Microsoft

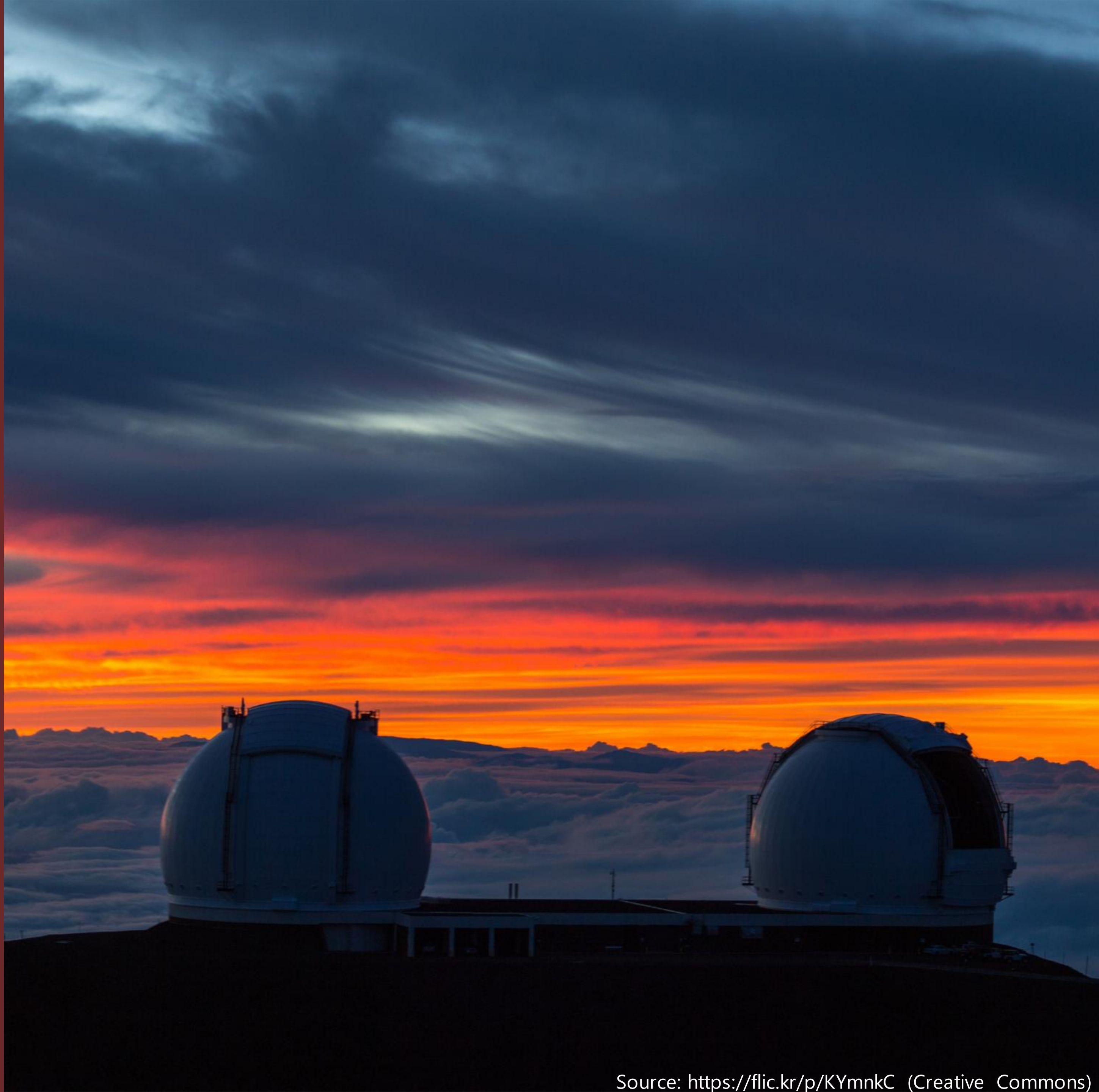
Above the clouds

protecting Microsoft and your data

Jelle Niemantsverdriet
National Security Officer

@jelle_n

linkedin.com/in/jelleniemantsverdriet/



Source: https://flic.kr/p/KYmnkC (Creative Commons)

Confidence.

Or Trust?

Source: https://flic.kr/p/6zoMtn (Creative Commons)

One cloud is not like the other

Whose responsibility is is anyway?

Source: https://flic.kr/p/5hdXSR (Creative Commons)

Are we talking about security *of* the cloud…

Source: https://www.publicdomainpictures.net/en/view-image.php?image=338689 (Creative Commons)

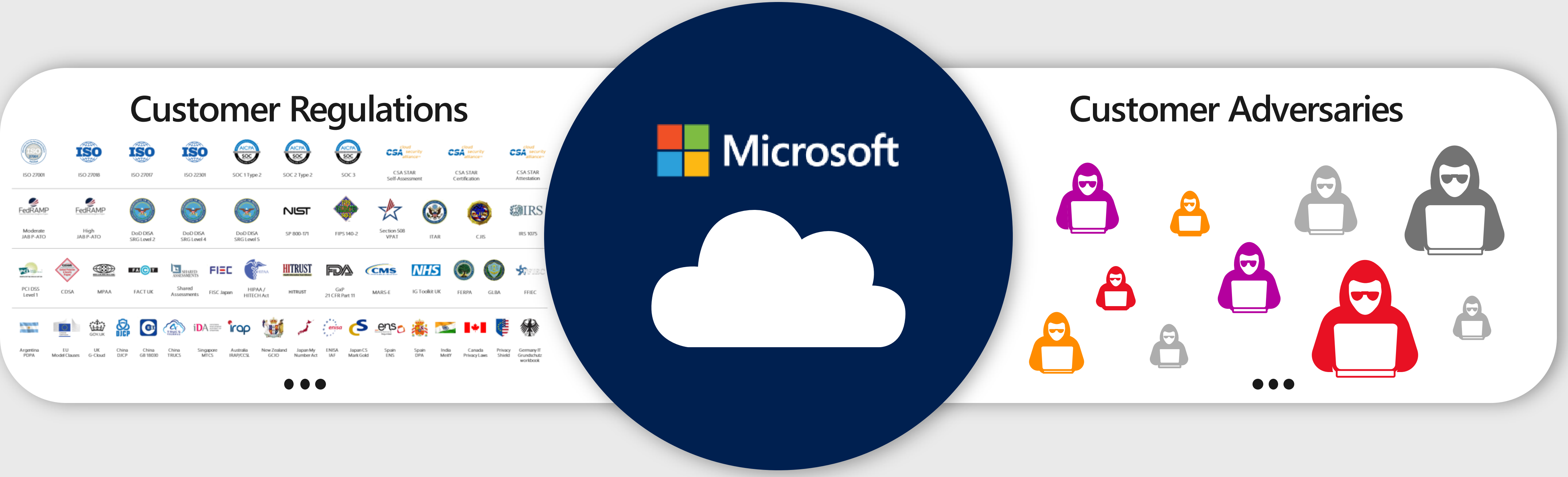
…or security *in* the cloud?

Source: https://www.publicdomainpictures.net/en/view-image.php?image=338689 (Creative Commons)

Scale matters and scale helps

Source: https://flic.kr/p/xAZ7ac (Creative Commons)

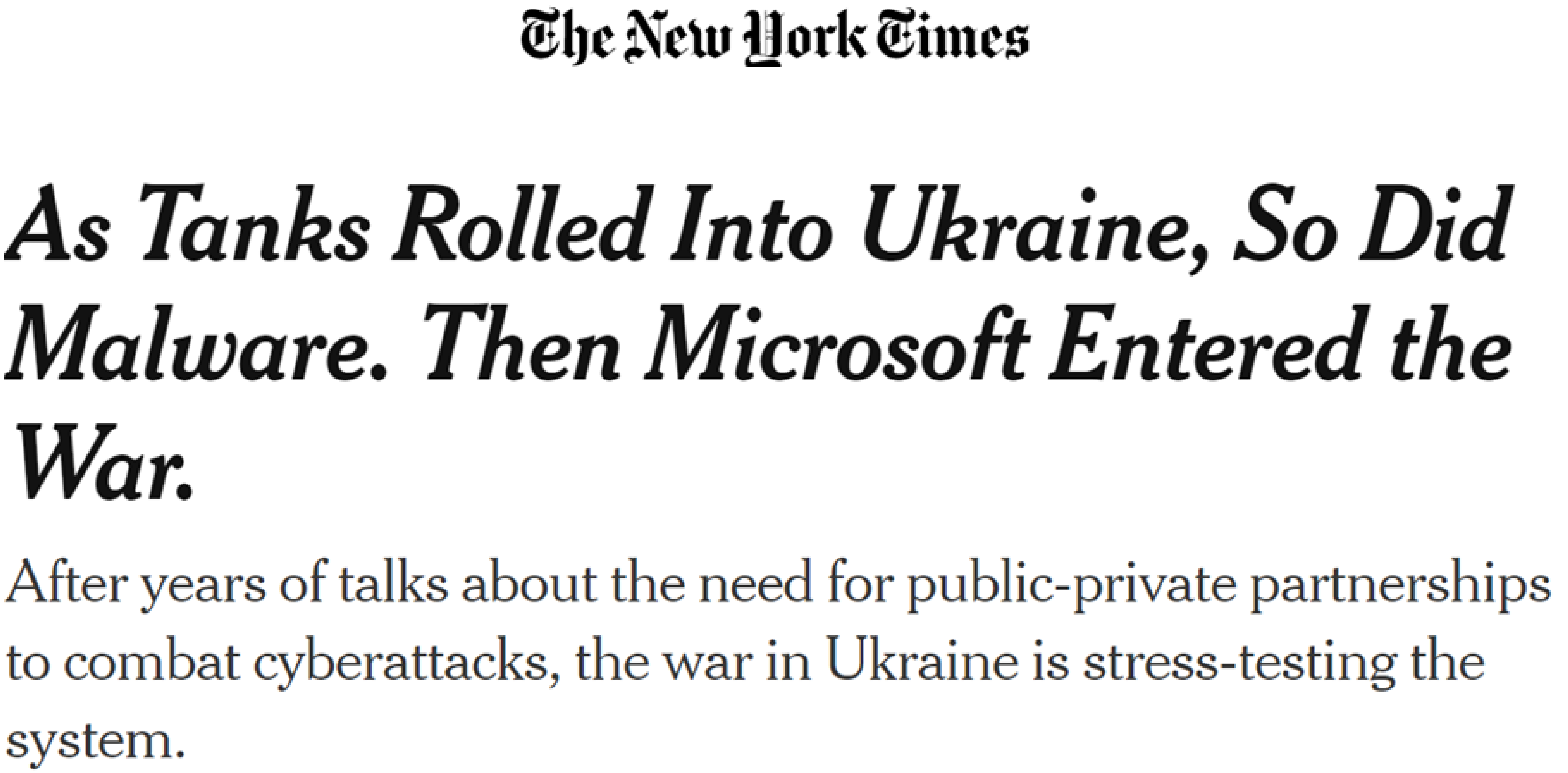
A Cloud Provider inherits…



Customer Regulations

Microsoft

Customer Adversaries



The New York Times

As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War.

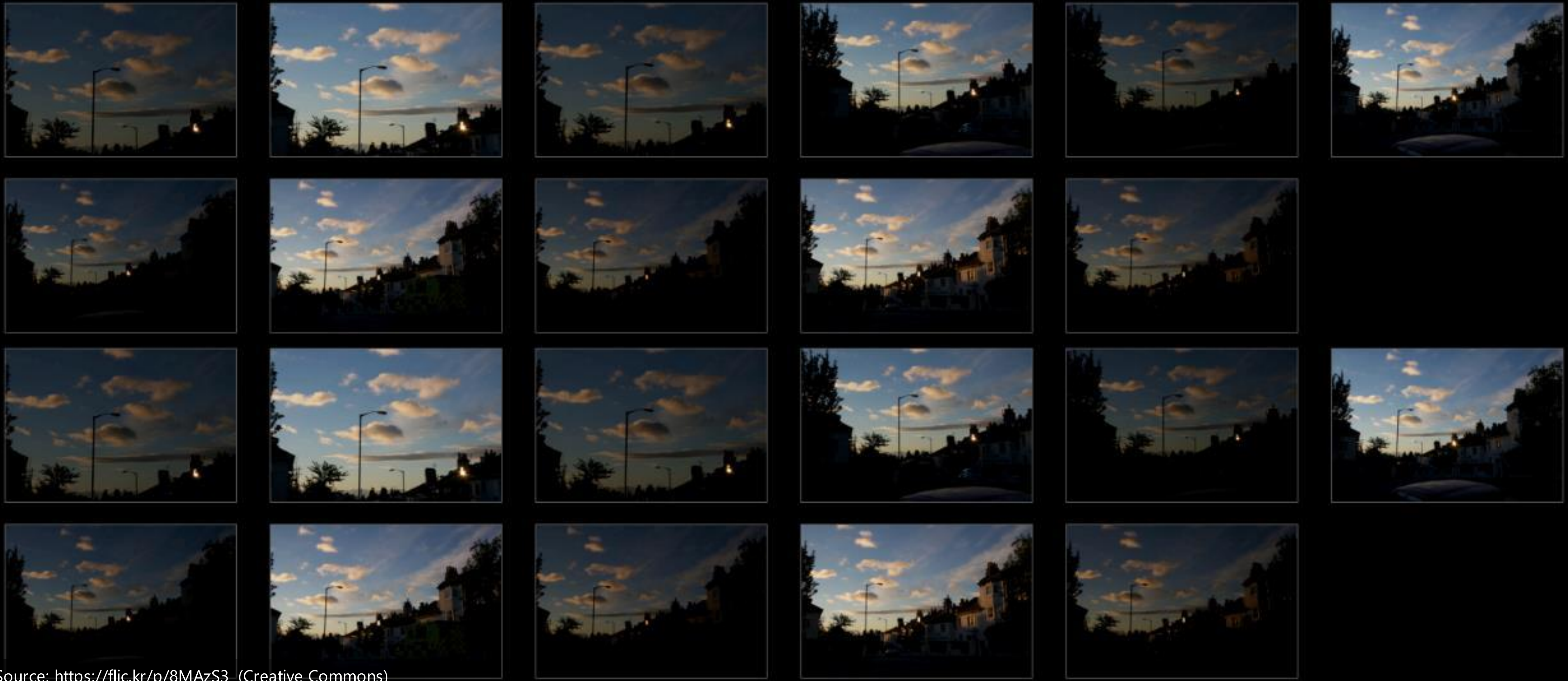
After years of talks about the need for public-private partnerships to combat cyberattacks, the war in Ukraine is stress-testing the system.

Source: New York Times, 28 February 2022 (https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html)

Sustain a government

Source: personal archive

Duplicate – yet unique

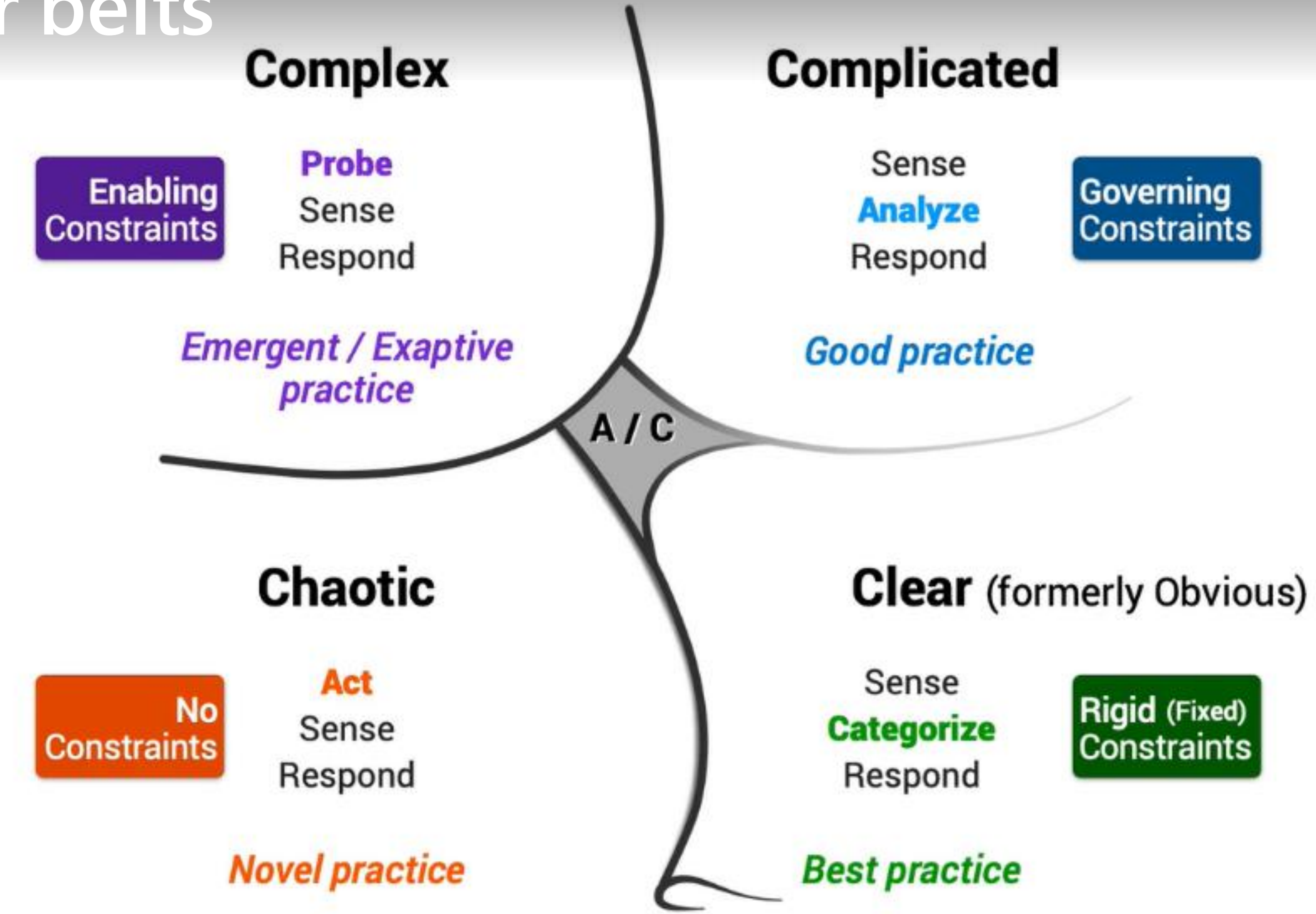


Source: https://flic.kr/p/8MAzS3 (Creative Commons)

The contract will take care of everything

Source: https://flic.kr/p/kFToD (Creative Commons)

Our environments are complex systems – not conveyor belts



Complex

Enabling Constraints

Probe
Sense
Respond

Emergent / Exaptive practice

Complicated

Sense
Analyze
Respond

Governing Constraints

Good practice

A / C

Chaotic

No Constraints

Act
Sense
Respond

Novel practice

Clear (formerly Obvious)

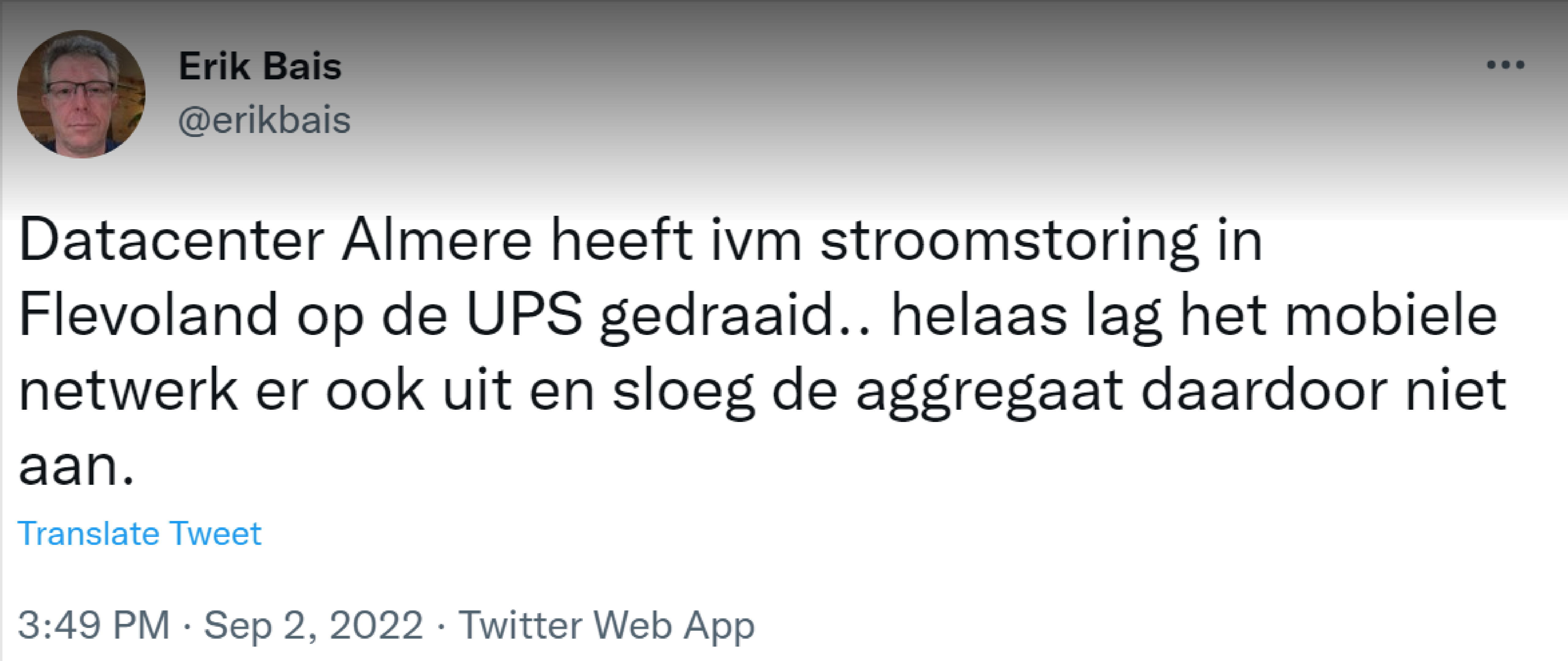
Sense
Categorize
Respond

Rigid (Fixed) Constraints

Best practice

Source: https://www.cognitive-edge.com/the-cynefin-framework/

The system is more than the sum of its components



Erik Bais

@erikbais

Datacenter Almere heeft ivm stroomstoring in Flevoland op de UPS gedraaid.. helaas lag het mobiele netwerk er ook uit en sloeg de aggregaat daardoor niet aan.

Translate Tweet

3:49 PM · Sep 2, 2022 · Twitter Web App

Source: https://twitter.com/erikbais/status/1565698446585171968

Resilience matters: be able to respond and recover

Source: https://flic.kr/p/oREwdW - Creative Commons

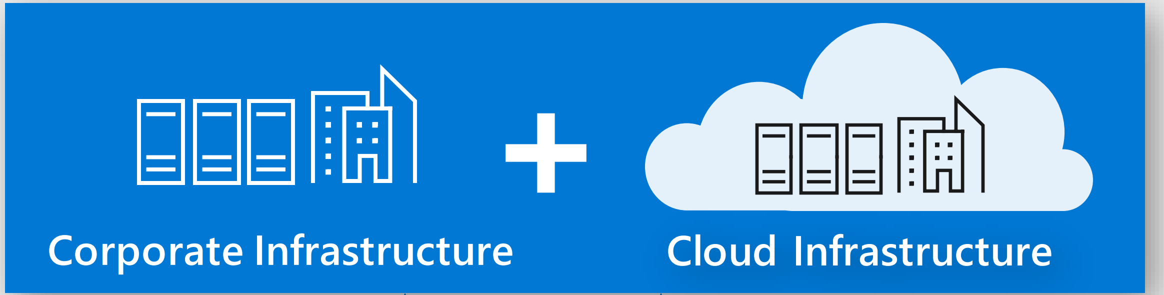
Microsoft protecting Microsoft

Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more…

Traditional Defenses

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties

Attackers View



People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more…

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more…

Security Development Lifecycle

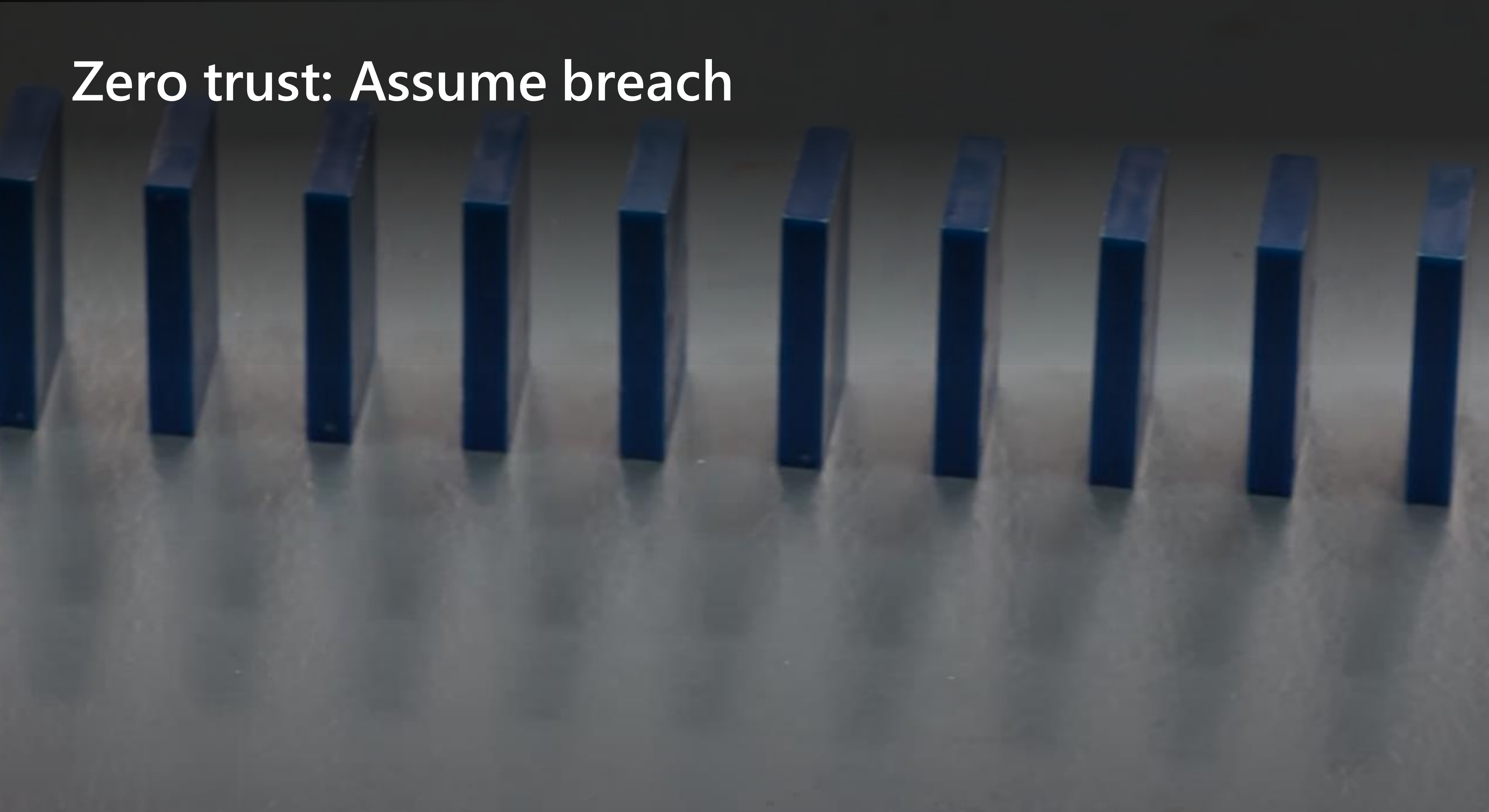
CDOC

Monitoring & Vigilance

Traditional: guard the castle walls

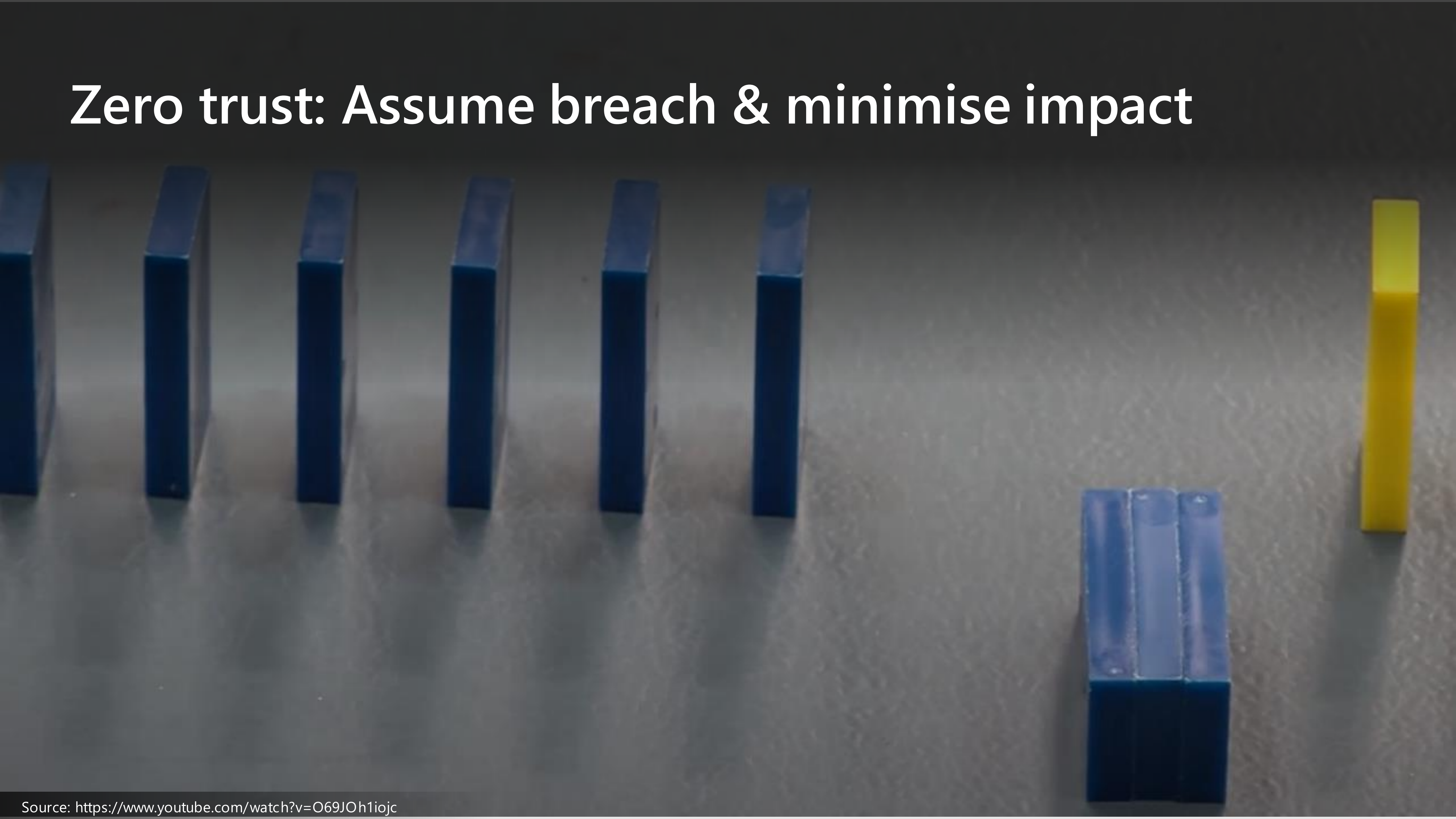
Source: https://flic.kr/p/7KY3mj (Creative Commons)

Zero trust: Assume breach



Source: https://www.youtube.com/watch?v=O69JOh1iojc

Zero trust: Assume breach & minimise impact



Source: https://www.youtube.com/watch?v=O69JOh1iojc

Zero trust: Verify explicitly

Source: https://twitter.com/Efteling/status/1035135919358181376/photo/1

Zero trust: Use least privileged access

Source: https://flic.kr/p/5zPpQL (Creative Commons)

Fundamental hygiene matters

98%

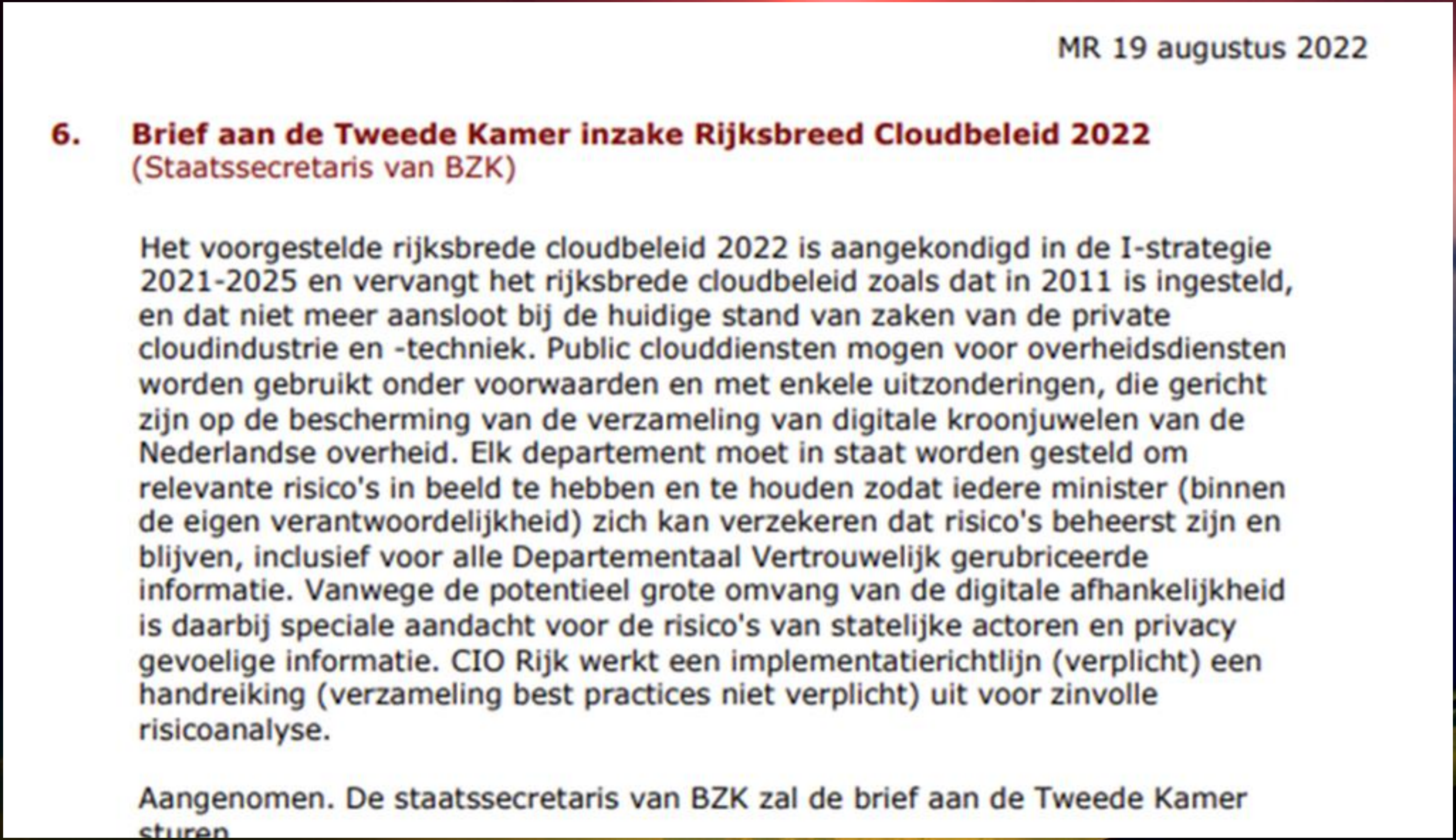
Basic security hygiene still protects against 98% of attacks

Key

- Enable multifactor authentication
- Apply Zero Trust principles
- Use modern anti-malware
- Keep up to date
- Protect data

Source: Microsoft Digital Defense Report (https://aka.ms/MDDR)

Source: https://flic.kr/p/6zoMtn (Creative Commons)



MR 19 augustus 2022

6. Brief aan de Tweede Kamer inzake Rijksbreed Cloudbeleid 2022
(Staatssecretaris van BZK)

Het voorgestelde rijksbrede cloudbeleid 2022 is aangekondigd in de I-strategie 2021-2025 en vervangt het rijksbrede cloudbeleid zoals dat in 2011 is ingesteld, en dat niet meer aansloot bij de huidige stand van zaken van de private cloudindustrie en -techniek. Public clouddiensten mogen voor overheidsdiensten worden gebruikt onder voorwaarden en met enkele uitzonderingen, die gericht zijn op de bescherming van de verzameling van digitale kroonjuwelen van de Nederlandse overheid. Elk departement moet in staat worden gesteld om relevante risico's in beeld te hebben en te houden zodat iedere minister (binnen de eigen verantwoordelijkheid) zich kan verzekeren dat risico's beheerst zijn en blijven, inclusief voor alle Departementaal Vertrouwelijk gerubriceerde informatie. Vanwege de potentieel grote omvang van de digitale afhankelijkheid is daarbij speciale aandacht voor de risico's van statelijke actoren en privacy gevoelige informatie. CIO Rijk werkt een implementatierichtlijn (verplicht) een handreiking (verzameling best practices niet verplicht) uit voor zinvolle risicoanalyse.

Aangenomen. De staatssecretaris van BZK zal de brief aan de Tweede Kamer sturen

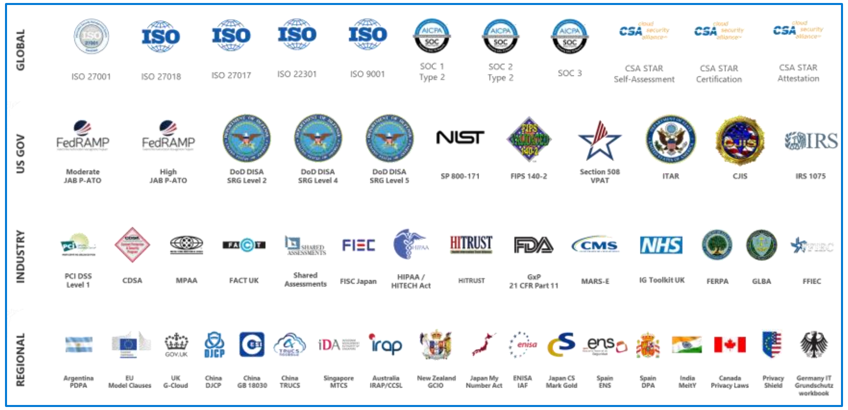
Those who give up security for privacy deserve neither (and will lose both)

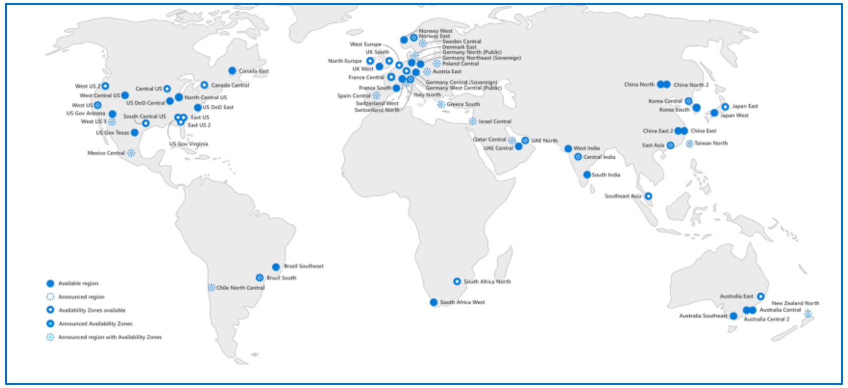
Our privacy principles

[Microsoft Privacy Principles | Microsoft Trust Center]

- You control your data
- You choose where your data is located/stored

  (150 Datacenters; >60 countries)
- Microsoft secures your data at rest and in transit
- Microsoft defends your data





Foundational customer agreements for online products and services;

Product Terms

Sets forth our standard contractual commitments to commercial customers that use Microsoft online services

Online Services Data Protection Addendum (DPA)

Sets forth our respective obligations around processing data in connection with Microsoft online services

Our commitments to commercial and public sector customers

✓ For service delivery

✓ For troubleshooting

✓ For maintenance and improvement

✗ No user profiling

✗ No advertising

✗ No market research

Controlled by you

We commit to strong privacy protections through greater user control and transparency

No data profiling

We will not share or use your data for marketing, advertising, or other commercial purposes

Strong legal protection

We do not provide governments with "back doors," encryption keys, or assistance to break encryption

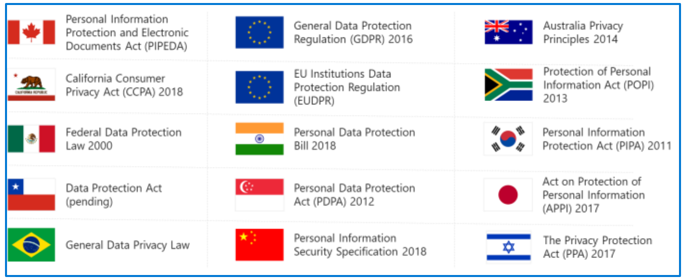
GDPR for all customers

We extend GDPR data protection rights to all customers worldwide, not just in Europe

Listening to customers

We actively collaboration with customers and regulators to foresee and shape compliance regulations

These commitments are integrated into our contractual agreements that govern how we process data and protect data privacy for commercial customers.



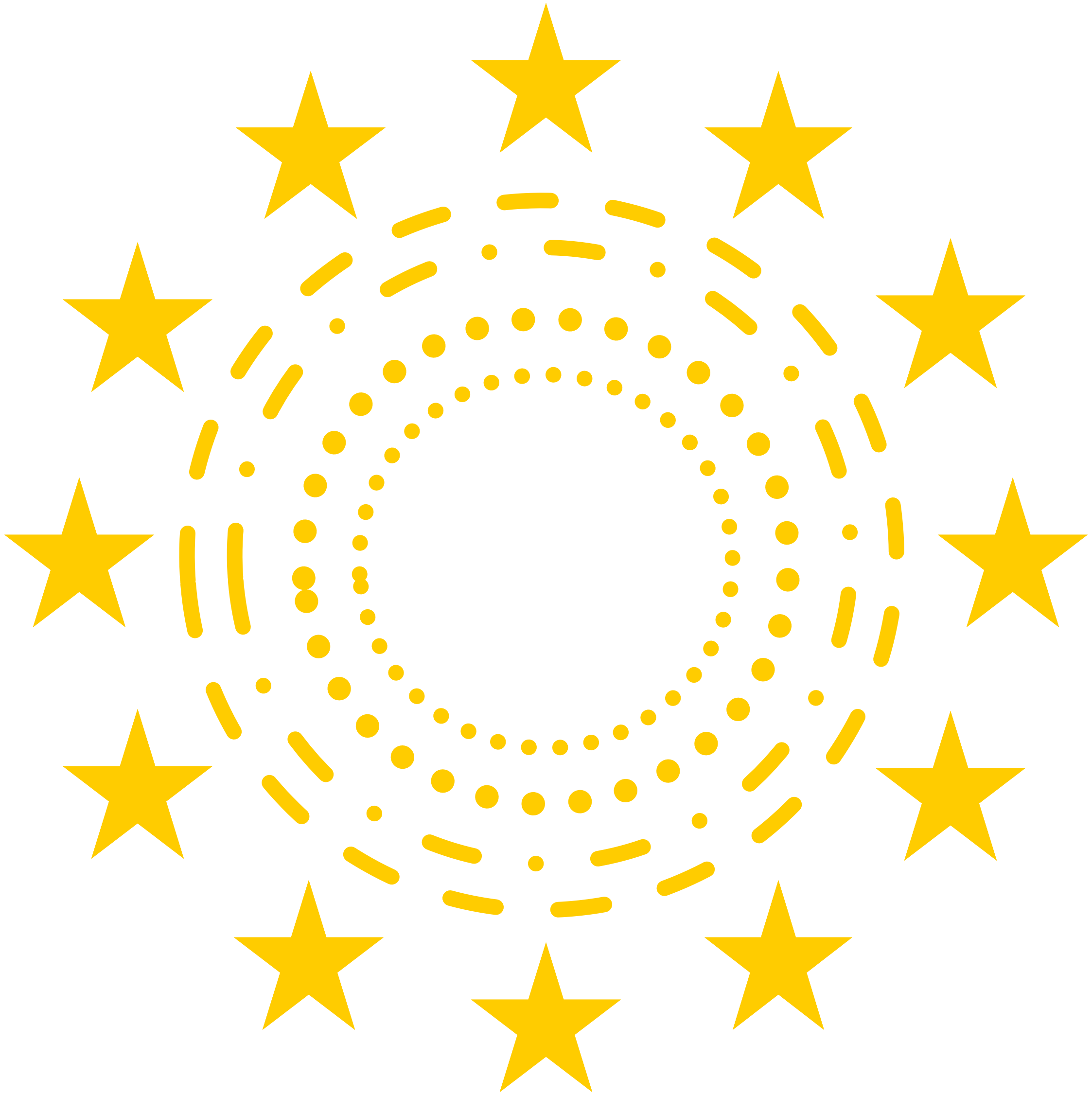
Personal Information Protection and Electronic Documents Act (PIPEDA)	General Data Protection Regulation (GDPR) 2016	Australia Privacy Principles 2014
California Consumer Privacy Act (CCPA) 2018	EU Institutions Data Protection Regulation (EUDPR)	Protection of Personal Information Act (POPI) 2013
Federal Data Protection Law 2000	Personal Data Protection Bill 2018	Personal Information Protection Act (PIPA) 2011
Data Protection Act (pending)	Personal Data Protection Act (PDPA) 2012	Act on Protection of Personal Information (APPI) 2017
General Data Privacy Law	Personal Information Security Specification 2018	The Privacy Protection Act (PPA) 2017

The EU Data Boundary for the Microsoft Cloud

What is the EU Data Boundary

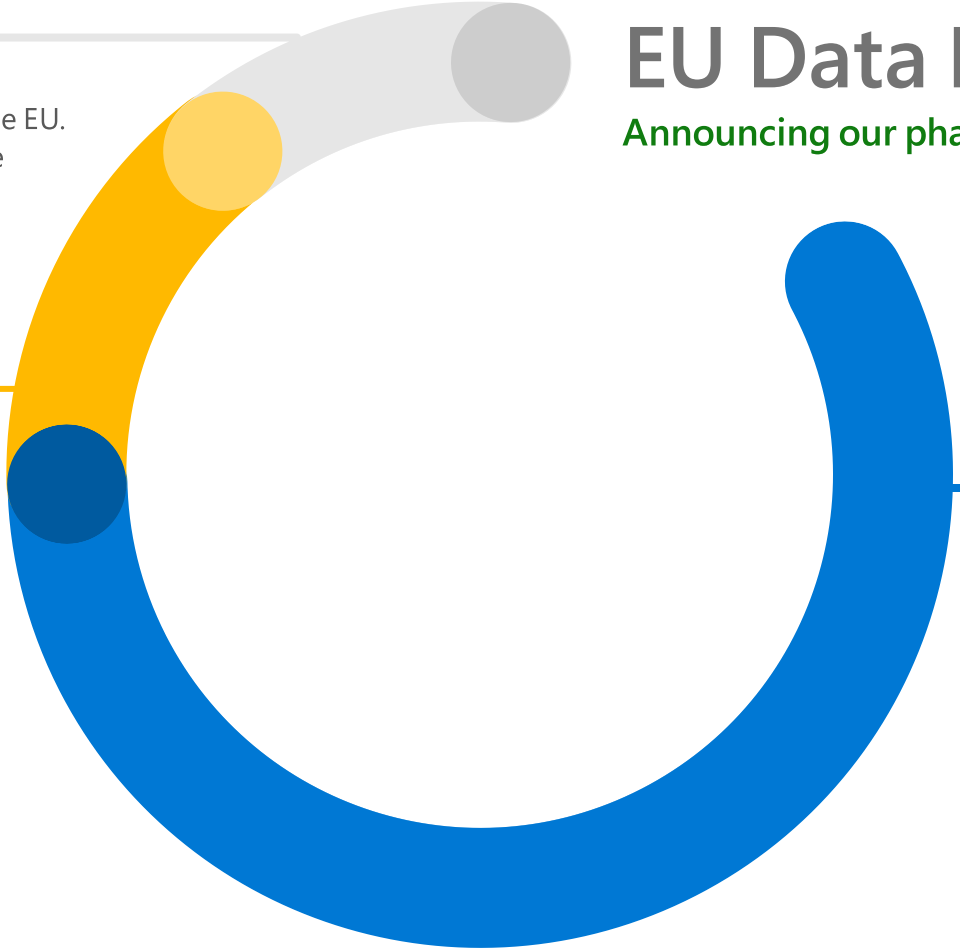
The Microsoft EU Data Boundary for the Microsoft Cloud is an industry-leading solution that further enables public sector and commercial customers the ability to store and process their customer data within the EU Data Boundary for **Microsoft 365, Azure, Power Platform, and Dynamics 365 online services**

The EU Data Boundary enhances Microsoft's data residency commitments for customer and personal data stored and processed in the European Union (EU) and the European Free Trade Association (EFTA).



EU Data Boundary Roadmap

Announcing our phased rollout for the EU Data Boundary



Phase 1
Customer data and documentation

January 1, 2023

Customer data storage & processing in the EU Data Boundary for the majority of Microsoft 365, Dynamics 365, Power Platform, and Azure Services.

Transparency documentation begins to roll out, inclusive of limited transfers.

Phase 1 brings by far the largest portion of your personal data into the scope of the EU Data Boundary and is **completed and available to our customers on 1 January 2023.**

Phase 2 | End of year – 2023
Pseudonymized personal data

Pseudonymized personal data that may be found in system generated logs stored & processed in EU for Microsoft 365, Dynamics 365, Power Platform, Azure services.

Phase 3 | 2024
Support data

Support Data:
Store support data in the boundary of the EU. Limit access to this data from outside the boundary of the EU.

Defending customer data: about government requests

- We **contractually** commit that we do not provide any government with direct, unfettered access to Customer Data.
- If a government demands Customer Data from us, it must follow applicable legal process.

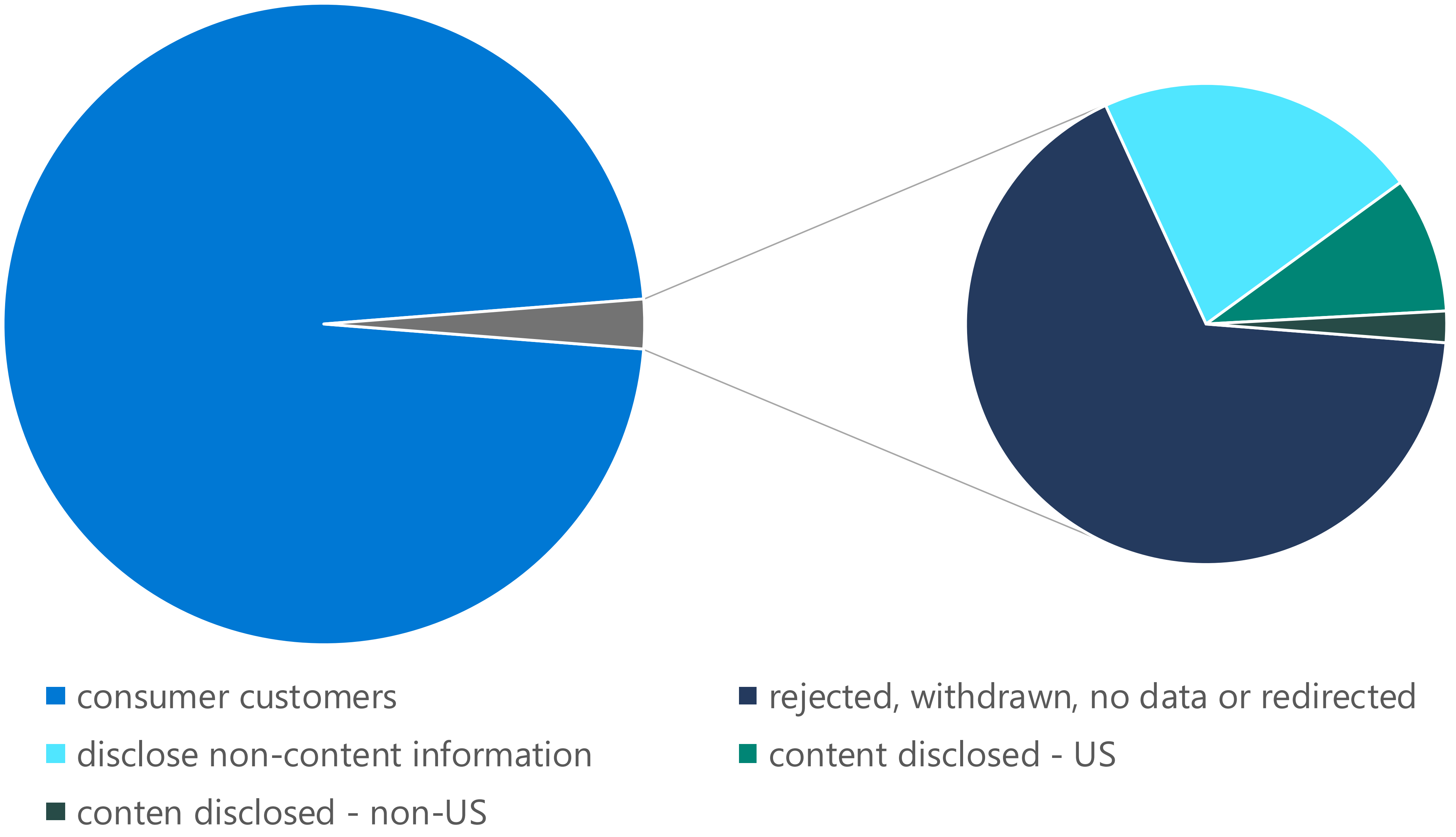
1. Valid legal request?

2. Redirection to customer

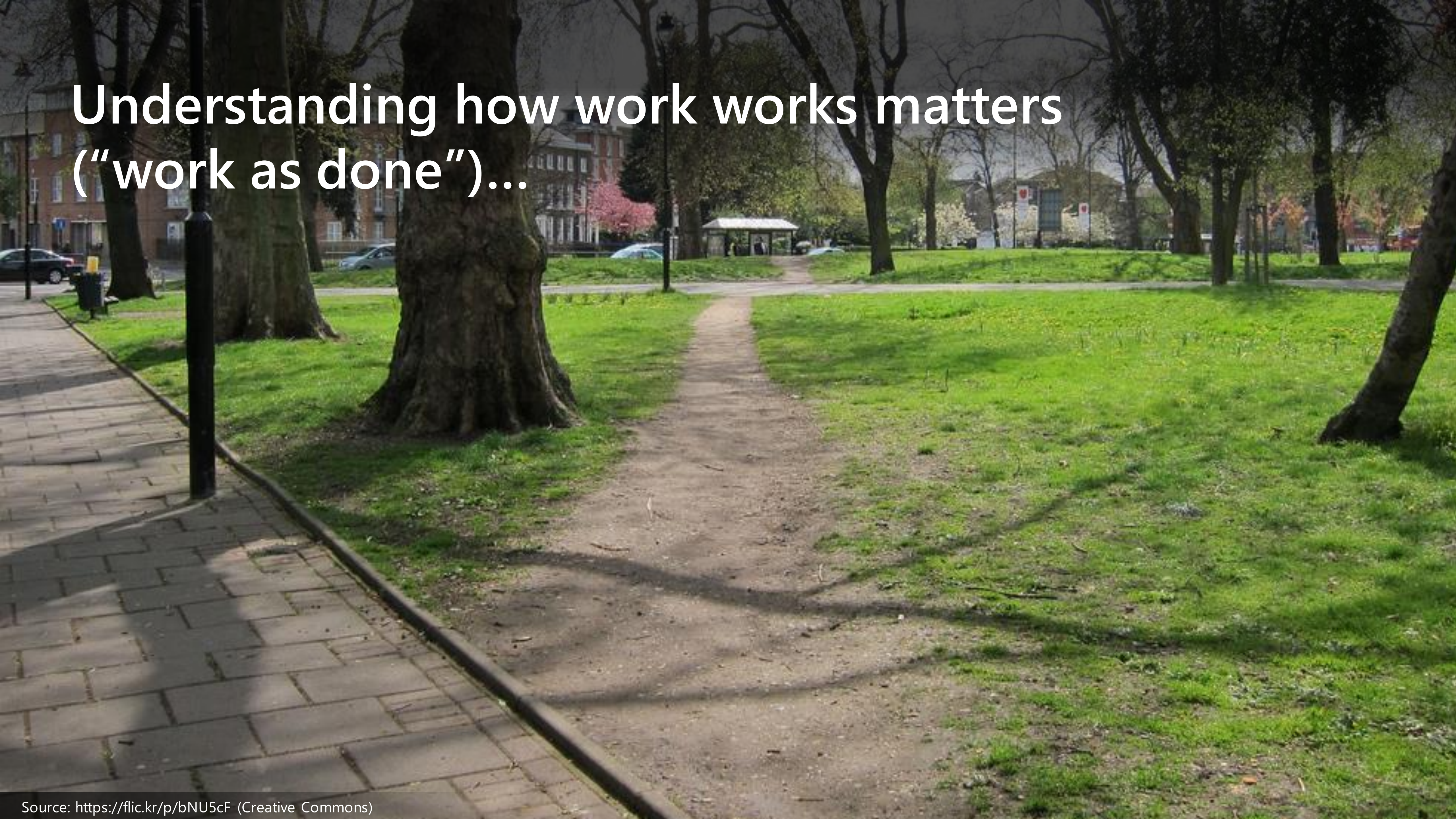
3. Notification

Microsoft process in responding to government requests and the CLOUD act: https://aka.ms/MSLERH

- Jan-Jun 2022: 5560 requests for **consumer** data, 96 of these for accounts outside of the USA.
- 142 requests from law enforcement around the world for accounts associated with **enterprise** cloud customers.
- In 95 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 47 cases, Microsoft was compelled to provide responsive information: 16 of these cases required the disclosure of some customer content and in 31 of the cases we were compelled to disclose non-content information only. Of the 16 instances that required disclosure of content data, 13 of those requests were associated with U.S. law enforcement.

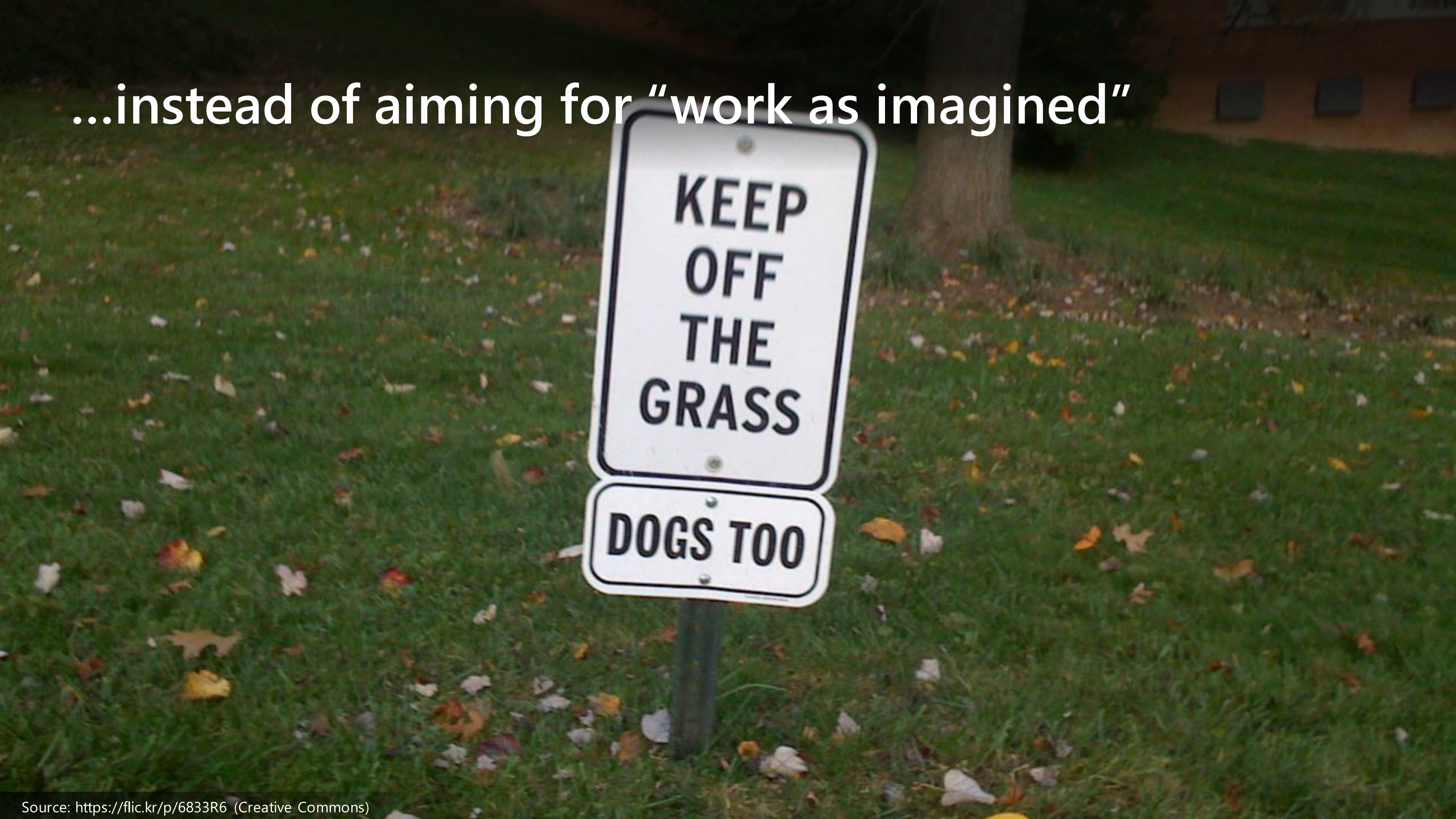

consumer customers
rejected, withdrawn, no data or redirected
disclose non-content information
content disclosed - US
conten disclosed - non-US

Understanding how work works matters (“work as done”)…



Source: https://flic.kr/p/bNU5cF (Creative Commons)

…instead of aiming for "work as imagined"



Source: https://flic.kr/p/6833R6 (Creative Commons)

Not keeping up is falling behind

So keep exploring

Source: https://flic.kr/p/6opsy3 (Creative Commons)

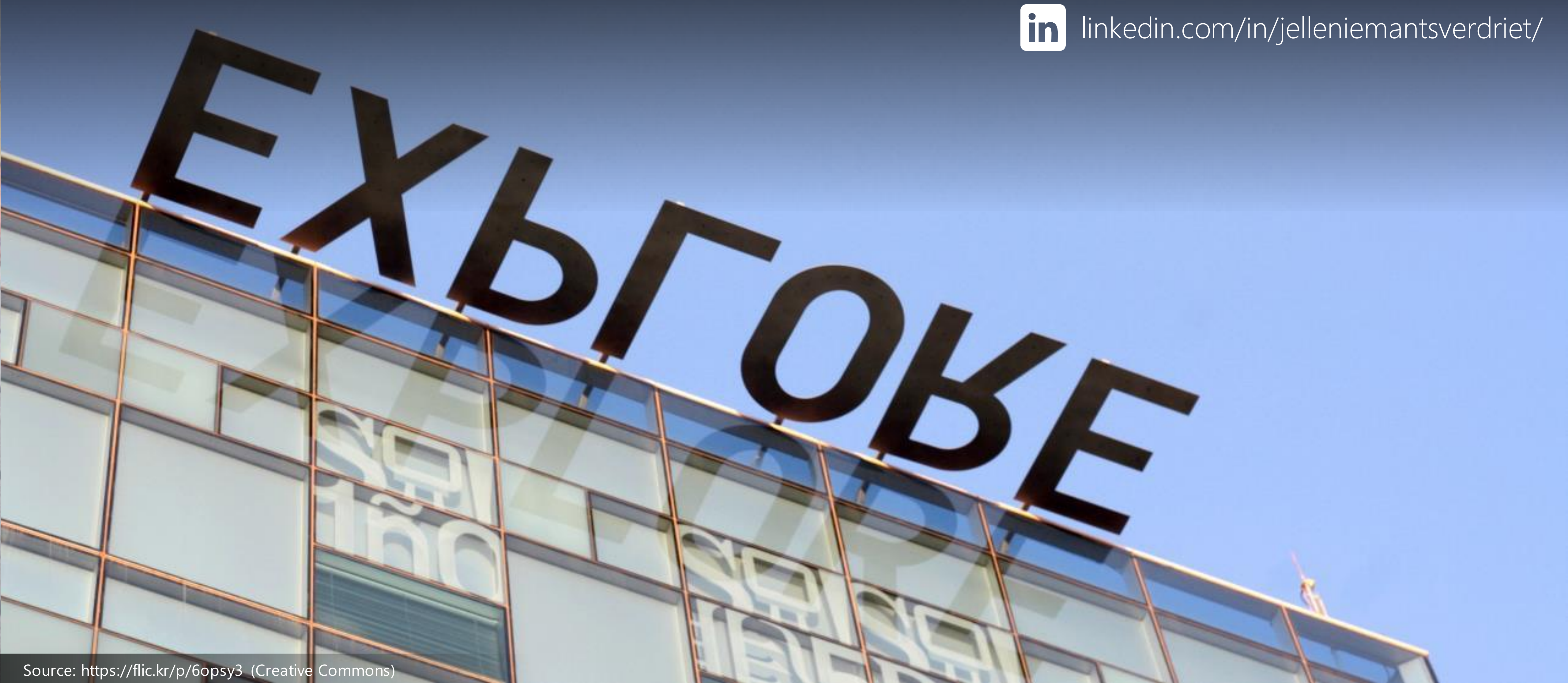
Thank you!

Jelle Niemantsverdriet

✉ jelle.niemantsverdriet@microsoft.com

@jelle_n

linkedin.com/in/jelleniemantsverdriet/



Source: https://flic.kr/p/6opsy3 (Creative Commons)

Cloud & Privacy: Dialogue – Control - Assurance

Further resources

Governance and risk management and assurance

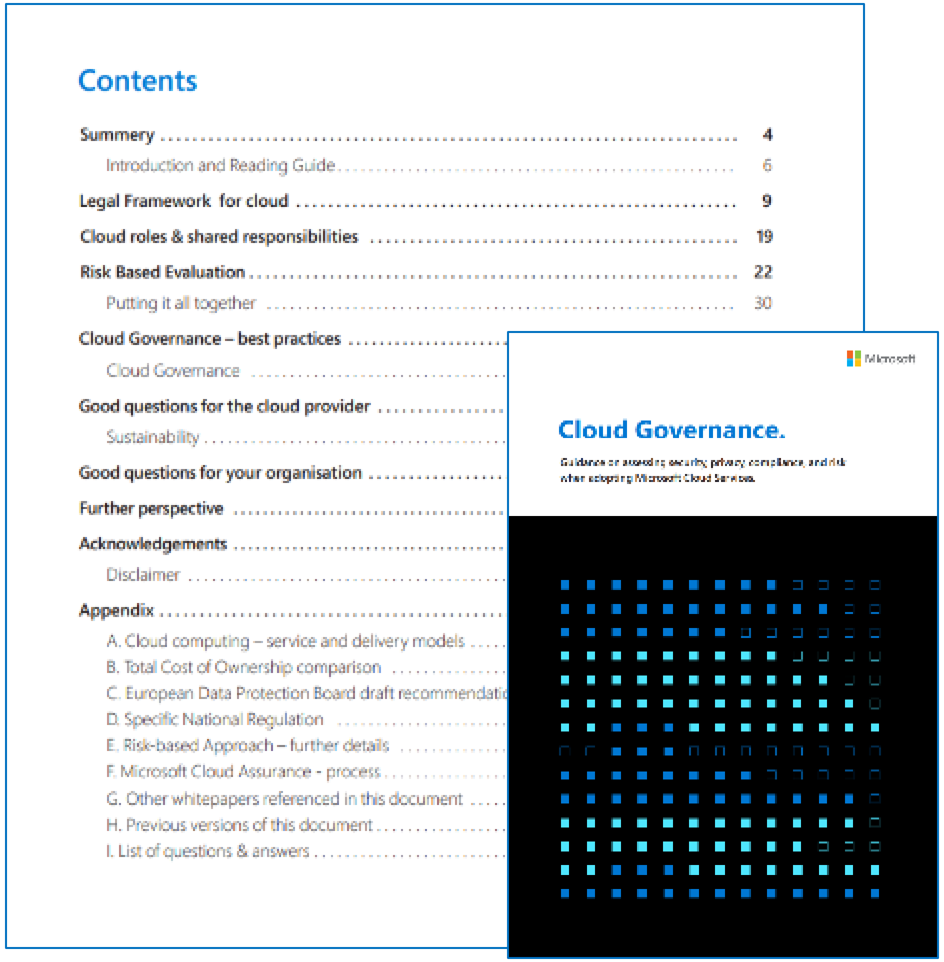
- Cloud Governance whitepaper: https://aka.ms/MSCloudGovernanceEN
- Whitepaper Capgemini; richtlijnen Microsoft Cloud: https://pulse.microsoft.com/uploads/prod/2021/10/White-Paper-Richtlijnen-Privacy-En-Informatiebeveiliging-Bij-Strategische-Adoptie-Microsoft-Cloud.pdf
- Online Trust Coalitie: https://ecp.nl/publicatie/whitepaper-otc-vertrouwen-in-de-cloud/
- Book “Tools & Weapons”; https://news.microsoft.com/on-the-issues/tools-and-weapons/

Microsoft assurance

- Contractual: https://aka.ms/dpa
- Data transfers: https://www.microsoft.com/en-us/trust-center/privacy
- Government access principles: https://blogs.microsoft.com/datalaw/our-practices/Law
- EU Data Boundary: https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/

Data transfers:

- https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en
- https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- https://www.intelligence.gov/how-the-ic-works
- https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf



Contents

Microsoft

Cloud Governance.

Guidance on assessing security, privacy, compliance, and risk when adopting Microsoft Cloud Services.