

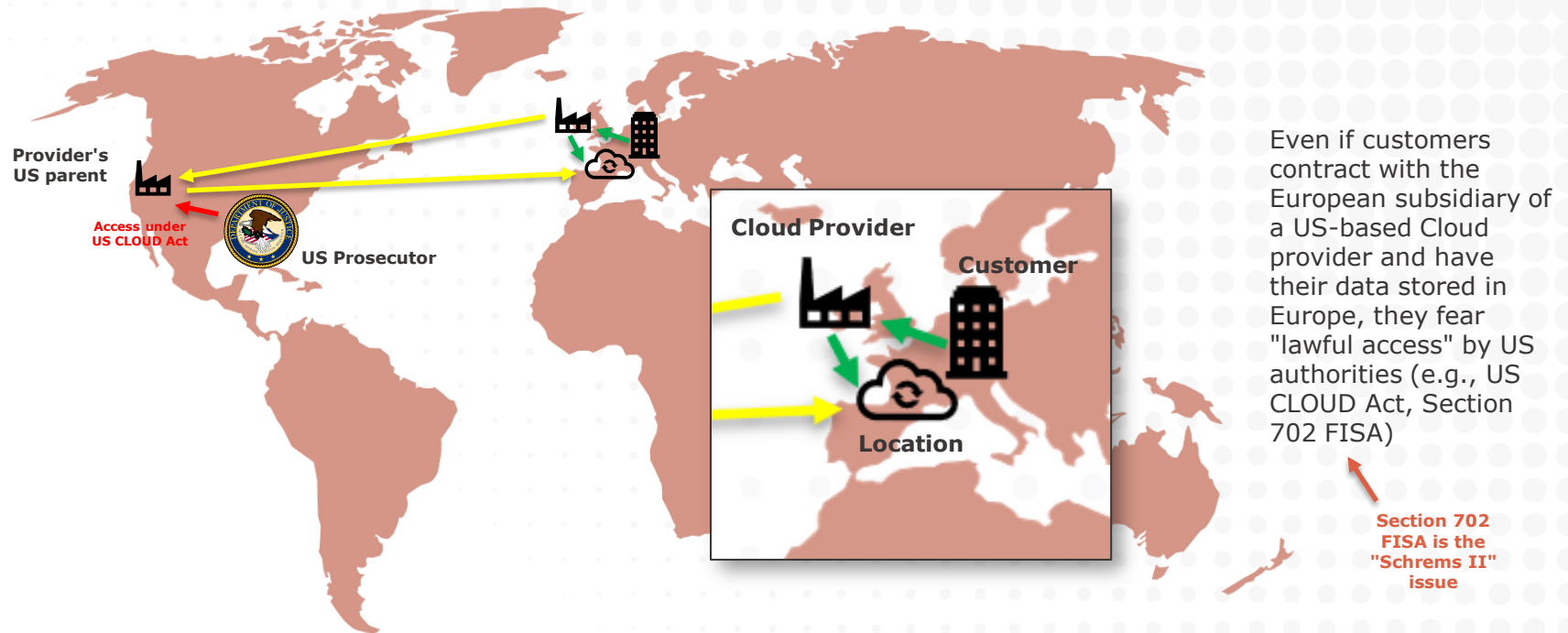
VISCHER

Cloud Risk Assessment.

The most discussed issue and the real ones

David Rosenthal, Partner, VISCHER AG
October 19, 2022

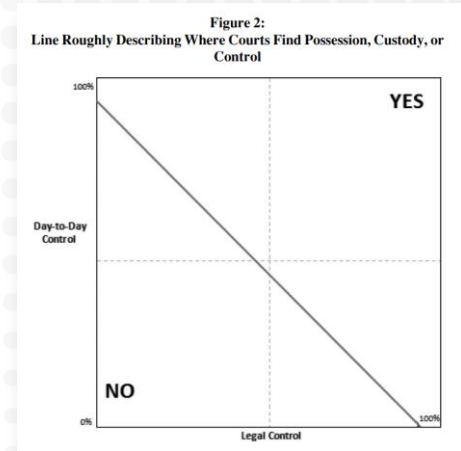
The discussed issue: Foreign Lawful Access



Can we address it?

- We **encrypt data "in-transit"**
 - We choose a **contract party located in Europe**
 - We choose **Switzerland** as **storage location**
 - We prevent **day-to-day-access from the U.S.**
 - We require the provider to **legally defend our data**
- This will not protect our data technically, but provide the provider **a legal argument to reject** foreign lawful access requests
- Example: US-law principle of "p/c/c"
 - Example: US-law principle of "International Comity"


Within two years, all major hyperscalers will be offering their services (almost) exclusively out of Europe



Source: Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in Journal of National Security Law & Policy, Vol. 10 No. 3, January 23, 2020 (<https://bit.ly/3t2xCS9>).

How do we assess it?

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
 Vgl. also see the FAQ at <https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf>

					
35					the data specifically requested by an authority.
36	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%	The Provider reserves the right to provide the service also from the USA. This means that the service is provided by subcontractors under the jurisdiction of the US authorities.
37	e) Probability that despite the technically limited access and the technical and organizational countermeasures in place ¹⁴⁾ , 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 ⁷⁾ (prerequisite no. 5)				As a rule, the employees of the provider and its subcontractors do not have access to the data. On the one hand, this is technically ensured by the concept of encryption in communication. On the other hand, the provider is contractually prohibited to grant access to employees, which in turn is ensured by instructions within the provider's organization. In addition, the subcontractor in turn is contractually prohibited to grant access to its employees.
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%	
37	Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures ¹⁴⁾)			0.40%	
38	f) Probability that if no liability of employee and realistic, and (prerequisite no. 6)				
39					
40					
41					
42					
43					
44					
45					
46					
47					
48					
49					
50					
51					
52					
53					
54					
55					
56					
57					
58					
59					
60					
61					
62					
63					
64					
65					
66					
67					
68					
69					
70					
71					
72					
73					
74					
75					
76					
77					
78					
79					
80					
81					
82					
83					
84					
85					
86					
87					
88					
89					
90					
91					
92					
93					
94					
95					
96					
97					
98					
99					
100					

Is the method recognized?

- Opinion of the Swiss Federal Chancellery: "**Good Practice**"
- Canton of Zurich: Our new "Standard" approach
- A Swiss law prosecutor: A "suitable approach"
- Established in Switzerland, promoted internationally (e.g., IAPP)
 - Swiss banks and other professional secrecy holders
 - Providers (e.g., Zoom)
 - Public institutions (e.g., Dutch government)
 - However, its use is not quite trivial ...
- **Opposition** by the Federal Data Protection and Information Commissioner and some cantonal data protection authorities in Switzerland (promoting the zero-risk-approach)

What about "EO 14086"?

Various questions remain open - what will the ECJ say about the EO?

- **Executive Order** of the U.S. President of October 7, 2022
 - Intended to address the legal **deficiencies** identified in "Schrems II" with regard to "signals intelligence" undertaken by the U.S.
 - Establishes independent redress mechanism for data subjects from "qualifying states" (e.g., EU, UK, Switzerland, provided they permit data transfers to the U.S.)
- The US will **launch a program** that allows US companies to self-certify to comply with data protection (similar to the former "Privacy Shield" program) → can be used as a basis for transferring data to the US (without EU SCC)
 - Adequacy decision probably in spring 2023
- Only indirectly affects transfers based on the **EU SCC**

The pressure to use this as a face-saving way out of the corner is IMHO high ...



The five questions management should really ask

	Strategy and general approach	Assessment of a specific project
Motivation & Alternatives	What are the key elements we hope to achieve by going to the cloud, and how well do we want to know about the alternatives?	What are the business, operational and other requirements for the project and why does the chosen solution outweigh other technologies (i.e. alternatives to the cloud), other cloud providers and the status quo?
Compliance	How do we go about systematically checking, documenting and ensuring compliance with our secrecy obligations and the various legal, regulatory and our own requirements throughout the life of a cloud project?	Do we comply with our secrecy obligations and the legal, regulatory and our own requirements with this project and how have we systematically checked, documented and ensured this for the entire duration of the envisaged cloud solution?
Organisation & Internal Control System (ICS)	What are we willing to do and require in order for our organization to understand, control and manage cloud providers and their solutions so that we can not only handle them properly, but also identify and address deviations from the intended target in a timely manner?	What precautions have we taken or are we taking to ensure that we understand, monitor and control the cloud provider and its cloud solution with our internal resources so well that we will be able to handle the cloud solution correctly in accordance with the requirements, detect deviations from the intended target in due time and eliminate them, including by having our ICS cover also the entire solution ("end-to-end")?
Business continuity	What are our requirements for business continuity in the event of an outage or data loss and for our ability to exit a cloud service in the short term (months) and medium term (12-18 months), and what level of effort are we willing to put into such ability?	What is our plan in the event that the cloud provider suddenly shuts down their service, the solution or our data is no longer available, or we need or want to move away from them or their solution in the short term (months) or medium term (12-18 months)?
Residual risk	How do we ensure that we properly assess and manage specific threats associated with a cloud project that could have significant consequences for the company, and how to we compare them with the residual risks we face otherwise or anyway?	What other threats does the cloud project pose that could have significant consequences for the company, how well do we have them under control, and how do the residual risks compare to the risks we would have without the project or anyway?

Structured Compliance & Risk Assessment

Cloud Solution: Description and Overview of Governance Documents

Protection Requirement Analysis

Third party data*	Confidentiality	Integrity	Availability
CID	Very High	Very High	High
Employee data (accounts)	Select ...	High	Normal
Employee data (in communication and work products)	Select ...	Select ...	Select ...
Data of other individuals (in communication and work products)	Select ...	Select ...	Select ...
Employee data (usage)	Select ...	Select ...	Select ...

* Note: This refers to all information processed by the solution that relates to natural or legal persons and in the protection of data processing to be processed

Maximum time limit for moving out: [150 days (derived from the notice period for new subcontractors) + 12 months (derived prior to the expiration of the contract)]

Alternate service provider in case of a service failure or emergency exit: [To be completed by IT, which it provides here]

Example as used for Swiss financial institutions

The first step of assessing compliance is to gather the information and assess the level of protection that is required

Structured Compliance & Risk Assessment

[illegible]

Example as used for Swiss
financial institutions

- Track 1: Define project and requirements
- Track 2: Assess provider, service and contract
- Track 3: Build solution, including set up service
- Track 4: Internal governance and compliance tasks

Only some 60 of the 150 Controls concern the provider and its contract; the remainder relates to measures on the part of the financial institution

Examples

disclosures required by law.				
"Defend your Data" obligation in case of foreign lawful access attempts	If the provider is confronted with disclosure or access orders from foreign authorities or courts in relation to content data, it will try to redirect the authorities or courts to the FI, and if this is not possible, it will use all legal means to challenge these orders as far and as long as possible. It will inform the FI of this, where permitted. This also applies with regard to authorities within the EEA, not only those outside the EEA, and it shall apply not only to personal data, but any	FINMA Circular 2018/03 (N23), Swiss DPA, GDPR, Professional Secrecy		
No access to pro	Must have, TIA	●	✓	Appendix C of the DPA (September 2021), in combination with M329
Factor				
Provider has a certain discretion which requests should be challenged.		3	1	3
		Risk accepted.		

Examples

Requirements also with regard to the project and the organizational measures to be taken

	be appropriate.	
No data loss or corruption during migration	The FI has a concept to ensure that there will be no loss or corruption of data when migrating from the old to the new solution (where applicable). This includes detecting deviations, reacting to them (e.g., by enabling a roll-back) and having all data properly decommissioned, deleted or archived at the old solution after a successful migration.	
Data at-rest encrypted	Content data "at-rest" (i.e. when in a "dormant" state/when stored) is encrypted.	
	steps taken thereto.	
Renewal management	A procedure (with responsibilities assigned) exists for ensuring that the contract with the provider will be renegotiated and renewed in time to permit an orderly repatriation in case such renewal should fail. This applies in particular for contracts that have a fixed term where renewal on the part of the provider is not guaranteed.	FIN Swi Sec
Service change triggers are	The staff handling the service, including its configuration, understand which	FIN

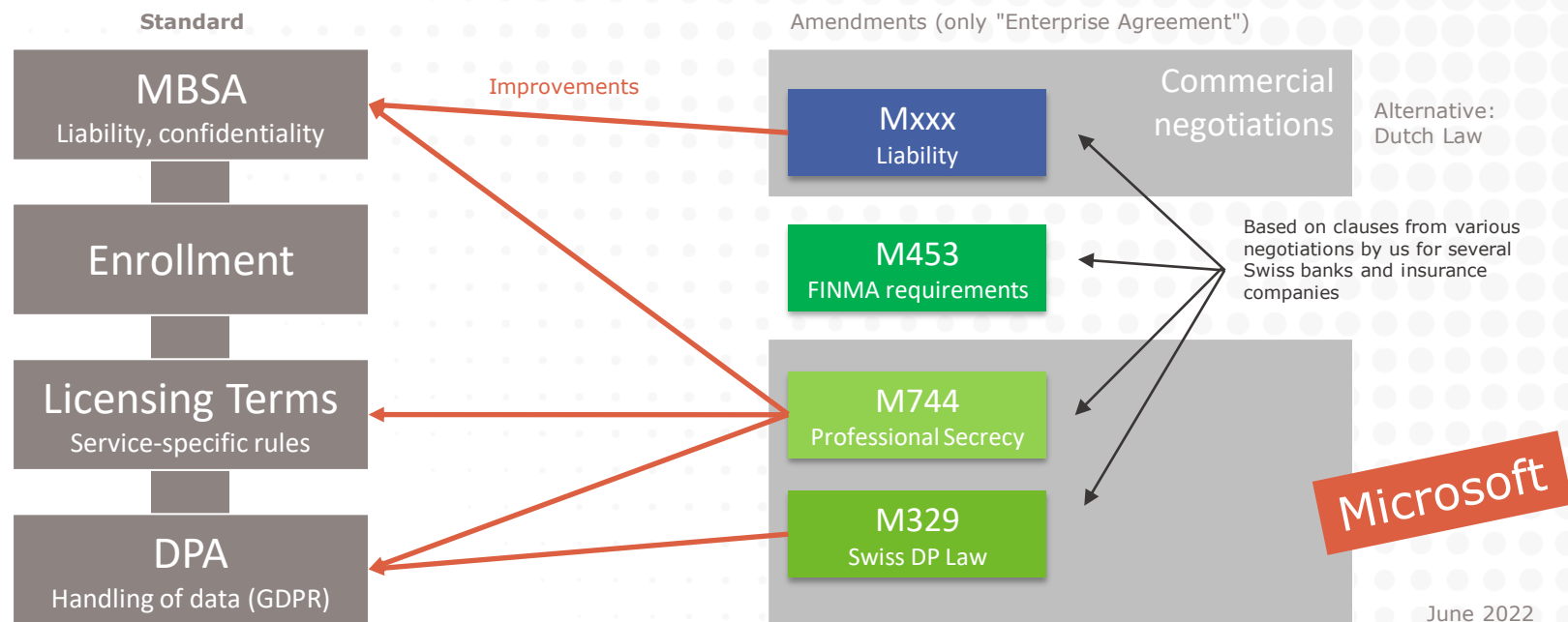
Structured Compliance & Risk Assessment

[illegible]

Example as used for Swiss public institutions

Some 55 risks to be assessed, with classical infosec risks only being considered here in an aggregated form

And what about negotiating contracts?



Summary

- The **public debate** about using the cloud is **misleading**
 - The issue of foreign lawful access is first and above all an issue for organizations that are subject to professional or official secrecy (e.g., banks, the government)
 - Even there, it can be handled; yet, there is no "zero risk"
- The cloud in a corporate environment is **not "plug and play"**
 - The challenges of the "shared responsibility model" are often underestimated
 - More focus and resources are needed for on service, provider and contract oversight and management than traditionally
 - The use of the cloud may increase security, but provides for other risks management should understand and accept beforehand

VISCHER

Questions?

drosenthal@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

Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00