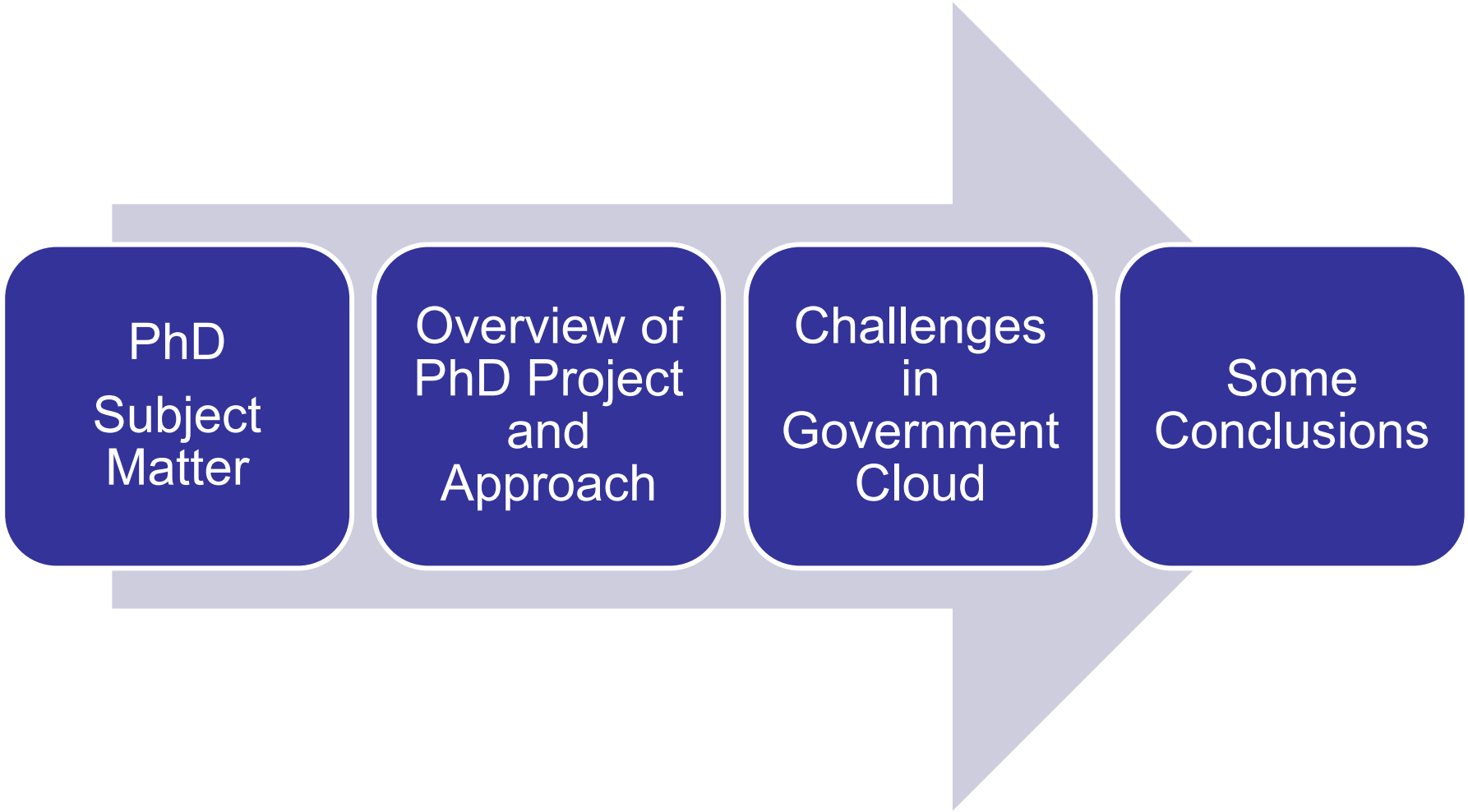
UiO : Faculty of Law
University of Oslo

"Government Cloud Procurement: Contracts, Data Protection, and the Quest for Compliance"

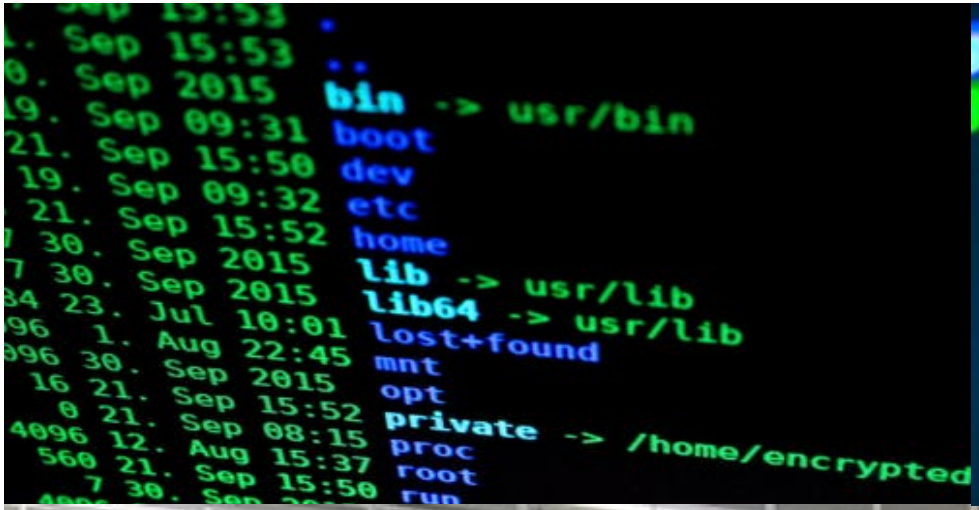
Kevin McGillivray
Skatteetaten (systemjurist)
Informasjonsforvaltning, juridisk stab

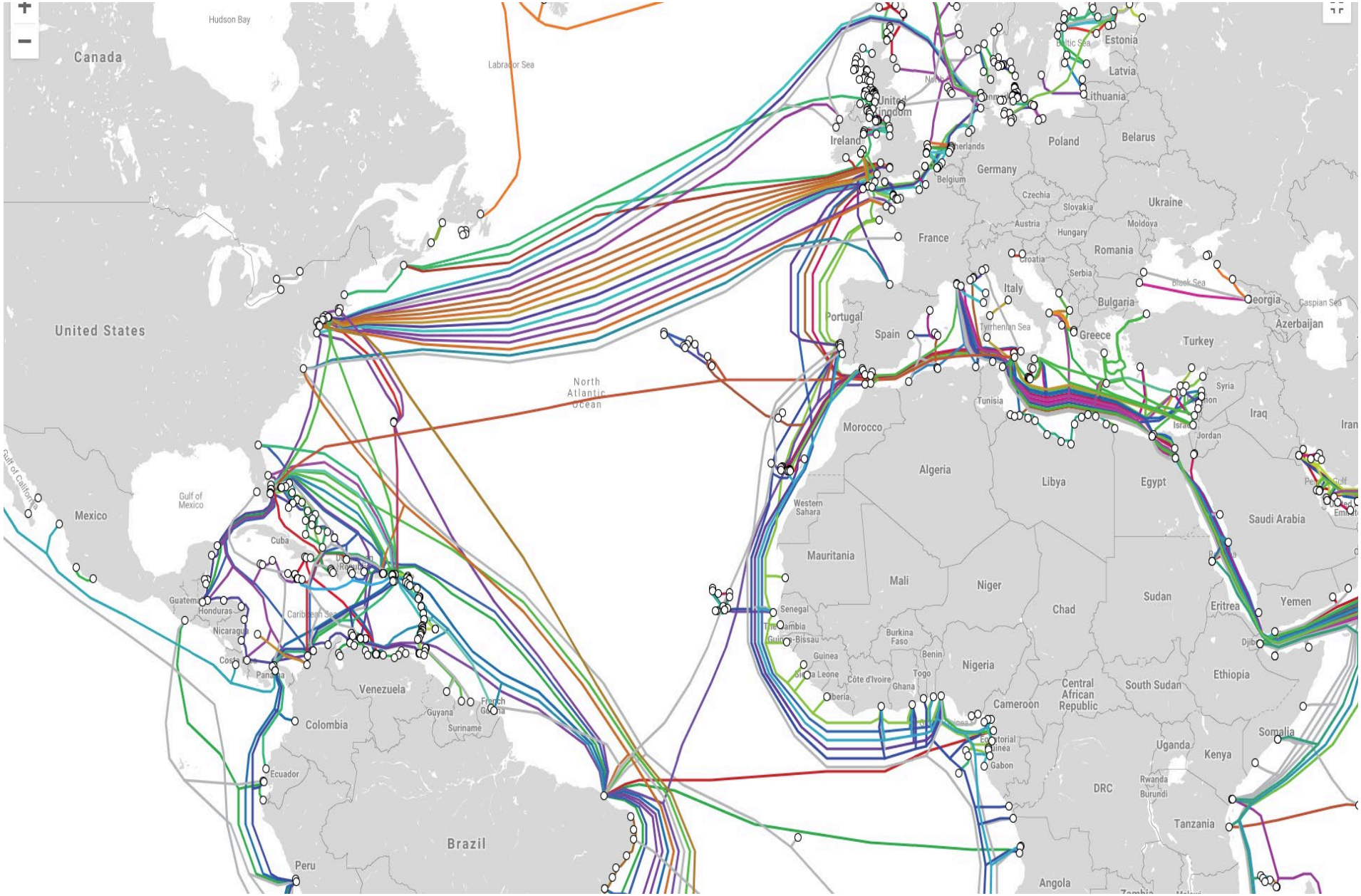
Forum rettsinformatikk 2019
september 4

Agenda


PhD Subject Matter
Overview of PhD Project and Approach
Challenges in Government Cloud
Some Conclusions

Why Cloud Computing?


. Sep 15:53 .
. Sep 15:53 ..
0. Sep 2015 bin -> usr/bin
9. Sep 09:31 boot
21. Sep 15:50 dev
19. Sep 09:32 etc
21. Sep 15:52 home
30. Sep 2015 lib -> usr/lib
7 30. Sep 2015 lib64 -> usr/lib
84 23. Jul 10:01 lost+found
96 1. Aug 22:45 mnt
096 30. Sep 2015 opt
16 21. Sep 15:52 private -> /home/encrypted
0 21. Sep 08:15 proc
4096 12. Aug 15:37 root
560 21. Sep 15:50 run


Hudson Bay
Canada
Labrador Sea
United States
North Atlantic Ocean
Gulf of Mexico
Mexico
Cuba
Honduras
Nicaragua
Costa Rica
Panama
Venezuela
Colombia
Ecuador
Peru
Brazil
Guyana
Suriname
French Guiana
Ireland
United Kingdom
Netherlands
Belgium
Germany
France
Portugal
Spain
Italy
Tyrrhenian Sea
Estonia
Latvia
Lithuania
Poland
Belarus
Czechia
Slovakia
Ukraine
Moldova
Austria
Hungary
Romania
Croatia
Serbia
Bulgaria
Greece
Black Sea
Georgia
Caspian Sea
Azerbaijan
Turkey
Syria
Iraq
Iran
Israel
Jordan
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Mauritania
Mali
Niger
Chad
Sudan
Eritrea
Yemen
Saudi Arabia
Senegal
Gambia
Guinea-Bissau
Guinea
Sierra Leone
Liberia
Côte d'Ivoire
Burkina Faso
Ghana
Togo
Benin
Nigeria
Cameroon
Central African Republic
South Sudan
Ethiopia
Somalia
Kenya
Uganda
Rwanda
Burundi
DRC
Tanzania
Angola
Equatorial Guinea
Gabon


West Central US
The Dalles, OR
US 2
Oregon
California
West US
US Gov Iowa
Central US
Council Bluffs, IA
Canada Central
Canada East
North Central US
AWS GovCloud
South Central US
Ohio
Berkeley County, SC
N. Virginia
East US
East US 2
US Gov Virginia
Ireland
North Europe
UK West
UK South
West Europe
Germany Northeast
Frankfurt
Germany Central
St. Ghislain, Belgium
China North
Beijing
Seoul
Japan East
Tokyo
Tokyo, Japan
Japan West
China East
East Asia
Changhua County, Taiwan
West India
Central India
Mumbai
South India
Southeast Asia
Singapore
São Paulo
Brasil South
Australia Ea
Sydney
Australia Southeast
Microsoft Azure
amazon
web services
Google Cloud Platform


There is NO CLOUD, just
other people's computers
fsfe.org

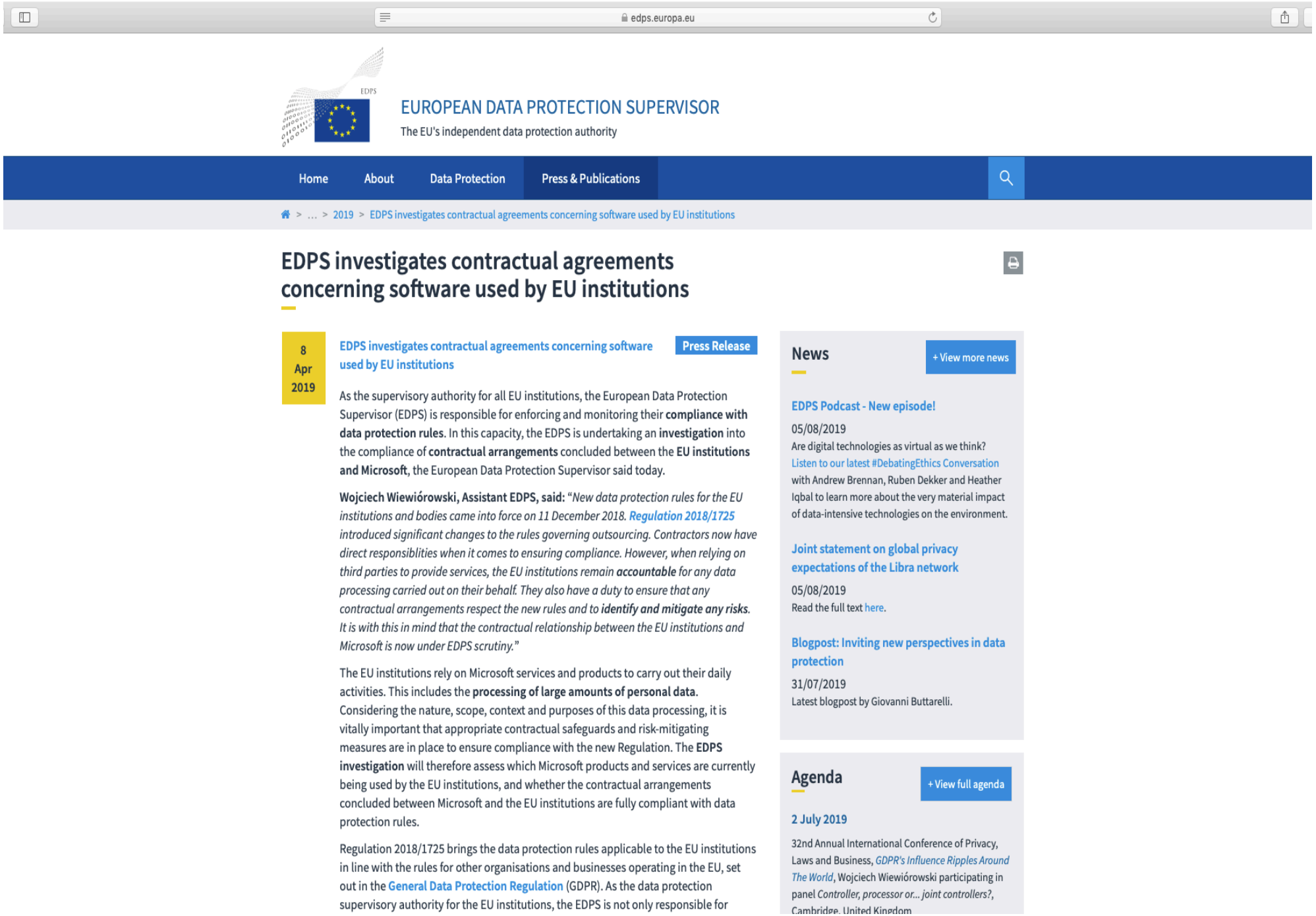
Why focus on government cloud?

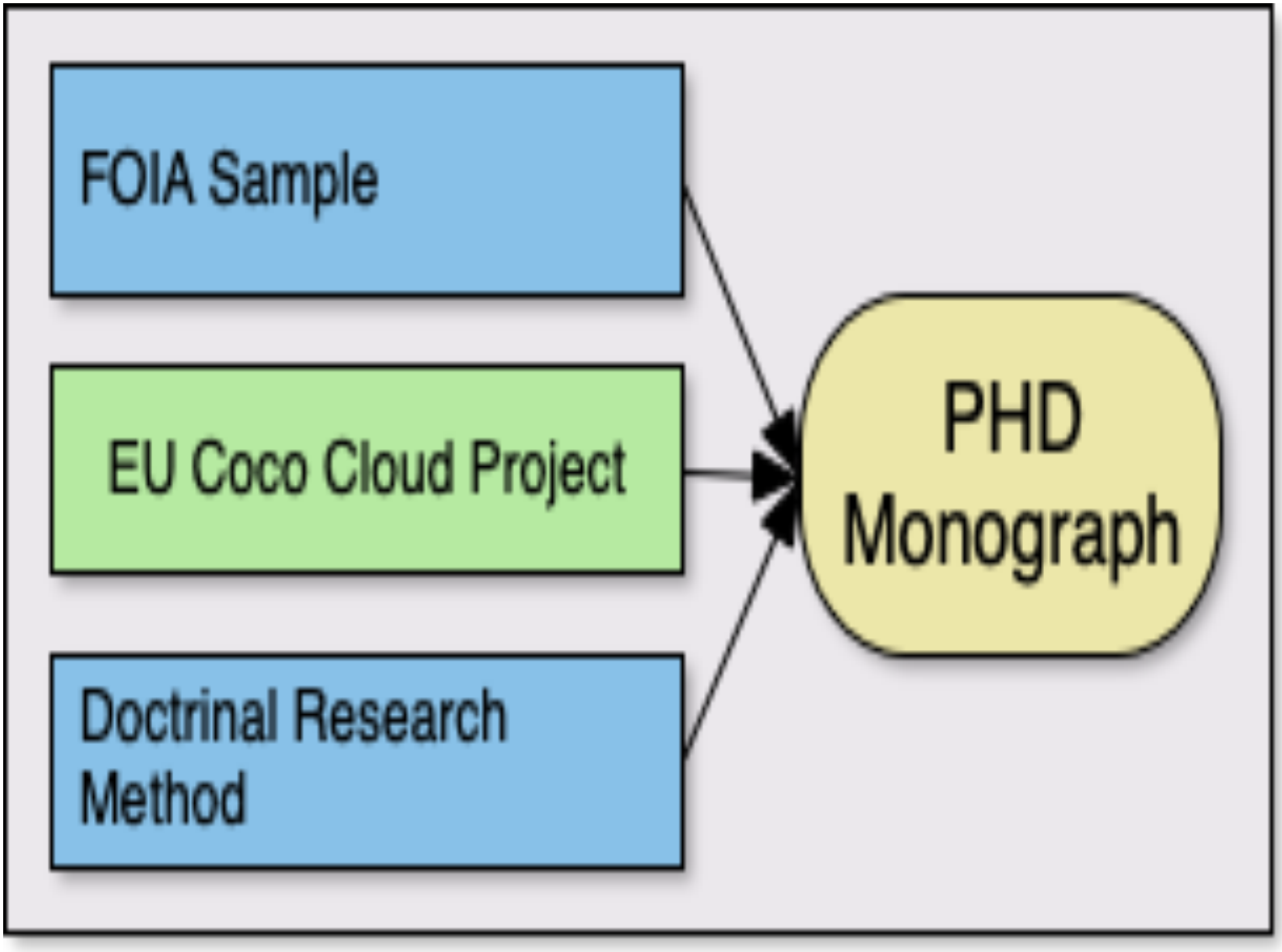
CLOUD

SHARE... E-MAIL THIS PAGE PRINTABLE FORMAT

CIA plans multibillion cloud buy for intelligence community

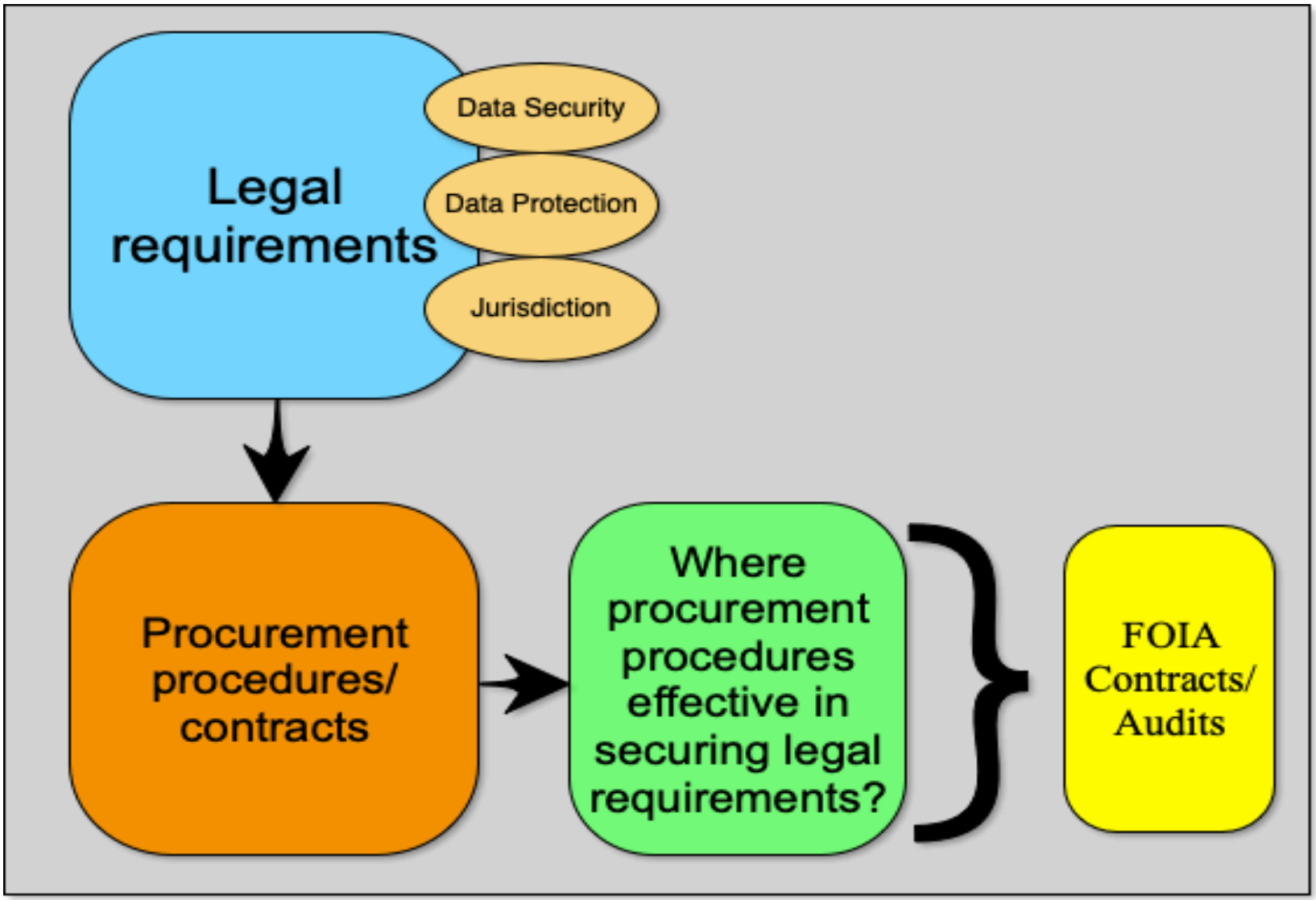
By Adam Mazmanian | Apr 01, 2019


edps.europa.eu
EDPS
EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority
Home
About
Data Protection
Press & Publications
> ... > 2019 > EDPS investigates contractual agreements concerning software used by EU institutions
EDPS investigates contractual agreements concerning software used by EU institutions
8 Apr 2019
EDPS investigates contractual agreements concerning software used by EU institutions
Press Release
As the supervisory authority for all EU institutions, the European Data Protection Supervisor (EDPS) is responsible for enforcing and monitoring their compliance with data protection rules. In this capacity, the EDPS is undertaking an investigation into the compliance of contractual arrangements concluded between the EU institutions and Microsoft, the European Data Protection Supervisor said today.
Wojciech Wiewiórowski, Assistant EDPS, said: "New data protection rules for the EU institutions and bodies came into force on 11 December 2018. Regulation 2018/1725 introduced significant changes to the rules governing outsourcing. Contractors now have direct responsiblities when it comes to ensuring compliance. However, when relying on third parties to provide services, the EU institutions remain accountable for any data processing carried out on their behalf. They also have a duty to ensure that any contractual arrangements respect the new rules and to identify and mitigate any risks. It is with this in mind that the contractual relationship between the EU institutions and Microsoft is now under EDPS scrutiny."
The EU institutions rely on Microsoft services and products to carry out their daily activities. This includes the processing of large amounts of personal data. Considering the nature, scope, context and purposes of this data processing, it is vitally important that appropriate contractual safeguards and risk-mitigating measures are in place to ensure compliance with the new Regulation. The EDPS investigation will therefore assess which Microsoft products and services are currently being used by the EU institutions, and whether the contractual arrangements concluded between Microsoft and the EU institutions are fully compliant with data protection rules.
Regulation 2018/1725 brings the data protection rules applicable to the EU institutions in line with the rules for other organisations and businesses operating in the EU, set out in the General Data Protection Regulation (GDPR). As the data protection supervisory authority for the EU institutions, the EDPS is not only responsible for
News
+ View more news
EDPS Podcast - New episode!
05/08/2019
Are digital technologies as virtual as we think? Listen to our latest #DebatingEthics Conversation with Andrew Brennan, Ruben Dekker and Heather Iqbal to learn more about the very material impact of data-intensive technologies on the environment.
Joint statement on global privacy expectations of the Libra network
05/08/2019
Read the full text here.
Blogpost: Inviting new perspectives in data protection
31/07/2019
Latest blogpost by Giovanni Buttarelli.
Agenda
+ View full agenda
2 July 2019
32nd Annual International Conference of Privacy, Laws and Business, GDPR's Influence Ripples Around The World, Wojciech Wiewiórowski participating in panel Controller, processor or... joint controllers?, Cambridge, United Kingdom


FOIA Sample
EU Coco Cloud Project
Doctrinal Research Method
PHD Monograph

Research Questions (1)

- When governments become cloud clients or users of cloud computing services, what are the primary legal requirements applicable?
  - How will the GDPR apply to and affect the use of cloud computing services?
  - What are the primary procurement challenges (openness, transparency, etc.)?
  - Jurisdictional challenges/problems/requirements
- What procurement procedures, standard contracts or technical means are governments in the EU and the US applying or developing to meet legal requirements when adopting cloud computing?
- Have these procurement procedures and risk assessment programs been effective or helped governments to meet legal requirements, particularly in the area of data privacy?


Legal requirements
Data Security
Data Protection
Jurisdiction
Procurement procedures/ contracts
Where procurement procedures effective in securing legal requirements?
FOIA
Contracts/
Audits

Research Questions (2)

- How are the responsibilities of governments different from other types of cloud clients?
- How *do* governments approach transparency and accountability when adopting cloud computing services?
- How *ought* governments obtain transparency and accountability when adopting cloud computing services?

PART I: SUBJECT MATTER, RESEARCH QUESTIONS AND METHODOLOGY

1 Introduction

2 Definitional, technical, and organizational aspects

PART II: LEGAL REQUIREMENTS APPLICABLE TO THE ADOPTION OF GOVERNMENT CLOUD

3 Government cloud adoption: challenges and obligations

4 Jurisdictional uncertainty and law enforcement access

5 Data privacy and data protection issues in cloud computing

PART III: PRIVATE ORDERING AND CLOUD COMPUTING CONTRACTS

6 Contracts used to procure cloud services: what is the role of contracts in cloud computing?

7 Study on cloud computing contracts (Part I): Methodology, contract structure, and negotiated terms

8 Study on cloud computing contracts (Part II): Standard terms, impact on governments, and lessons learned

9 Dissertation Conclusion

Role of contracts—the law of the parties

Getting Beyond Boilerplate

- Standard Contracts Provided to Consumers and SMEs Available
  - Many studies evaluating B2C (or B**2**SME) contracts
  - Many problems were apparent
- Negotiated B2B Cloud Contracts
  - Limited Ability to Access/Assess the “Law of the Parties”
  - Interested in Contractual Structure, Prime Clauses, Specific Requirements (SOW, SLAs)
  - QMUL Study

B2B terms often limited to the parties to the contract

"Neither party will disclose confidential information in violation of the terms and conditions of this Agreement, to any third party, without the prior written consent of the other Party…including the terms and conditions…[]"

US Agency Name	Number of Contracts/ Documents	Number of Pages	Date Provided	Request Completed/ Fulfilled
Agency for International Development (US Aid)	0	0	N/A	No
Bureau of Ocean Energy Management	1	55	10 Dec 2015	Yes
Consumer Financial Protection Bureau (CFPB)	2	109	27 May 2015	Yes
Department of Commerce (DoC)	1	184	17 July 2015	Yes
Department of Energy (DoE)	10	147	14 April 2016	Yes
Department of the Interior (DoI)	5	400	23 Oct 2015	Yes
Department of Labor (DoL) Office of Inspector General	1	72	10 Aug 2017	Partial
Department of Transportation (DoT)	8	276	21 Dec 2015	Yes
Environmental Protection Agency (EPA)	16	279	23 Aug 2017	Yes
Federal Aviation Administration (FAA)	3	139	26 Apr 2016	Yes
Federal Housing Finance Agency (HUD)	1	17	29 Oct 2015	Yes
Geological Survey Department of the Interior	2	84	1 June 2015	Partial
National Aeronautics and Space Administration (NASA)	2	50	28 May 2015	No
National Endowment for the Humanities (NEH)	2	72	8 June 2015	Yes
Office of Personnel Management (OPM)	15	554	2 May 2015	Partial
US Postal Service (USPS)	6	172	29 May 2015	Yes
Total: 16 agencies	75	2,610		

G-Cloud Customer/Cloud Adopter	Number of Contracts/ Documents	Number of Pages	Date of Contract	Contract Type
British Library	1	23	20 February 2014	Call Off Contract
Police and Crime Commissioner for Avon & Somerset – and- Iken Business Limited	2	74	17 March 2014	Framework Agreement and Call Off Contract
Sprint II Model Contract (Framework Agreement) Thames Valley Police Authority -and- Specialist Computing Services	2	173	21 March 2012	Framework Agreement
UK Crown Commercial Service (Standard Contract)	1	34	8 May 2017	G-Cloud 9 Framework Agreement[24]
UK Crown Commercial Service (Standard Contract)	1	39	8 May 2017	G-Cloud 9 Call-Off Contract
UK Crown Commercial Service (Standard Contract)	1	27	23 Oct 2015	N/A
UK Crown Commercial Service (Standard Contract)	1	9	8 May 2017	Collaboration agreement
UK Crown Commercial Service (Standard Contract)	1	3	8 May 2017	Alternative clauses
UK Crown Commercial Service (Standard Contract)	1	6	8 May 2017	Standard Guarantee
Total: Contracts	11	388		

Varied Responses

PROCUREMENT SENSITIVE

[redacted]

[redacted]

[Ex 3, 39 USC 410(c)(2)]

University of California
Lawrence Berkeley National Laboratory

DATA SECURITY AND INFORMATION MANAGEMENT REQUIREMENTS
(COVERED AND NON-COVERED DATA)

Article 1 – Data, Information and Intellectual Property Ownership Rights

The University or the Federal Government own and retain all rights to data and information generated by, stored by, or otherwise provided to the Subcontractor through the Service as described in the Subcontract (collectively hereinafter "University Data"). Unless the University Data is "Covered Data" as that term is defined in *Article 4 - Access to Information Characterized as Covered Data*, below, it is referred to herein as "Non-Covered Data". The Subcontractor shall use University Data only in the course of providing the Service to the University. The Subcontractor shall not otherwise disseminate, analyze, read, or claim ownership to University Data in any manner, except as necessary to provide the Service to the University.

Article 2 – Facilities

All facilities used by the Subcontractor to store and process University Data shall adhere to highest industry security standards and be no less protective than the security standards at facilities where the Subcontractor stores and processes its own information of a similar nature. The Subcontractor acknowledges it has implemented and shall maintain at least industry standard systems and procedures to ensure the security, integrity, availability and confidentiality of University Data in order to protect against credible threats of hazards to the security, integrity, availability and confidentiality of University Data and to protect against unauthorized access to or use of University Data.

Article 3 – Data Transfer and Storage

As part of providing the Service, the Subcontractor may transfer, store and process University Data in the continental United States. Unless otherwise agreed to in writing by the University, the Subcontractor shall not transfer, store, or process University Data outside the continental United States.

Article 4 – Access to Information Characterized as Covered Data

4.1 In performance of the Service, the University may provide the Subcontractor access to confidential University information, including, but not limited to, personal information, employee records, health care information, or financial information (hereinafter "Covered Data"). Notwithstanding the manner in which or from whom Covered Data is received, the Subcontractor hereby acknowledges all Covered Data is subject to state, federal or local laws, ordinances, rules or regulations restricting use and disclosure of such information, including, but not limited to the following:

- California Information Practices Act (California Civil Code Section 1798 et seq.);
- California Constitution Article 1, Section 1; and Gramm-Leach-Bliley Act (Title 15, United States Code, Sections 6801(b) and 6805(b)(2)) [applicable to financial transactions];
- Family Educational Rights and Privacy Act (Title 20, United States Code, Section 1232g) [applicable to student records and information from student records];
- Privacy Act of 1974 (Title 5, United States Code, Section 552a) [pertaining to personal information];
- Health Insurance Portability and Accountability Act of 1996 (Title 42, United State Code, Section 201) [applicable to health care information].

4.2 The Subcontractor shall maintain the privacy of, and shall not release, Covered Data without full compliance with all applicable state and federal laws, University policies, and terms and conditions of the

Government Cloud Approaches

- (1) Marketplace and Procurement Model
  - Procurement framework for purchasing solutions from external providers (CSPs) in a defined marketplace (e.g. G-cloud, US FedRAMP/GSA).
- (2) Resource Pooling Model
  - Common infrastructure or platform accessible by many governmental entities creating a “pool” of resources where agencies can create applications (example: Sara Network, Spain).
- (3) Standalone Applications Model
  - Creating or “cloudifying” existing applications at the individual agency level (e.g. storage)

G-Cloud (UK)

- Marketplace and procurement model
- Goal is to create an easy method for public sector buyers to obtain cloud
  - Procurement tenders for cloud every 6-9 months
  - Short-term agreements intended to meet EU procurement requirements

Uses two main contracts

- (1) Framework Agreement and
- (2) Call-off Contract
  - Using Suppliers terms
  - Maximum length of contract is 2 years

GOV.UK
Digital Marketplace

FedRAMP
Federal Risk Authorization Management Program

- Government-wide standard for federal agencies adopting cloud
- “Do once, use many times” framework

Government specific “concrete” procurement problems

- Bidding and procurement processes
  - “Pay-for-use” or “Pay-as-you-go” arrangements rather than fixed prices—may even violate procurement laws
  - Procurement contracts focused on either software or hardware—some cloud services (SaaS) fall inbetween
  - Many frameworks call for CSPs to meet general outsourcing requirements
  - Rigid frameworks/timeframes
- Local Storage Requirements (Archives etc.)
- Culture of government IT
- Some required standards (ISO etc.) unavailable for cloud computing

Broader policy issues

- Availability of services when gov't becomes dependent on a third-party (email, medical journals etc.)
  - Delegation and duty to citizens
- Transparency, accountability, legitimacy
  - Compliance with FOIA?
- Loss of competence/management over strategic resources
  - Long-term planning/cyber security etc.
- Competition/ Cloud Market
- Data sovereignty and control over information assets (census, health data etc.)

Definitional Problems

- Many agencies failed classify services as “cloud computing” under the NIST (or internal definitions)
- Department of Energy (DoE)
  - Over $30 million in cloud contracts—but did not properly classify them
  - DoE listed 44 services as “cloud” audits found 130
- Not defining services as “cloud” resulted in a failure to apply FedRAMP and other controls

Non-Disclosure Agreements (NDAs)

- Many US contracts did not contain required NDAs
- Other agencies had an NDA with the primary contractor, but the clause did not flow down to subcontractors
- “Release to one release to all” rule
  - Limited ability to object to release of procurement sensitive materials under FOIA

Service Level Agreements (SLAs)

- Performance requirements (availability "uptime" etc.)
  - SOW: What has to be accomplished
  - SLA: How well
- Lack of standardized or model SLAs in the US and Europe often cited as a barrier
  - ISO/IEC 19086-1:2016 Service level agreement (SLA) framework
  - EU Projects
  - Codes of conduct
  - EC C-SIG

Service Level Agreements (SLAs)

- Federal agencies are required to:
  - **(1)** Obtain SLAs providing specific guarantees
  - **(2)** Have a means to measure performance
  - "Credible consequence" for failure to meet SLAs
- Many US federal agencies failed to include SLAs or other performance metrics.
  - EPA paid $2.3 million for services that were not performed
- Very difficult to hold CSPs liable/show breach for poor performance without SLA
- Subject to "good faith"

Responsibilities of Partners and Subcontractors

- Often many layers/partners providing a cloud service
- Federal Agencies are required to have in place “back-to-back” or “flow down” contracts
- Prior approval/control over subcontractors
- Prevents accountability from being lost in the supply chain

Apple sued for not disclosing that 'iCloud storage' relies on third-party cloud services

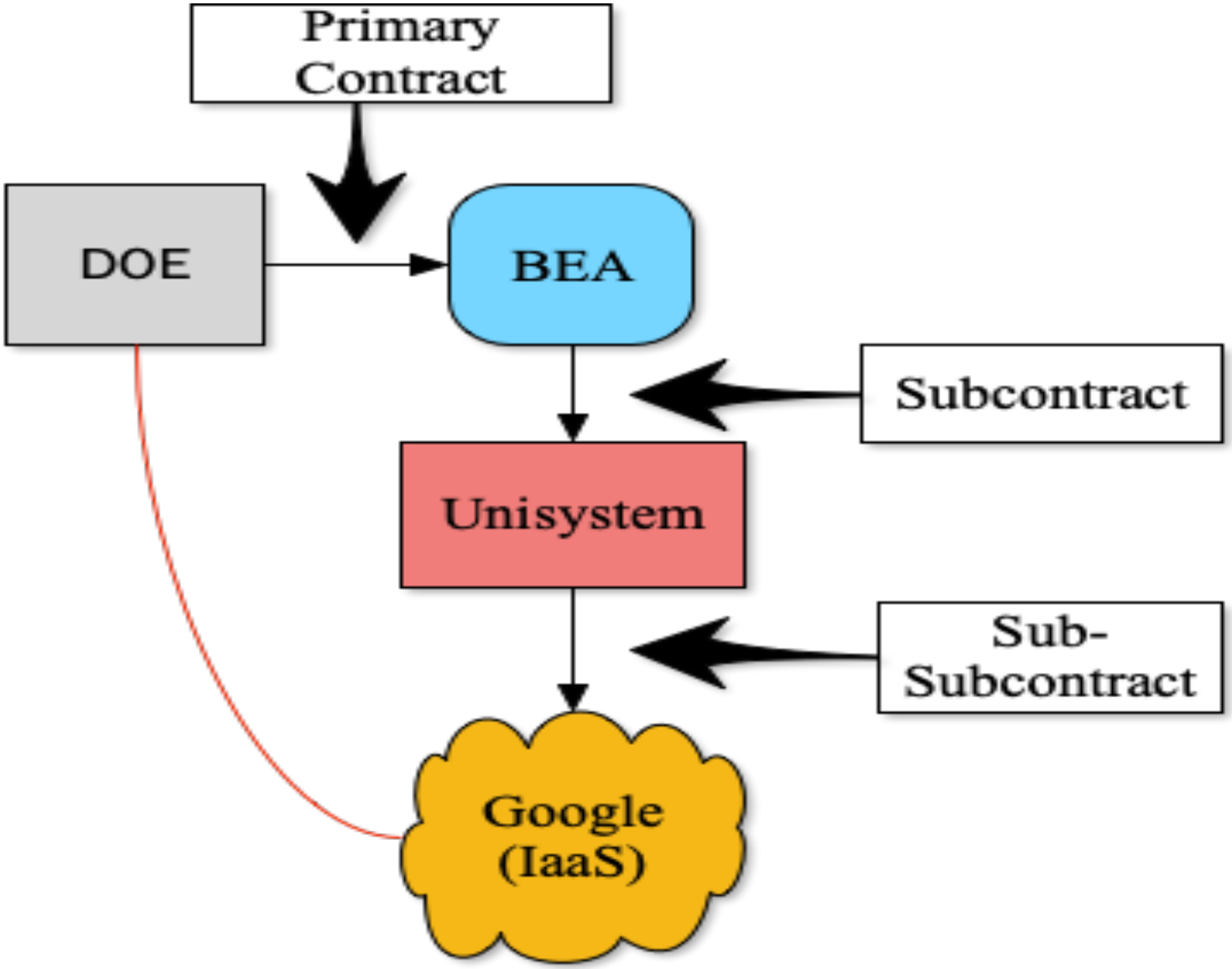
Two iCloud users have filed a complaint, charging they paid the "Apple premium" for cloud storage under the presumption that Apple would store their data on its own servers.

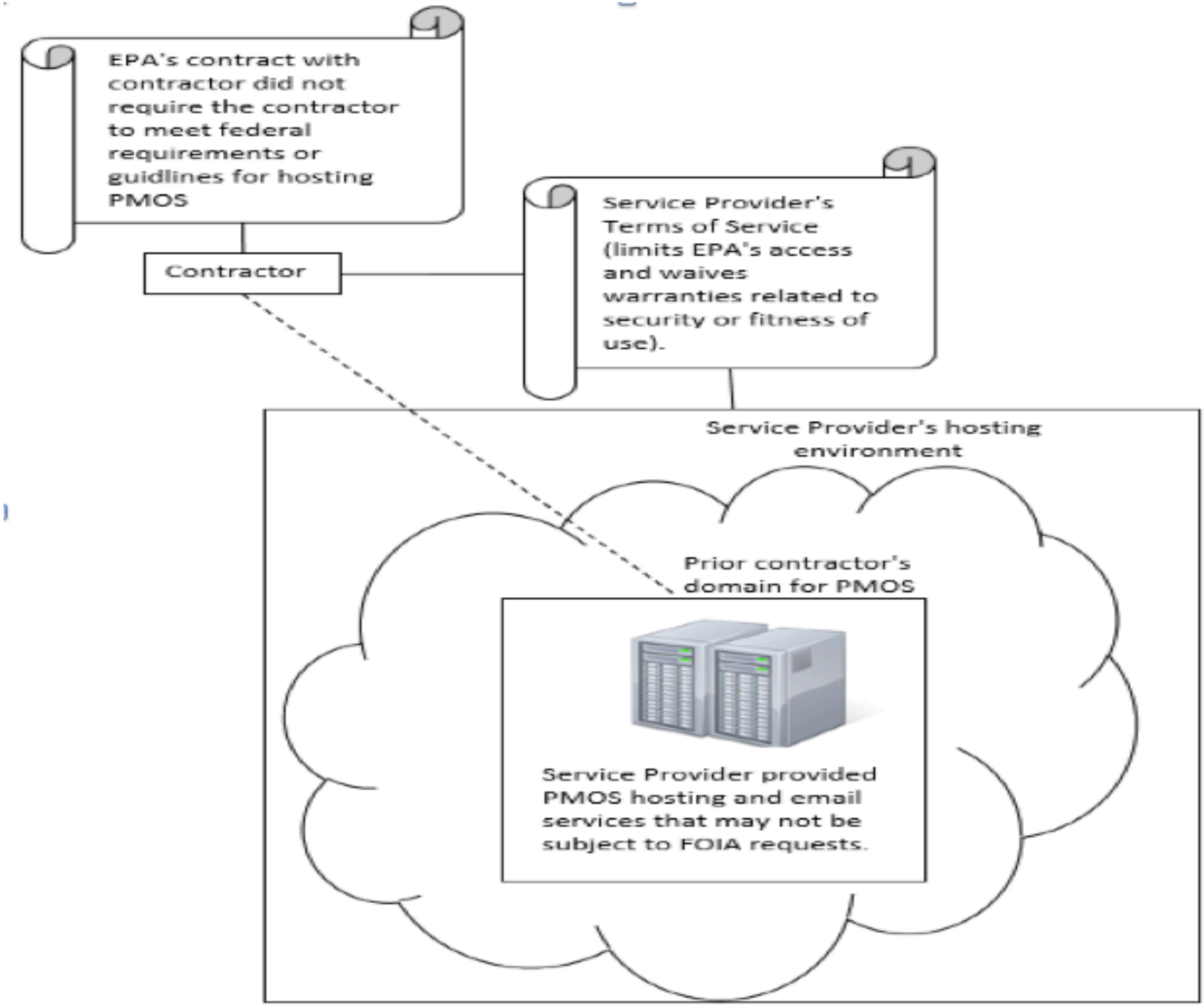
By Stephanie Condon for Between the Lines | August 15, 2019 -- 17:16 GMT (10:16 PDT) | Topic: Cloud

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANDREA M. WILLIAMS AND JAMES STEWART, On Behalf of Themselves And All Others Similarly Situated, Plaintiff, v. APPLE, INC., Defendant.	**No.** **CLASS ACTION COMPLAINT** **Class Action** **Jury Trial Demanded**


Primary Contract
DOE
BEA
Subcontract
Unisystem
Sub-Subcontract
Google (IaaS)


EPA's contract with contractor did not require the contractor to meet federal requirements or guidlines for hosting PMOS
Contractor
Service Provider's Terms of Service (limits EPA's access and waives warranties related to security or fitness of use).
Service Provider's hosting environment
Prior contractor's domain for PMOS
Service Provider provided PMOS hosting and email services that may not be subject to FOIA requests.

EPA Terms of Service (TOS)

- Access to data, warranties, indemnification, choice of law and forum, variation clauses etc.
- EPA contract limited primary contractor (prior consent) but allowed for:
  - "…unilateral changes to the terms of the service agreement by posting to the subcontractor's website."
- EPA did not have terms requiring sub-contractors to preserve data etc.

Dept. of Labor (DOL) and Portability

- GCS provided a SaaS solution for financial management to the DOL
  - GCS was processing over $170 billion worth of DOL transactions
- GCS raided by FBI for immigration (among other) violations
- FBI investigation resulted in GCS's bankruptcy

DOL and Portability (2)

- DOL was “locked-in” to its CSP
- Contract did not require GCS to return data in a usable form and was unclear on data ownership.
- DOL could not perform the function without GCS
- Result: DOL had to buy its own data from GCS (or its creditors) for $23.5 million
- Unclear "end of relationship" terms

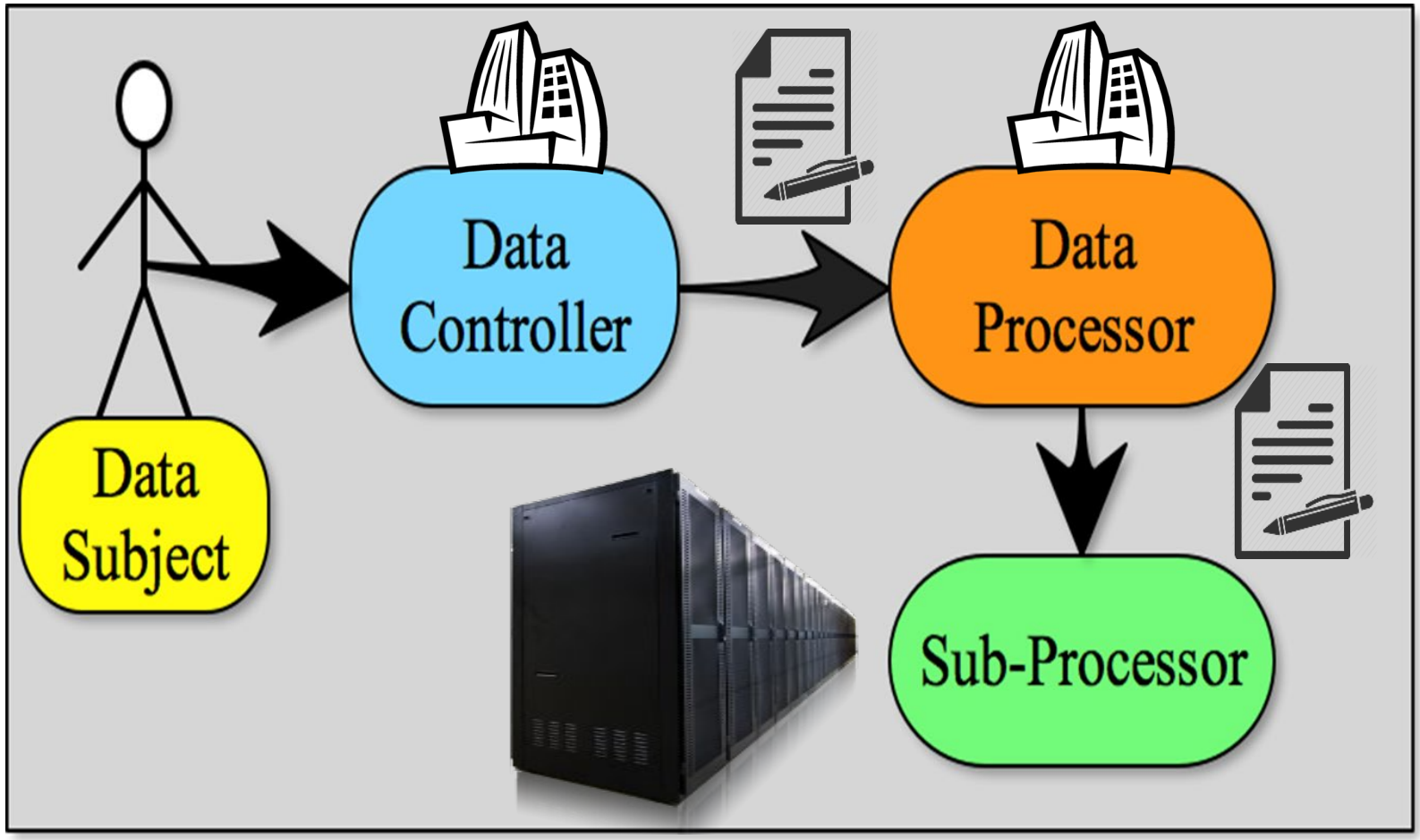
Mandatory Rules/ Immutable Defaults

Limits to the 'private legislation' that may impact cloud computing contracts:

- Competition law
- Tax law
- Tort law
- Employment law
- Consumer protection
- Data protection law
- Other areas with strong public policy considerations

In B2B and B2G agreements focusing on contractual matters, a high level choice/freedom to choose terms.

Responsibility for data under the GDPR



GDPR and contract terms

- “[c]ustomer agrees that….Google is merely a data-processor”
- “…the Parties agree to be bound by the Standard Contractual Clauses *with the following modifications* that are required to take into account the special requirements of cloud computing and its uniform offering to all customers”.

Public Sector Directive 2014/24/EU provides the following requirement:

(77) When drawing up technical specifications, contracting authorities should take into account requirements ensuing from Union law in the field of data protection law, in particular in relation to the design of the processing of personal data (data protection by design).

Looking forward…

Thank You!

- Questions?
- Comments?