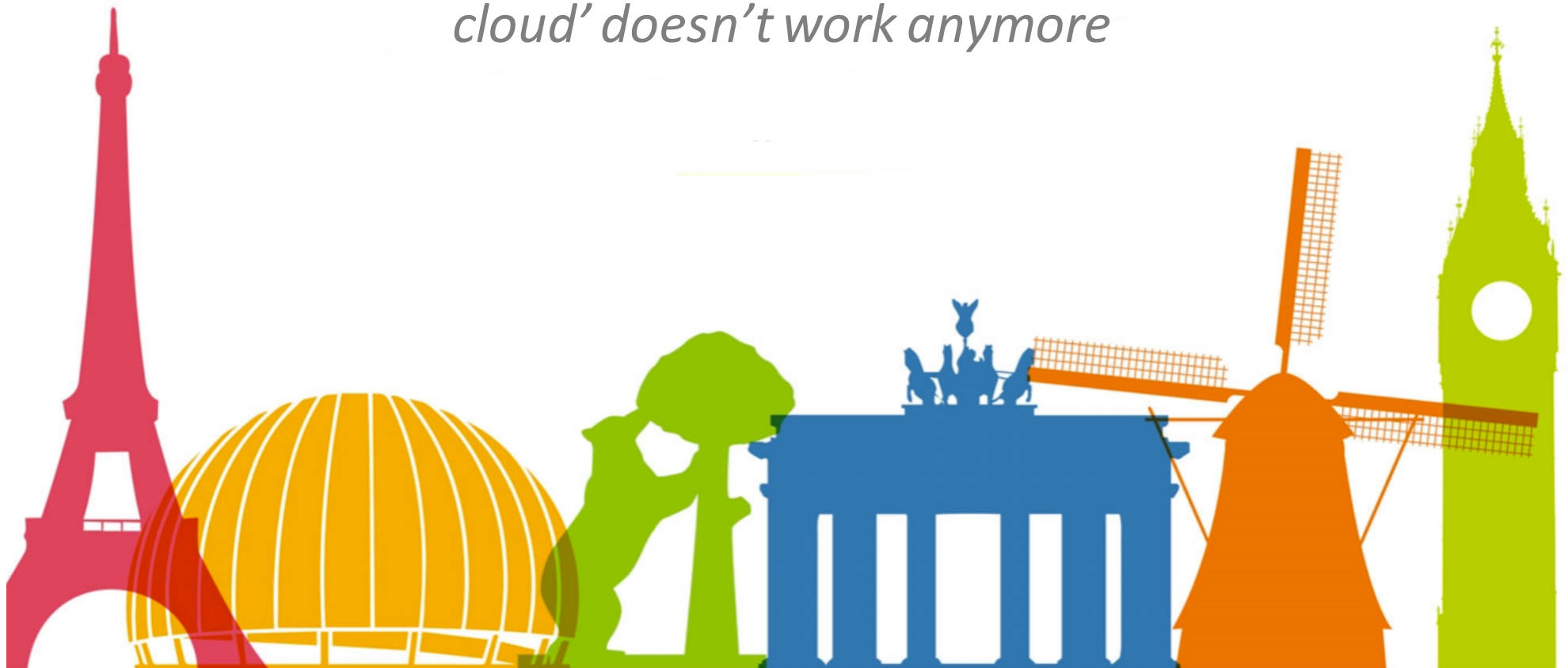




Data Sovereignty in the Cloud: Why 'somewhere in the cloud' doesn't work anymore



Hello from Zettabox!



Alexander Guy

Head of Growth and Business Development
Zettabox

alex@zettabox.com

@alexanderwguy19



The Plan

- 1 **Current Cloud Storage Market Strengths**
- 2 **Data Sovereignty and Protection in 2016**
- 3 **Criticism vs. Control in the Cloud**
- 4 **What does this mean for NRENs?**



1

Current Cloud Storage Market Strengths



Cloud Storage benefits



**Remote
access to
content**



**Multi-device
functionality**



**Ability to share
files and
collaborate easily**



**Easy to use
interface and
apps**



**Increases
teamwork and
collaboration**



Current Market for Cloud Storage



Microsoft Azure



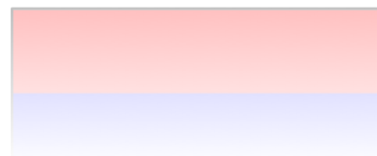
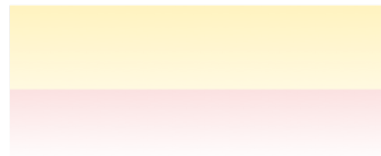
But where is your data?

My data? I don't know. Somewhere in the cloud.



The Problem

Regulators across the European Union and beyond are mandating that organizations prove consumer data remains in-country.



2

Data Sovereignty and Protection in 2016



So what is Data Sovereignty?

“

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. ”

[\(source\)](#)



GDPR is a step to ensure Data Sovereignty in Europe

- General Data Protection Regulation (GDPR) is a recently ratified law intended to **standardise data protection**, storage and privacy in the EU.
- Signed into law last week, the GDPR was developed with **cloud providers and personal data in mind**.
- The GDPR will “**give users back the right to decide on their own private data**,” including by strengthening rules on data subject consent and on processing of sensitive data.
- The next phase of the cloud will allow customers and companies to **choose where their data is stored**.



What is at stake?

“
There's no United Nations of data; each country is looking at its own specific types of data. The only way to deal with it is to store specific data in-country.”

-TechCrunch 2015



3

Response to Data Sovereignty Laws



Microsoft and Deutsche Telekom



Microsoft



Deutsche
Telekom



Is a “data trustee” enough?

- Last November, Microsoft publicly made waves when they announced Deutsche Telekom would be their **“data trustee”** in Germany, an attempt by the company to store German customers’ data in the country.
- Yet, the data centres where this data is stored are still owned by Microsoft, raising questions as to **who actually owns the customer** and if regulators will indeed be satisfied.
- Microsoft’s insistence that it cannot access data without the consent of the trustee is at odds with the US Attorney General who has **repeatedly affirmed the American government’s right** to extract data from American-owned company’s data centres.
- The uncertainty around this issue creates an opportunity a wholly European solution that **prevents this practice**.



Critics of Data Sovereignty

- 1 It's expensive
- 2 It takes too much time to migrate
- 3 "I don't really care if someone looks at my data"
- 4 No one will be able to enforce it



Let's break that down



All major cloud providers operate at the same cost base. Europeans providers **are beginning to match this across IaaS and SaaS sectors.**

Migrating from one software to another is about the same burden everywhere. **Adopting GDPR-compliant tools will not take more time than alternatives.**

Compliance is different across sectors and industries. Businesses and consumers in the **“Sensitive Data Storage” space, Data Sovereignty is a form of protection.**

Governments across the EU are addressing data sovereignty laws rapidly in the post- Safe Harbour world. **The enforcement question will be answered soon.**



4

What does this mean for NRENs?



Protecting Academics, Researchers and Staff



CLOUD STORAGE
& BACKUP
COMPLIANT
WITH EU DATA
PROTECTION/
SOVEREIGNTY
RULES



NO 3RD PARTY
MONITORING/
DATA MINING OF
CUSTOMER DATA



PROTECTION OF
INTELLECTUAL
PROPERTY &
RESEARCH



BUILT-IN PRIVATE,
CONTENT-
CENTRED
MESSAGING



MAINTAINING
THE RIGHT TO BE
FORGOTTEN &
TOTAL CONTROL
OF IDENTITY



Looking ahead to 2018 when GDPR comes into effect

- 1 Tougher contractual clause rules
- 2 Proliferation of “Local Clouds”
- 3 Privacy Shield comes under fire
- 4 Clamping down on shadow IT practices
- 5 Right to be forgotten fight intensifies
- 6 Expanded power of associations



But there is good news!

Cloud companies across Europe are beginning to address the issues of data sovereignty and ownership in the cloud.

- 1 Major cloud providers are starting offering EU companies and consumers **more control of their cloud storage location**.
- 2 Previous data protection regulation was in place for 15 years. After this change, the **law is unlikely to alter substantially for at least a decade**.
- 3 From a user perspective, access to compliant services is only getting easier, with **adoption simple and fast**.
- 4 Options that meet data sovereignty are already available, offering **locally-hosted cloud storage** across the EU.



Questions



THANKS FOR LISTENING
WE'LL BE ANSWERING QUESTIONS NOW