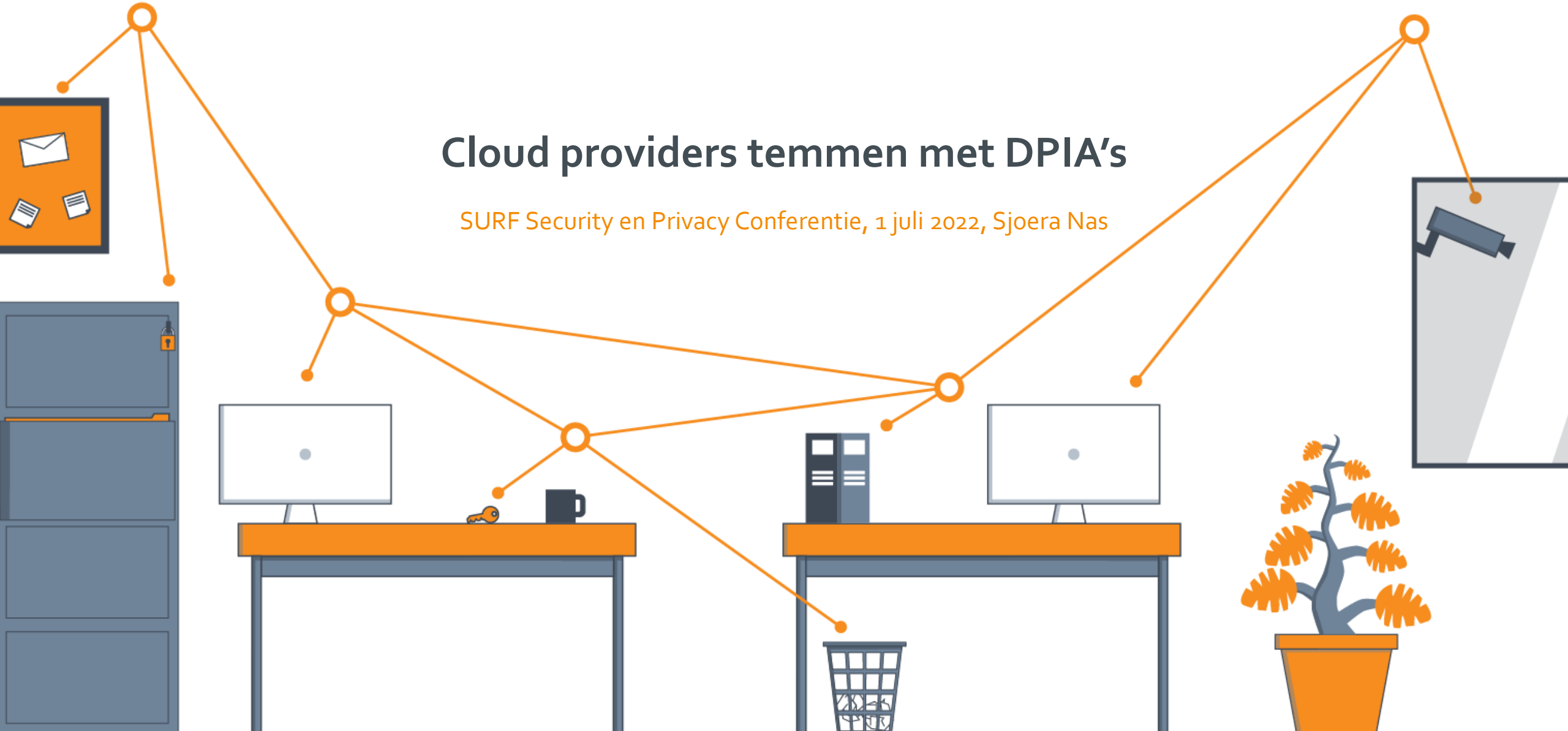
PRIVACY COMPANY

Cloud providers temmen met DPIA's

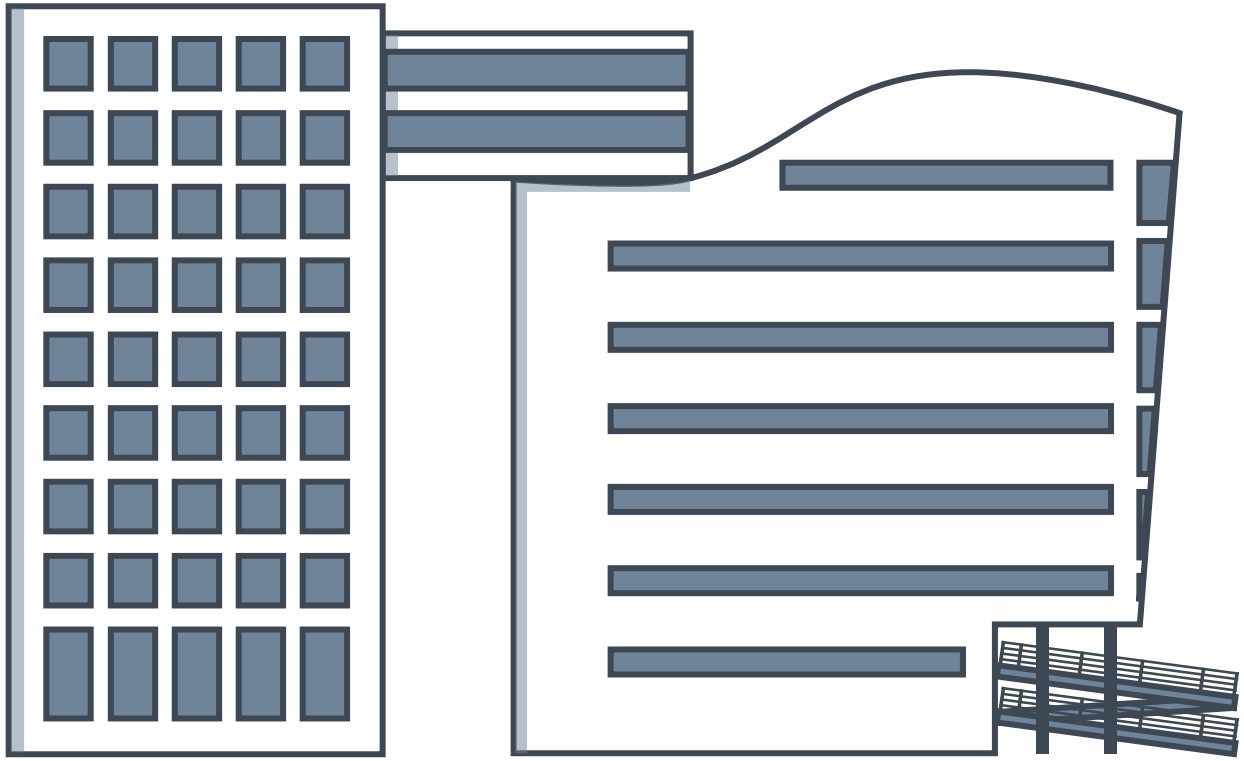
SURF Security en Privacy Conferentie, 1 juli 2022, Sjoera Nas



Agenda

- Hoe doe je een DPIA op clouddiensten?
- Doorgifte van persoonsgegevens naar de VS: hoe doe je een DTIA?
- Resultaten SURF en Rijk bij onderzochte cloud providers

Wat is Privacy Company?



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

DPIAs (inclusief werk in uitvoering)

Microsoft Intune

salesforce

SAP

Microsoft Office 2016

Windows 10 Enterprise

Azure

aws

Microsoft Edge

IBM Cloud

Google Workspace

BlackBerry

ORACLE CLOUD

zoom

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

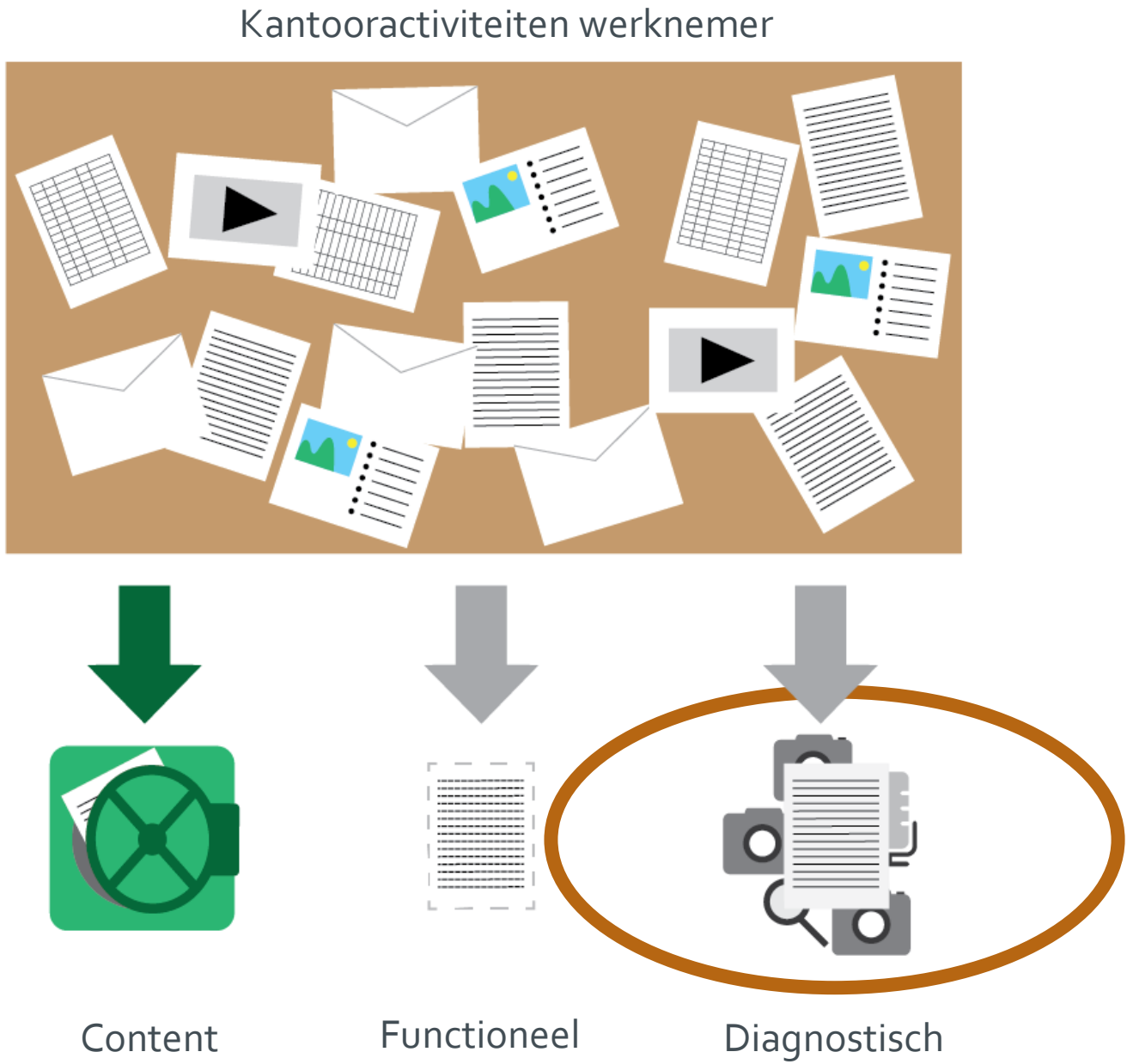
DPIA aanpak gebaseerd op het Rijks DPIA model

DPIA aanpak Privacy Company: juridisch en technisch

Analyse raamwerk contracten

vaak veel verschillende documenten

Techniek: verschillende soorten gegevens

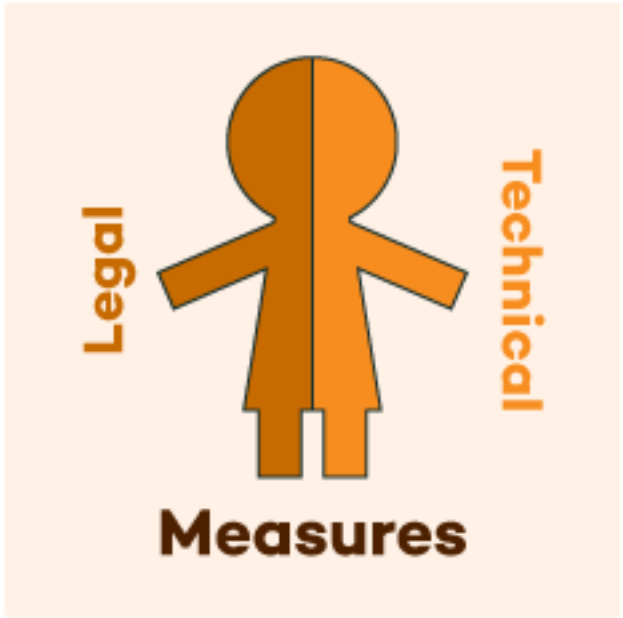


Twee soorten diagnostische gegevens: telemetrie en server logs

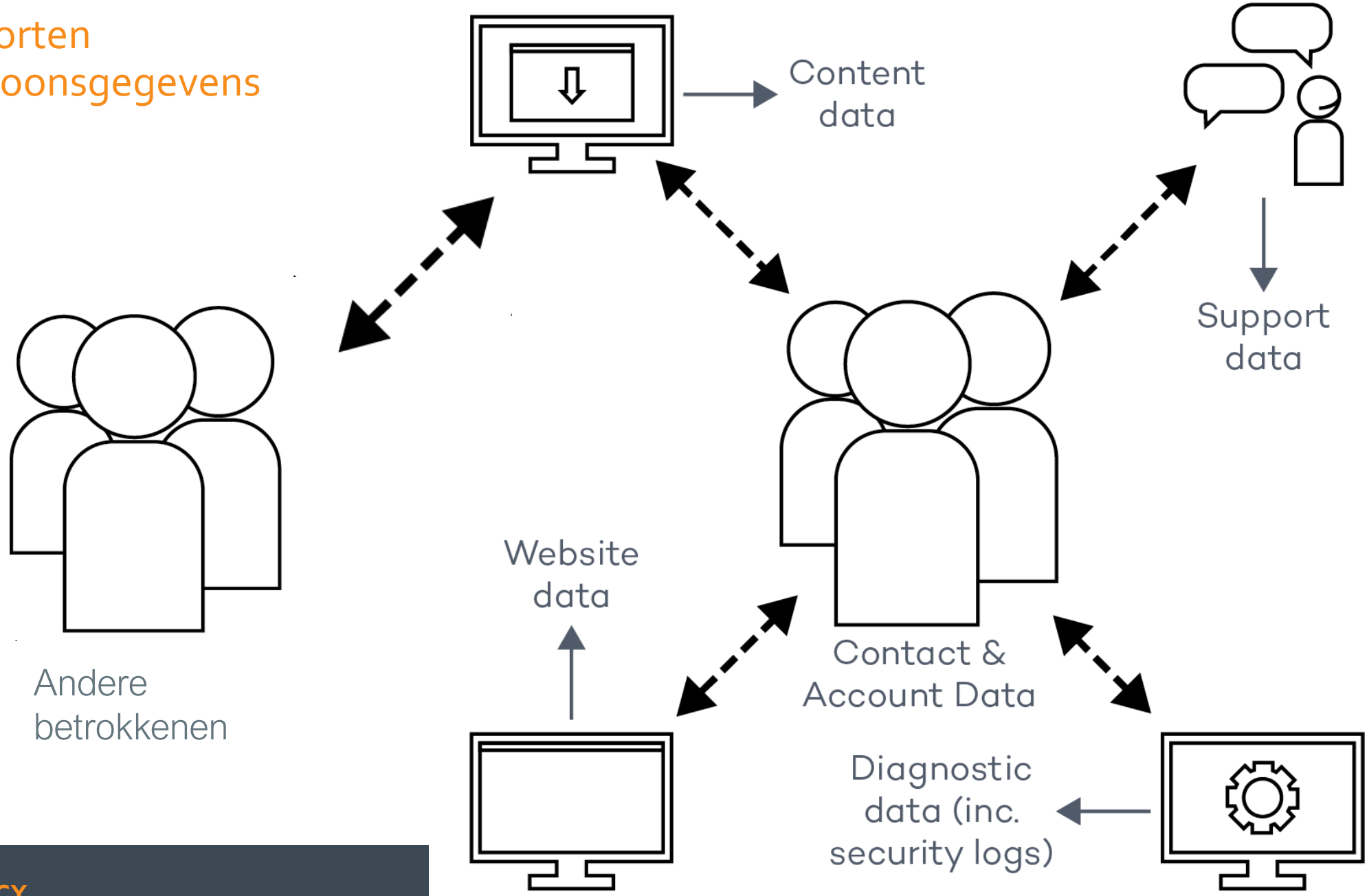
- Geïnstalleerde software applicaties en browsers verzamelen en verzenden gegevens over het individuele gebruik van de diensten: telemetrie
- Dat verkeer is anders dan strikt functioneel verkeer: geen vraag en antwoord, behalve ontvangstbevestiging!
- Daarnaast registreren de cloudproviders alle handelingen in eigen logbestanden: service generated server logs

Onderzoeksmethoden bij cloudproviders

DPIA in 4 delen



5 soorten persoonsgegevens



Hoofdvragen DPIA

Vraag	Analysemethode
Welke persoonsgegevens verwerkt de leverancier en is dat voldoende transparant?	Onderscheppen netwerkverkeer, inzageverzoek, gebruik andere hulpmiddelen leverancier, analyse beschikbare openbare documentatie (website)
Treedt de leverancier op als verwerker of (ook) als (gezamenlijke) verantwoordelijke?	Analyse van alle contractdocumenten, inclusief consumenten privacy- en cookieverklaring
Voor welke doelen worden de gegevens verwerkt?	Analyse juridische stukken, dialoog met leverancier
Doet de leverancier aan data protection by default / kan de instelling de verwerking beperken?	Analyse interface beheerders en eindgebruikers
Hoe lang worden de gegevens bewaard?	Dialoog met leverancier
Is er sprake van doorgifte, naar welke landen en welke waarborgen biedt de leverancier?	Analyse contractdocumenten, dialoog met leverancier
Houdt de leverancier zich aan ander toepasselijk recht, zoals BIO of ePrivacy cookieregels?	Analyse contractdocumenten, vergelijk met aangetroffen verkeer
Zijn er nog organisatiepecifieke risico's?	Interviews met admins en eindgebruikers,controle op aanwezigheid analytics over werkgedrag medewerkers

Terugkerende hoge risico's (voor de DPIA's en onderhandelingen!)

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

Terugkerend probleem: de cloud provider als verantwoordelijke

Gezamenlijke verantwoordelijkheid provider en Enterprise/EDU klant

- Cloud providers treden op papier vaak op als verwerker, maar dat geldt alleen voor de inhoudelijke gegevens die je er als klant instopt.
- Zelfs als de verwerkersovereenkomst over 'alle persoonsgegevens' gaat, kunnen er doelen instaan die de provider feitelijk zelf bepaalt, zoals gebruik voor 'improvement of services' of 'research' of 'business intelligence'.
- De meeste providers vergeten de diagnostische en website data te beschrijven
- Daardoor kun je feitelijk gezamenlijk verantwoordelijk zijn, zonder geldige overeenkomst. Meestal geen grondslag voor de verwerkingen in het (commerciële) belang van de provider
- Interessante uitleg Griekse DPA over Cisco als gezamenlijk verantwoordelijke met scholen voor WebEx voor online lessen: https://www.dpa.gr/sites/default/files/2021-11/50_2021anonym.pdf

Resultaten onderhandelingen met cloudproviders

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

Februari 2019: Microsoft kondigt wereldwijde verbeteringen in Office aan

> Retouradres Postbus 20301 2500 EH Den Haag

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

Datum 20 december 2018

Onderwerp Reactie op berichtgeving in de media ov
door Microsoft.

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

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

De minister van Binnenlandse Zaken en Koninkrijksrelaties bevordert vanuit de

Microsoft CEO Satya Nadella | Stephen Brashear/Getty Images

Microsoft to update Office Pro Plus after Dutch ministry questions privacy

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

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

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

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

January 8, 2020

Updated Microsoft Online Servic available to our customers arour

By The Microsoft 365 Marketing Team

Share

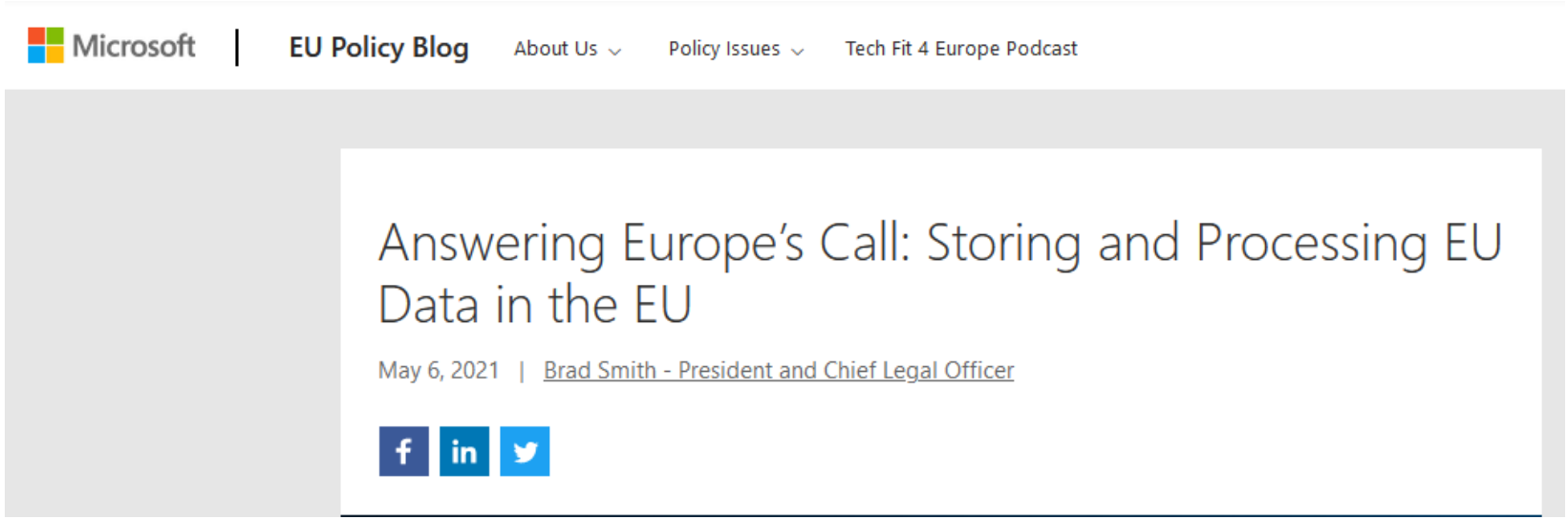
Today, we published the updated Microsoft Online Services Terms with the changes

As Julie Brill, Microsoft's Corporate Vice President for Privacy and Regulatory Affairs, 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.

Afspraken over beperkte verwerkingen eigen doelen

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

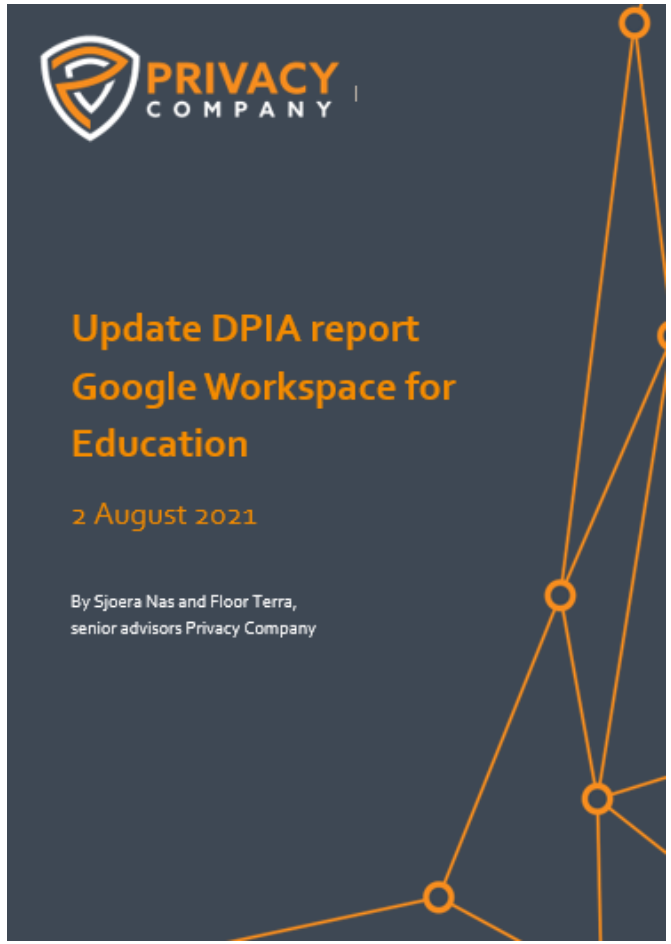
Mei 2021: Microsoft belooft alle gegevens eind 2022 in de EU te verwerken



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

Google verbeteringen onderhandeld door SURF

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



33 doelen Google's algemene privacyverklaring

1. **Providing our service**
2. **Help users share content** by suggesting recipients from their contacts.
3. **Maintaining the service by tracking outages**
4. **Troubleshooting user reported issues**
5. **Make improvements to the services**, for example *understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.* This 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 help advertisers understand the performance of their ad campaigns.*
17. **Communicate with you to interact with you directly**. *For example, we may send you a notification if we detect suspicious activity*,
18. **Inform you** *about upcoming changes or improvements to our services*.
19. **Marketing** *to inform users about our services*
20. **Provide support if you contact Google**, *to help solve any issues you might be facing.*
21. **Improve the safety of our services**. *This includes detecting, preventing, and responding to fraud, security risks, and technical issues that could harm Google, our users, or the public.*
22. **Detect abuse** such as spam, malware, and illegal content by analyzing your content
23. **Protecting against harm to the rights, property or safety of Google, our users, or the public** *as required or permitted by law, including [also slightly differently defined as: "Fulfilling obligations to our partners like developers and rights holders AND Enforcing legal claims, including investigation of potential violations of applicable Terms of Service]*
24. **Disclosing information to government authorities** *Also slightly differently defined as: "To respond to legal process or an enforceable governmental request."*
25. **Improve the reliability of our services**. *We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services.*
26. **Use algorithms to recognize patterns in data**. *For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.*
27. **Combining information among all services and across devices to improve Google's services and the ads delivered by Google,** *For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.*
28. **Help other users identify you**, *If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo.*
29. **Use cookies for many purposes**. *We use them, for example, to remember your safe search preferences, to make the ads you see more relevant to you, to count how many visitors we receive to a page, to help you sign up for our services, to protect your data, or to remember your ad settings.*
30. **To allow specific partners to collect information from your browser or device** *for advertising and measurement purposes using their own cookies or similar technologies*
31. **Performing research**, *Performing research that improves our services for our users and benefits the public*
32. **When necessary for legitimate business or legal purposes** *such as security, fraud and abuse prevention, or financial record-keeping.*
33. **Other purposes not covered in this Privacy Policy,** *we'll ask for your consent, for example, 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.
    - if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant.
    - Process your payment information when you buy extra storage for Google Drive.

Resultaten DPIA's in het nieuws

ITPro

{* 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 U

14

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

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

Now, after what Privacy Company, a data consultancy employed by Dutch

Microsoft en Zoom verbeteringen

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

Microsoft en Zoom verbeteringen

Effectieve audit rechten. Het Rijk heeft de bevindingen van de eerste jaarlijkse audit bij Microsoft al gepubliceerd: de tweede wordt nu uitgevoerd.
Anonimiseren volgens richtlijnen WP29/EDPB
Publieke documentatie van telemetrie en service generated server logs
Dataminimalisatieknoppen bij Microsoft voor het telemetrieniveau en het gebruik van 'Controller Connected Experiences'
Microsoft heeft een Data Viewer Tool gebouwd voor inzage in de telemetrie: Zoom werkt hieraan

Resultaten andere DPIA's op Microsoft, Google and Zoom

SIGN IN

The Register

SIG

{* SAA

Du

Zoom

NEWS | IT | NE

JURIDISCHE ZAKEN

'Risico dat VS Europese data van Microsoft

22 February 2022

Netherlands: Dutch Government publishes a DPIA on Microsoft

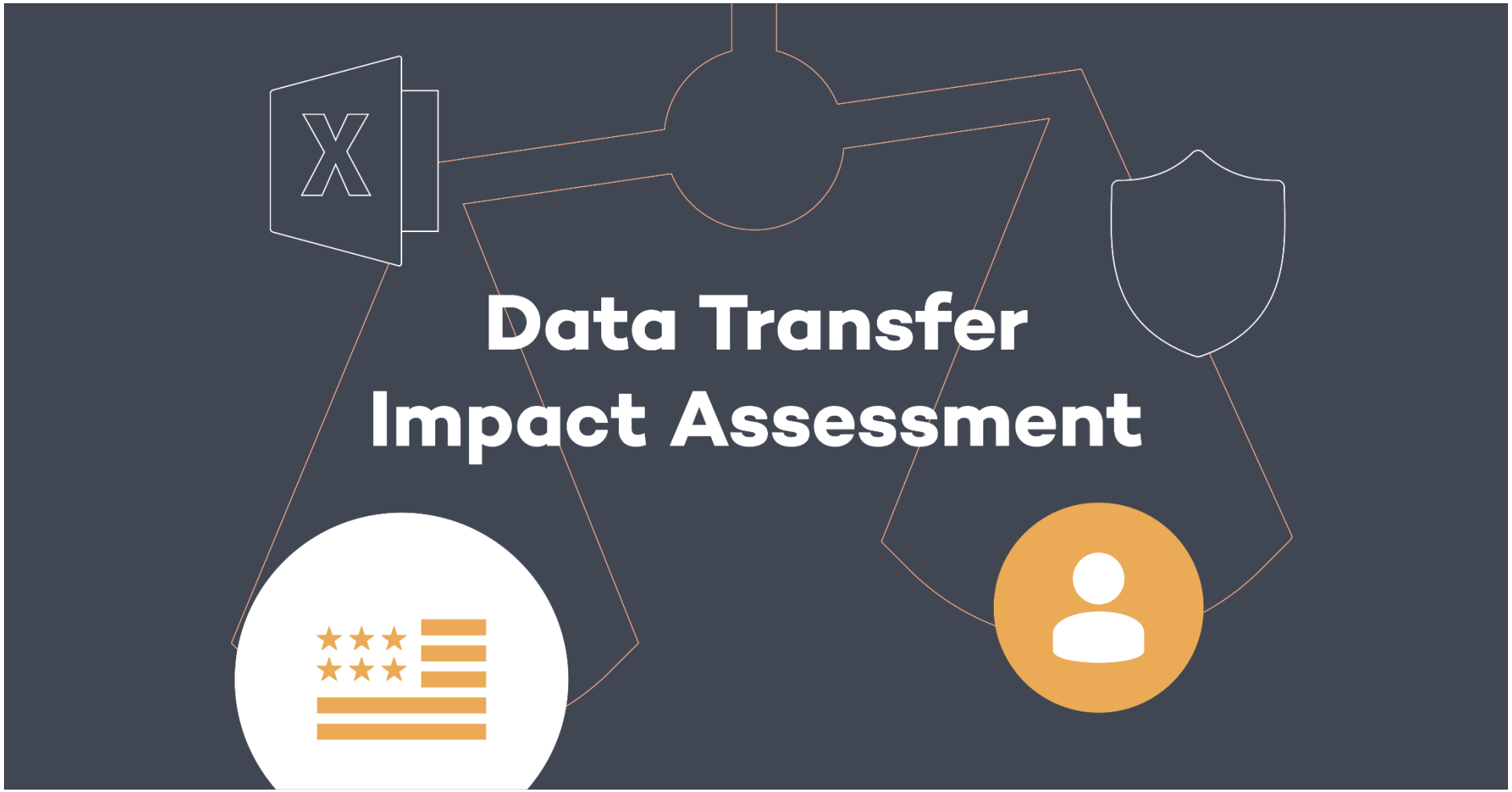
Privacy Impact Assessments | Sensitive Personal Data | Encryption | Third Countries

The Dutch Government published, on 16 February 2022, a Data Protection Impact Assessment ('DPIA'), which assessed the data protection risks of the professional use of Microsoft Teams in combination with OneDrive, SharePoint Online, and the Azure Active Directory. In particular, the DPIA was conducted by the Ministry of Justice, the Strategisch Leveranciersmanagement Microsoft Rijk ('SLM Rijk') who are the central negotiator for Microsoft, Google, and Amazon Web Service products and services for Dutch central government organisations, and by SURF B.V.

protection impact assessment). Toch lijkt de kans dat de Amerikaanse overheid via Microsoft data in handen krijgt zeer klein. Experts denken dat het kritische privacy-oordeel alsnog flinke impact kan hebben.

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

Data Transfer Impact Assessment



Legal remedies to US surveillance after 'Schrems II'

Sep 3, 2020 Save This

Nieuws

Oostenrijkse toezichthouder: gebruik Google Analytics in strijd met AVG

donderdag 13 januari 2022, 12:19 door **Redactie**, 19 **reacties**

Het gebruik van Google Analytics is in strijd met de AVG, zo heeft de Oostenrijkse privacytoezichthouder DSB geoordeeld. De uitspraak kan gevolgen voor zeer veel websites in de Europese Unie hebben.

Wordt 2022 het jaar waarin Amerikaanse cloud tools de EU-regels moeten respecteren of de EU moeten verlaten?

French GDPR ruling addresses US surveillance powers

OUT-LAW NEWS | 31 Mar 2021 | 10:14 am | 4 min. read

German State's Data Processing Authority Offers Strict Guidance On Post-Schrems II Data Transfers

Nieuws - 14 januari 2022 - 10:22

Gebruik Google Analytics binnenkort mogelijk verboden

De Autoriteit Persoonsgegevens waarschuwt dat het gebruik van Google Analytics binnenkort mogelijk niet meer is toegestaan. De collega's in Oostenrijk verboden het al en Nederland wil binnen enkele weken zelf zijn conclusies trekken.

PRIVACY COMPANY

Waarom een DTIA?

- VS databeschermingsniveau niet adequaat volgens EHvJn (de Schrems-II uitspraak)
- Van de EDPB mag doorgifte alleen als de problematische wetgeving in de praktijk niet van toepassing is: je moet dus een risico-afweging doen
- *"You may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer".* (para 43)
- Als 'exporteur' moet je verschillende bronnen raadplegen. Deze bronnen moeten "*relevant, objectief, betrouwbaar en verifieerbaar zijn en voor het publiek beschikbaar of anderszins toegankelijk*". Je mag niet vertrouwen op "*gedocumenteerde praktijkervaring van de importeur met relevante eerdere gevallen van verzoeken*" alleen.

Juridische ontwikkelingen VS

- De meeste grote cloudproviders publiceren transparency statistics: het aantal bevragingen over zakelijke (Enterprise/Education) klanten is heel erg laag.
- Maar: het aantal *gagging orders* neemt schrikbarend toe. De New York Times schrijft: "*the number of these requests has soared in recent years to* ***thousands a week****, putting Apple and other tech giants like Google and Microsoft in an uncomfortable position between law enforcement, the courts and the customers whose privacy they have promised to protect*."
- In een opinie-artikel in de Washington Post waarschuwt Brad Smith van Microsoft: *prosecutors too often are exploiting technology to abuse our fundamental freedoms*.

https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/

Toepasselijke Amerikaanse opsporings en surveillance wetgeving

- EOP 12.333 (aangepast door PPD-28, gericht op backbone providers zoals AT&T)
- FISA 702, van toepassing op *electronic communication service providers*
- National Security Letter, gebaseerd op de Electronic Communications Privacy Act
- FISA warrant type a bestaande accountgegevens en metadata
- FISA warrant type b toekomstige inhoud en metadata (tap)
- FISA business records order
- FISA pen register act (zoals uitgebreid door de US Patriot ACT naar internet communicatie)
- US Cloud Act
- US Stored Communications Act
- Andere onderdelen US Patriot Act/nog onbekende bevoegdheden??

Zie de uitgebreide tabel in de recente Teams en Zoom DPIA's van SLM Rijk en SURF

Pen Register Act uit 1986

ATTACHMENT A

WhatsApp LLC

Type of facility	Number or identifier	Subscriber/customer name, if known	Identity of subject of criminal investigation, if known
WhatsApp account	[redacted]	Unknown	Unknown
WhatsApp account		Unknown	Unknown
WhatsApp account		Unknown	Unknown
WhatsApp account		Unknown	Unknown
WhatsApp account		Unknown	Unknown
WhatsApp account		Unknown	Unknown
WhatsApp account		Unknown	Unknown

Forbes

EDITORS' PICK | Jan 17, 2022, 11:55am EST | 20.117 views

WhatsApp Ordered To Help U.S. Agents Spy On Chinese Phones—No Explanation Required

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

The U.S. doesn't need to know whom they're targeting or show probable cause when ordering Facebook, WhatsApp or any tech company to help agencies spy on users in secret, newly unsealed court documents show.

https://www.forbes.com/sites/thomasbrewster/2022/01/17/whatsapp-ordered-to-spy-on-chinese-phones-by-america-no-explanation-given/

Komt er een nieuw dataverdrag tussen de EU en de VS?

POLITICOPRO

CYBERSECURITY & 9 OTHERS

Political pressure wins out as U.S. secures preliminary EU data deal

Ursula von der Leyen and Joe Biden stepped in to push through a political deal for data transfers that will likely be tested in court.

BY: VINCENT MANANCOURT, MARK SCOTT | 03/25/2022 09:33 AM EDT

BRIEFING ROOM

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework

MARCH 25, 2022 • STATEMENTS AND RELEASES

The United States and the European Commission have committed to a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union when it struck down in 2020 the Commission's adequacy decision underlying the EU-U.S. Privacy Shield framework.

This Framework will reestablish an important legal mechanism for transfers of EU personal data to the United States. The United States has committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities. This deal in principle reflects the strength of the enduring U.S.-EU relationship, as we continue to deepen our partnership based on our shared democratic values.

Maar houdt Privacy Shield 2.0 lang stand?

Opinion Events Jobs HILL.TV Changing America

TRENDING: UKRAINE RUSSIA SUPREME COURT JOE BIDEN COVID-19 SPONSORED: MISUNDERSTOOD: THE HUAWEI STORY

THE HILL

The Supreme Court just made a US-EU Privacy Shield agreement even harder

BY PATRICK TOOMEY AND ASHLEY GORSKI, OPINION CONTRIBUTORS — 03/21/22 07:00 AM EDT
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

https://thehill.com/opinion/judiciary/598899-the-supreme-court-just-made-a-us-eu-privacy-shield-agreement-even-harder

Max Schrems bereidt zich voor op Schrems-III

noyb

News Projects Resources Support us! About us EN

HOME > NEWS > "PRIVACY SHIELD 2.0"? - FIRST REACTION BY MAX SCHREMS

"Privacy Shield 2.0"? - First Reaction by Max Schrems

Mar 25, 2022

- A decision can quickly be challenged with the European Court of Justice. *noyb* expects to be able to get any new agreement that does not meet the requirements of EU law back to the CJEU within a matter of months e.g. via civil litigation and preliminary injunctions. The CJEU may even take preliminary action, if a deal is clearly violating previous judgements.

noyb funding goal

68 %

INVEST IN PRIVACY!

Follow us!

Media Coverage

https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

Uitspraken toezichthouders en jurisprudentie over doorgifte na Schrems-II

- Vlaamse toezichthouder verbiedt gebruik AWS voor onderwijsdatabank (september 2020)
- Vlaamse Raad van State keurt gebruik AWS alsnog goed (augustus 2021)
- Franse DPA CNIL verbiedt gebruik Microsoft Azure voor gezondheidsgegevens en AWS voor vaccinatie-afspraken (2020)
- Franse Raad van State keurt beiden alsnog goed, onder voorwaarden (oktober 2020 en maart 2021)
- Beierse DPA verbiedt gebruik van Mailchimp (maart 2021)
- Portugese DPA legt boete op aan Portugees CBS voor gebruik Cloudflare (april 2021)
- Portugese èn Italiaanse DPA treden op tegen 'Respondus' proctoring software (mei en september 2021)
- Griekse DPA berispt en sommeert onderwijsministerie voor gebruik Cisco Webex (november 2021)
- Wiesbaden DPA verbiedt gebruik Akamai als subverwerker van Deense cookie consent provider (december 2021)
- Oostenrijkse DPA verbiedt gebruik Google Analytics op gezondheidswebsite (december 2021)
- EDPS verbiedt gebruik Google Analytics op website Europees Parlement (januari 2022)
- AP waarschuwt dat gebruik Google Analytics mogelijk wordt verboden (januari 2022)
- Franse CNIL en Italiaanse Garante verbieden meermaals het gebruik van Google Analytics (februari, maart en juni 2022)

Eind 2022 uitkomsten EDPB en EDPS onderzoek cloudgebruik in de publieke sector

EDPB launches first coordinated action

18 October 2021 **EDPB**

Following the EDPB's decision to set up a **Coordinated Enforcement Framework** in October 2020, the EDPB has now decided to launch the proposal for its first coordinated action on the use of Cloud based services by the public sector. In a coordinated action, the EDPB prioritizes a certain topic for supervisory authorities to work on at the national level. The results of these national actions are then bundled and analysed, generating deeper insight into the topic and allowing for targeted follow-up on both the national and the EU level.

The EDPS opens two investigations following the "Schrems II" Judgement

27 May 2021

The EDPS opens two investigations following the "Schrems II" Judgement

Press Release

The EDPS launched two investigations today, one regarding the **use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by European Union institutions, bodies and agencies (EUIs)** and one regarding the **use of Microsoft Office 365 by the European Commission**.

https://edpb.europa.eu/news/news/2021/edpb-launches-first-coordinated-action_en

Twee DTIA's gepubliceerd

Teams, SharePoint, OneDrive en de Azure AD (Rijk en SURF)

https://slmmicrosoftrijk.nl/?smd_process_download=1&download_id=5286

Zoom (SURF en Rijk)

https://www.surf.nl/files/2022-03/dtia-zoom-8-feb-2022_0.ods

DTIA in 7 stappen: gebaseerd op model Rosenthal

1. *Describe the intended transfer* (wat voor soort persoonsgegevens, zijn er subverwerkers? Aparte DTIA's!)
2. *Define the DTIA parameters* (welke wetgeving is er in het derde land van toepassing)
3. *Probability that the foreign authority has a legal claim* (is die wetgeving van toepassing op de provider?)

4a. *Probability that the claim is successful* (kans dat de gegevens in leesbare vorm worden opgevraagd, berekend over meerdere jaren)

4b. *Probability of access through mass surveillance* (kans dat de gegevens worden onderschept op de kabels)

5. *Overall assessment* (optelsom risico percentages)
6. *Data subject risks* (kans x impact, afh. van de aard van de gegevens)
7. *Safeguards* (incidentele of structurele doorgifte, zijn er SCC's)

Voorbeeld 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 licence

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:	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]
f)	Categories of data subjects concerned:	
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 otherwise) to give up its request for the data in plain text	100%	0,00		*The probability is zero if the customers follow the recommendation to apply end 2 end encryption (If answer to C26= Yes; the likelihood is higher)*
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%			*If e2ee is applied*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	0%	0,00%		*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%	*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%	0,00%		*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

Voorbeeld 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%		*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%	0,00%		*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*	*(= anonymised 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.*

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

Low

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:		Place, Date:	
'SURF / PRIVACY COMPANY'		**Signed:**	
Note: Under the EU SCC's, the TIA is to be adopted by both the data exporter and importer.		By:	

PRIVACY COMPANY

Uitkomsten risico-afweging

- Microsoft en Zoom hebben de facto nog nooit persoonsgegevens van Europese publieke sector klanten aan Amerikaanse opsporingsdiensten verstrekt. Dat is *inclusief* gagging orders.
- Microsoft en Zoom verwerken vanaf eind dit jaar *alle* persoonsgegevens in de EU. Dan kunnen ze nog steeds vorderingen krijgen onder FISA 702 en de US Cloud Act, maar daartegen zullen ze zich met alle juridische middelen verzetten. Tussen bevel en uitvoering zitten meerdere maanden: de provider moet de klant dan informeren op grond van de SCC dat hij niet meer in staat is zich aan de afspraken uit de SCC te houden.
- Als je zeer gevoelige of bijzondere persoonsgegevens verwerkt in een clouddienst, moet je die gegevens versleutelen met een eigen sleutel (end-to-end encryptie), ook al is het risico op toegang theoretisch. Je kunt dan *niet* volstaan met encryptie die door de provider wordt aangeboden.

Conclusies 1/2

- Wantrouw uitspraken van een provider dat er geen persoonsgegevens worden verwerkt
- Je moet technisch onderzoek doen om te begrijpen welke persoonsgegevens er worden verwerkt
- Voer handelingen uit in een testomgeving, onderschep het uitgaande netwerkverkeer en dien een formeel inzageverzoek in.
- Controleer welke gegevens de provider verzamelt via de website (bv inloggen op een browsertool, inloggen als beheerder, indienen support ticket)
- Documenteer alle gegevens die je direct en indirect aan je leverancier verstrekt in je verwerkingsregister: vergeet de externe betrokkenen niet waarmee je communiceert!

Conclusies 2/2

- Doe dit niet alleen: laat de onderhandelingen over aan SURF en probeer nog meer schaalgrootte te bereiken op Europees niveau
- Het is heel effectief om de DPIA te delen met de provider: om samen mitigerende maatregelen te bespreken en afspraken vast te leggen in een strak tijdschema
- De provider moet de DTIA invullen, daarna kun je die zelf aanvullen en samen ondertekenen.
- Bij Amerikaanse providers werkt het heel goed om een Engelstalige DPIA en DTIA te schrijven, en aan te kondigen dat je die gaat publiceren
- De toezichthouders beginnen nu te handhaven op het ontbreken van een DPIA en DTIA: hoog risico op reputatieverlies.

Wees ook een trimtab!

Buckminster R. Fuller

“Something hit me very hard once, thinking about what one little man could do. Think of the Queen Mary — the whole ship goes by and then comes the rudder. And there's a tiny thing at the edge of the rudder called a trimtab.
It's a miniature rudder. Just moving the little trim tab builds a low pressure that pulls the rudder around. Takes almost no effort at all. So I said that the little individual can be a trimtab. Society thinks it's going right by you, that it's left you altogether. But if you're doing dynamic things mentally, the fact is that you can just put your foot out like that and the whole big ship of state is going to go.
› I said, call me Trimtab.”

PRIVACY COMPANY

Vragen?

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

Maanweg 174
Den Haag