Ministerie van Justitie en Veiligheid

Update V – zomer 2019

AVG en afspraken met Microsoft

Paul van den Berg

Sjoera Nas

15 augustus 2019

De meest waardevolle asset op aarde is niet langer olie maar data.

bron: economist.com 6 mei 2017

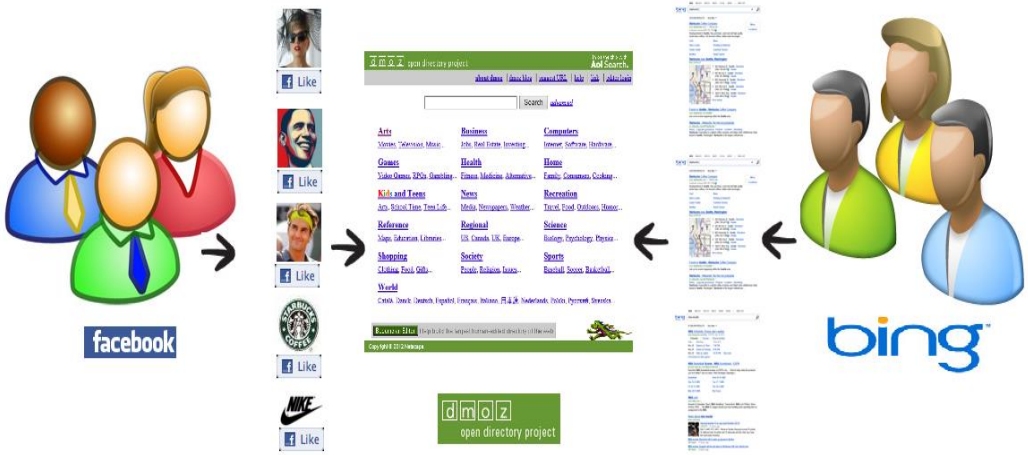
De data-economie vereist een nieuwe aanpak van antitrustregels

Cleaning Up Data Access for Partners

"Of the dozen partners that we identified as continuing to access data, only two, ***Microsoft*** *and Sony,* ***continued to access*** *limited types of friends data. This was old code supporting known experiences for people, such as being able to use Facebook on PlayStation or to sync their friends' contact information with another service. (Updated on July 24, 2019 at 9:50AM PT to correct the Playstation example.) Based on our previous commitments, we are ending these partners' access to friend data* ***immediately****. This was our mistake, and we are correcting it."*

facebook Newsroom

Persbericht Facebook **24 juli 2019**



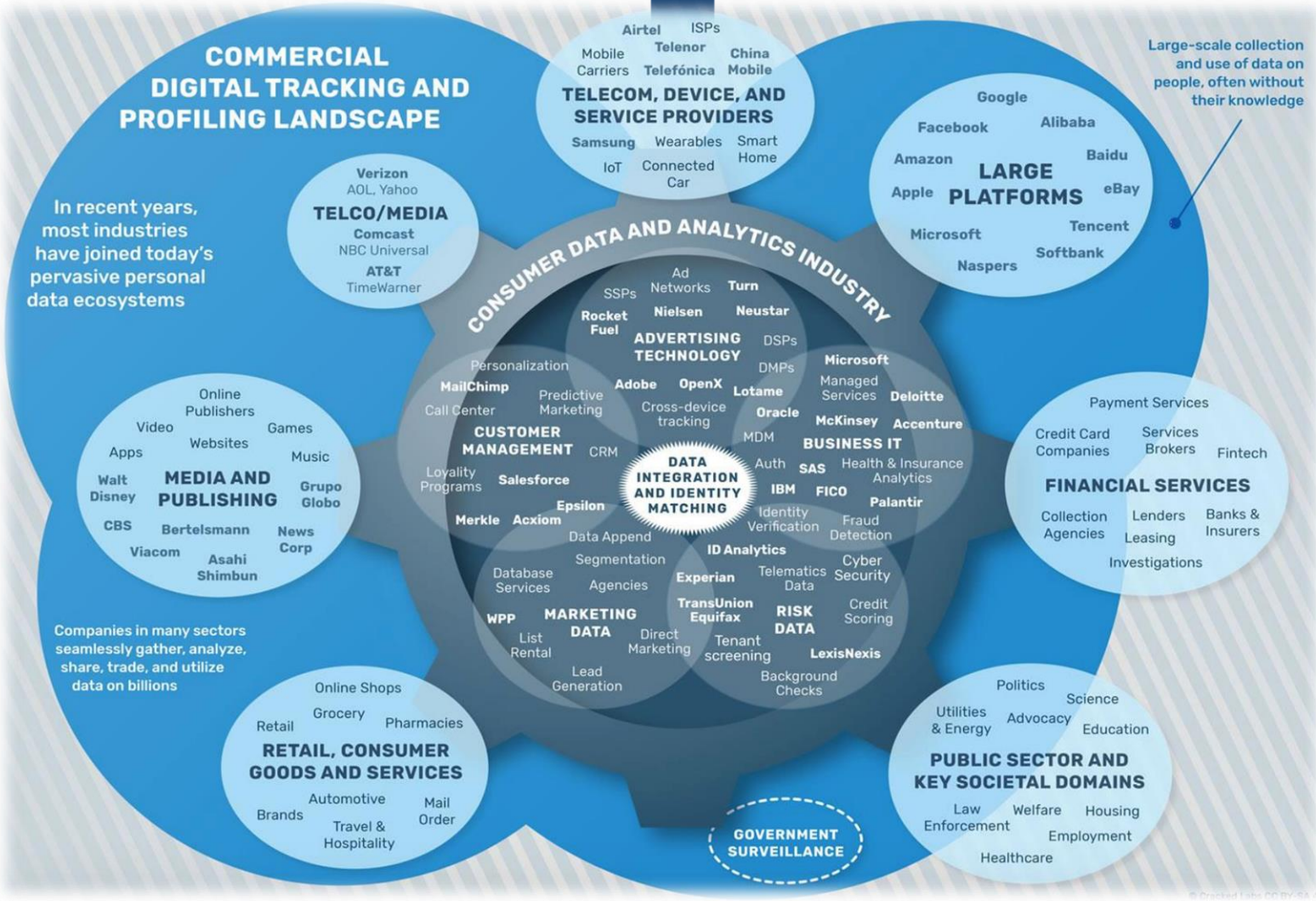
"We conclude that it is indeed feasible to infer ***important demographic data of users*** *from their query history based on labelled Likes data and believe that this approach could provide valuable information for personalization and* ***monetization*** *even in the absence of demographic data."*

bron: https://www.microsoft.com/en-us/research/publication/inferring-the-demographics-of-search-users/ januari 2013

Microsoft luistert ook mee……

Microsoft collects voice data to provide and improve voice-enabled services like search, voice commands, dictation or translation services. We strive to be transparent about our collection and use of voice data to ensure customers can make informed choices about when and how their voice data is used.

Microsoft gets customers' permission before collecting and using their voice data. We also put in place several procedures designed to prioritize users' privacy before sharing this data with our vendors, including de-identifying data, requiring non-disclosure agreements with vendors and their employees, and requiring that vendors meet the high privacy standards set out in European law.


COMMERCIAL DIGITAL TRACKING AND PROFILING LANDSCAPE
In recent years, most industries have joined today's pervasive personal data ecosystems
Companies in many sectors seamlessly gather, analyze, share, trade, and utilize data on billions
Large-scale collection and use of data on people, often without their knowledge
CONSUMER DATA AND ANALYTICS INDUSTRY
DATA INTEGRATION AND IDENTITY MATCHING
TELECOM, DEVICE, AND SERVICE PROVIDERS
Airtel
ISPs
Telenor
Mobile Carriers
Telefónica
China Mobile
Samsung
Wearables
Smart Home
IoT
Connected Car
TELCO/MEDIA
Verizon
AOL, Yahoo
Comcast
NBC Universal
AT&T
TimeWarner
LARGE PLATFORMS
Google
Facebook
Alibaba
Amazon
Baidu
Apple
eBay
Microsoft
Tencent
Softbank
Naspers
ADVERTISING TECHNOLOGY
Ad Networks
SSPs
Turn
Rocket Fuel
Nielsen
Neustar
DSPs
DMPs
Personalization
MailChimp
Predictive Marketing
Adobe
OpenX
Lotame
Call Center
Cross-device tracking
CUSTOMER MANAGEMENT
CRM
Loyality Programs
Salesforce
Epsilon
Merkle
Acxiom
Data Append
Segmentation
Database Services
Agencies
WPP
MARKETING DATA
List Rental
Direct Marketing
Lead Generation
Microsoft
Managed Services
Deloitte
Oracle
McKinsey
Accenture
MDM
BUSINESS IT
Auth
SAS
Health & Insurance Analytics
IBM
FICO
Palantir
Identity Verification
Fraud Detection
ID Analytics
Experian
Telematics Data
Cyber Security
TransUnion
Equifax
RISK DATA
Credit Scoring
Tenant screening
LexisNexis
Background Checks
MEDIA AND PUBLISHING
Online Publishers
Video
Games
Websites
Apps
Music
Walt Disney
Grupo Globo
CBS
Bertelsmann
News Corp
Viacom
Asahi Shimbun
FINANCIAL SERVICES
Payment Services
Credit Card Companies
Services Brokers
Fintech
Collection Agencies
Lenders
Banks & Insurers
Leasing
Investigations
RETAIL, CONSUMER GOODS AND SERVICES
Online Shops
Grocery
Retail
Pharmacies
Automotive
Brands
Mail Order
Travel & Hospitality
PUBLIC SECTOR AND KEY SOCIETAL DOMAINS
Politics
Science
Utilities & Energy
Advocacy
Education
Law Enforcement
Welfare
Housing
Employment
Healthcare
GOVERNMENT SURVEILLANCE

Update V – take aways today

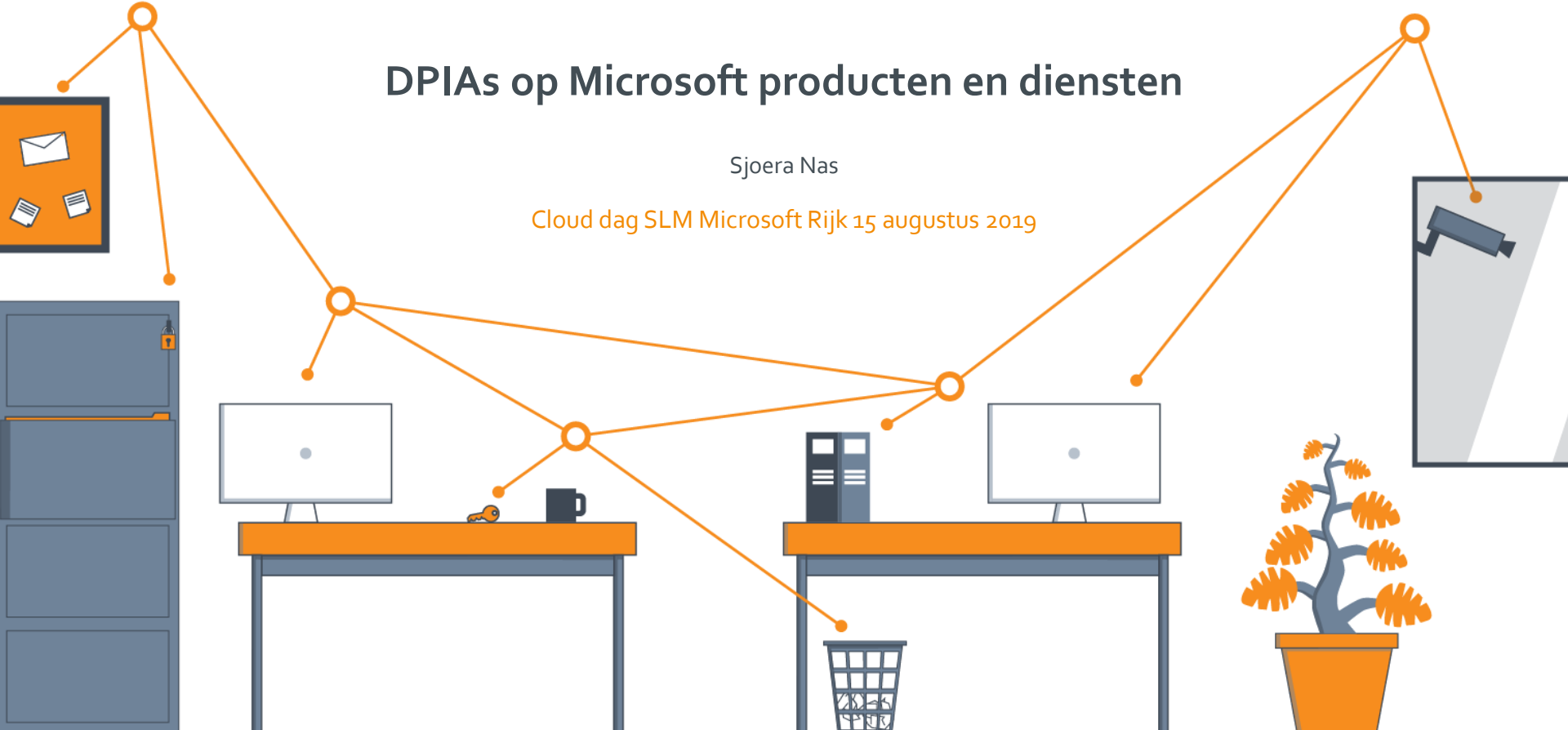
- DPIA’s bevindingen en resultaten
- Welke aanpassingen heeft Microsoft gedaan?
- Wat betekenen de voorwaarden die aan de Rijksbrede MBSA zijn toegevoegd voor de deelnemers?
- Wat zijn de voordelen van deelnemen aan de Rijksbrede MBSA?
- Wat betekent dit voor partijen die (nog) niet deelnemen of niet kunnen deelnemen aan de Rijksbrede MBSA?
- Hoe zorg ik dat ik de Microsoft-producten AVG-compliant kan gebruiken?
- Als ik nog niet deelneem aan de Rijksbrede MBSA, hoe kan ik daarop aansluiten?

PRIVACY COMPANY

DPIAs op Microsoft producten en diensten

Sjoera Nas

Cloud dag SLM Microsoft Rijk 15 augustus 2019



Wat is Privacy Company?

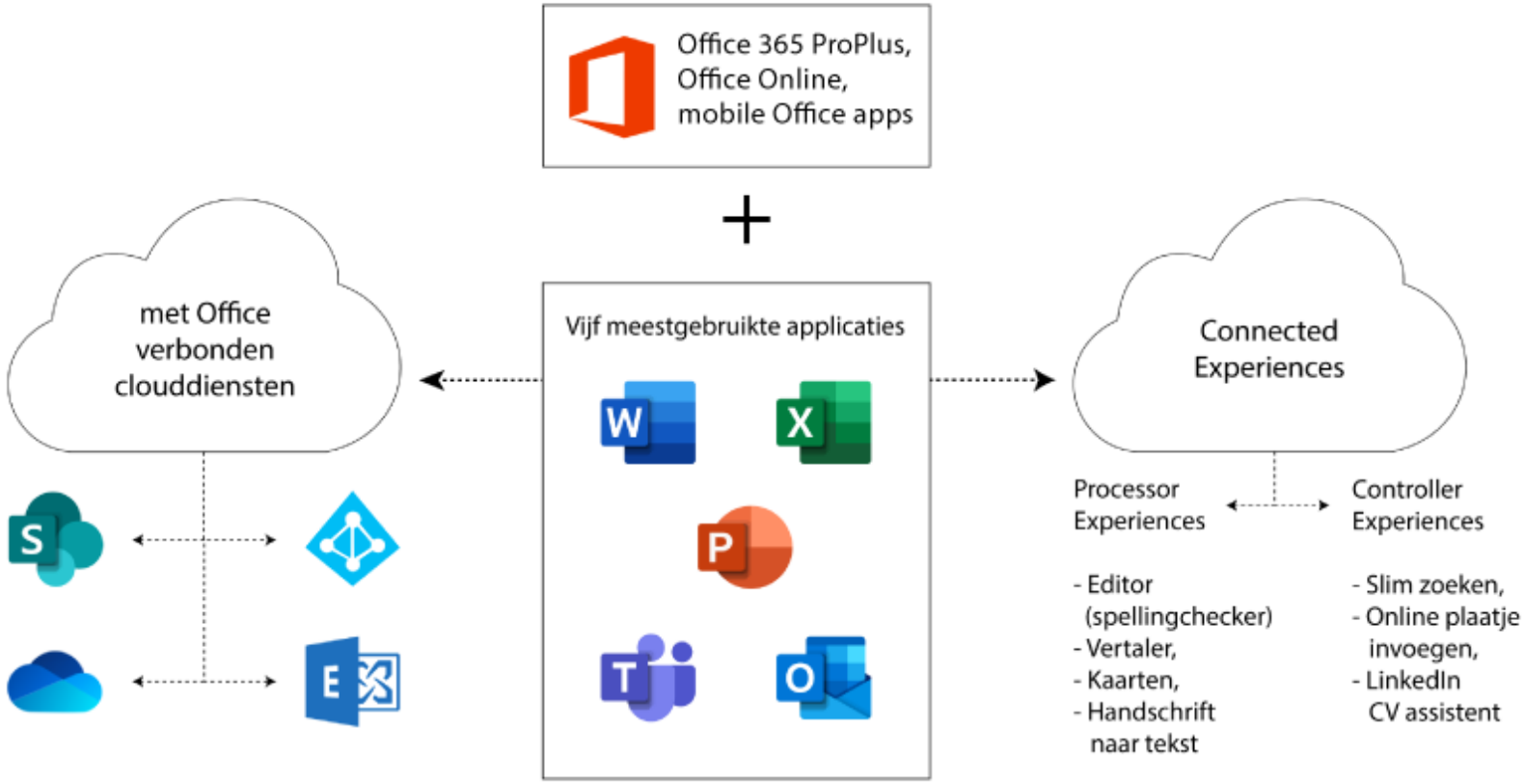
- Opgericht in 2014
- Team van 30+ veelzijdige professionals
- Gericht op praktische oplossingen
- Advies, training, privacy management tooling, FG diensten, ePrivacy en informatiebeveiliging

Agenda

- Wat zijn diagnostische gegevens?
- Wat voorafging: resultaten eerste DPIA Office 365 ProPlus
- Uitkomsten nieuwe DPIA Office 365 ProPlus versie 1905
- Uitkomsten nieuwe DPIA Windows 10 Enterprise versie 1809, met preview versie 1903
- Uitkomsten nieuwe DPIA testomgeving in Azure cloud
- Uitkomsten nieuwe DPIA Office Online en mobiele Office apps

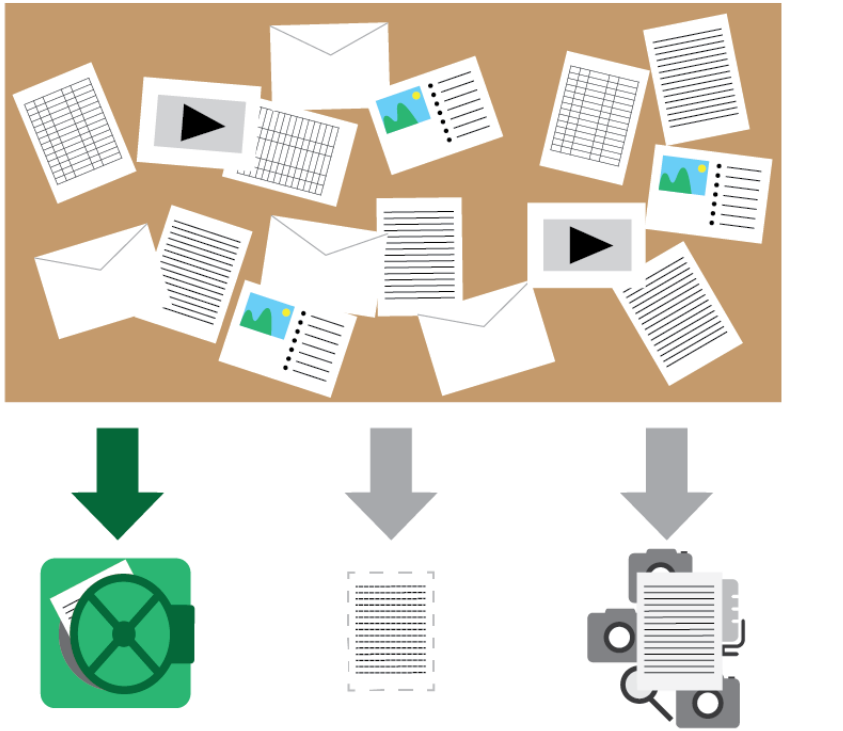
Op de 300.000 rijkswerk-plekken wordt niet alleen Windows 10 gebruikt, maar ook Microsoft Office Proplus en soms de Exchange mailserver, en SharePoint Online/OneDrive for Business

Office 365 software en online diensten



Techniek

Kantooractiviteiten werknemer



Content

Functioneel

Diagnostisch

Diagnostische gegevens zijn persoonsgegevens

Microsoft verwerkt persoonsgegevens over het individuele gebruik van haar software en diensten

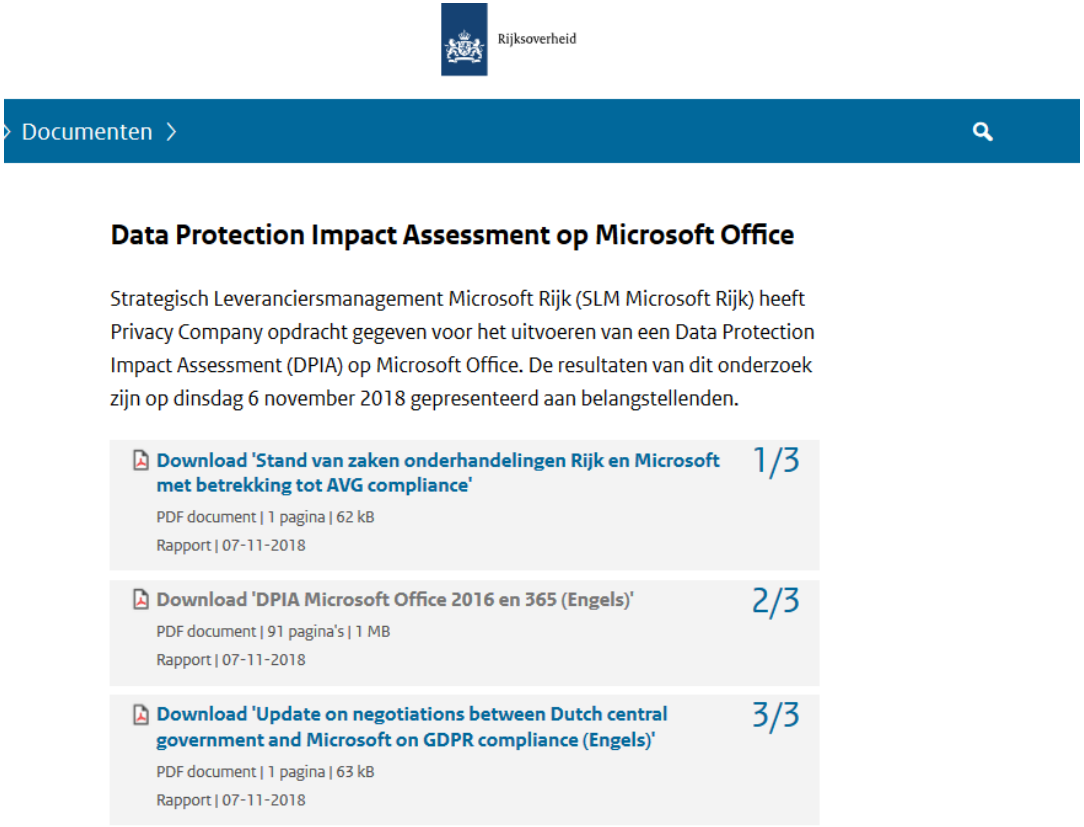
- Elk gegeven (nummer, foto, omschrijving, online identificator etc.)
- Betreffende (in verband te brengen met, koppelen datasets)
- Identificatie van natuurlijke personen (geen overledenen of rechtspersonen)

Ook pseudoniemen zijn persoonsgegevens

- Artikel 4(5) AVG: *Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat* (…)
- De diagnostische gegevens zijn persoonsgegevens
- Microsoft slaat alle telemetriegegevens langdurig op in één database. *Hashing* helpt niet zolang Microsoft over de formule beschikt.

November 2018: openbare DPIA Office ProPlus voor Rijksoverheid

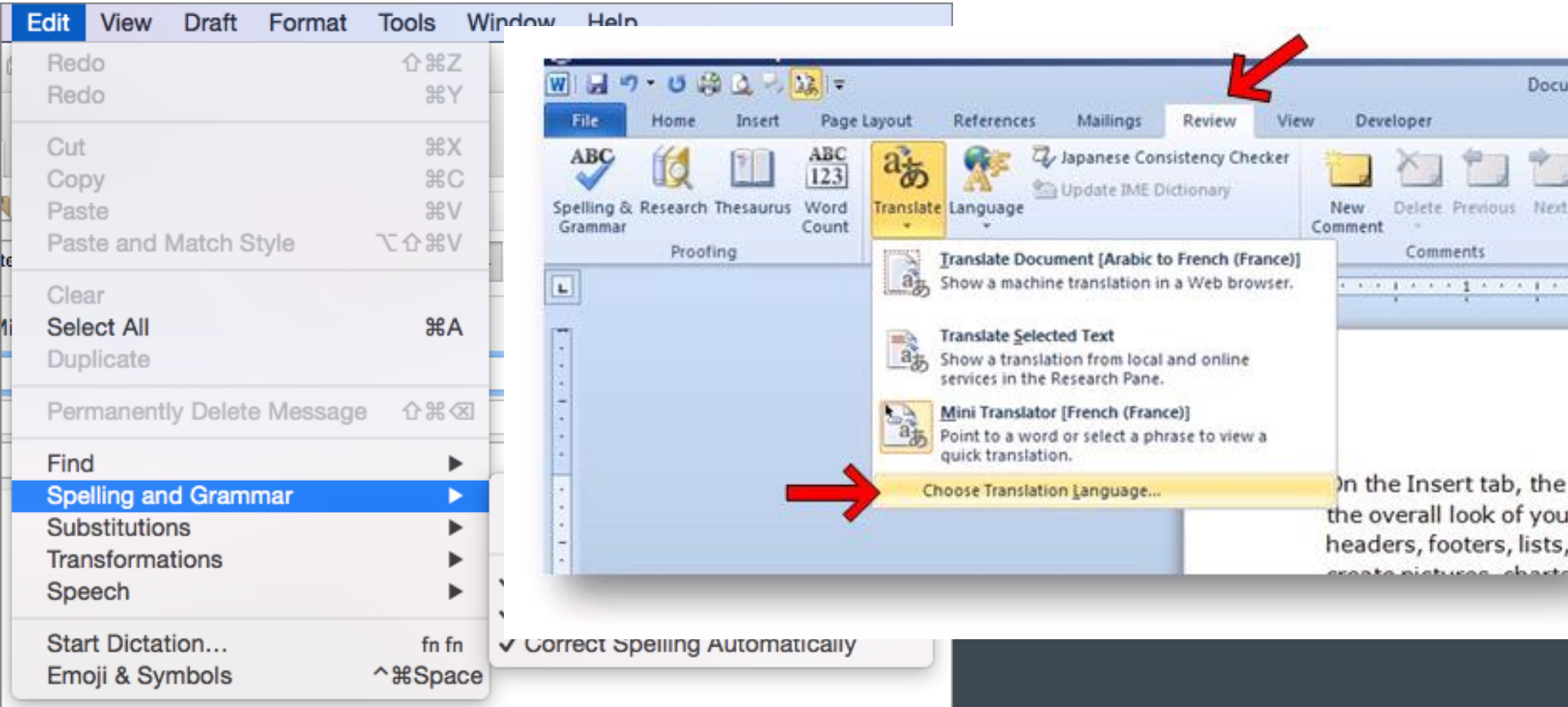
- DPIA uitgevoerd in opdracht van SLM Rijk op Office 365 ProPlus.
- Office ProPlus blijkt zelf ook telemetrie-gegevens te verzamelen, op nog veel grootschaliger wijze dan via Windows.



8 hoge risico's ProPlus

1. Gebrek aan transparantie
2. Gebrek aan keuzemogelijkheden
3. Onrechtmatige opslag van gevoelige/gerubriceerde persoonsgegevens
4. Onjuiste kwalificatie van Microsoft als verwerker
5. Gebrek aan doelbinding

Gebrek aan doelbinding leidde tot hoge risico's bij gebruik online diensten zoals spellingchecker



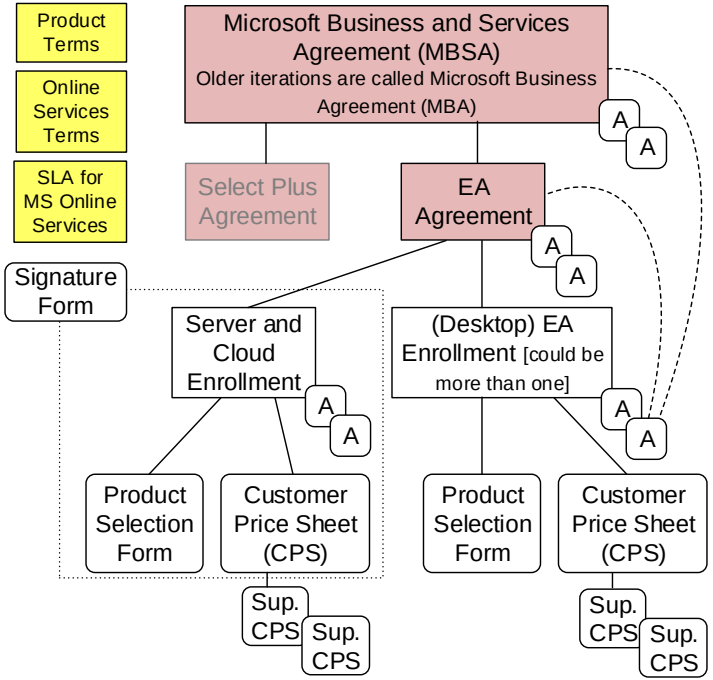
8 hoge risico's ProPlus

1. Gebrek aan transparantie
2. Gebrek aan keuzemogelijkheden
3. Onrechtmatige opslag van gevoelige/gerubriceerde persoonsgegevens
4. Onjuiste kwalificatie van Microsoft als verwerker
5. Gebrek aan doelbinding

Verschil tussen verantwoordelijke en verwerker

Contractstructuur Office 365 en online diensten

Microsoft als verwerker: contract met de organisatie



Controller Connected Experiences, mobiele apps, Windows 10 Enterprise

Microsoft Services Agreement

Microsoft Privacy Statement

Microsoft als verantwoordelijke: vraagt gebruikers om toestemming

8 hoge risico's ProPlus

1. Gebrek aan transparantie
2. Gebrek aan keuzemogelijkheden
3. Onrechtmatige opslag van gevoelige/gerubriceerde persoonsgegevens
4. Onjuiste kwalificatie van Microsoft als verwerker
5. Gebrek aan doelbinding

Doelen Microsoft als verwerker

1. Beveiliging
2. Up to date houden
3. Goed werkend houden
4. Product ontwikkeling
5. Product innovatie
6. Algemene afgeleide gegevens gebaseerd op lange termijn analyses
7. Het tonen van gerichte aanbevelingen op het scherm aan de gebruiker
8. Elk doeleinde dat Microsoft hiermee verenigbaar acht

Doelen Microsoft als verantwoordelijke

1. Alle verenigbare doelen met het aanbieden van de diensten
2. Aanbieden van de diensten
3. Product verbetering
4. Personalisering, inclusief gerichte advertenties
5. Product activering
6. Product ontwikkeling / innovate
7. Beveiliging en troubleshooting
8. Veiligheid (tegen bv virussen/malware)
9. Updates
10. Algemene Business Intelligence
11. Bescherming rechten en eigendom
12. Onderzoek

8 hoge risico's ProPlus

5. Onvoldoende controle over subverwerkers en de feitelijke gegevensverwerking
6. Doorgifte van alle soorten Office diagnostische gegevens naar de VS, op basis van het Privacy Shield, terwijl de geldigheid hiervan onderwerp is van een procedure bij het Europees Hof van Justitie
7. Te lange bewaartermijn van de diagnostische gegevens en het ontbreken van een middel om historische diagnostische gegevens te verwijderen (anders dan het vernietigen van het gebruikersaccount).

Klachten over doorgifte naar VS bij het Europese Hof van Justitie

Franse NGO La Quadrature du Net tegen de Europese Commissie over Privacy Shield: zitting uitgesteld tot na Schrems-2

Max Schrems vs de Ierse DPA over de SCC: zitting 9 juli 2019, advies AG verwacht 12 december 2019

Februari 2019: Microsoft kondigt wereldwijde wijzigingen aan van Office ProPlus

> 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

april 2019: EDPS kondigt onderzoek aan naar contracten Microsoft

EDPS investigates contractual agreements concerning software used by EU institutions

8 Apr 2019

EDPS investigates contractual agreements concerning software used by EU institutions

Press Release

As the supervisory authority for all EU institutions, the European Data Protection Supervisor (EDPS) is responsible for enforcing and monitoring their **compliance with data protection rules**. In this capacity, the EDPS is undertaking an **investigation** into the compliance of **contractual arrangements** concluded between the **EU institutions and Microsoft**, the European Data Protection Supervisor said today.

april 2019: EDPS kondigt onderzoek aan naar contracten Microsoft

EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Home | About | Data Protection | Press & Publications

> ... > Blog > We need to talk about terms and conditions

We need to talk about terms and conditions

Monday, 29 April, 2019

Giovanni Buttarelli

30 april blog Julie Brill, VP Privacy Microsoft

Increasing transparency and customer control over data

Apr 30, 2019 | Julie Brill - Corporate Vice President and Deputy General Counsel, Microsoft

Today we are announcing new steps to give customers increased transparency and control over their data that is used by Microsoft's major products.

https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-and-customer-control-over-data/

Julie Brill schrijft:

In recent months we've heard from customers – especially those in Europe – with questions about the data that is collected from their devices when they use our products and services. *(…)*

– information should be ***easier to find****,* ***easier to understand****, and* ***easier to act*** *on through the tools we provide.*

Bron: Microsoft blog: **Microsoft appoints globally respected regulator to privacy leadership role**

Wijzigingen lenteversie 2019 (vanaf versie 1904)

Easier to act:

Mogelijkheid tot uitzetten telemetrie, of keuze voor 'required' of 'optional' , vergelijkbaar met opties in Windows 10 Enterprise

Diagnostic data sent from Office 365 ProPlus to Microsoft

Diagnostic data is used to keep Office secure and up-to-date, detect, diagnose and remediate problems, and also make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office.

This diagnostic data is collected and sent to Microsoft about Office client software being used on computers running Windows in your organization.

There are three levels of diagnostic data for Office 365 ProPlus client software that you can choose from:

- **Required** The minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it's installed on.
- **Optional** Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.
- **Neither** No diagnostic data about Office client software running on the user's device is collected and sent to us. This option, however, significantly limits our ability to detect, diagnose, and remediate problems your users may encounter using Office.

Easier to find:

documentatie over inhoud van telemetrie-berichten Office

Microsoft | Docs Windows Microsoft Azure Visual Studio Office More

Office 365 ProPlus / Diagnostic data / Required diagnostic data

Feedback Share

- rols
- with policy
- Diagnostic data
  - Required diagnostic data
  - Optional diagnostic data
  - Using the Diagnostic Data Viewer
- Connected experiences
- Essential services

Download PDF

Required diagnostic data for Office

05/16/2019 • 71 minutes to read • Contributors

Important

The information in this article applies to Version 1904 or later of the following Office client software installed on a computer running Windows:

- Office 365 ProPlus and Office 365 Business
- Office 365 Personal, Office 365 Home, or other versions of Office that are part of an Office 365 subscription.
- Project and Visio that come with some subscription plans, such as the Project Online Professional plan or Visio Online Plan 2.

Diagnostic data is used to keep Office secure and up-to-date, detect, diagnose and fix problems, and also make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office.

PRIVACY COMPANY

Voorbeeld telemetrie uitleg

Activity

Information to understand the success of the collection event itself.

This category contains the following fields:

- **AggMode** - Tells the system how to aggregate activity results. Allows us to reduce the amount of information uploaded from a user's machine by aggregating activity results into a single event that gets sent periodically.
- **Count** - The number of times the activity happened if the count is from an aggregated event. Allows us to determine how often an activity succeeded or failed based on the aggregation mode of the activity.
- **CV** - A value that identifies the relationship between activities and sub-activities. Allows us to rebuild the relationship between nested activities.
- **Duration** - The length of time the activity took to execute. Allows us to identify performance issues that are negatively impacting the users experience.
- **Result.Code** - An application defined code to identify a given results. Allows us

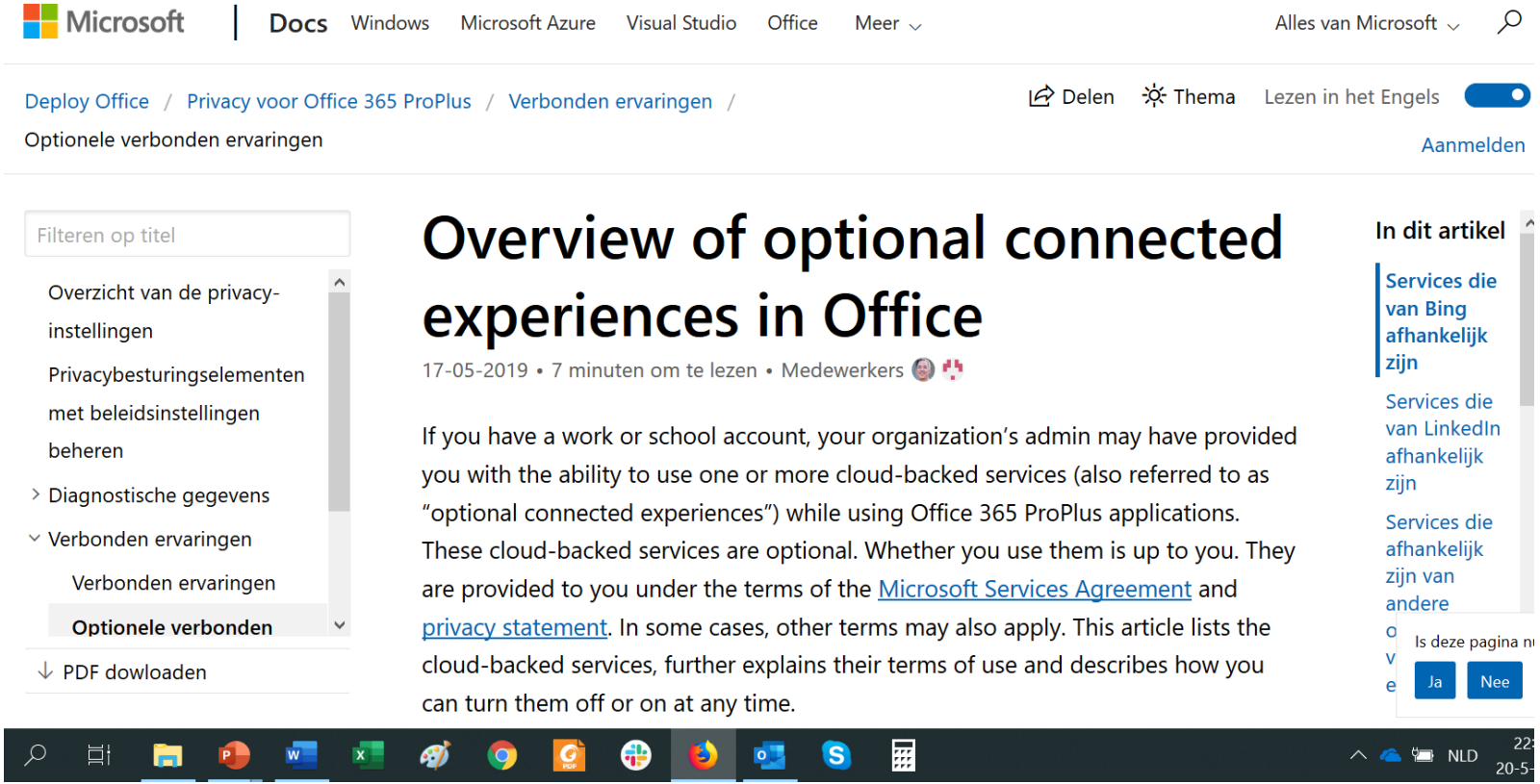
In this article

Wijzigingen lenteversie 2019

Easier to understand

Gebruik zelfde Data Viewer tool als bij Windows 10

Sinds lente 2019: *Optionele verbonden ervaringen*



Resterende Controller Connected Experiences

3D-kaarten	LinkedIn CV-assistent
Kaartgrafieken	Office Store
Onlineafbeeldingen invoegen	Online Video insluiten
Online-3D-modellen invoegen	Onderzoek
PowerPoint Snelstart	Weerbalk in Outlook
Onderzoeker	Feedback (behalve in Outlook)
Slim zoeken	Een functie voorstellen (in Outlook)

Bevindingen nieuwe DPIA Office 365 ProPlus versie 1905

- Beperkt aantal telemetrieberichten op niveaus Neither en Required
- Geen inhoud uit bestanden, e-mails of conversaties, en geen direct identificerende gegevens zoals gebruikersnamen of e-mailadressen
- De berichten die betrekking hebben op de Processor (verwerker) Connected Experiences zoals de spellingchecker en de vertaalmodule bevatten ook géén fragmenten van de inhoud.

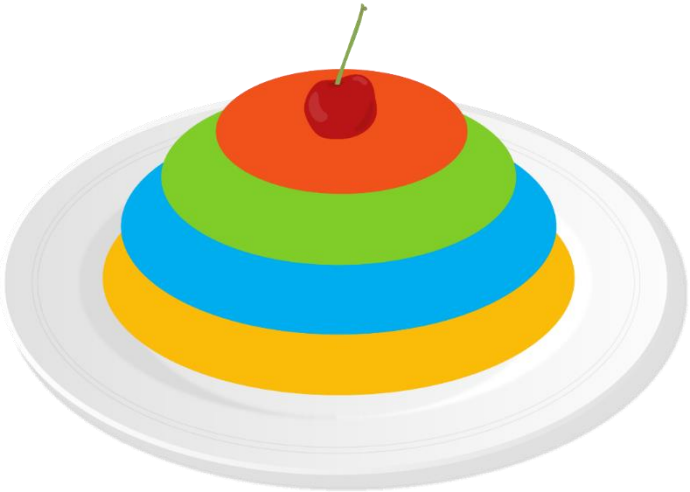
Bevindingen nieuwe DPIA Office 365 ProPlus versie 1905

- Sommige berichten op het niveau Required bevatten wel gevoeligere informatie, zoals het exacte aantal pagina's, alinea's, regels, woorden, karakters, spaties, plaatjes en citaten in een Word bestand, of de exacte tijd in milliseconden dat een betrokkene actief bezig was met een bestand.

- Er zijn twee soorten telemetrie die doorgaan ONDANKS telemetrie op laagste niveau: Essentiële service gegevens en Essentiele diensten.

Resultaten onderhandelingen Microsoft

- Dankzij technische en contractuele maatregelen géén hoge privacyrisico's meer
- Beheerders moeten wel de adviezen volgen om telemetrie op 'Neither' te zetten en Controller Connected Experiences uit



Verbod DPA Hessen op gebruik Office 365 door scholen

- Hessische DPA persbericht 12 juli 2019: verbod op gebruik door scholen van Office 365 en andere cloud oplossingen ivm risico's doorgifte naar de VS

- Hessische DPA persbericht 2 augustus 2019: scholen mogen voorlopig wel gebruik maken van Office 365 als ze de telemetrie uitzetten.

MUST READ: Capital One hacker took data from more than 30 companies, new court docs reveal

Microsoft Office 365: Banned in German schools over privacy fears

State of Hesse says student and teacher information could be "exposed" to US spy agencies.

By Cathrin Schaer | July 12, 2019 -- 10:00 GMT (11:00 BST) | Topic: Cloud

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

DATENSCHUTZ INFORMATIONSFREIHEIT INFOTHEK SERVICE PRESSE

Presse > Pressemitteilungen > Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessisc

Pressemitteilungen

Pressekontakt

Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen

02.08.2019

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat sich nach den Gesprächen mit Microsoft dazu entschlossen, den Einsatz von Office 365 in hessischen Schulen unter bestimmten Voraussetzungen und dem Vorbehalt weiterer Prüfungen vorläufig zu dulden.

Juni 2019: DPIA op Windows 10 Enterprise

- Microsoft is een verantwoordelijke voor de verwerking van diagnostische gegevens over Windows 10
- Microsoft verwerkt de gegevens voor 12 doelen uit haar algemene (op consumenten gerichte) privacyverklaring
- Onderzoek gedaan naar de inhoud van telemetrie op Security niveau: heel weinig gegevens, en géén gegevens uit de inhoud van bestanden

Juni 2019: DPIA op Windows 10 Enterprise

Alle waargenomen telemetrieberichten op Security:

- DxgKrnlTelemetry.GPUAdapterInventoryV2
- Microsoft.OSG.DU.DeliveryOptClient.DownloadCompleted
- Microsoft.OSG.DU.DeliveryOptClient.DownloadStarted
- Microsoft.Windows.StoreAgent.Telemetry.CompleteInstallOperationRequest
- Microsoft.Windows.StoreAgent.Telemetry.EndAcquireLicense
- Microsoft.Windows.StoreAgent.Telemetry.EndDownload
- Microsoft.Windows.StoreAgent.Telemetry.EndInstall
- Microsoft.Windows.StoreAgent.Telemetry.EndScanForUpdates
- Microsoft.Windows.StoreAgent.Telemetry.EndSearchUpdatePackages
- Microsoft.Windows.StoreAgent.Telemetry.EndStageUserData
- Microsoft.Windows.StoreAgent.Telemetry.FulfillmentComplete
- Microsoft.Windows.StoreAgent.Telemetry.FulfillmentInitiate
- Microsoft.Windows.StoreAgent.Telemetry.InstallOperationRequest
- Microsoft.Windows.StoreAgent.Telemetry.SearchForUpdateOperationRequest
- SoftwareUpdateClientTelemetry.CheckForUpdates
- SoftwareUpdateClientTelemetry.Download
- SoftwareUpdateClientTelemetry.Install
- SoftwareUpdateClientTelemetry.UpdateDetected
- TelClientSynthetic.HeartBeat_5

- Deze telemetrieberichten bevatten géén inhoud van bestanden, bestandsnamen, surfgedrag of gegevens over individueel appgebruik
- Elk bericht bevat twee unieke identifiers voor het apparaat en de gebruiker en een precies datumtijdstempel
- Microsoft publiceert geen limitatieve lijst welke berichten zij op Security verzamelt: alleen algemene informatie

Gezamenlijke verantwoordelijkheid

- Als een hyperscale provider zich niet gedraagt als verwerker, zijn de zakelijke afnemers snel *de facto* gezamenlijk verantwoordelijk voor de gegevens over het gebruik als bedoeld in artikel 26 van de AVG
- De beheerders hebben weliswaar beperkte invloed (bepaalde opties uitzetten) maar ook bij ongelijke rollen kun je gezamenlijk verantwoordelijk zijn (EU HvJ Facebook Fanpage, Jehova Getuigen en Fashion ID over Like knop)
- Het is niet geloofwaardig dat Microsoft verantwoordelijk is (en geen verwerker) voor geïnstalleerde software zoals Windows 10 en mobiele apps

Risico's bepalen

De ICO heeft een matrix gemaakt om de risico's te bepalen

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		

5 hoofdcategorieën van risico's

1. Verlies van controle op het gebruik van de gegevens
2. Verlies van vertrouwelijkheid
3. Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen
4. Heridentificatie van gepseudonimiseerde gegevens
5. Onrechtmatige (verdere) verwerking

Deze risico's moeten worden afgewogen tegen de kans (de mate van waarschijnlijkheid waarin de negatieve gevolgen voor de betrokkenen kunnen voorkomen), en tegen de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Vier risico's Windows 10 Enterprise

Gebrek aan doelbinding en grondslag als verantwoordelijke	Verlies van controle, onrechtmatige verwerking
Gebrek aan controle over derde partijen/verwerkers en toezicht via audits op de feitelijke gegevensverwerking	Verlies van controle, verlies vertrouwelijkheid, onrechtmatige verwerking, heridentificatie gepseudonimiseerde gegevens
De doorgifte van diagnostische persoonsgegevens naar de Verenigde Staten	Verlies van controle, onrechtmatige verwerking, verlies vertrouwelijkheid, heridentificatie gepseudonimiseerde gg
De lange bewaartermijn van de diagnostische persoonsgegevens	Heridentificatie gepseudonimiseerde gg, geen uitoefening individueel recht op verwijdering

Risico inschatting

- Vier keer grote kans dat risico zich voordoet, maar impact laag door beperkte hoeveelheid niet-gevoelige gegevens

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 3 4	Laag risico 1 2
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

Conclusie: <u>géén hoge dataprotectierisico's</u> voor betrokkenen als de telemetrie op Security staat èn cloud synchronisatie via Windows Tijdlijn geblokkeerd is.

Juni 2019: DPIA op Azure VM's

- Een overheidsorganisatie verwerkt grootschalig gevoelige en bijzondere persoonsgegevens
- Wil met de testomgeving en de productieomgeving naar Azure
- De verwerking van diagnostische gegevens is beperkt tot een kleine groep beheerders, testers en ontwikkelaars
- Onderzoek naar risico's van Azure Stack en Public Cloud

11 doelen Microsoft verwerking Azure

1. De diensten aanbieden
2. Alle doelen die Microsoft daarmee verenigbaar acht
3. Het voorkomen, opsporen en verhelpen van problemen
4. Productinnovatie
5. Aanbieden van gepersonaliseerde ervaringen
6. Onderzoek
7. Analyse van het gebruik
8. Het oplossen van fouten in de software (debugging)
9. Systeembrede gezondheidsanalyse
10. Systeembrede analyse met machine learning
11. Beveiliging van de diensten

Conclusies Azure VM's

- Bij de huidige werkwijze van deze organisatie is er al een groot aantal hoge dataprotectierisico's, onder andere door risico's op heridentificatie gepseudonimiseerde gegevens
- Bij verhuizing naar Azure Stack geen nieuwe risico's
- Bij verhuizing naar Azure public cloud 5 nieuwe risico's, vooral ivm doorgifte persoonsgegevens naar de VS

Hoge risico's en getroffen maatregelen

TEST EN PRODUCTIE OMGEVING	
Geen volledige inzage en geen recht op verwijdering loggegevens admins en developers	Rijk: doelbinding en recht op controle via audits van de feitelijke naleving van de afspraken, ook bij subverwerkers.
	Organisatie: Zet de logging van Azure uit waar mogelijk
PRODUCTIE OMGEVING	
Negatieve profilering van betrokkene in database ten gevolge van onrechtmatige toegang door statelijke actoren (ook mbt contactgegevens werknemers)	Organisatie: pas encryptie toe op transport, gebruik Azure Disk Encryption en Azure Key Vault.
	EU: Sluit verdrag met de VS over toegang voor opsporing (zodat Microsoft niet in strijd hoeft te handelen met art. 48 AVG)
Gemotiveerde beheerder die misbruik maakt van zijn bevoegheden	Organisatie: pas encryptie toe op transport, gebruik Azure Disk Encryption en Azure Key Vault.
	Rijk: doelbinding en recht op controle via audits van de feitelijke naleving van de afspraken, ook bij subverwerkers .
Microsoft of een subverwerker wordt wettelijk verplicht om specifieke persoonsgegevens te verstrekken	Organisatie: pas encryptie toe op transport, gebruik Azure Disk Encryption en Azure Key Vault.
	EU: Sluit verdrag met de VS over toegang voor opsporing (zodat Microsoft niet in strijd hoeft te handelen met art. 48 AVG)
	Rijk: doelbinding en recht op controle via audits van de feitelijke naleving van de afspraken, ook bij subverwerkers .
Onrechtmatige verwerking van logbestanden door lange bewaartermijnen bij Microsoft	Rijk: doelbinding voor de Azure cloud logs
	Organisatie: voeg regels aan bestaand logbeleid

Juni 2019: DPIA op Office Online en de mobiele Office apps

Technische bevindingen

- Er is géén data viewer tool om telemetrie te decoderen
- Technisch verzamelt Microsoft een beperkt aantal gegevens via de apps, geen gevoelige gegevens
- Via Office Online verzamelt Microsoft wel inhoudelijke gegevens zoals e-mailheaders and bestandsnamen op de system-gegenereerde logbestanden bij gebruik van clouddiensten (Exchange Online, SharePoint Online en OneDrive for Business)
- Microsoft heeft géén volledige inzage gegeven in diagnostische gegevens uit eigen logbestanden

Juni 2019: DPIA op Office Online en de mobiele Office apps

Juridische bevindingen

- Microsoft gedraagt zich als een verantwoordelijke voor de verwerking van diagnostische gegevens over gebruik van de mobiele Office apps
- Microsoft verwerkt de gegevens van de mobiele apps voor 14 doelen uit haar algemene privacyverklaring
- Dit zijn ook doelen zoals adverteren en het sturen van gepersonaliseerde berichten
- Omdat Microsoft de doelen bepaalt, zijn de organisaties gezamenlijk verantwoordelijk met Microsoft

Gegevensverkeer naar Braze via iOS apps

- Vanuit drie apps op iOS wordt verkeer verzonden naar het Amerikaanse marketingbedrijf Braze: Word, PowerPoint en Excel
- Dat verkeer wordt verzonden ongeacht of je bent ingelogd op je overheidsaccount of niet
- Reactie Microsoft: géén datalek, mag volgens algemene voorwaarden, maar al het ingelogde verkeer valt wél onder de privacygaranties Rijk


```
{
 "api_key": "6f0a70f2-5359-45f8-9106-7507478bc55f",
 "app_version": "2.25",
 "device_id": "F8189EAF-313E-4199-97F6-9D1E861508F3",
 "events": [
  {
   "data": {
    "key": "PowerPoint_EditFile",
    "value": 1
   },
   "name": "inc",
   "session_id": "4F35E555-74A8-40E0-88D6-840FD41F9BE9",
   "time": 1559901297.509,
   "user_id": "80a89116-f786-44b0-b048-a490f1c84444"
  },
  {
   "data": {
    "n": "_EditFile",
    "p": {
     "AppName": "PowerPoint"
    }
   },
   "name": "ce",
   "session_id": "4F35E555-74A8-40E0-88D6-840FD41F9BE9",
   "time": 1559901297.509,
   "user_id": "80a89116-f786-44b0-b048-a490f1c84444"
  }
 ],
 "sdk_version": "3.12.0",
 "time": 1559901307.526232
}
```

Conclusies DPIA op Office Online en de mobiele Office apps

Vijf hoge risico's

1. Gebrek aan transparantie
2. Geen technische opt-out Controller Connected Experiences en mobiele Office apps
3. Onrechtmatige verzameling en opslag gevoelige soorten persoonsgegevens door de Controller Connected Experiences
4. Gebrek aan doelbinding mobiele apps en Contr. Connected Experiences
5. Niet genoeg controle op subverwerkers en feitelijke verwerkingen

Vier lage risico's

6. Geen controle over aard en hoeveelheid diagnostische gegevens
7. Chilling effect van personeelsvolgsysteem
8. Lange bewaartermijn van diagnostische gegevens
9. Doorgifte van (beperkte hoeveelheid) diagnostische gegevens naar de VS

Conclusies DPIA op Office Online en de mobiele Office apps

Ernst van de gevolgen voor de betrokkene(n)	Ernstige gevolgen	Laag risico 9	Hoog risico 3	Hoog risico 1a, 1b
	Enige negatieve gevolgen	Laag risico 9	Medium risico 3	Hoog risico 2, 4, 5
	Minimale gevolgen	Laag risico 8,9	Laag risico 7,8	Laag risico 6
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

Vragen?

sjoera.nas@privacycompany.nl

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

Maanweg 174
Den Haag

Microsoft als een cloudpartner voor het Rijk

- Steeds meer belangstelling voor cloud-diensten.
- Gezien de ontwikkelingen in de markt onvermijdelijk.
- Hoe kunnen we op gecontroleerde en veilige manier gebruik maken van Microsoft's cloud-diensten zoals Office 365 en Azure?

Resultaten (contract)onderhandelingen 1/3

De meeste Online producten zoals Office 365 en Azure zijn gezien de contractaanpassingen voor de Rijksoverheid op verantwoorde wijze in te zetten:

- Microsoft verwerkt de verzamelde gegevens voor drie doelen: voor het leveren van de dienst, de dienst up-to-date en veilig houden.
- Dit geldt zowel voor de inhoudelijke Customer Data, als voor de diagnostische gegevens over het individuele gebruik van de diensten
- Microsoft garandeert dat zij de twee soorten gegevens NIET gebruikt voor profilering, data-analyse, marktonderzoek en adverteren, tenzij de afnemer daar expliciet om vraagt.

Resultaten (contract)onderhandelingen 2/3

- Microsoft zal gegevens anonimiseren volgens de richtlijnen van de privacytoezichthouders uit 2014 (WP216)
- Om naleving van Microsoft op de contractuele bepalingen en de AVG te kunnen controleren, een verantwoordelijkheid van de verwerkingsverantwoordelijke, heeft de Nederlandse Staat een procedure voor uitoefening van de verbeterde **auditrechten** bedongen.
  - Deze audits vinden jaarlijks plaats, waarna een samenvatting van de bevindingen zal worden gepubliceerd op de website van SLM

Resultaten (contract)onderhandelingen 3/3

- Ook expliciet verbod op reclame (tips) voor eigen producten en diensten van Microsoft die je niet hebt gekocht of niet gebruikt
- Organisaties kunnen de Controller Connected Services centraal uitzetten. Let op: dit kan nu **nog** niet in Office Online en de mobiele apps!
- Om misverstanden te voorkomen, geeft Microsoft ook een uitputtende lijst van doelen waarvoor zij zelfstandig verantwoordelijk is, zoals het versturen van rekeningen

Beperkingen

- Rijksafspraken zijn momenteel alleen beschikbaar indien organisaties aangesloten zijn bij SLM Rijk dus **niet** beschikbaar voor gemeentes, leden van SURF, gezondheidszorg, NGO's etc.
- De afspraken gelden alleen voor diensten waarvoor Microsoft een verwerker is. Dus niet voor de mobiele apps, voor Windows 10 Enterprise en voor een paar Controller Connected Experiences
- De afspraken gelden wel voor Azure, Office Online en alle core online diensten. Ook voor de nieuwe Office 365 ProPlus versie, niet voor Office 2012/2016/2019

Advies SLM Rijk over Office 365 ProPlus 1/3

- Zet de ‘Controller Connected Experiences uit ’
- Gebruik versie 1905 of hoger van Office 365 ProPlus en zet het telemetrie level naar ‘Neither’.
- Zet de Linked-In integration met Microsoft employee work accounts uit.
- Afhankelijk van de specifieke situatie in iedere organisatie is het gebruik van Customer Lockbox en Customer Key te overwegen om de inhoud van bestanden nog beter te beschermen.

Advies SLM Rijk over Office 365 ProPlus 2/3

Zet het sturen van data voor het Customer Experience Improvement Program uit.

Maak geen gebruik van Office Online en de mobiele Office apps die onderdeel zijn van de Office 365 licentie tot de vijf hoge risico's die beschreven worden in het addendum van de DPIA, zijn gemitigeerd.

Volg ook de aanvbevelingen van de Duitse collega's (BSI) http://bit.ly/2XFoG6

Advies SLM Rijk over Office 365 ProPlus 3/3

Implementeer STARTTLS en DANE:

Wie : Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

Wat : Mailverkeer tussen mailservers verloopt via SMTP. STARTTLS in combinatie met DANE gaan, in aanvulling op SMTP, afluisteren of manipuleren van dit mailverkeer door internetcriminelen tegen.

Verplicht ?: Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) heeft een streefbeeldafspraak gemaakt, waarvan de voortgang ieder halfjaar wordt gemeten. Ook advies AP, NCSC en EC

Info: https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

Advies SLM Rijk over Windows 10 Enterprise

Gebruik Windows 10 vanaf versie 1903

(met telemetrie-setting ‘Security’ en Timeline Cloud sync uit)

- Dit geeft voldoende Windows 10 Enterprise functionaliteit met beperkte uitstroom van diagnostische gegevens.
- Windows Update for Business voor de PC werkt nu ook op Security niveau
- SLM heeft input gegeven voor een structurele oplossing voor Windows 10 Enterprise klanten. Daardoor komt er op afzienbare termijn een oplossing voor Windows 10 met telemetrieniveaus hoger dan de Security instelling.

Microsoft assouplit la règle de télémétrie pour les PC gérés avec Windows Update for Business

Gregg Keizer, Computerworld (adaptation Jean Elyan) , publié le 08 Aout 2019

0 Réaction

Les entreprises soucieuses de la vie privée ne seront plus obligées de définir le « niveau de données de diagnostic »

By Gregg Keizer

Senior Reporter, Computerworld | 07 AUGUST 2019 13:12 PT

SUIVRE TOUTE L'ACTUALITÉ

Advies SLM Rijk over Office Online en de apps

Voorlopig niet gebruiken, om twee redenen:

- Microsoft beschouwt zich als zelfstandige verantwoordelijke voor de mobiele Office apps, er gaat verkeer naar tenminste één derde partij (Braze) ondanks garantie dat ingelogd verkeer onder de OST valt
- Het is nog niet mogelijk om de Connected Experiences uit te zetten in Office Online en in de mobiele Office apps

Kamerbrief 1 juli 2019

"Gezien de behaalde resultaten zoals hierboven beschreven ziet SLM Microsoft Rijk, vanuit AVG-perspectief geen bezwaren voor bij SLM Microsoft aangesloten organisaties Microsoft Office ProPlus, Windows 10 Enterprise en Azure te gebruiken.

Het blijft altijd de eigen afweging van een organisatie als verwerkingsverantwoordelijke om te besluiten of en welk product of dienst geschikt is voor een specifieke toepassing. Hierbij dienen ook andere factoren zoals informatiebeveiligingsaspecten en specifieke wet- en regelgeving voor de organisatie gewogen te worden."

Bron: kamerbrief 1 juli 2019

Overige wet- en regelgeving

Elke organisatie moet voldoen aan relevante wet- en regelgeving, ook als de organisatie gebruik maakt van clouddiensten.

Voorbeelden hiervan zijn:

- Algemene Verordening Gegevensbescherming (AVG)
- Voorschrijft Informatiebeveiliging Rijksdienst -Bijzondere Informatie (VIR-BI)
- Archiefwet
- Wet veiligheidsonderzoeken
- Telecommunicatiewet
- Wet Openbaarheid Bestuur (WOB)
- Wet Elektronisch Bestuurlijk Verkeer
- Wet Politiegegevens

Eén voor allen, allen voor één

- Zelfde voorwaarden voor alle partijen in de publieke sector
- (en eigelijk ook voor de zakelijke markt)
- Streven naar een “geharmoniseerde set van inkoopvoorwaarden”

Essentiële lessen als je ‘de cloud in wilt’

Denk Groot, Begin Klein, Ga Snel!

- Heb de moed te veranderen
- Weet waar je heen gaat
- Vraag hulp aan partners en bondgenoten
- Koester de cultuur die je wilt
- Betwist aannames
- Moedig experimenteren aan

Strategisch Leveranciersmanager Microsoft Rijk

Paul van den Berg

E-mail: p.j.van.den.berg@minjenv.nl
Telefoon: 06 – 50 05 76 06