always act as data processor?
6. Does the Dutch government have an effective right to audit?
7. What are the risks of the transfer of personal data to the USA?
8. How long are diagnostic data retained?

5 types of personal data




DATA
METADATA

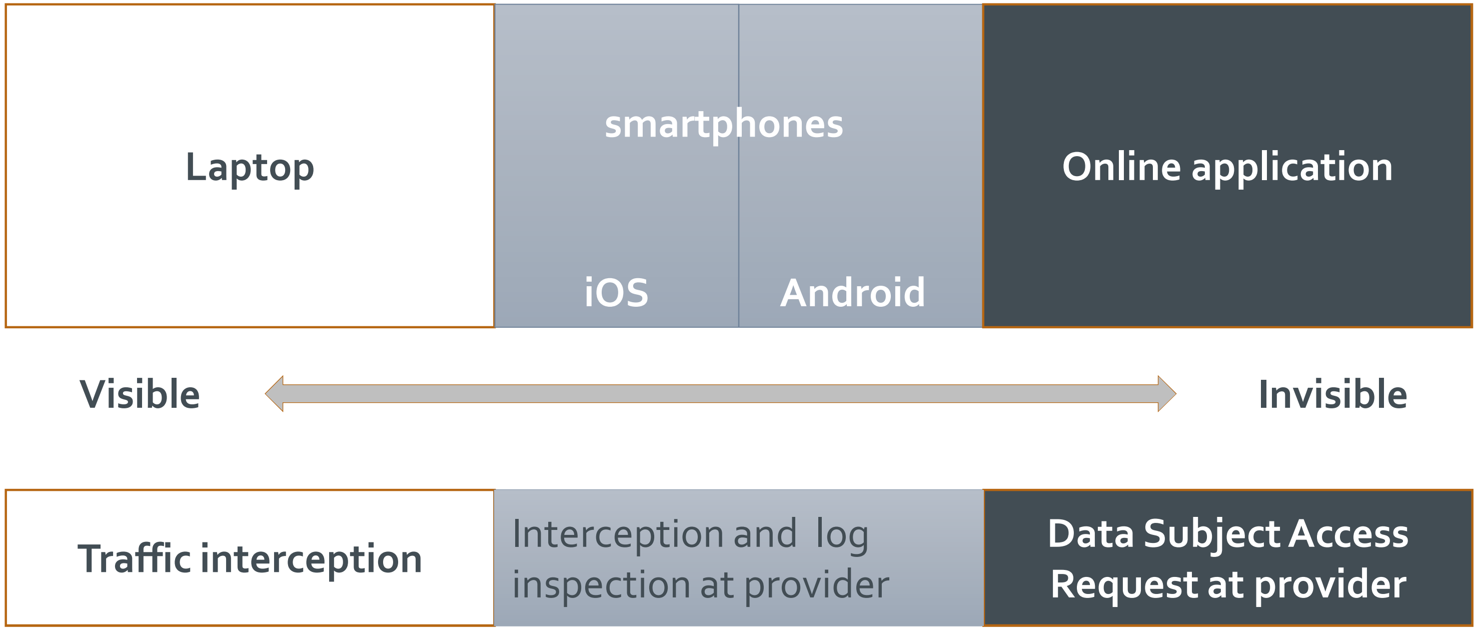
Two types of diagnostic data: telemetry and server logs

- Installed software applications and browsers collect and transmit data on individual use of the services: telemetry

- That traffic is different from strictly functional traffic: no question and answer except acknowledgement!

- In addition, cloud providers record all operations in their own log files: service generated server logs

Inspection methods processing at cloud providers



Laptop

smartphones

iOS

Android

Online application

Visible

Invisible

Traffic interception

Interception and log inspection at provider

Data Subject Access Request at provider

Key legal questions DPIA

1. Are the data personal data?
2. Is the data processing sufficiently transparent?
3. What are the purposes of the processing?
4. Can the admin minimise the data collection?
5. Does the provider always act as data processor?
6. Does the Dutch government have an effective right to audit?
7. What are the risks of the transfer of personal data to the USA?
8. How long are diagnostic data retained?

Trigger keywords for the processing

General Busines Intelligence • Aggregating usage da

Testing • Research • Use of data for machine learning

okies / pixels • Any purpose the supplier deems com

analysis / general inferences based on long term ana

Profiling • Personalisation of the service • Marketing

ct development • Showing targeted recommendati

s for which we seek your consent • Product innovat

33 purposes Google general privacy statement

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 purposes 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*

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, to*
    - 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

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 adds** 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

Key legal questions DPIA

1. Is the data processing sufficiently transparent?
2. What are the purposes of the processing?
3. Can the admin minimise the data collection?
4. Does the provider always act as data processor?
5. Does the Dutch government have an effective right to audit?
6. What are the risks of the transfer of personal data to the USA?
7. How long are diagnostic data retained?

Key problem: cloud provider as data controller

Processor
Controller

Cloud providers either third parties or joint controllers

- Cloud providers often claim to act as data processor, but formal roles and contracts are not leading
- If a processor allows itself to determine processing purposes in its own interest, such as marketing or product innovation, it factually behaves as controller
- Most cloud providers 'forget' to describe the Diagnostic and Website Data: lack of transparency
- If the provider is a third party, or a joint controller, the key data protection risks are that the customer does not have a legal ground for the processing, that there is no purpose limitation, and end users cannot exercise their data protection rights

Main results of negotiations with US cloud providers

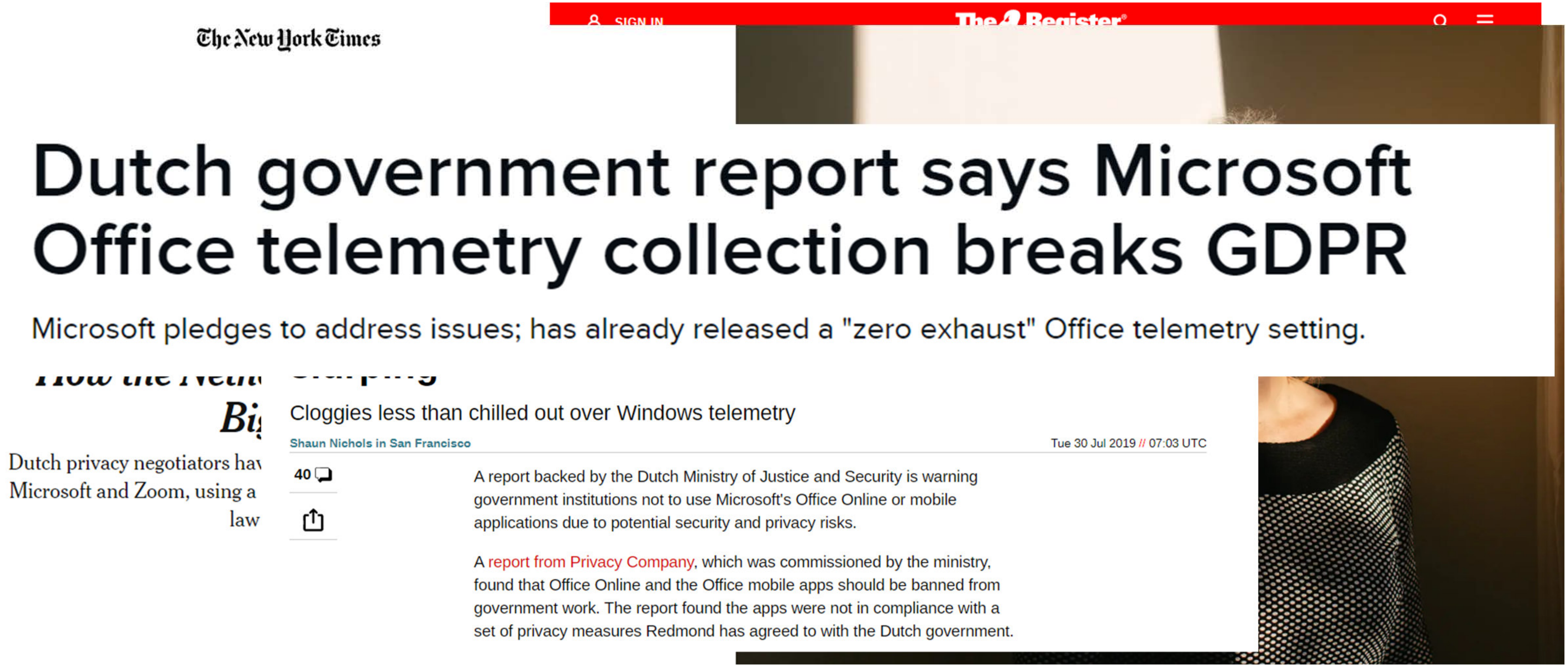
- Strict processor agreements for all types of personal data
- Limitative list of 'further' processing for the legimate business purposes of the provider
- Strict purpose limitation as processor: provide the service, keep it up-to-date and fault-free, including support, and secure the data
- Construction of viewing tool so that end users can view telemetry data themselves
- Comprehensive public documentation on the different types of personal data processed
- Agreements reflected in contracts with all sub-processors
- Audit right: trust but verify
- Moving most processing to a European cloud

Agree on some legitimate business purposes

The provider is allowed to 'further' process some limited personal data, preferably aggregated, as an independent controller, but only when strictly necessary for its own legitimate business purposes

- sending bills and fighting (license) fraud
- approaching commercial contacts for CRM
- measuring the use of the public website
- aggregating limited account and metadata for strictly necessary purposes such as managing capacity
- disclosing personal data to law enforcement and security services, but only if it 1) is not allowed to forward the demand to its customer, 2) is also not allowed to inform the customer and 3) cannot refuse the demand through legal proceedings. A cloud provider in a 3d country violates the GDPR when disclosing personal data to a government authority without MLAT.

Results of DPIA’s on Microsoft, Google, Zoom, Meta and AWS



Dutch government report says Microsoft Office telemetry collection breaks GDPR

Microsoft pledges to address issues; has already released a "zero exhaust" Office telemetry setting.

Bi

Dutch privacy negotiators hav
Microsoft and Zoom, using a
law

Cloggies less than chilled out over Windows telemetry

Shaun Nichols in San Francisco

Tue 30 Jul 2019 // 07:03 UTC

A report backed by the Dutch Ministry of Justice and Security is warning government institutions not to use Microsoft's Office Online or mobile applications due to potential security and privacy risks.

A report from Privacy Company, which was commissioned by the ministry, found that Office Online and the Office mobile apps should be banned from government work. The report found the apps were not in compliance with a set of privacy measures Redmond has agreed to with the Dutch government.

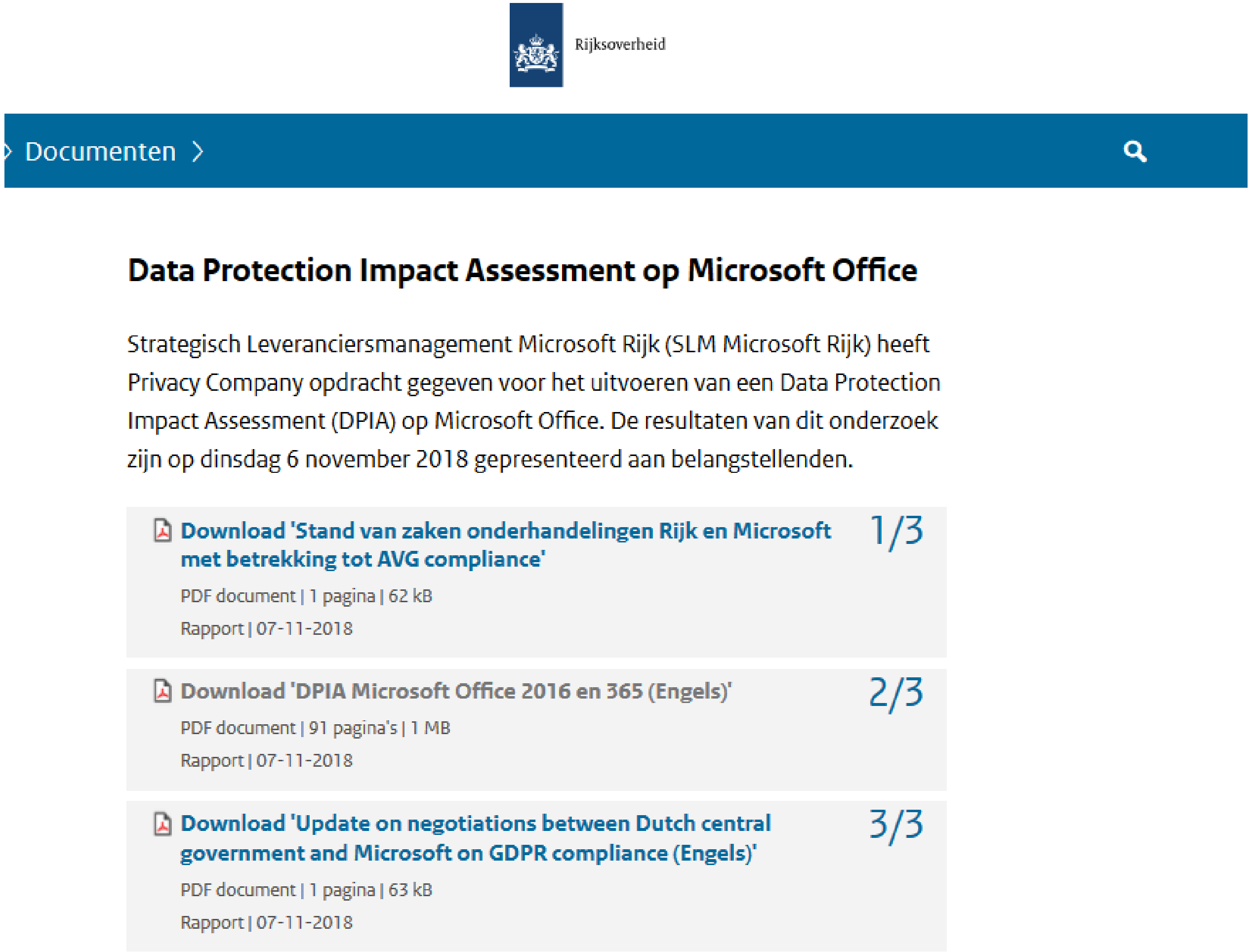
DPIA results Microsoft

DPIAs on Microsoft Office 365, Intune, DKE, Defender, Windows 10/11

DPIAs published in English at https://slmmicrosoftrijk.nl/downloads-dpias/

November 2018: first public DPIA report Office ProPlus for Central Dutch Gov.

- DPIA for SLM Microsoft Rijk on Office 365 ProPlus.
- Office 365 ProPlus collects its own telemetry data, separate from Windows, on a much larger scale
- No transparency about telemetry



Data Protection Impact Assessment op Microsoft Office

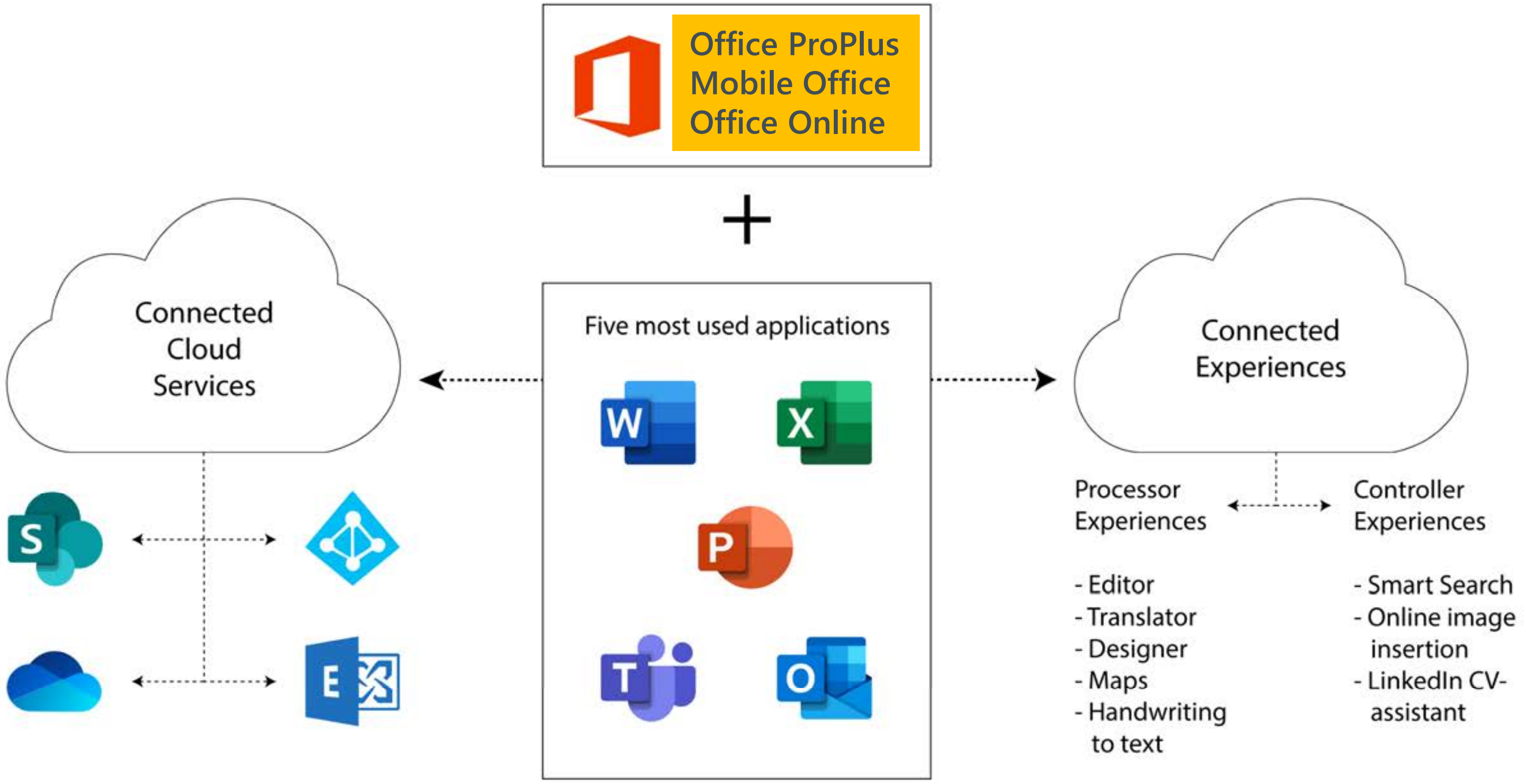
Strategisch Leveranciersmanagement Microsoft Rijk (SLM Microsoft Rijk) heeft Privacy Company opdracht gegeven voor het uitvoeren van een Data Protection Impact Assessment (DPIA) op Microsoft Office. De resultaten van dit onderzoek zijn op dinsdag 6 november 2018 gepresenteerd aan belangstellenden.

Download 'Stand van zaken onderhandelingen Rijk en Microsoft met betrekking tot AVG compliance' 1/3
PDF document | 1 pagina | 62 kB
Rapport | 07-11-2018

Download 'DPIA Microsoft Office 2016 en 365 (Engels)' 2/3
PDF document | 91 pagina's | 1 MB
Rapport | 07-11-2018

Download 'Update on negotiations between Dutch central government and Microsoft on GDPR compliance (Engels)' 3/3
PDF document | 1 pagina | 63 kB
Rapport | 07-11-2018

Services and applications in Office 365



Office ProPlus
Mobile Office
Office Online

+

Connected Cloud Services

Five most used applications

Connected Experiences

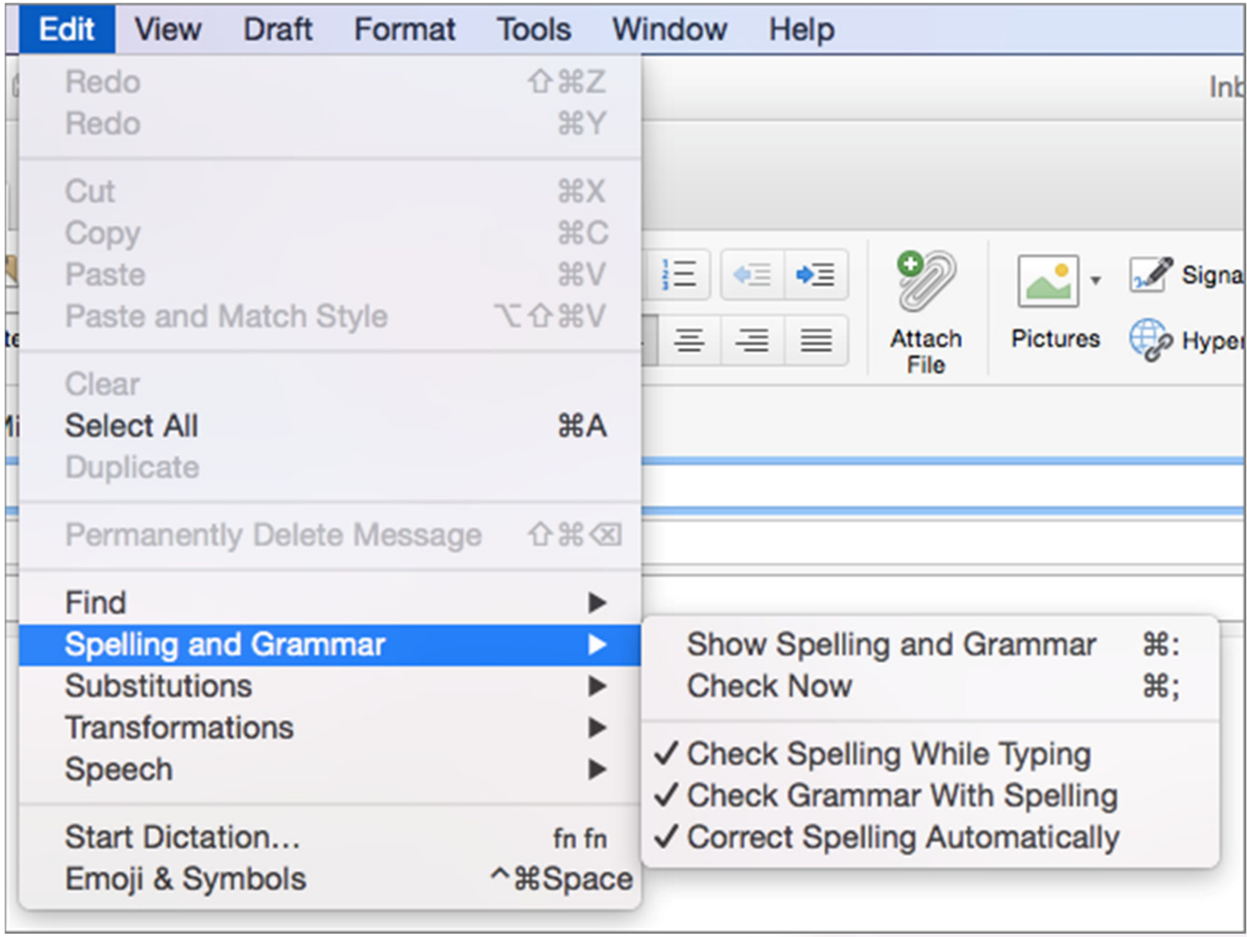
Processor Experiences

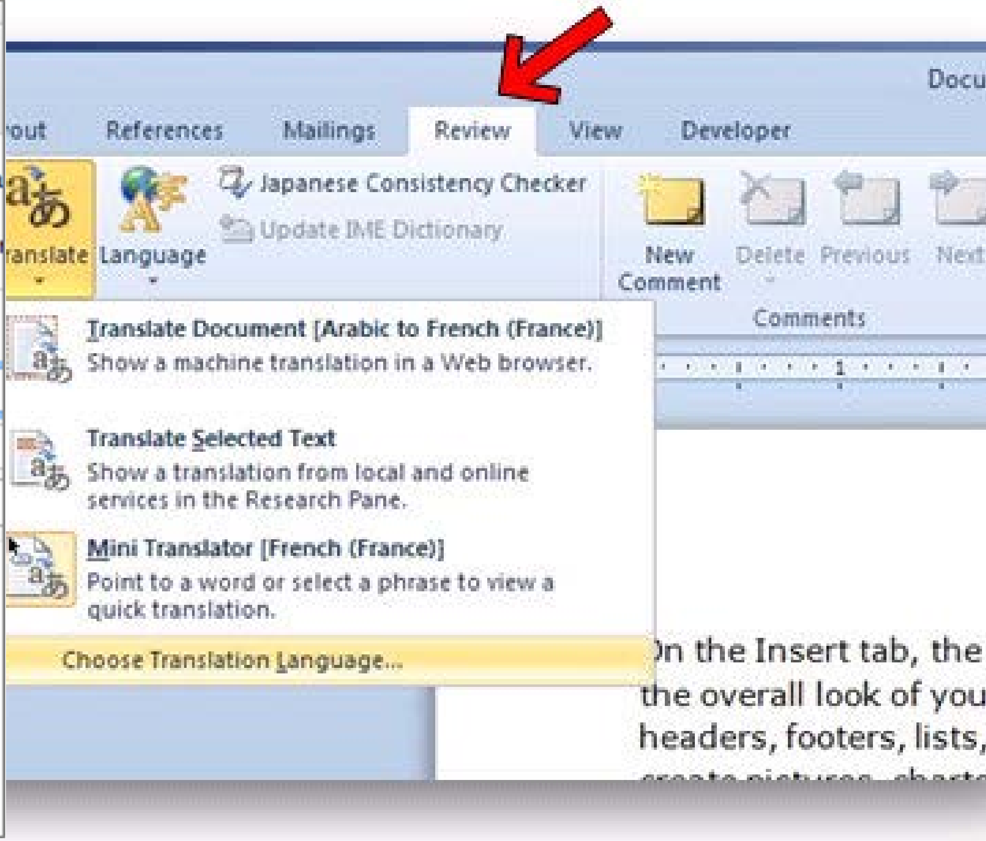
- Editor
- Translator
- Designer
- Maps
- Handwriting to text

Controller Experiences

- Smart Search
- Online image insertion
- LinkedIn CV-assistant

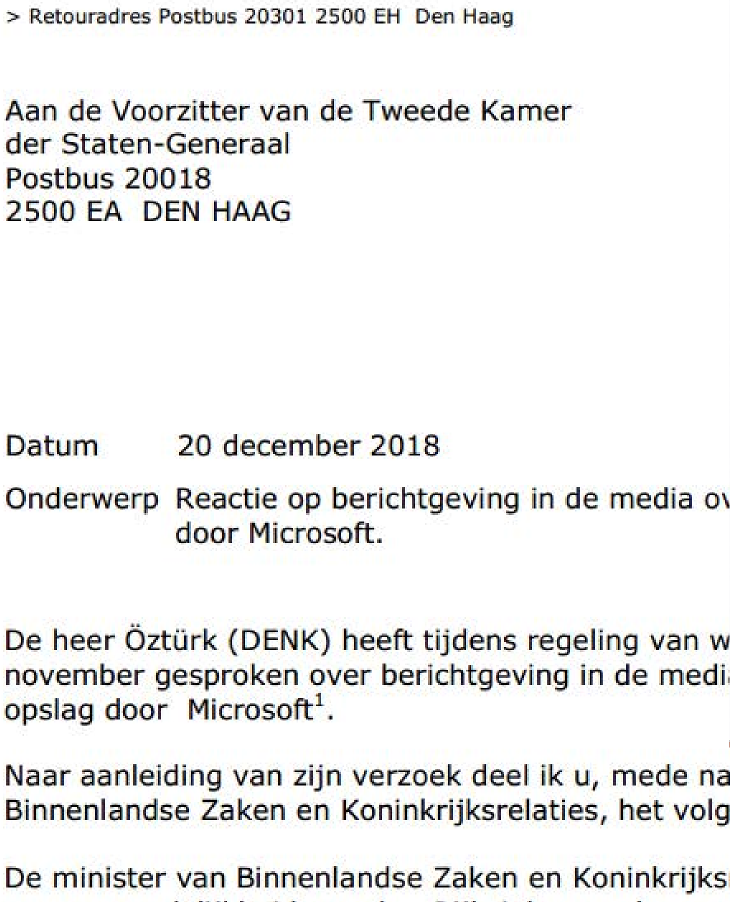
High risks through transfer of content Connected Services




Docu
out
References
Mailings
Review
View
Developer
ranslate
Language
Japanese Consistency Checker
Update IME Dictionary
New Comment
Delete
Previous
Next
Comments
Translate Document [Arabic to French (France)]
Show a machine translation in a Web browser.
Translate Selected Text
Show a translation from local and online services in the Research Pane.
Mini Translator [French (France)]
Point to a word or select a phrase to view a quick translation.
Choose Translation Language...

On the Insert tab, the
the overall look of you
headers, footers, lists,

February 2019: Microsoft announces global changes in Office



> Retouradres Postbus 20301 2500 EH Den Haag

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

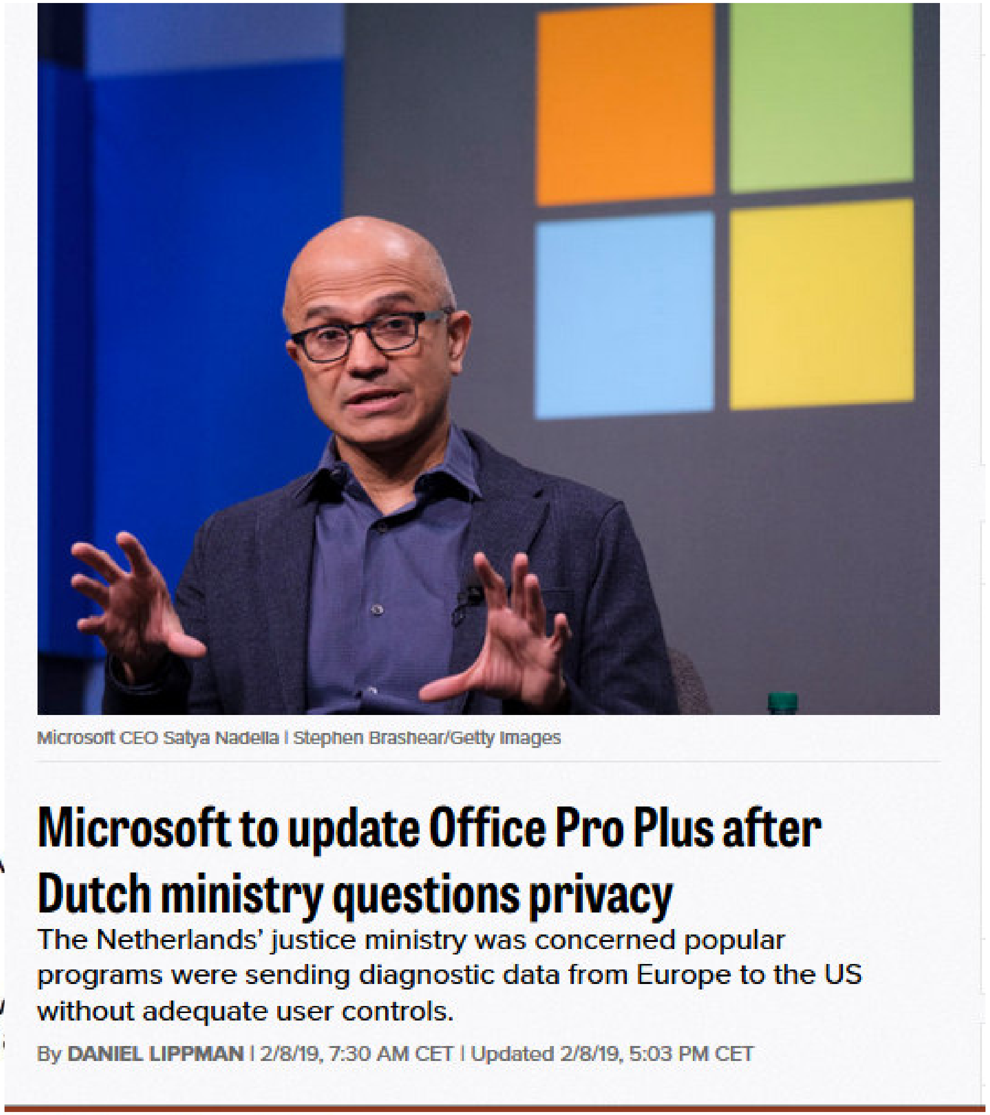
Datum 20 december 2018

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



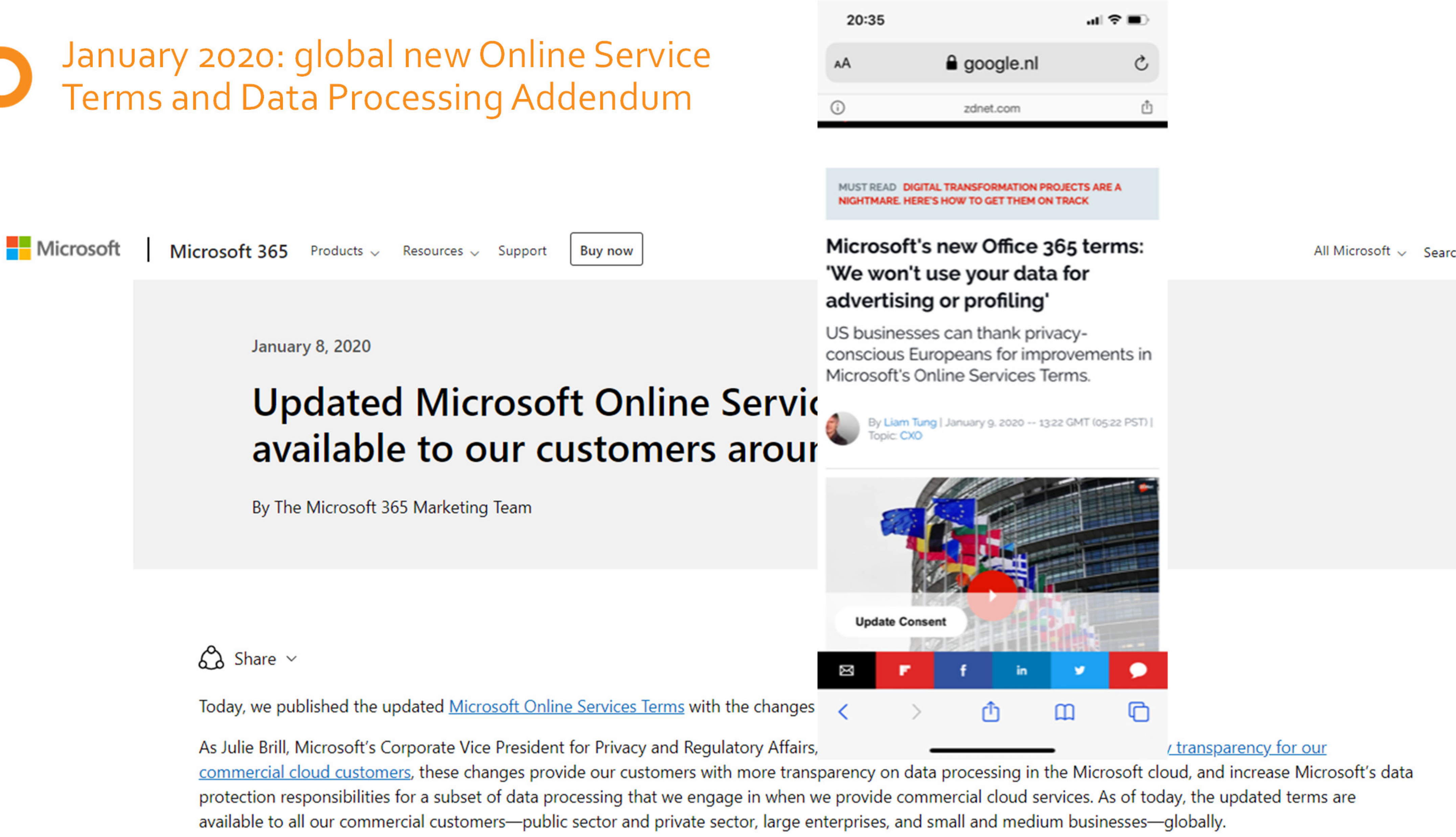
Microsoft CEO Satya Nadella | Stephen Brashear/Getty Images

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

January 2020: global new Online Service Terms and Data Processing Addendum



January 8, 2020

Updated Microsoft Online Servic
available to our customers arour

By The Microsoft 365 Marketing Team

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, transparency for our 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

Specific legal improvements Dutch government

Privacy guarantees apply to *all* personal data

Limitation to 3 purposes: (1) to provide and improve the service, (2) keeping the service up-to-date, and (3) secure.

Prohibition on profiling, market research, targeted ads and data analytics. Ban on ‘recommendations’ for products not purchased or used by the customer

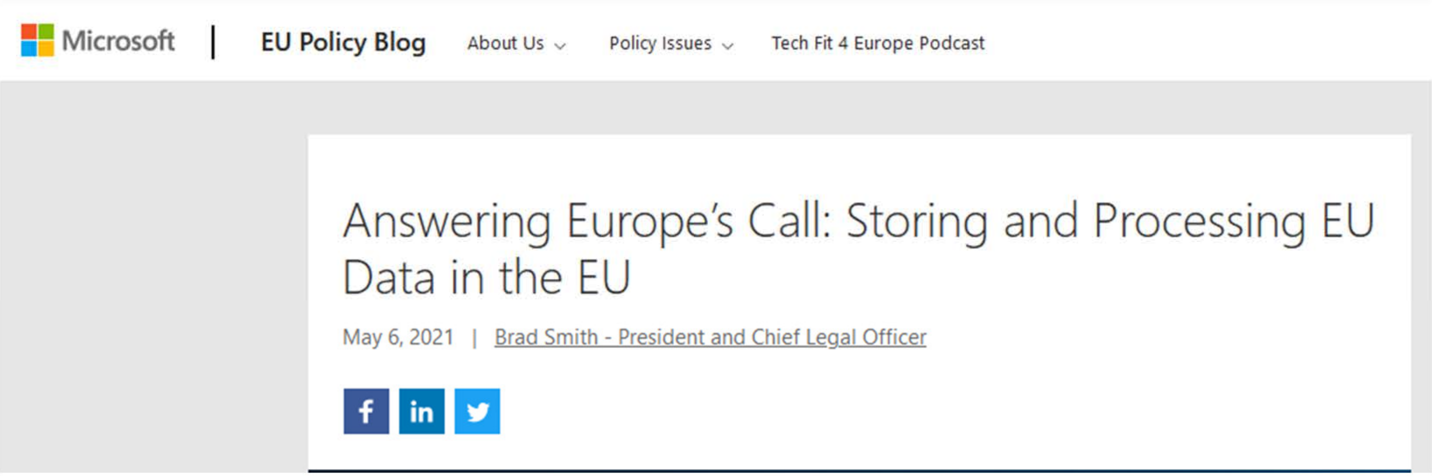
Effective audit rights. The Dutch gov has published the findings of the first annual audit, and will soon publish the findings of the second audit

Anonymisation according to EDPB guidelines

Worldwide technical improvements Microsoft Office

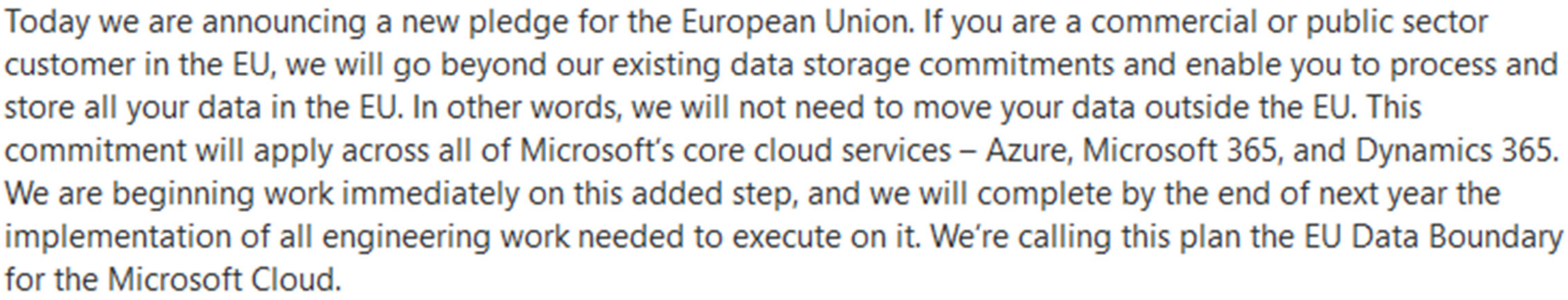
Public documentation telemetry
Admins can choose telemetry level: Required, Optional or Neither (Dutch gov recommends to choose Neither)
Users can check the dataflow via the data viewer tool
Many Connected Experiences now in data processor role
Admins can centrally disable different connected experiences

May 2021 new Microsoft promise: *all* personal data in the EU



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

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

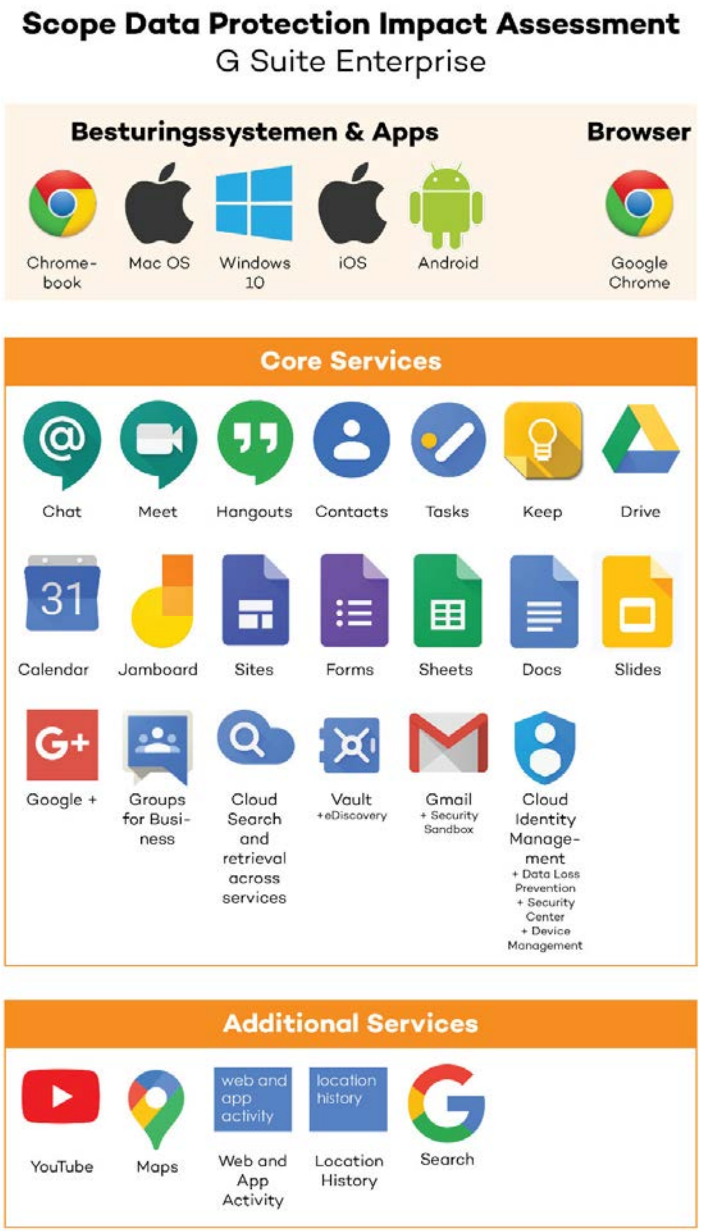


Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the 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.

DPIA on Google Workspace (prev. G-Suite)

Scope of Google Workspace DPIAs

- Two different DPIA's: for Dutch gov (Enterprise) and for two Dutch universities (Education)
- 3 platforms: Chromebook, MacOS and Windows 10, plus iOS and Android apps
- 20 Core Services
- 5 Addditional Services + Chrome
- 3 *Features* (Spelling, Explore en Translate)
- 1 Related Service (Feedback)



Scope Data Protection Impact Assessment
G Suite Enterprise

Additional Services

+ Google ChromeOS
& Chrome browser

App Maker	Blogger	Campaign Manager
Chrome Web Store	FeedBurner	Fusion Tables
Google Ad Manager	Google Ads	Google AdSense
Google Alerts	Google Analytics	Google Bookmarks
Google Books	Google Chrome Sync	Google Classroom
Google Cloud Platform	Google Custom Search	Google Data Studio
Google Domains	Google Earth	Google Finance
Google Groups	Google In Your Language	Google Maps
Google My Business	Google My Maps	Google News
Google Partners	Google Payments	Google Photos
Google Play	Google Play Console	Google Public Data
Google Scholar	Google Search Console	Google Shopping
Google Takeout	Google Translator Toolkit	Google Trips
Individual Storage	Location History	Merchant Center
Mobile Test Tools	Partner Dash	Play Books Partner Center
Project Fi	Science Journal	Search Ads 360
Studio	Third-party App backups	Tour Creator
Web and app activity	YouTube	

Key privacy problems with Google Workspace

- Google is a processor for Core Services but data controller for all other services, such as YouTube, Search and Chrome, and for all Diagnostic Data. Google processes for 33 purposes as controller, plus 22 purposes for Chrome.
- As processor Google thinks it may process both Content and Diagnostic Data for any purpose it deems compatible. In total Google process for 17 broad purposes.
- Gov and universities enable Google to further process the personal data it obtains as processor in a role as controller: this makes them joint controllers with Google
- Lack of transparency about the different kinds of personal data Google generates and collects, no data subject access provided to telemetry data and cookies

CNIL fined Google 50 million euro for vague purposes

The restricted committee observes in particular that ***the purposes of processing are described in a too generic and vague manner, and so are the categories of data processed for these various purposes****.*

Essential information, such as the data processing purposes, *the data storage periods or the categories of personal data used for the ads personalization, are* ***excessively disseminated across several documents****, with buttons and links on which it is required to click to access complementary information. The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions.*

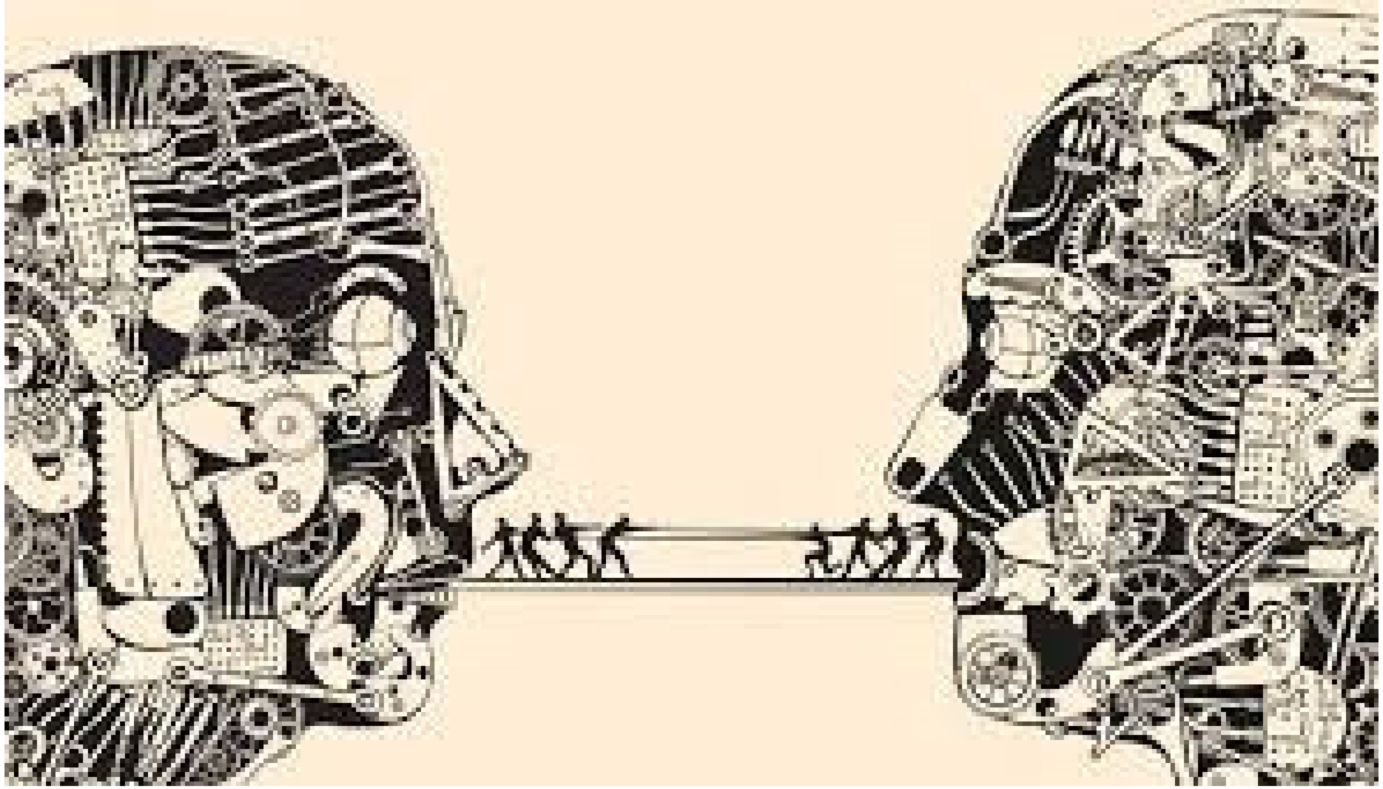
Conclusions July 2020: 11 high and 3 low risks

1. Lack of purpose limitation Content data: loss of confidentiality of personal data, loss of control, risk of re-identification
2. Lack of purpose limitation Diagnostic data: loss of control, unlawful processing
3. Lack of transparency Substantive data: loss of control
4. Lack of transparency Diagnostic data: loss of control, risk of re-identification
5. No legal ground for Google and universities: loss of control, unlawful processing
6. Lack of privacy controls for administrators and users: loss of control and loss of confidentiality
7. Privacy-unfriendly default settings: Loss of control and loss of confidentiality
8. Single Google Account: Loss of control, loss of confidentiality
9. Lack of control over sub-processors: Loss of control, loss of confidentiality
10. Lack of control over transmission of personal data by Features to external websites: loss of control, loss of confidentiality, risk of re-identification
11. Inability to exercise data subjects' rights

Low risks

1. Cloud provider: unauthorised access to content and metadata: loss of control, loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing
2. Employee monitoring system: chilling effect to exercise (related) rights
3. Impossibility to delete historical diagnostic data: increased risk of re-identification of pseudonymised data and unlawful (further) processing

Negotiation results after 7 months of negotiatons (Feb 2021)



Ryger, On the Verge of Understanding, Shuttershock royalty-free

8 high and 3 low risks

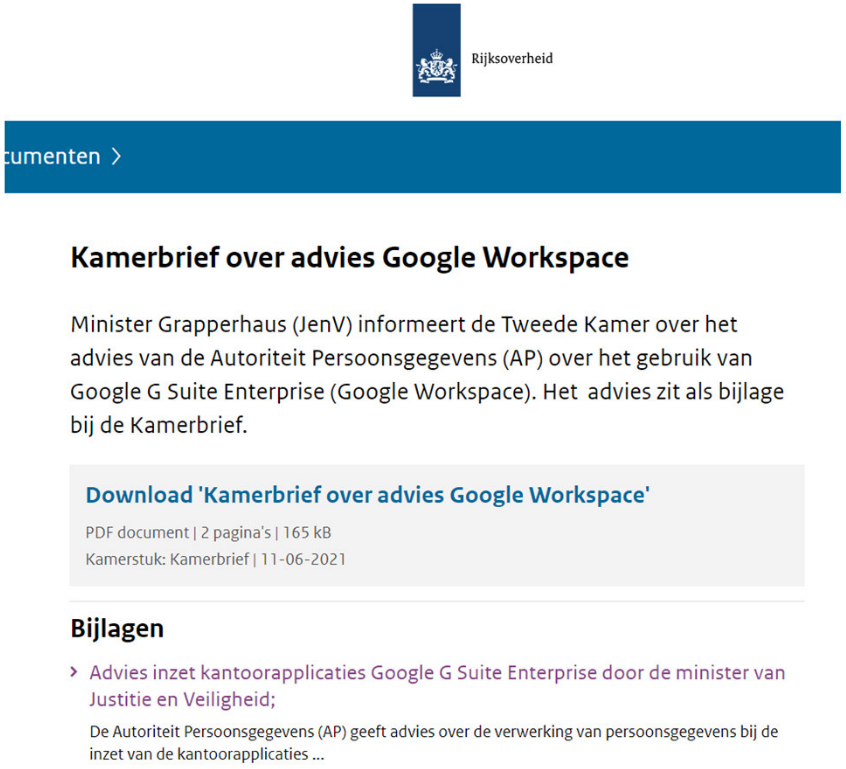
1. Lack of purpose limitation Content data: loss of confidentiality of personal data, loss of control, risk of re-identification
2. Lack of purpose limitation Diagnostic data: loss of control, unlawful processing
3. Lack of transparency Substantive data: loss of control
4. Lack of transparency Diagnostic data: loss of control, risk of re-identification
5. No basis for Google and universities: loss of control, unlawful processing
6. Lack of privacy controls for administrators and users: loss of control and loss of confidentiality
7. ~~Privacy-unfriendly default settings: Loss of control and loss of confidentiality~~
8. ~~Single Google Account: Loss of control, loss of confidentiality~~
9. Lack of control over sub-processors: Loss of control, loss of confidentiality
10. ~~Lack of control over transmission of personal data by Features to external websites: loss of control, loss of confidentiality, risk of re-identification~~
11. Inability to exercise data subjects' rights

Low risks

1. Cloud provider: unauthorised access to content and metadata: loss of control, loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing
2. Employee monitoring system: chilling effect to exercise (related) rights
3. Impossibility to delete historical diagnostic data: increased risk of re-identification of pseudonymised data and unlawful (further) processing

Request for help to Dutch Data Protection Authority

- Prior consultation ex art. 36 GDPR for the Dutch government (does not yet use Google Workspace), filed 15 Feb 2021
- Request for advice ex art. 58 GDPR for the Dutch universities, secondary and primary schools (very high penetration of Chromebooks and Workspace)
- Reply from Dutch DPA 11 June 2021: **stop using Google Workspace for Education before the new school year if the problems are not solved**



Kamerbrief over advies Google Workspace

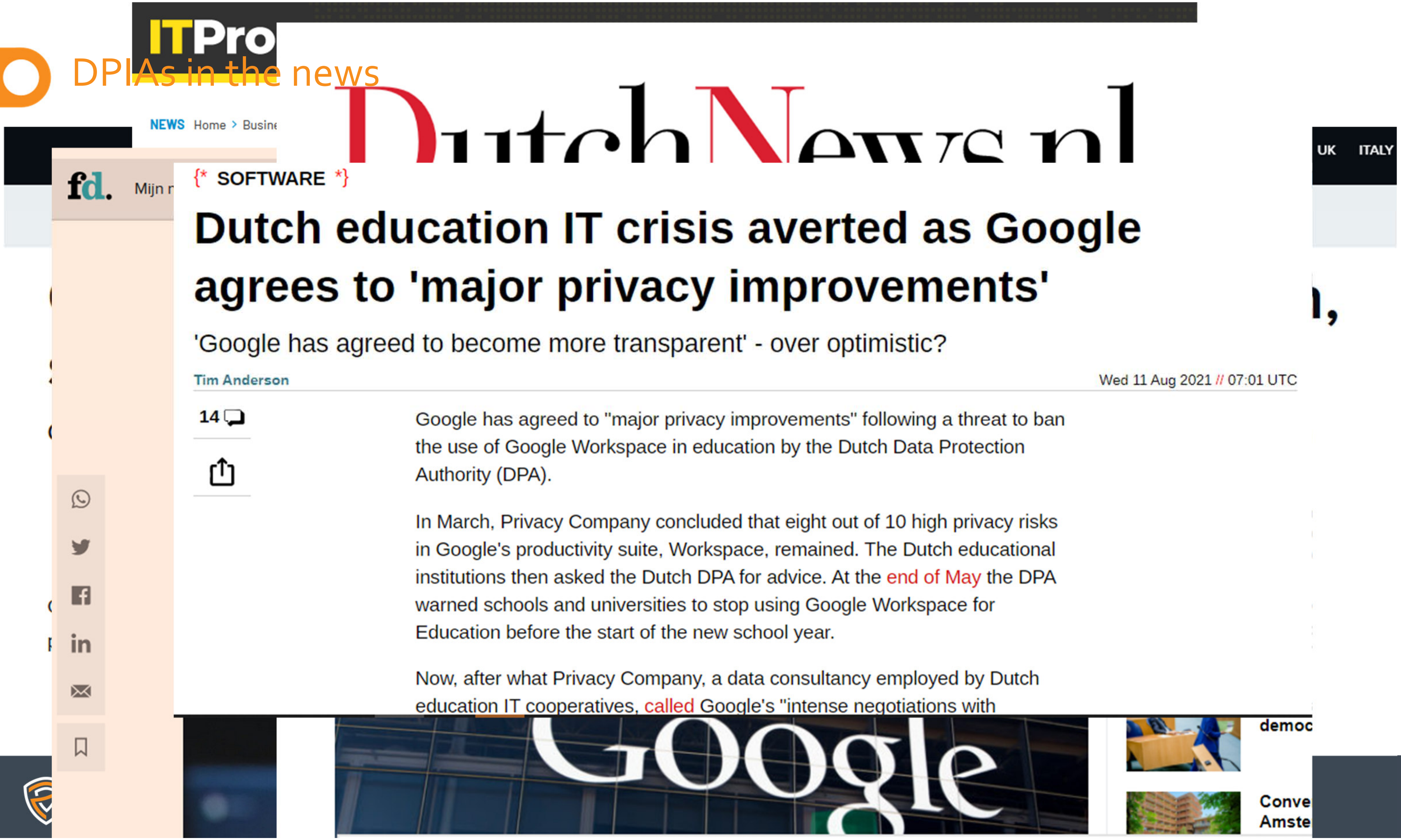
Minister Grapperhaus (JenV) informeert de Tweede Kamer over het advies van de Autoriteit Persoonsgegevens (AP) over het gebruik van Google G Suite Enterprise (Google Workspace). Het advies zit als bijlage bij de Kamerbrief.

Download 'Kamerbrief over advies Google Workspace'
PDF document | 2 pagina's | 165 kB
Kamerstuk: Kamerbrief | 11-06-2021

Bijlagen

› Advies inzet kantoorapplicaties Google G Suite Enterprise door de minister van Justitie en Veiligheid;
De Autoriteit Persoonsgegevens (AP) geeft advies over de verwerking van persoonsgegevens bij de inzet van de kantoorapplicaties ...

DPIAs in the news



{* SOFTWARE *}

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 UTC

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).

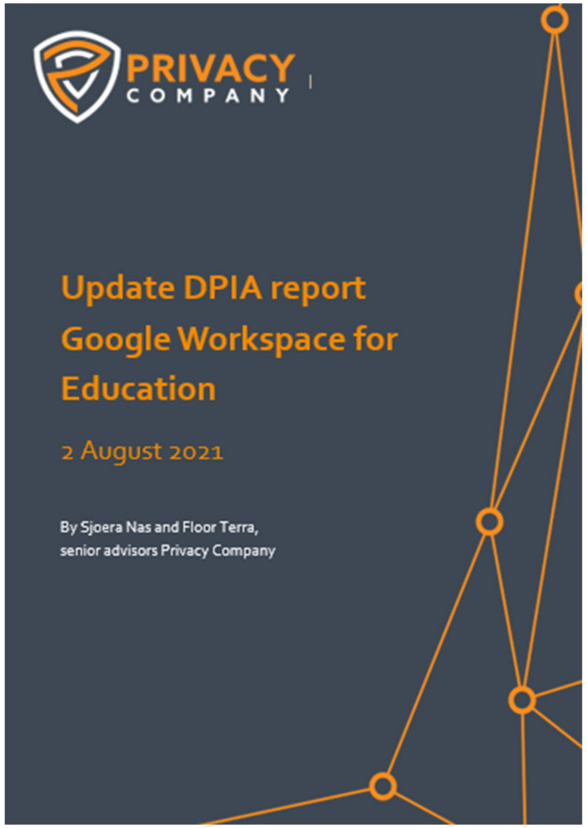
In March, Privacy Company concluded that eight out of 10 high privacy risks in Google's productivity suite, Workspace, remained. The Dutch educational institutions then asked the Dutch DPA for advice. At the end of May the DPA warned schools and universities to stop using Google Workspace for Education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

August 2021: Google Update report for schools/universities

High risks mitigated by the following measures:

- Google to act as data processor for the Diagnostic Data, processes for only 3 purposes
- Google will publish much more documentation
- Google will become a data processor for the Chrome browser and Chrome OS on Chromebooks in 2 years
- Organisations must themselves take a lot of measures to mitigate risks of remaining Google controller services



PRIVACY COMPANY

Update DPIA report Google Workspace for Education

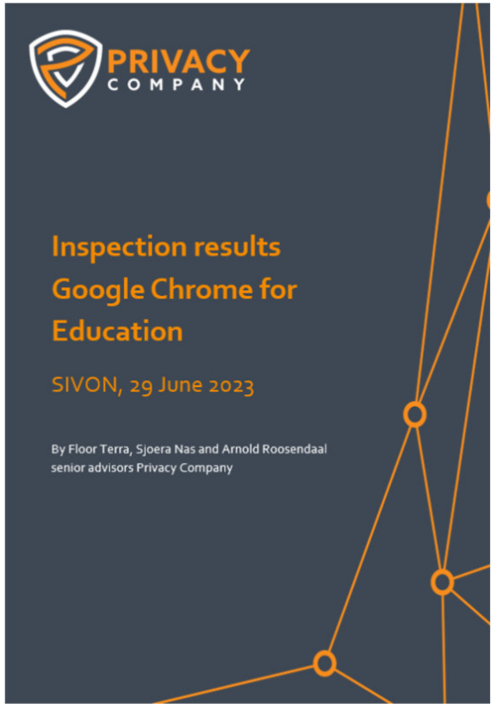
2 August 2021

By Sjoera Nas and Floor Terra,
senior advisors Privacy Company

https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education

New reports published about Workspace and managed ChromeOS and Chrome browser

- Dutch DPA warned the Dutch minister of Education in March 2023: ensure full compliance before 1 July 2023, or stop using Workspace in Dutch schools and universities.
- Reality: 80% of primary schools in the Netherlands use the 'free' Fundamental Workspace edition: a switch to for example Microsoft Office would be very costly.
- Inspection results of Google's delivery of promises from July 2021: Google has effectively mitigated the high risks, or reduced them to a low risk.



PRIVACY COMPANY

Inspection results Google Chrome for Education

SIVON, 29 June 2023

By Floor Terra, Sjoera Nas and Arnold Roosendaal
senior advisors Privacy Company

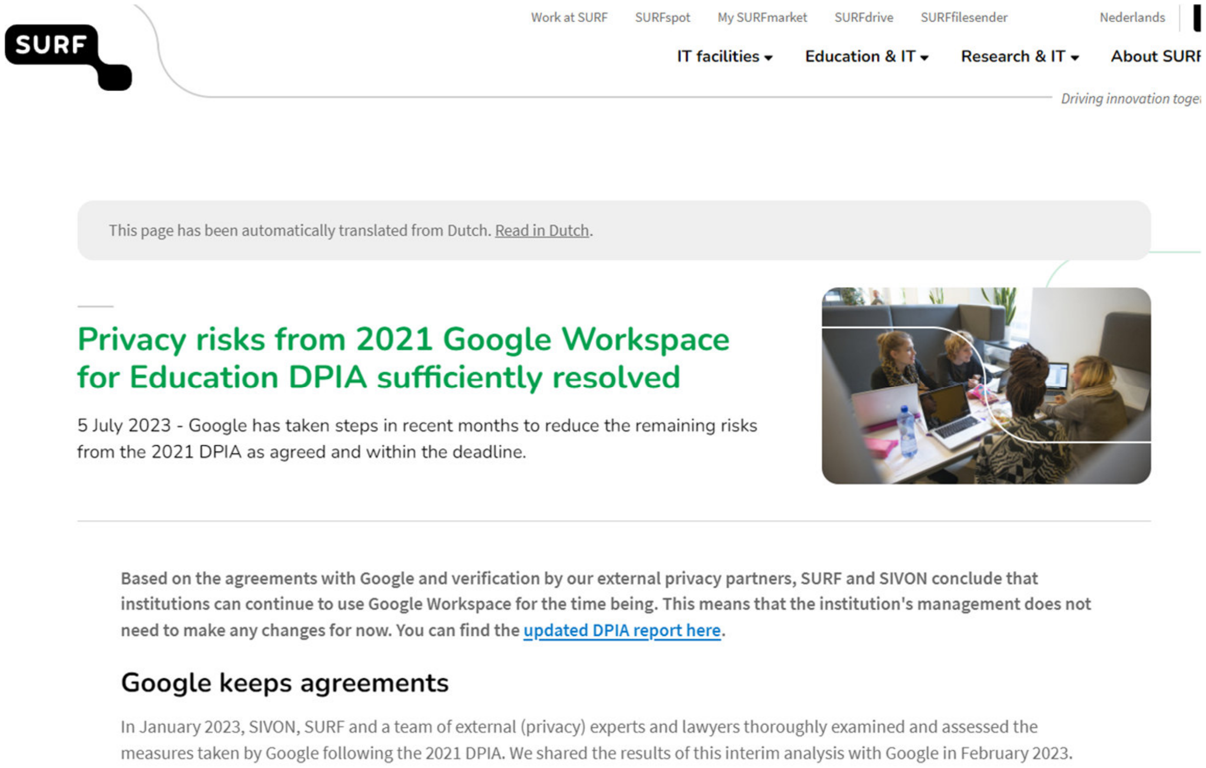
Check the new reports at: https://sivon.nl/alles-over-de-dpias-op-google-workspace-chromeos/

Mitigating measures Google

- Google has built an Diagnostic Information Tool (DIT), and has documented Telemetry from Workspace Enterprise and Education.
- Google has published new documentation about data subject access requests
- Google has released a processor version of managed ChromeOS and Chrome browser (mid August 2023)
- More settings are privacy by default for K-12
- Google has enabled Client Side Encryption for Meet/Drive/Gmail and Calendar
- Google is working on European Sovereign Controls
- SIVON has published detailed guidance for schools what settings to apply in Chrome and in Workspace.

Check the manual with privacyfriendly settings at https://sivon.nl/wp-content/uploads/2023/07/Handleiding-ChromeOS-en-Chrome-browser-SIVONSURF.pdf

New inspections Chrome and Workspace June 2023



This page has been automatically translated from Dutch. Read in Dutch.

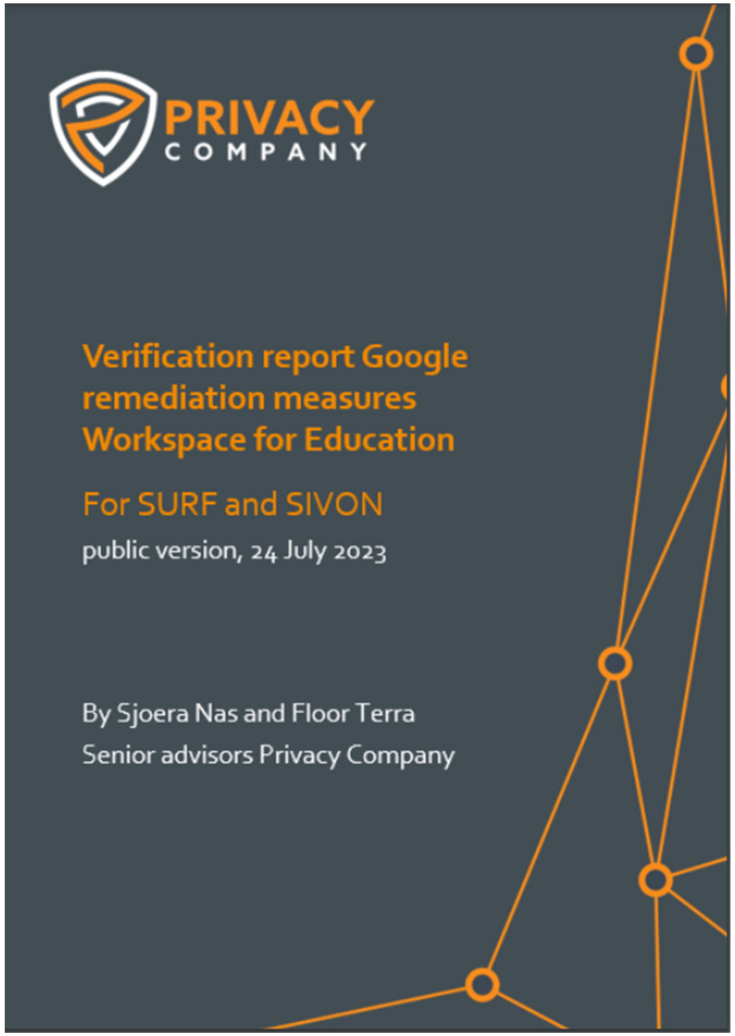
Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved

5 July 2023 - Google has taken steps in recent months to reduce the remaining risks from the 2021 DPIA as agreed and within the deadline.

Based on the agreements with Google and verification by our external privacy partners, SURF and SIVON conclude that institutions can continue to use Google Workspace for the time being. This means that the institution's management does not need to make any changes for now. You can find the updated DPIA report here.

Google keeps agreements

In January 2023, SIVON, SURF and a team of external (privacy) experts and lawyers thoroughly examined and assessed the measures taken by Google following the 2021 DPIA. We shared the results of this interim analysis with Google in February 2023.



Verification report Google remediation measures Workspace for Education

For SURF and SIVON

public version, 24 July 2023

By Sjoera Nas and Floor Terra

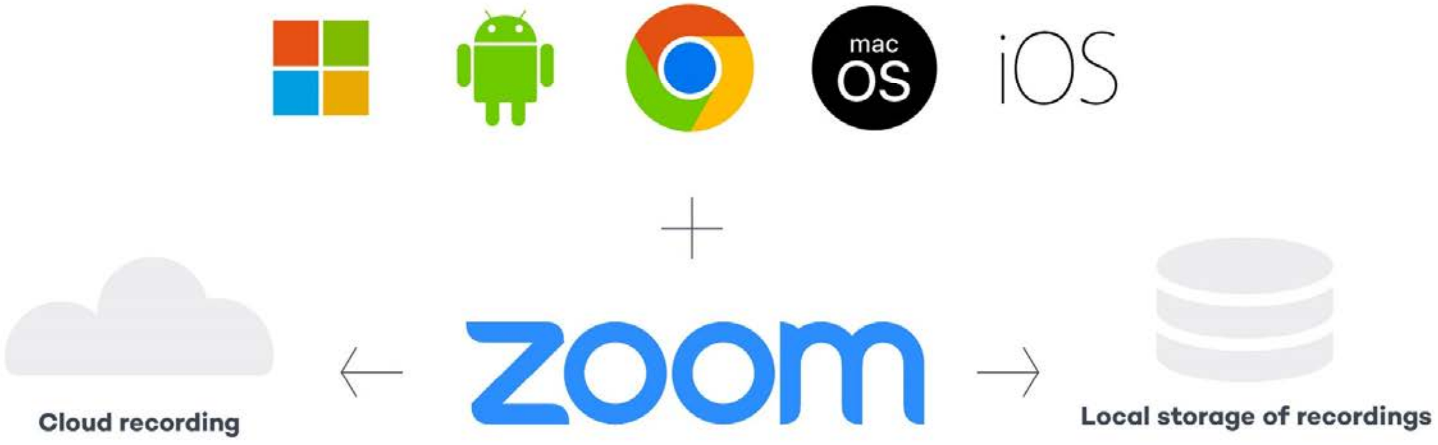
Senior advisors Privacy Company

https://www.surf.nl/en/privacy-risks-from-2021-google-workspace-for-education-dpia-sufficiently-resolved

Unsolved issues

- Schools must still disable Workspace *Additional Services* (YouTube, Search) because Google remains a data controller.
- CSE is not available for the free *Fundamentals* version of Workspace.
- During the inspection we found new risks - Google will have to solve these risks.
- The inspection report does not address the risks of transfer of personal data to third countries (different from the USA). We are still testing Google Meet encryption, and expect to finalise a separate DTIA on the use of Google Meet before the end of September 2023.

Scope of Zoom DPIA

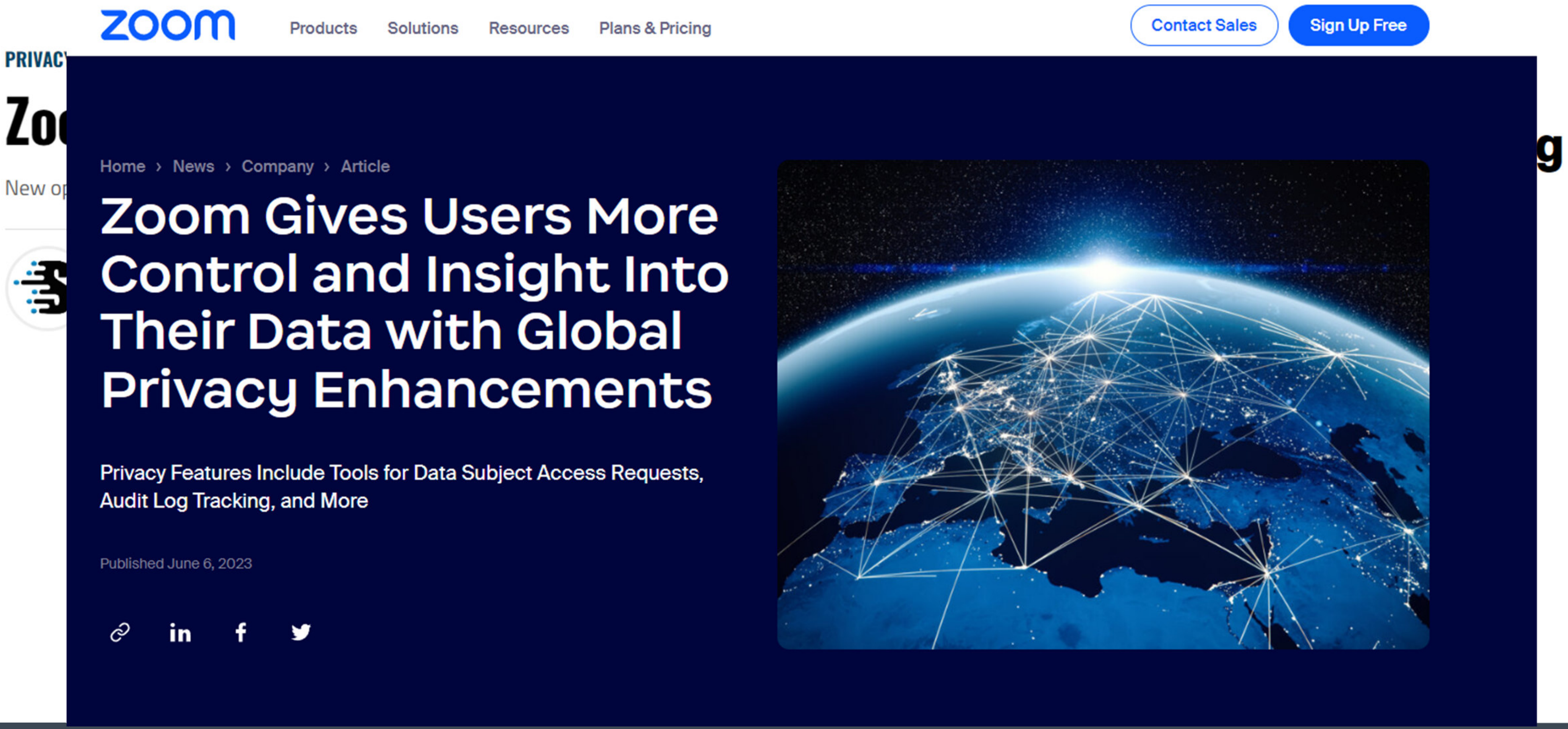


Zoom DPIA and DTIA

- Initial tech analysis between September and November 2020
- Completed part A (tech findings) in April 2021, including several rounds of input from Zoom
- May 2021 DPIA completed: 9 high, and 3 low data protection risks, even though Zoom already offered E2EE for meetings. Main problem: role as data controller
- DPIA not published pending intense negotations with Zoom
- Strong involvement of leadership at Zoom: weekly meetings with large team of developers. The negotiated GDPR-proof agreement is available for all EU customers
- March 2022: publication of completely revamped DPIA: six low, and no more high risks, including DTIA on use of support desk in the Phillipines

https://www.privacycompany.eu/blogpost-en/new-dpia-for-surf-and-dutch-government-on-zoom-all-high-risks-solved

Verification results June 2023



PRIVAC

Zo

New op

g

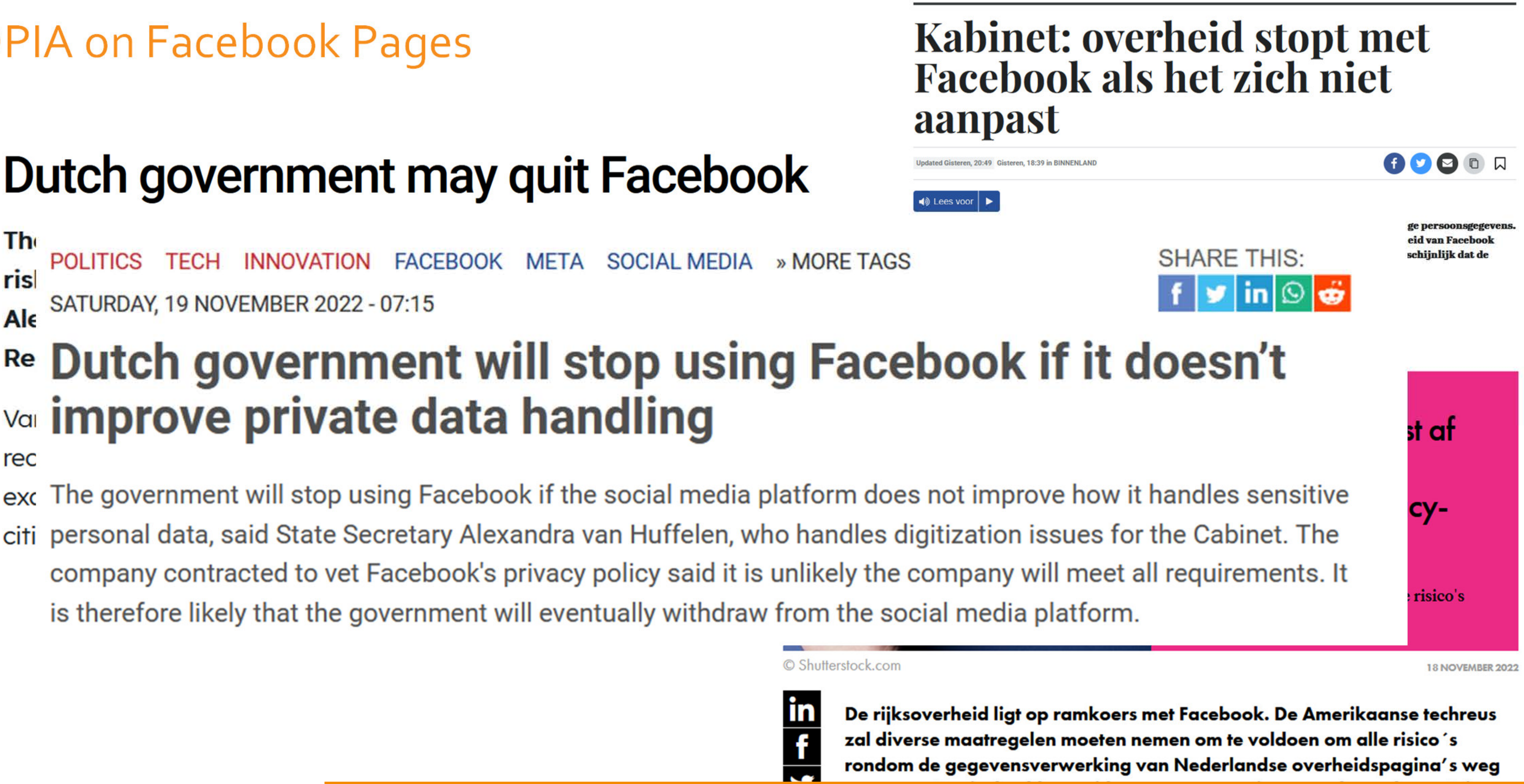
Home › News › Company › Article

Zoom Gives Users More Control and Insight Into Their Data with Global Privacy Enhancements

Privacy Features Include Tools for Data Subject Access Requests, Audit Log Tracking, and More

Published June 6, 2023

DPIA on Facebook Pages



Kabinet: overheid stopt met Facebook als het zich niet aanpast

Updated Gisteren, 20:49 Gisteren, 18:39 in BINNENLAND

Lees voor

ge persoonsgegevens.
eid van Facebook
schijnlijk dat de

Dutch government may quit Facebook

Th
risl
Ale
Re

Va
rec
exc
citi

POLITICS TECH INNOVATION FACEBOOK META SOCIAL MEDIA » MORE TAGS

SHARE THIS:

SATURDAY, 19 NOVEMBER 2022 - 07:15

Dutch government will stop using Facebook if it doesn't improve private data handling

The government will stop using Facebook if the social media platform does not improve how it handles sensitive personal data, said State Secretary Alexandra van Huffelen, who handles digitization issues for the Cabinet. The company contracted to vet Facebook's privacy policy said it is unlikely the company will meet all requirements. It is therefore likely that the government will eventually withdraw from the social media platform.

st af

cy-

risico's

© Shutterstock.com

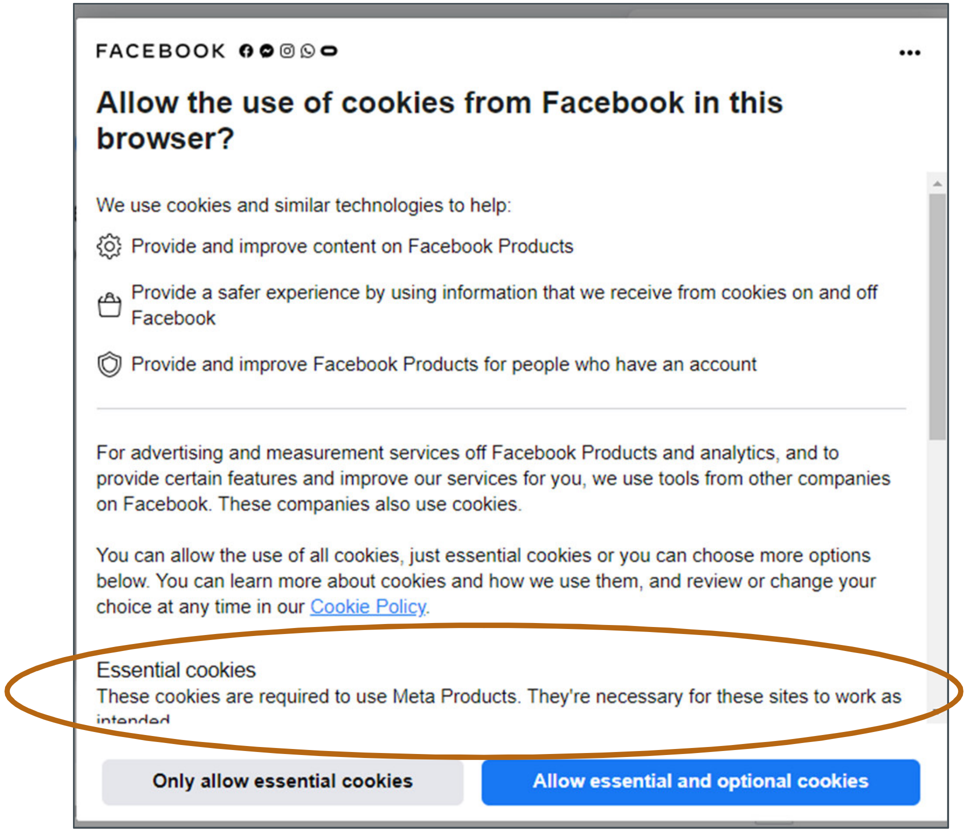
18 NOVEMBER 2022

De rijksoverheid ligt op ramkoers met Facebook. De Amerikaanse techreus zal diverse maatregelen moeten nemen om te voldoen om alle risico´s rondom de gegevensverwerking van Nederlandse overheidspagina's weg

https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/18/kamerbrief-over-onafhankelijk-onderzoek-naar-facebookpaginas-overheid

DPIA findings

- Lack of clarity about the types of personal data Facebook collects about visitors, especially cookies. Those cookies are also used on websites outside Facebook, and also on visitors without a Facebook account.
- Lack of transparency on the logic/algorithms used to determine what posts and ads users see in their news feed: not even via view request
- At least 15 purposes for processing, but not specifically and not exhaustively formulated
- Misleading consent question: Facebook places datr tracking cookie if a visitor says 'No' to non-essential cookies (*Essential* cookies only)
- Facebook is a joint controller....



FACEBOOK

Allow the use of cookies from Facebook in this browser?

We use cookies and similar technologies to help:

Provide and improve content on Facebook Products

Provide a safer experience by using information that we receive from cookies on and off Facebook

Provide and improve Facebook Products for people who have an account

For advertising and measurement services off Facebook Products and analytics, and to provide certain features and improve our services for you, we use tools from other companies on Facebook. These companies also use cookies.

You can allow the use of all cookies, just essential cookies or you can choose more options below. You can learn more about cookies and how we use them, and review or change your choice at any time in our Cookie Policy.

Essential cookies

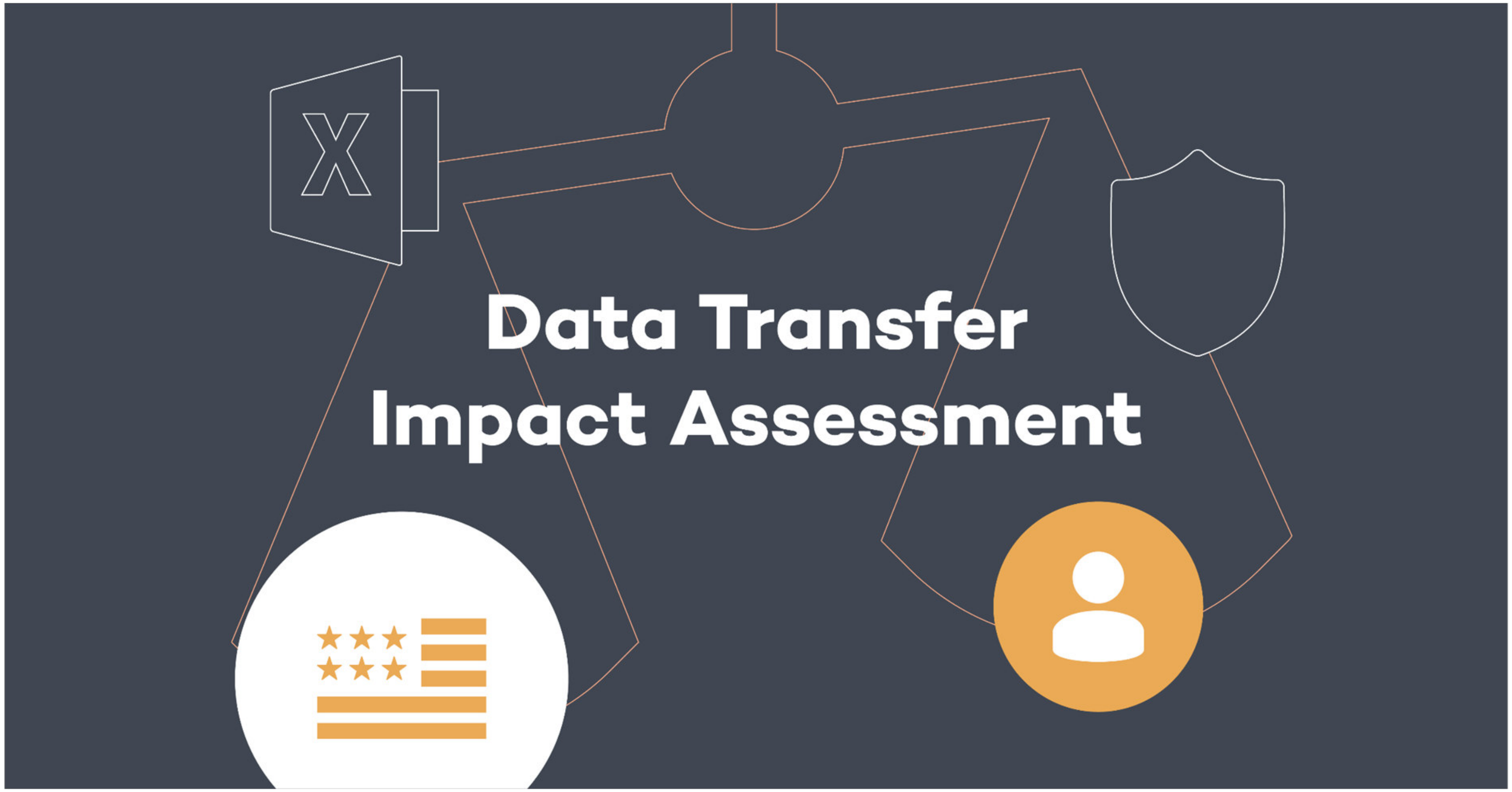
These cookies are required to use Meta Products. They're necessary for these sites to work as intended

Only allow essential cookies
Allow essential and optional cookies

If not a joint controller: then Facebook is a third party

- Compare it to hosting a conference in an event hall
- The hall's owner offers the space for free, but requires all visitors to register with their real identity, and preferably as much other information as possible about their interests and their friends
- The government cannot impose any requirement on data collection and processing: under its own privacy statement, the owner is allowed to pass on visitor data to all of its 'partners', 'advertisers' and 'other trusted parties'.
- The event hall makes good cheer for its content-strong government congress, but has organised the walking route so that visitors have to walk past 10 other events first, with free fast food (rage-inducing messages!). To get to the government congress, you have to take the stairs to the eighth floor.

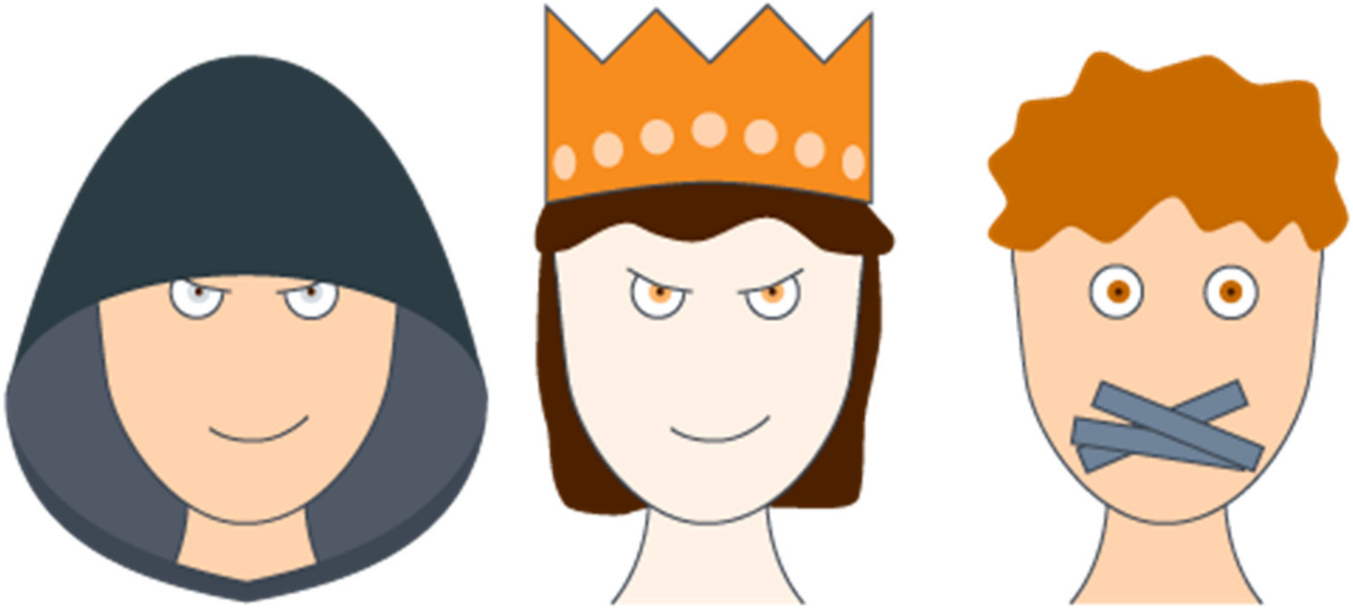
Data Transfer Impact Assessment



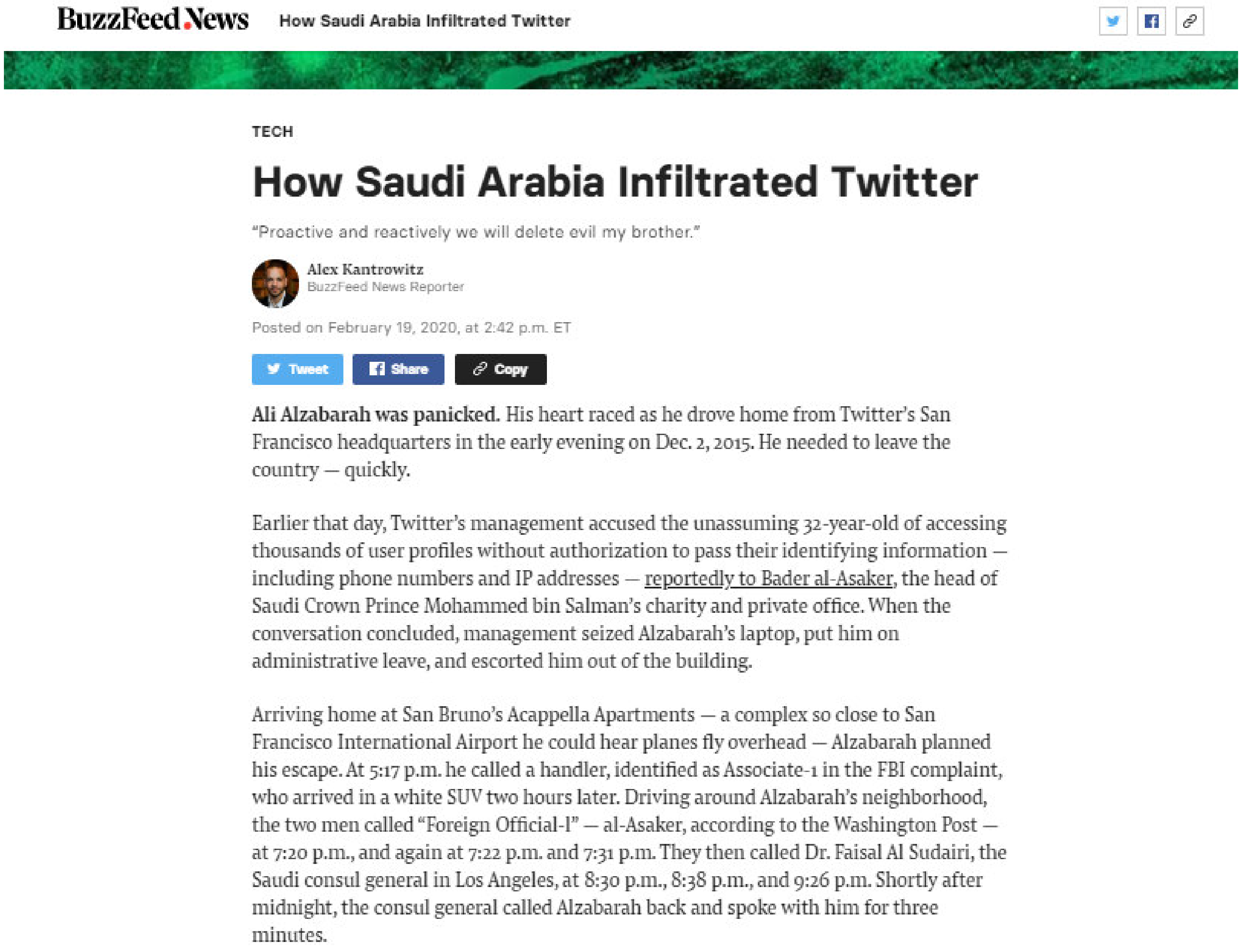
Why perform a DTIA now that the USA are adequate again?

- You can rely on an adequacy decision, even if you use SCC, and regardless if the US company you export to has registered as participant in the Data Privacy Framework.
- But: Schrems-III is in the making, we advise our customers to continue to use SCC, also to ensure a harmonised set of rules with subprocessors in third countries.
- If you rely on SCC for transfer to third countries (for example for the support desks from your cloud provider), you have to assess if there is problematic legislation that applies to your transferred data in practice.
- We use the model created by the Swiss lawyer David Rosenthal to calculate the risk.

Three threat vectors for transferred data in third countries



Blackmailed or bribed employees



BuzzFeed News How Saudi Arabia Infiltrated Twitter

TECH

How Saudi Arabia Infiltrated Twitter

“Proactive and reactively we will delete evil my brother.”

Alex Kantrowitz
BuzzFeed News Reporter

Posted on February 19, 2020, at 2:42 p.m. ET

Ali Alzabarah was panicked. His heart raced as he drove home from Twitter’s San Francisco headquarters in the early evening on Dec. 2, 2015. He needed to leave the country — quickly.

Earlier that day, Twitter’s management accused the unassuming 32-year-old of accessing thousands of user profiles without authorization to pass their identifying information — including phone numbers and IP addresses — reportedly to Bader al-Asaker, the head of Saudi Crown Prince Mohammed bin Salman’s charity and private office. When the conversation concluded, management seized Alzabarah’s laptop, put him on administrative leave, and escorted him out of the building.

Arriving home at San Bruno’s Acappella Apartments — a complex so close to San Francisco International Airport he could hear planes fly overhead — Alzabarah planned his escape. At 5:17 p.m. he called a handler, identified as Associate-1 in the FBI complaint, who arrived in a white SUV two hours later. Driving around Alzabarah’s neighborhood, the two men called “Foreign Official-I” — al-Asaker, according to the Washington Post — at 7:20 p.m., and again at 7:22 p.m. and 7:31 p.m. They then called Dr. Faisal Al Sudairi, the Saudi consul general in Los Angeles, at 8:30 p.m., 8:38 p.m., and 9:26 p.m. Shortly after midnight, the consul general called Alzabarah back and spoke with him for three minutes.

Three DTIAs published

Teams, SharePoint, OneDrive en de Azure AD (Dutch government and universities)
https://slmmicrosoftrijk.nl/?smd_process_download=1&download_id=5286

Zoom (universities and Dutch government)
https://www.surf.nl/files/2022-03/dtia-zoom-8-feb-2022_0.ods

AWS (Dutch government)
https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/DTIA-Dutch-Government-AWS-.pdf

DTIA in 7 steps: based on the Rosenthal model

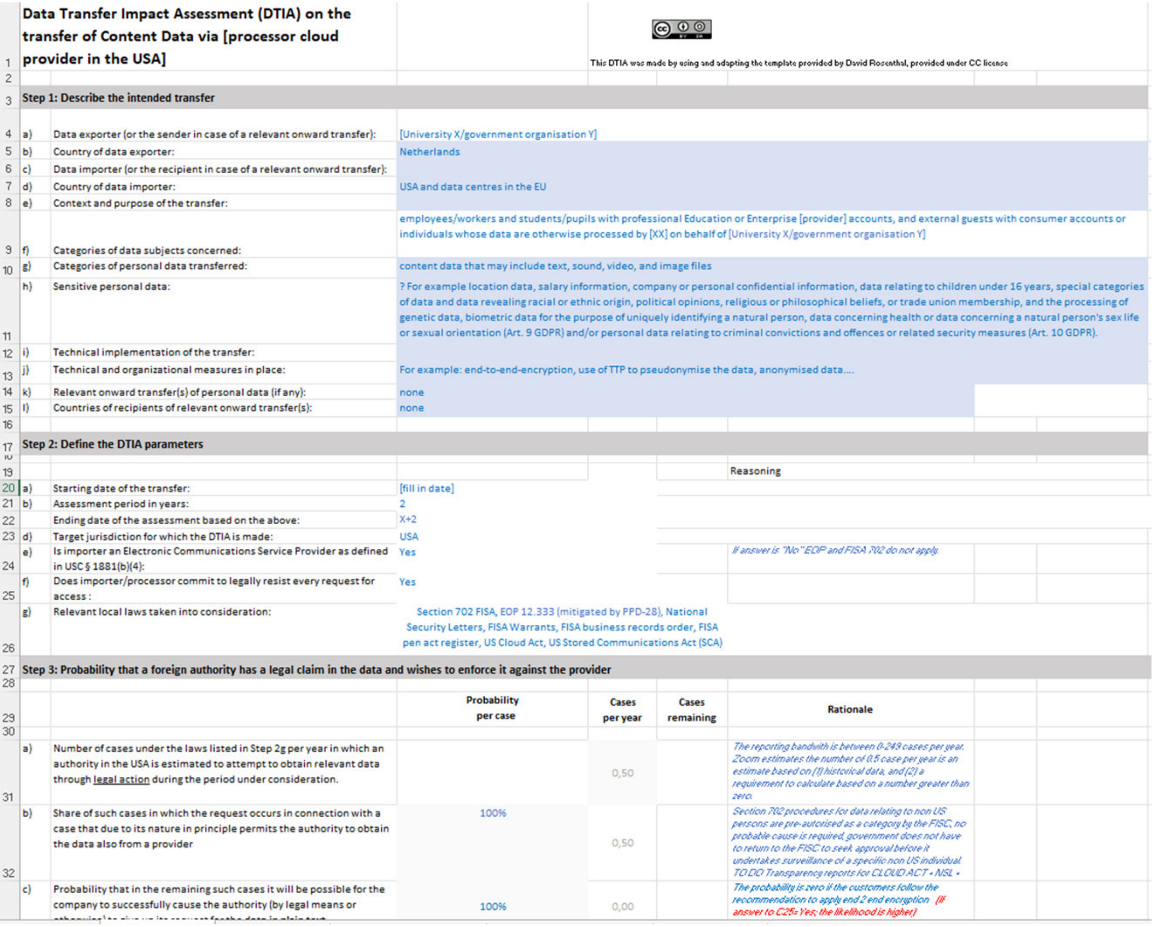
1. *Describe the intended transfer* (what kind of personal data, are there any subprocessors? -> separate DTIAs!)
2. *Define the DTIA parameters* (what applicable law in the third country)
3. *Probability that the foreign authority has a legal claim* (does that law apply to your data processed by this specific provider)

4a. *Probability that the claim is successful* (chance that the data can be ordered in legible format, calculated over multiple years)

4b. *Probability of access through mass surveillance* (chance that the data can be intercepted in legible format via cables/wires)

5. *Overall assessment* (multiplication risk percentages)
6. *Data subject risks* (chance x impact, depending on the nature of the data)
7. *Safeguards* (incidental or structural transfers, E2EE, what legal guarantees, track record, are there SCCs)

Example of DTIA in Excel 1/2



Data Transfer Impact Assessment (DTIA) on the transfer of Content Data via [processor cloud provider in the USA]

This DTIA was made by using and adapting the template provided by David Rosenthal, provided under CC license

Step 1: Describe the intended transfer

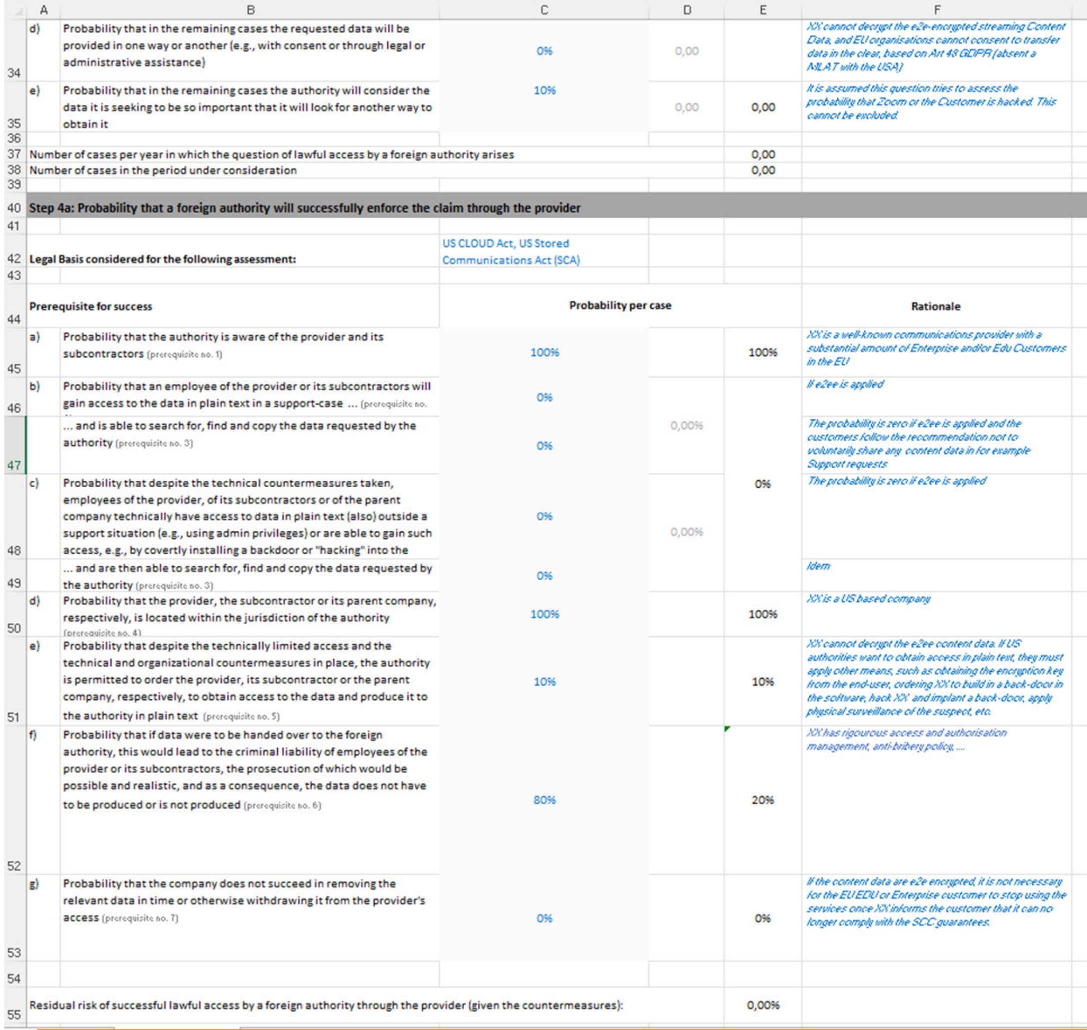
a)	Data exporter (or the sender in case of a relevant onward transfer):	[University X/government organisation Y]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	
d)	Country of data importer:	USA and data centres in the EU
e)	Context and purpose of the transfer:	
f)	Categories of data subjects concerned:	employees/workers and students/pupils with professional Education or Enterprise [provider] accounts, and external guests with consumer accounts or individuals whose data are otherwise processed by [XX] on behalf of [University X/government organisation Y]
g)	Categories of personal data transferred:	content data that may include text, sound, video, and image files
h)	Sensitive personal data:	? For example location data, salary information, company or personal confidential information, data relating to children under 16 years, special categories of data and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9 GDPR) and/or personal data relating to criminal convictions and offences or related security measures (Art. 10 GDPR).
i)	Technical implementation of the transfer:	
j)	Technical and organizational measures in place:	For example: end-to-end-encryption, use of TTP to pseudonymise the data, anonymised data....
k)	Relevant onward transfer(s) of personal data (if any):	none
l)	Countries of recipients of relevant onward transfer(s):	none

Step 2: Define the DTIA parameters

			Reasoning
a)	Starting date of the transfer:	[fill in date]	
b)	Assessment period in years:	2	
	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	*If answer is "No" EOP and FISA 702 do not apply.*
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	Section 702 FISA, EOP 12.333 (mitigated by PPD-28), National Security Letters, FISA Warrants, FISA business records order, FISA pen act register, US Cloud Act, US Stored Communications Act (SCA)	

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The reporting bandwith is between 0-249 cases per year. Zoom estimates the number of 0.5 case per year is an estimate based on (1) historical data, and (2) a requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*Section 702 procedures for data relating to non US persons are pre-autorised as a category by the FISC, no probable cause is required, government does not have to return to the FISC to seek approval before it undertakes surveillance of a specific non US individual. TO DO Transparency reports for CLOUD ACT + NSL +*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or	100%	0,00		*The probability is zero if the customers follow the recommendation to apply end 2 end encryption (If answer to C25= Yes; the likelihood is higher)*



A	B	C	D	E	F
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	0%	0,00		*XX cannot decrypt the e2e-encrypted streaming Content Data, and EU organisations cannot consent to transfer data in the clear, based on Art 48 GDPR (absent a MLAT with the USA)*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,00	0,00	*It is assumed this question tries to assess the probability that Zoom or the Customer is hacked. This cannot be excluded.*
Number of cases per year in which the question of lawful access by a foreign authority arises				0,00	
Number of cases in the period under consideration				0,00	

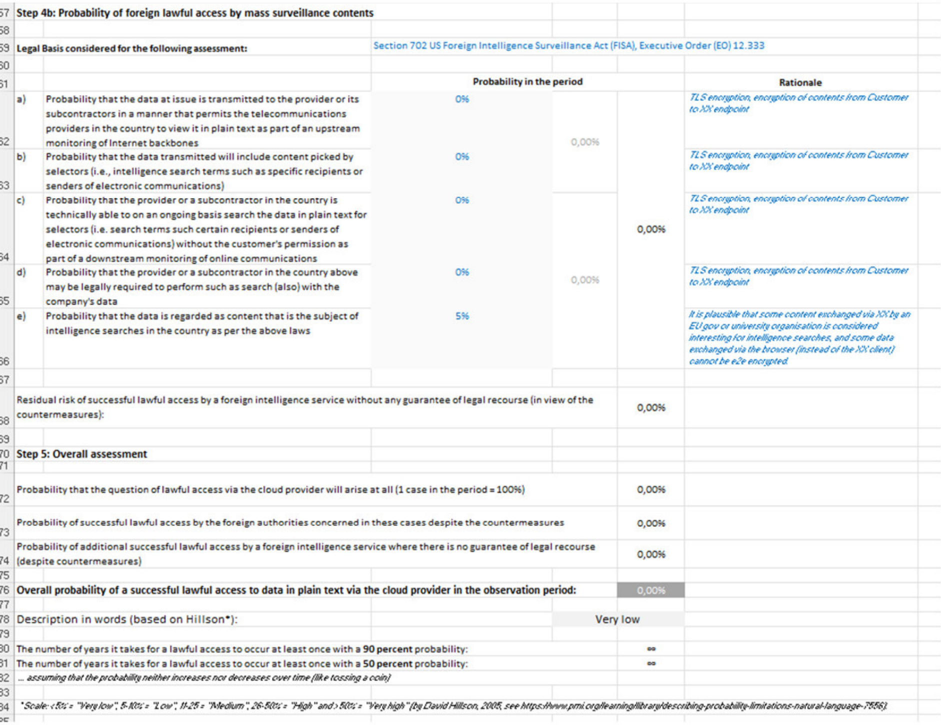
Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment:		US CLOUD Act, US Stored Communications Act (SCA)			
Prerequisite for success		**Probability per case**			**Rationale**
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*XX is a well-known communications provider with a substantial amount of Enterprise and/or Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no.	0%	0,00%	0%	*If e2ee is applied*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	0%			*The probability is zero if e2ee is applied and the customers follow the recommendation not to voluntarily share any content data in for example Support requests*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the	0%	0,00%		*The probability is zero if e2ee is applied*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	0%			*Idem*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*XX is a US based company*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	10%		10%	*XX cannot decrypt the e2ee content data. If US authorities want to obtain access in plain text, they must apply other means, such as obtaining the encryption key from the end-user, ordering XX to build in a back-door in the software, hack XX and implant a back-door, apply physical surveillance of the suspect, etc.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*XX has rigourous access and authorisation management, anti-bribery policy, ...*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	0%		0%	*If the content data are e2e encrypted, it is not necessary for the EU EDU or Enterprise customer to stop using the services once XX informs the customer that it can no longer comply with the SCC guarantees.*
Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures):				0,00%	

Modified model based on David Rosenthal

PRIVACY COMPANY

Example of DTIA in Excel 2/2



Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12.333

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,00%	*TLS encryption, encryption of contents from Customer to XX endpoint*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*TLS encryption, encryption of contents from Customer to XX endpoint*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%	0,00%		*TLS encryption, encryption of contents from Customer to XX endpoint*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	0%			*TLS encryption, encryption of contents from Customer to XX endpoint*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	5%			*It is plausible that some content exchanged via XX by an EU gov or university organisation is considered interesting for intelligence searches, and some data exchanged via the browser (instead of the XX client) cannot be e2e encrypted.*

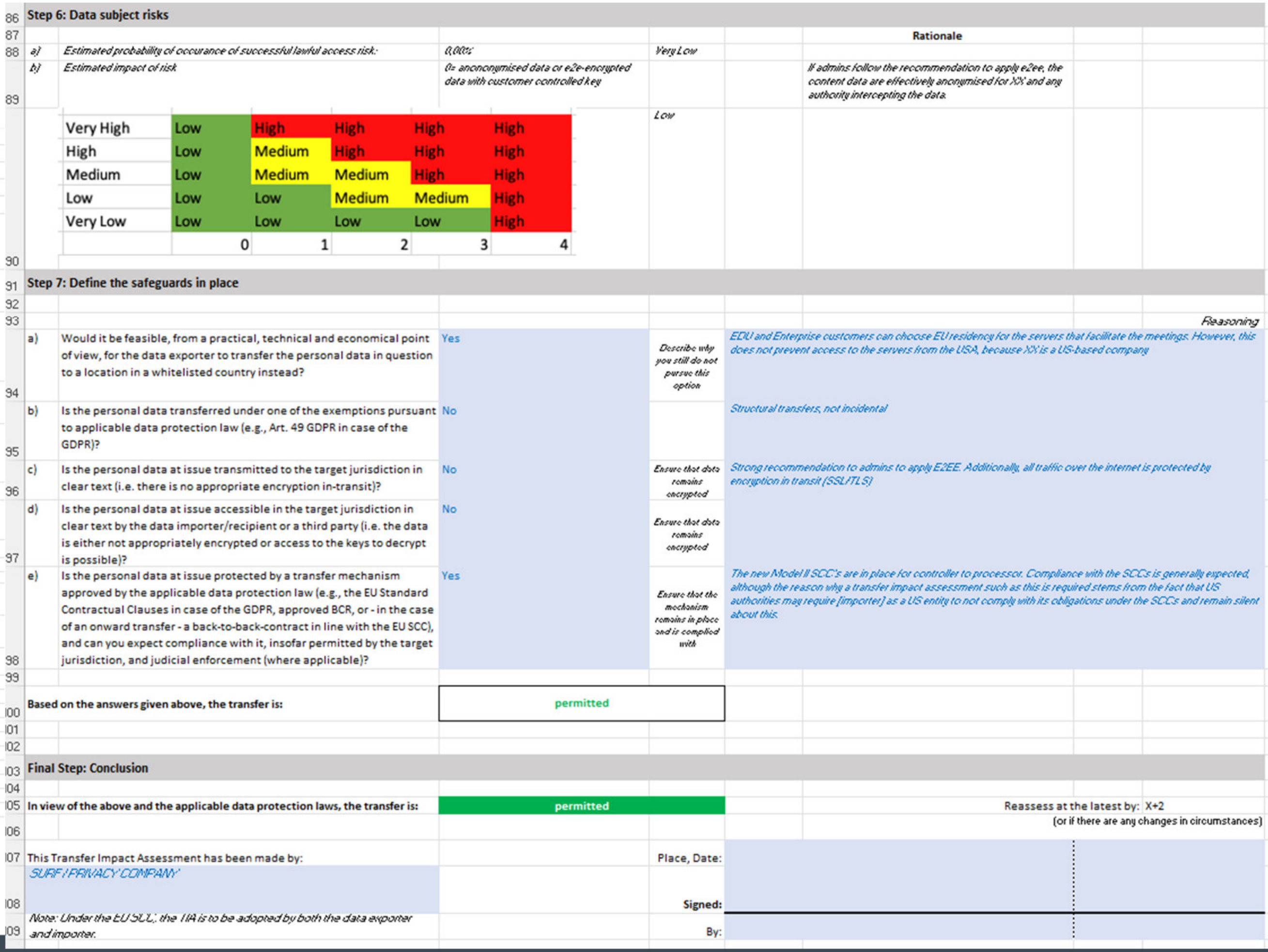
Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,00%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	0,00%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	0,00%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,00%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,00%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	∞

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

**Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556)*



Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,00%*	*Very Low*	
b)	*Estimated impact of risk*	*0= anonomymised data or e2e-encrypted data with customer controlled key*		*If admins follow the recommendation to apply e2ee, the content data are effectively anonymised for XX and any authority intercepting the data.*
			Low	

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Step 7: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*EDU and Enterprise customers can choose EU residency for the servers that facilitate the meetings. However, this does not prevent access to the servers from the USA, because XX is a US-based company*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Structural transfers, not incidental*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Strong recommendation to admins to apply E2EE. Additionally, all traffic over the internet is protected by encryption in transit (SSL/TLS)*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	No	*Ensure that data remains encrypted*	
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The new Model II SCC's are in place for controller to processor. Compliance with the SCCs is generally expected, although the reason why a transfer impact assessment such as this is required stems from the fact that US authorities may require [importer] as a US entity to not comply with its obligations under the SCCs and remain silent about this.*

Based on the answers given above, the transfer is: permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: permitted

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SURF / PRIVACY COMPANY

Place, Date:

Signed:

Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.

By:

Main outcomes transfer risk assessments

- Our published DTIAs focus on the risks of transfer to the USA: but the Zoom DTIA includes an assessment of transfer to the Philippines.
- Microsoft, Zoom and AWS have never provided personal data of European public sector customers to US law enforcement and security agencies. That's *including* gagging orders. AWS limits this guarantee to Content Data and to law enforcement.
- Zoom process all personal data in the EU, except for incidental security and trust&safety transfers. Microsoft will complete its EU Data Boundary by the end of 2024. AWS only allows storage of Content Data in the EU.
- These cloud providers can still receive disclosure orders from government authorities in third countries, but they contractually promise they will resist with all legal means.

Lessons learned

Conclusions 1/2

- Distrust claims by a provider that no personal data are being processed.
- You need to do technical research to understand what personal data are being processed.
- Examine the data processing in a test environment, intercept outgoing network traffic and submit a formal data subject access request.
- Check what data the provider collects through its website (e.g. when you sign in to a browser tool, log in as administrator, submit a support ticket).
- Be patient, and keep on asking questions. It takes a long time for globally operating cloud providers to make changes, but if they do, these are usually global changes.
- A DPIA on a cloud provider is never finished: you have to keep on verifying agreed mitigation measures.

Conclusions 2/2

- Don’t try to create privacy-improvements by yourself with BigTech: create leverage through a national umbrella organisation, and/or at European level.
- It is very effective to share the findings from the DPIA with the provider: to discuss mitigating measures together and to agree on a tight timeframe for improvements.
- It works very well to write a DPIA and DTIA in English and to announce that you are going to publish them.
- Consider a prior consultation with the national Data Protection Authority if the supplier is unwilling to mitigate risks.

PRIVACY COMPANY

Questions?

www.linkedin.com/in/sjoera

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

Maanweg 174
Den Haag