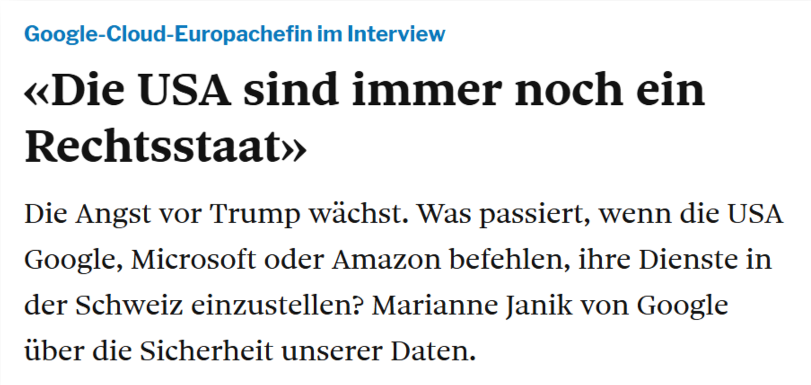
VISCHER

The Cloud in Times of Geopolitical Turbulence.

How to deal with it?

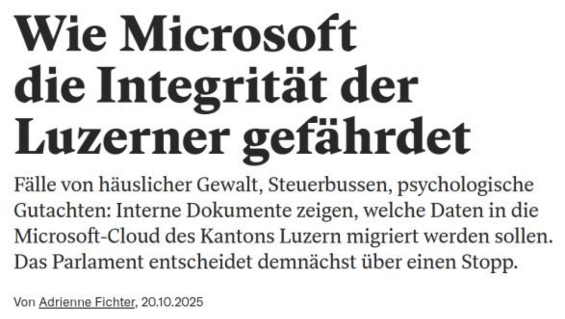
David Rosenthal, VISCHER AG
November 13, 2025



Google-Cloud-Europachefin im Interview

«Die USA sind immer noch ein Rechtsstaat»

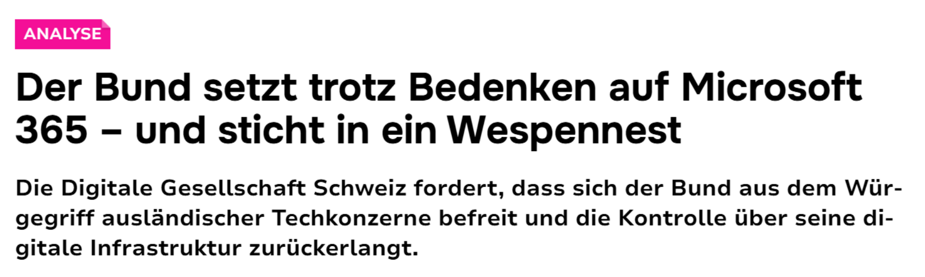
Die Angst vor Trump wächst. Was passiert, wenn die USA Google, Microsoft oder Amazon befehlen, ihre Dienste in der Schweiz einzustellen? Marianne Janik von Google über die Sicherheit unserer Daten.



Wie Microsoft die Integrität der Luzerner gefährdet

Fälle von häuslicher Gewalt, Steuerbussen, psychologische Gutachten: Interne Dokumente zeigen, welche Daten in die Microsoft-Cloud des Kantons Luzern migriert werden sollen. Das Parlament entscheidet demnächst über einen Stopp.

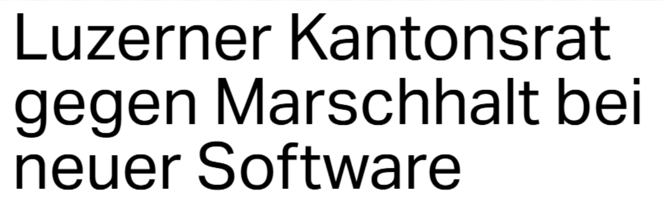
Von Adrienne Fichter, 20.10.2025



ANALYSE

Der Bund setzt trotz Bedenken auf Microsoft 365 – und sticht in ein Wespennest

Die Digitale Gesellschaft Schweiz fordert, dass sich der Bund aus dem Würgegriff ausländischer Techkonzerne befreit und die Kontrolle über seine digitale Infrastruktur zurückerlangt.



Luzerner Kantonsrat gegen Marschhalt bei neuer Software

A political debate …

… but not really for corporations

Sources: tagesanzeiger.ch, watson.ch, republik.ch, swissinfo.ch

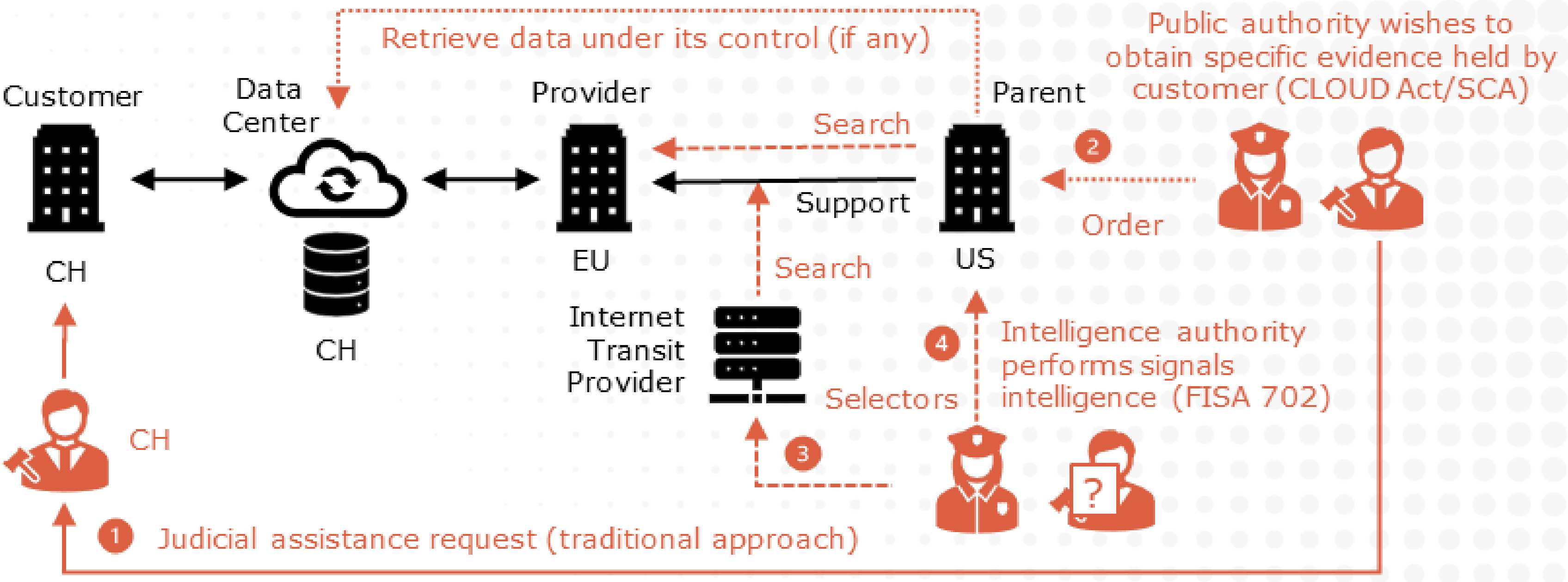
The issues

- **In the past**
  - Data protection law (Section 702 FISA)
  - Official and professional secrecy (SCA / CLOUD Act)

- **Today**
  - ~~Data protection law~~
  - Official ~~and professional~~ secrecy (SCA / CLOUD Act, "Trump")
  - Digital sovereignty ("Trump")

Note: Everyone seems concerned "only" about the US, not other European countries (however, the "E-Evidence" package is coming)

The issue of lawful access

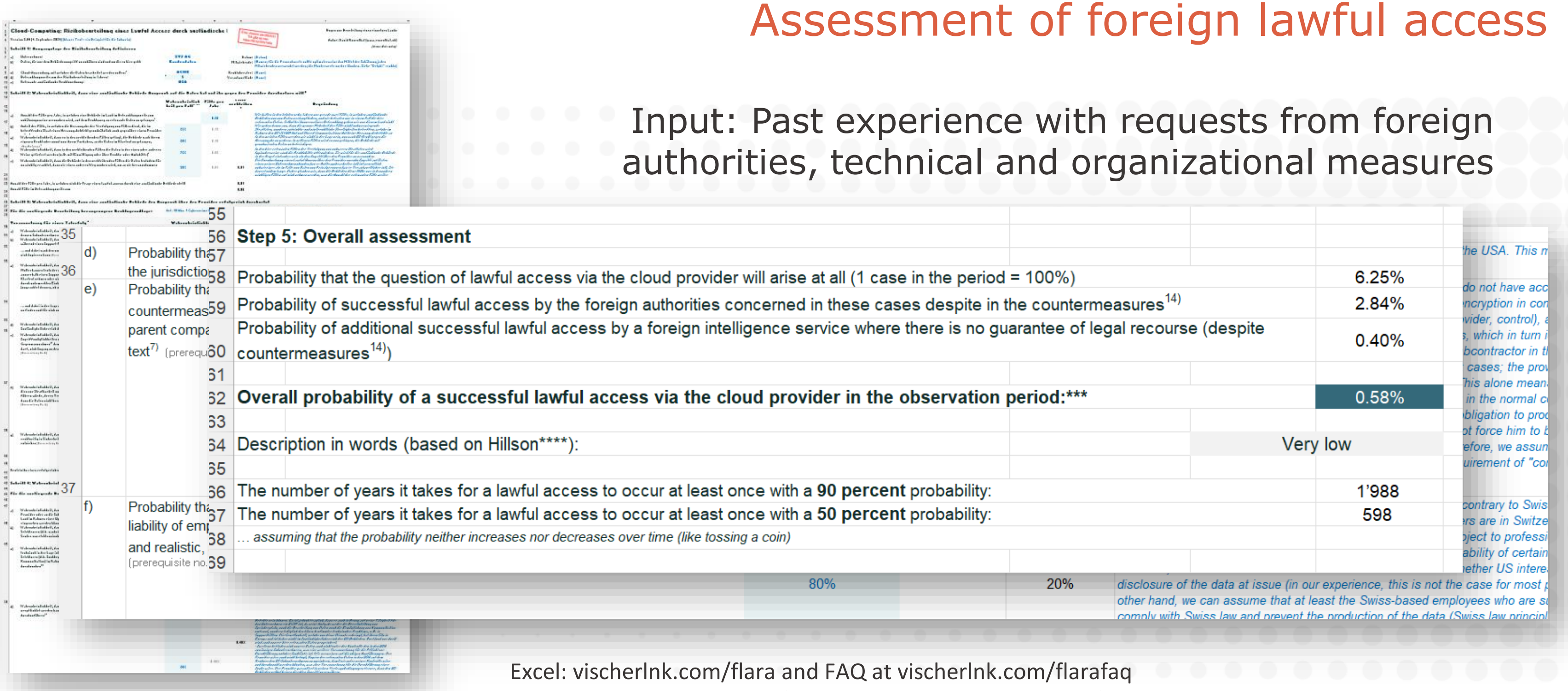

Retrieve data under its control (if any)
Public authority wishes to obtain specific evidence held by customer (CLOUD Act/SCA)
Customer
Data Center
Provider
Parent
Search
2
Support
Order
CH
EU
US
Search
CH
Internet Transit Provider
4
Intelligence authority performs signals intelligence (FISA 702)
Selectors
CH
3
?
1
Judicial assistance request (traditional approach)

How it is addressed in practice

- **Effective measures to mitigate US lawful access**
  - Counterparty in Europe
  - Confidentiality and defend-your-data clause
  - Data "at-rest" only in Switzerland
  - Restriction on operator access (e.g., "Customer Lockbox")
  - Zero data retention (e.g., use of LLM endpoints)
  - Technical access restrictions ("EU Data Boundary" for Microsoft)
- **US cloud providers (and others) have been recognized as providing an adequate level of data protection**
  - Transfer is permitted under data protection law (incl. Swiss DPA)
  - "CLOUD Act"-style legislation exists also here (cf. Art. 18 CCC)

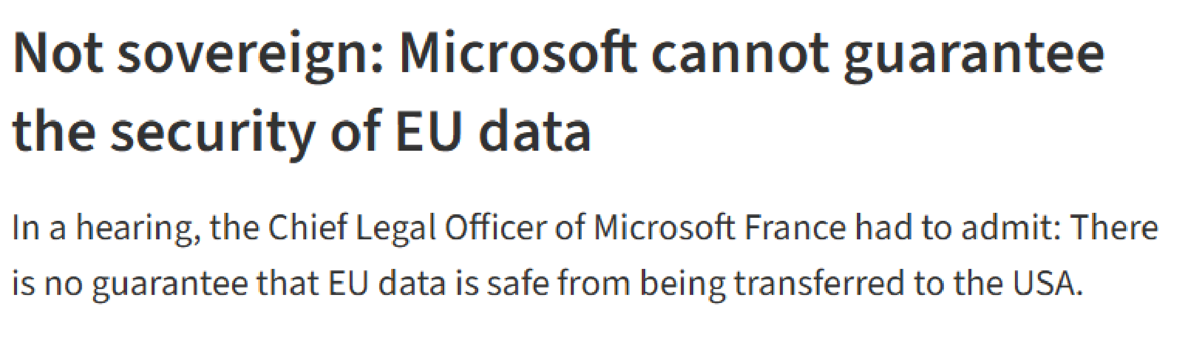
Assessment of foreign lawful access

Input: Past experience with requests from foreign authorities, technical and organizational measures



55		
56	**Step 5: Overall assessment**	
57		
58	Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	6.25%
59	Probability of successful lawful access by the foreign authorities concerned in these cases despite in the countermeasures[14)]	2.84%
60	Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures[14)])	0.40%
61		
62	**Overall probability of a successful lawful access via the cloud provider in the observation period:*****	0.58%
63		
64	Description in words (based on Hillson****):	Very low
65		
66	The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	1'988
67	The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	598
68	*… assuming that the probability neither increases nor decreases over time (like tossing a coin)*	
69		

Excel: vischerlnk.com/flara and FAQ at vischerlnk.com/flarafaq
See also the article at bit.ly/2HaEet5 and appendix at bit.ly/2H8MyZY.



Not sovereign: Microsoft cannot guarantee the security of EU data

In a hearing, the Chief Legal Officer of Microsoft France had to admit: There is no guarantee that EU data is safe from being transferred to the USA.

Source: heise.de

Can any solution guarantee that the US or any other government will never ever access such data?

What about access by hackers? Is there any guarantee?

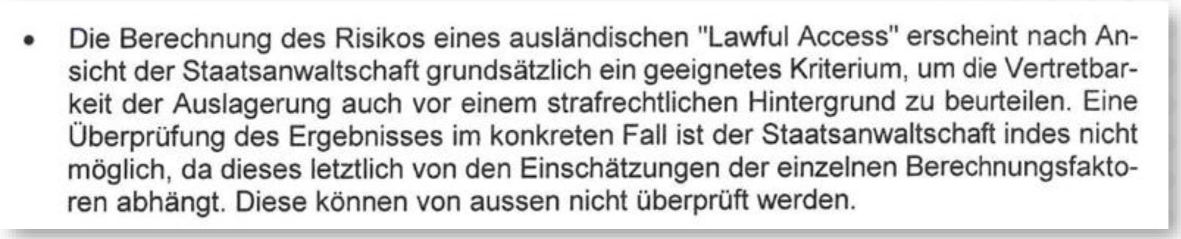
Q: Can you guarantee before our committee, under oath, that the data of French citizens entrusted to Microsoft via Ugap will never be transferred, following an injunction from the US government, without the explicit agreement of the French authorities?

A: No, I cannot guarantee that, but once again, it has never happened before.

Source: : https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html#toc2 (June 10, 2025)

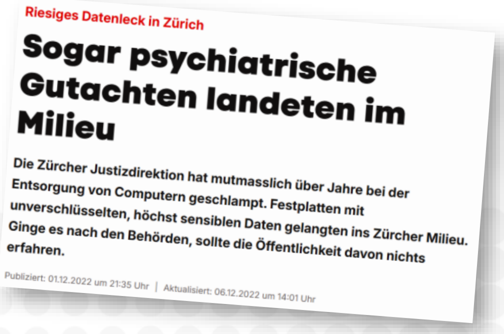
Risk-based approach

- Applies not only with regard to access by hackers, but also to foreign government (and anything else)
- In the public sector, a balancing of interests is required, e.g., weighing security, functionality and cost interests versus loss of control (due to the outsourcing)
- Professional and official secrecy require no guarantee



- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

Excerpt from: Letter from the Basel-Stadt public prosecutor's office following a workshop on calculating the risk of foreign authority access in the context of a cloud project of the University Hospital of Basel



Riesiges Datenleck in Zürich

Sogar psychiatrische Gutachten landeten im Milieu

Die Zürcher Justizdirektion hat mutmasslich über Jahre bei der Entsorgung von Computern geschlampt. Festplatten mit unverschlüsselten, höchst sensiblen Daten gelangten ins Zürcher Milieu. Ginge es nach den Behörden, sollte die Öffentlichkeit davon nichts erfahren.

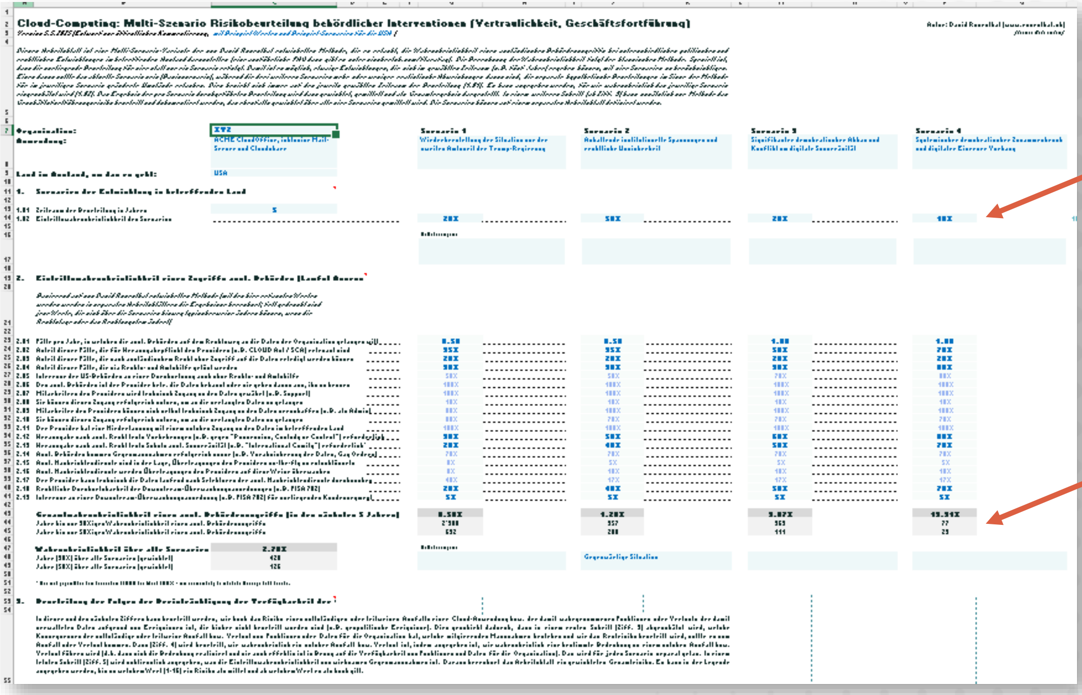
Publiziert: 01.12.2022 um 21:35 Uhr | Aktualisiert: 06.12.2022 um 14:01 Uhr

Source: blick.ch

Prevailing opinion by legal professionals, academia and authorities

Dissenting: DSB ZH and her followers

USA: Has the situation changed?



Cloud-Computing: Multi-Szenario Risikobeurteilung behördlicher Interventionen (Vertraulichkeit, Geschäftsfortführung)

[illegible]

		Szenario 1	Szenario 2	Szenario 3	Szenario 4
Organisation:	XYZ				
Anwendung:	ACME CloudOffice, inklusive Mail-Server und Cloudablage	Wiederherstellung der Situation vor der zweiten Amtszeit der Trump-Regierung	Anhaltende institutionelle Spannungen und rechtliche Unsicherheit	Signifikanter demokratischer Abbau und Konflikt um digitale Souveränität	Systemischer demokratischer Zusammenbruch und digitaler Eiserner Vorhang
Land im Ausland, wo das es geht:	USA				
1. Szenarien der Entwicklung im betreffenden Land					
1.01 Zeitraum der Beurteilung in Jahren	5				
1.02 Eintrittswahrscheinlichkeit des Szenarios		20%	50%	20%	10%
2. Eintrittswahrscheinlichkeit eines Zugriffs ausl. Behörden (Lawful Access)					
2.01–2.19 [illegible]		[illegible]	[illegible]	[illegible]	[illegible]
Gesamtwahrscheinlichkeit eines ausl. Behördenzugriffs (in den nächsten 5 Jahren)		0.58%	1.20%	3.07%	15.94%
Wahrscheinlichkeit über alle Szenarien	2.78%				

3. Beurteilung der Folgen der Beeinträchtigung der Verfügbarkeit der

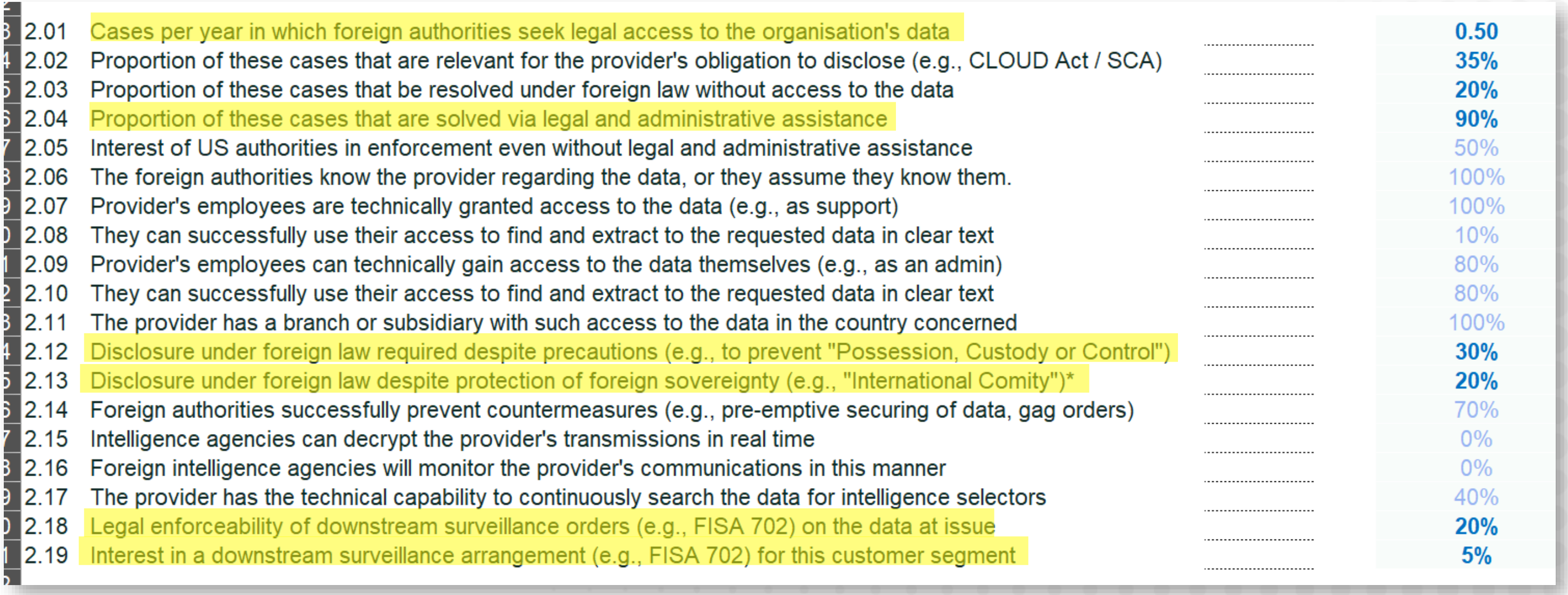
[illegible]

Four scenarios can be defined and assessed

Weighted average result

vischerlnk.com/flara
vischerlnk.com/flarafaq
vischerlnk.com/3HAvcVB (Blog)

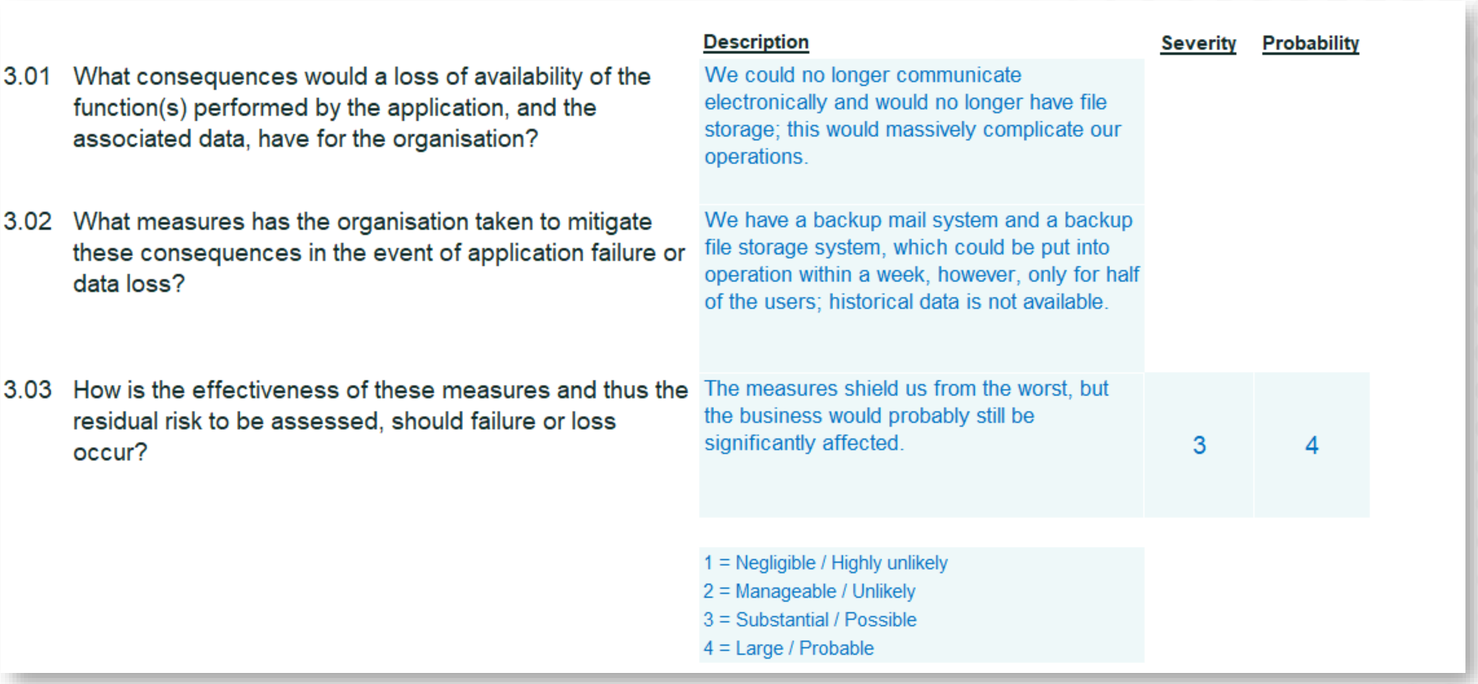
Has the situation changed?



3	2.01	Cases per year in which foreign authorities seek legal access to the organisation's data	0.50
4	2.02	Proportion of these cases that are relevant for the provider's obligation to disclose (e.g., CLOUD Act / SCA)	35%
5	2.03	Proportion of these cases that be resolved under foreign law without access to the data	20%
6	2.04	Proportion of these cases that are solved via legal and administrative assistance	90%
7	2.05	Interest of US authorities in enforcement even without legal and administrative assistance	50%
8	2.06	The foreign authorities know the provider regarding the data, or they assume they know them.	100%
9	2.07	Provider's employees are technically granted access to the data (e.g., as support)	100%
0	2.08	They can successfully use their access to find and extract to the requested data in clear text	10%
1	2.09	Provider's employees can technically gain access to the data themselves (e.g., as an admin)	80%
2	2.10	They can successfully use their access to find and extract to the requested data in clear text	80%
3	2.11	The provider has a branch or subsidiary with such access to the data in the country concerned	100%
4	2.12	Disclosure under foreign law required despite precautions (e.g., to prevent "Possession, Custody or Control")	30%
5	2.13	Disclosure under foreign law despite protection of foreign sovereignty (e.g., "International Comity")*	20%
6	2.14	Foreign authorities successfully prevent countermeasures (e.g., pre-emptive securing of data, gag orders)	70%
7	2.15	Intelligence agencies can decrypt the provider's transmissions in real time	0%
8	2.16	Foreign intelligence agencies will monitor the provider's communications in this manner	0%
9	2.17	The provider has the technical capability to continuously search the data for intelligence selectors	40%
0	2.18	Legal enforceability of downstream surveillance orders (e.g., FISA 702) on the data at issue	20%
1	2.19	Interest in a downstream surveillance arrangement (e.g., FISA 702) for this customer segment	5%

Mainly at issue: The erosion of the rule of law and the separation of power/judicial independence

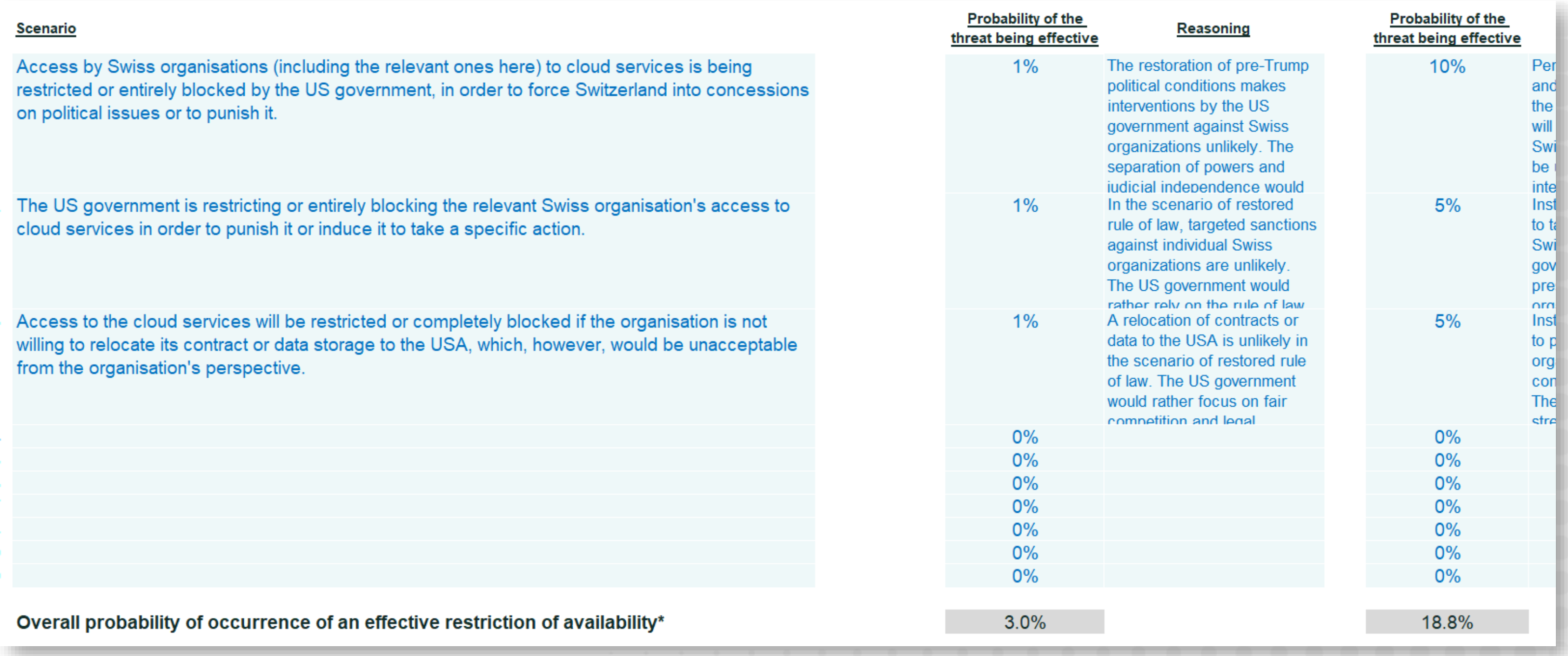
Bonus: The "political pull the plug" risk



		Description	Severity	Probability
3.01	What consequences would a loss of availability of the function(s) performed by the application, and the associated data, have for the organisation?	We could no longer communicate electronically and would no longer have file storage; this would massively complicate our operations.		
3.02	What measures has the organisation taken to mitigate these consequences in the event of application failure or data loss?	We have a backup mail system and a backup file storage system, which could be put into operation within a week, however, only for half of the users; historical data is not available.		
3.03	How is the effectiveness of these measures and thus the residual risk to be assessed, should failure or loss occur?	The measures shield us from the worst, but the business would probably still be significantly affected.	3	4

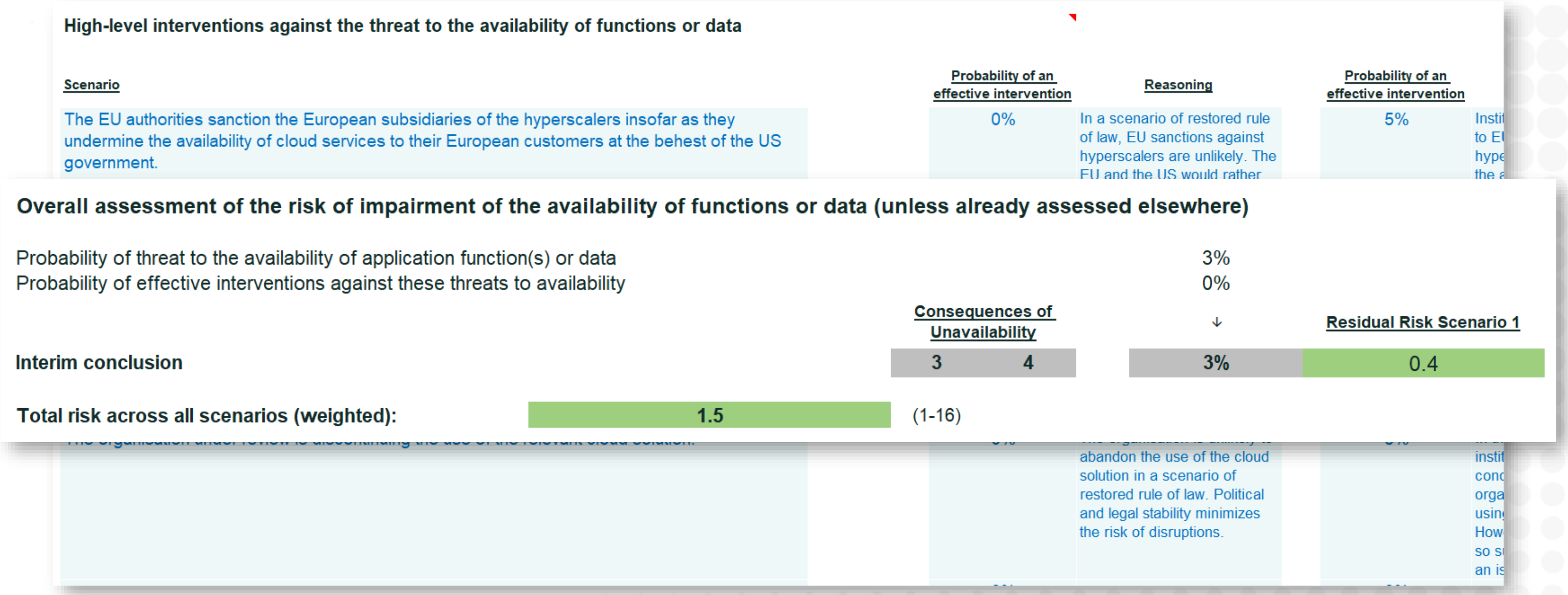
1 = Negligible / Highly unlikely
2 = Manageable / Unlikely
3 = Substantial / Possible
4 = Large / Probable

Bonus: The "political pull the plug" risk



Scenario	Probability of the threat being effective	Reasoning	Probability of the threat being effective	
Access by Swiss organisations (including the relevant ones here) to cloud services is being restricted or entirely blocked by the US government, in order to force Switzerland into concessions on political issues or to punish it.	1%	The restoration of pre-Trump political conditions makes interventions by the US government against Swiss organizations unlikely. The separation of powers and judicial independence would	10%	Per and the will Swi be inte
The US government is restricting or entirely blocking the relevant Swiss organisation's access to cloud services in order to punish it or induce it to take a specific action.	1%	In the scenario of restored rule of law, targeted sanctions against individual Swiss organizations are unlikely. The US government would rather rely on the rule of law	5%	Inst to t Swi gov pre org
Access to the cloud services will be restricted or completely blocked if the organisation is not willing to relocate its contract or data storage to the USA, which, however, would be unacceptable from the organisation's perspective.	1%	A relocation of contracts or data to the USA is unlikely in the scenario of restored rule of law. The US government would rather focus on fair competition and legal	5%	Inst to p org con The stre
	0%		0%	
	0%		0%	
	0%		0%	
	0%		0%	
	0%		0%	
	0%		0%	
	0%		0%	
Overall probability of occurrence of an effective restriction of availability*	3.0%		18.8%	

Bonus: The "political pull the plug" risk



High-level interventions against the threat to the availability of functions or data

Scenario	Probability of an effective intervention	Reasoning	Probability of an effective intervention	
The EU authorities sanction the European subsidiaries of the hyperscalers insofar as they undermine the availability of cloud services to their European customers at the behest of the US government.	0%	In a scenario of restored rule of law, EU sanctions against hyperscalers are unlikely. The EU and the US would rather	5%	Insti to E hype the a
The organisation under review is discontinuing the use of the relevant cloud solution.	[illegible]	The organisation is unlikely to abandon the use of the cloud solution in a scenario of restored rule of law. Political and legal stability minimizes the risk of disruptions.	[illegible]	in t instit conc orga usin How so s an is

Overall assessment of the risk of impairment of the availability of functions or data (unless already assessed elsewhere)

Probability of threat to the availability of application function(s) or data	3%
Probability of effective interventions against these threats to availability	0%

	Consequences of Unavailability		↓	Residual Risk Scenario 1
Interim conclusion	3	4	3%	0.4

Total risk across all scenarios (weighted): 1.5 (1-16)

Conclusion

- The Trump Administration does raise **valid concerns** with regard to the use of US-based clouds
- There are **many factors** to consider (e.g., **security**), and no solution (including OSS) satifies them all
- We need to have a **less emotional** and more **fact-based** discussion about the topic (we are not yet there …)
- Among Swiss **corporations**, the concerns about the impact of the Trump Administration on US cloud risks is very limited
- The **dependency** issue re Microsoft was **ignored** for years due to an irrational focus on the US CLOUD Act
- Therefore, everyone should do their own **risk assessment** and have a "**Plan B**" (and "Plan C") in their drawer

DE | EN | FR | 中文 Contact
VISCHER
Home Services Team Knowledge Careers
Home › Knowledge
Share:

How to deal with US cloud risks in times of Trump.

DATA & PRIVACY, BLOG

6 May 2025

The first 100 days of Donald Trump's US administration have already caused considerable uncertainty as to where the USA is heading. This also raises questions about the use of cloud services from US hyperscalers: Is the data still safe from the US authorities? And could the US administration weaponize cloud providers for their own purposes given Europe's dependence? We have expanded our standardised method for assessing the risk of foreign lawful access so that these questions can now also be assessed and documented.

Looking back: In 2019, I was commissioned by a large Swiss bank to answer the question of which technical and organisational measures are required when using a US cloud in order to reduce the residual risk of US lawful access to an acceptable minimum under Swiss banking secrecy based on laws such as the US CLOUD Act. I developed a statistical method with which the risk could be divided into 19 conditions and systematically addressed. In 2020, I published the method in the form of an Excel spreadsheet as open source (available here with an FAQ).

vischerlnk.com/3HAvcVB

vischerlnk.com/flara
vischerlnk.com/flarafaq

VISCHER

Thank you for your attention!

david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Esplanade Pont-Rouge 9C
Postfach
1200 Genf 26, Schweiz
T +41 58 211 35 00

More materials:
www.rosenthal.ch