LUCENTUM
Privacy and Technology Law

Supply Chain Security: Outsourcing and other business models

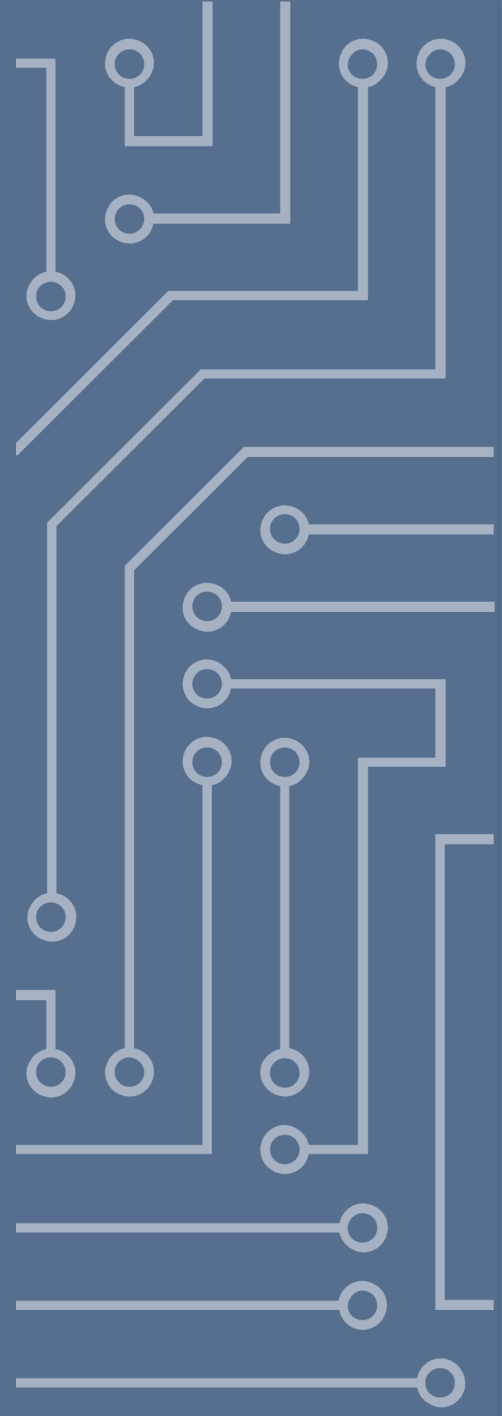
A Software Law Perspective

Tobias Edvardsson

2024-11-13

Overview

- Introduction
- Common Business Models
  - In-house
  - License and Support
  - Open Source
  - Subscriptions and AD/AM
  - Outsourcing
- Cloud Computing
  - Cloud Corporations
- Legal Challenges



Introduction

LUCENTUM
Privacy and Technology Law

The Data Storm

Year	Global Internet trafic
1992	100 GB per day
1997	100 GB per hour
2002	100 GBps
2007	2,000 GBps
2014	16,144 GBps
2020	74,074 GBps

Source: Cisco VNI, 2019

The Compliance Storm

- EU Data Act
- EU Data Governance Act (DGA)
- EU NIS 2 Directive (NIS2)
- EU Digital Operational Resilience Act (DORA)
- EU Cybersecurity Act (CSA)
- EU Cyber Resilience Act (Proposal)
- EU Cyber Solidarity Act (Proposal)
- EU General Data Protection Regulation (GDPR)
- EU e-Privacy Regulation (Proposal)
- EU AI Act
- EU AI Liability Directive (Proposal)
- EU Digital Services Act (DSA)
- EU Digital Markets Act (DMA)

Information Security

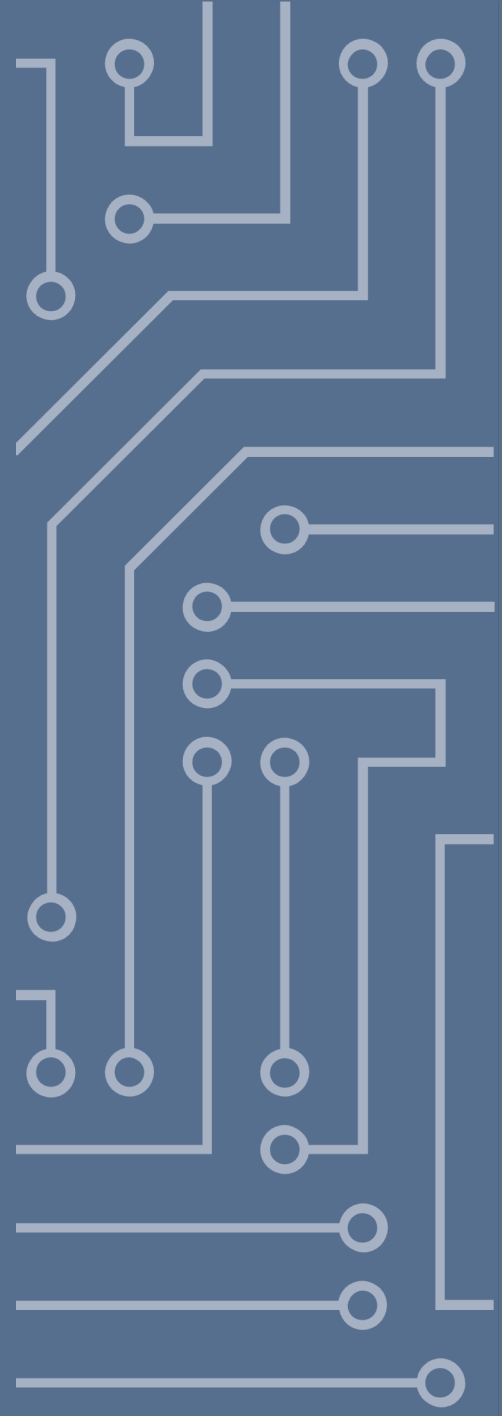
LUCENTUM
Privacy and Technology Law

Aspects of Business

LUCENTUM
Privacy and Technology Law

Key Takeaway #1

Business Models have a direct impact on both Information Security and Legal matters



Global IT Market 2023 (estimate)

Global IT Market

USD 4,723,215,000,000

Global IT Service

USD 1,420,905,000,000

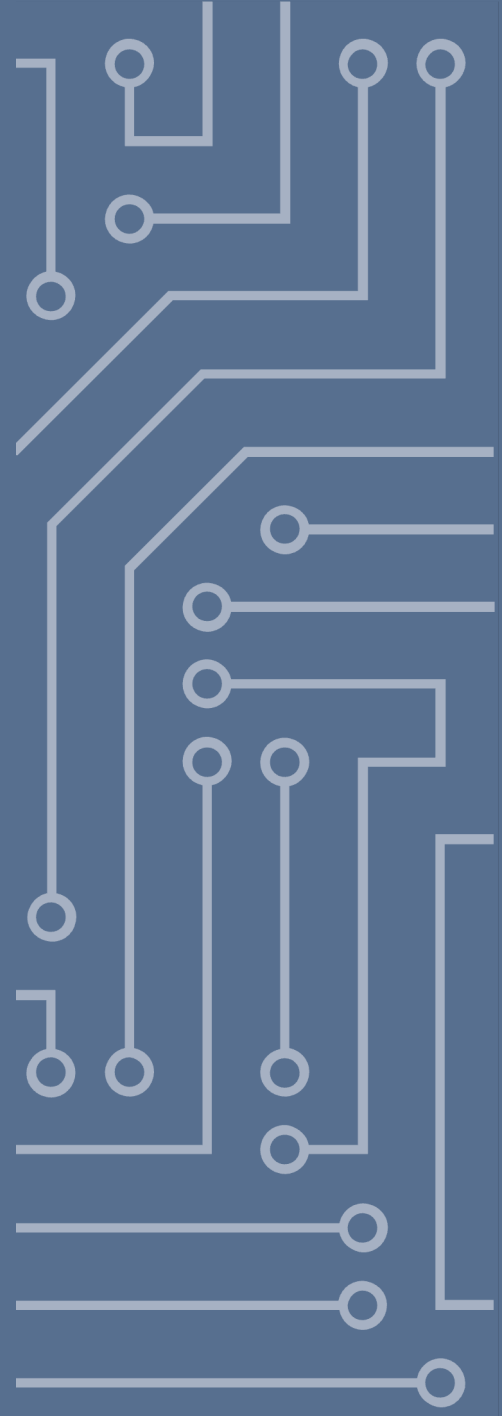
Source: Gartner

Global Data Market

Almost immeasurable

(or USD 27.3 billion, depending on definition)

Source: Statista

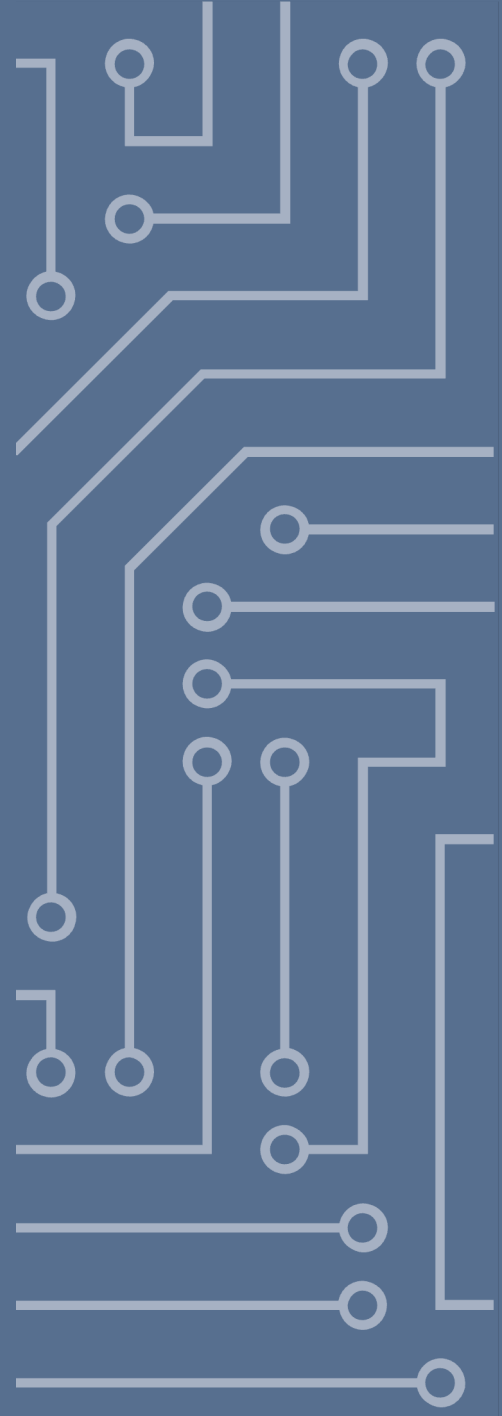


Information Security

Information security is the protection of the **confidentiality**, **integrity**, **authenticity**, **availability** and **utility** of information (data).

Key Takeaway #2

Information Security must be regarded from both a positive and a negative perspective

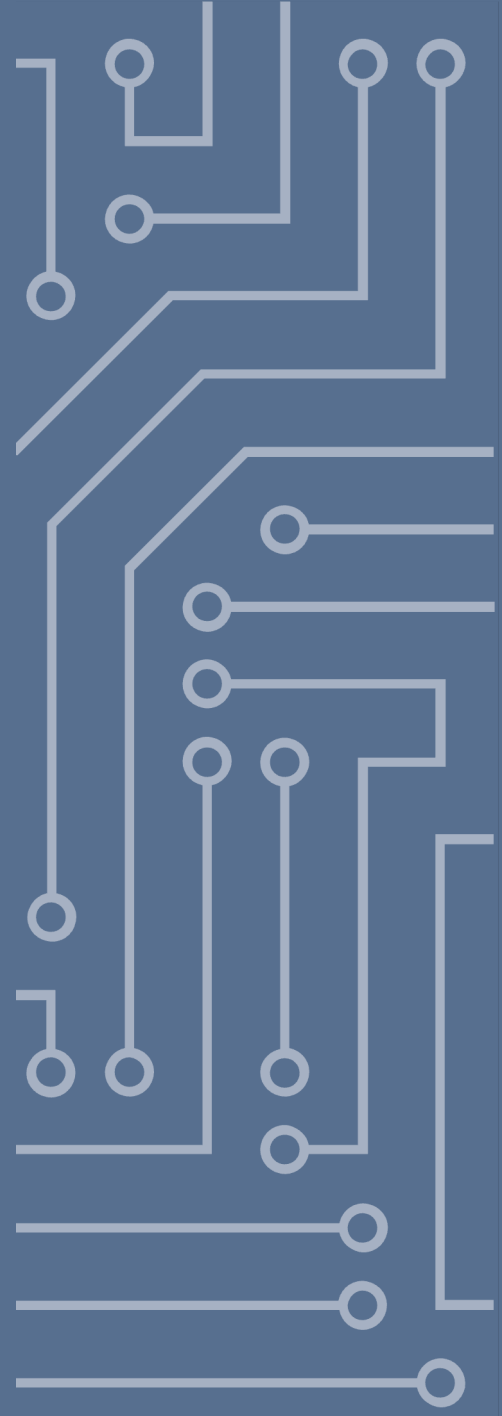


Key Takeaway #3

From a philosophical perspective continental contract law and information security have the same foundation:

Ein Tier heranzüchten, das versprechen darf

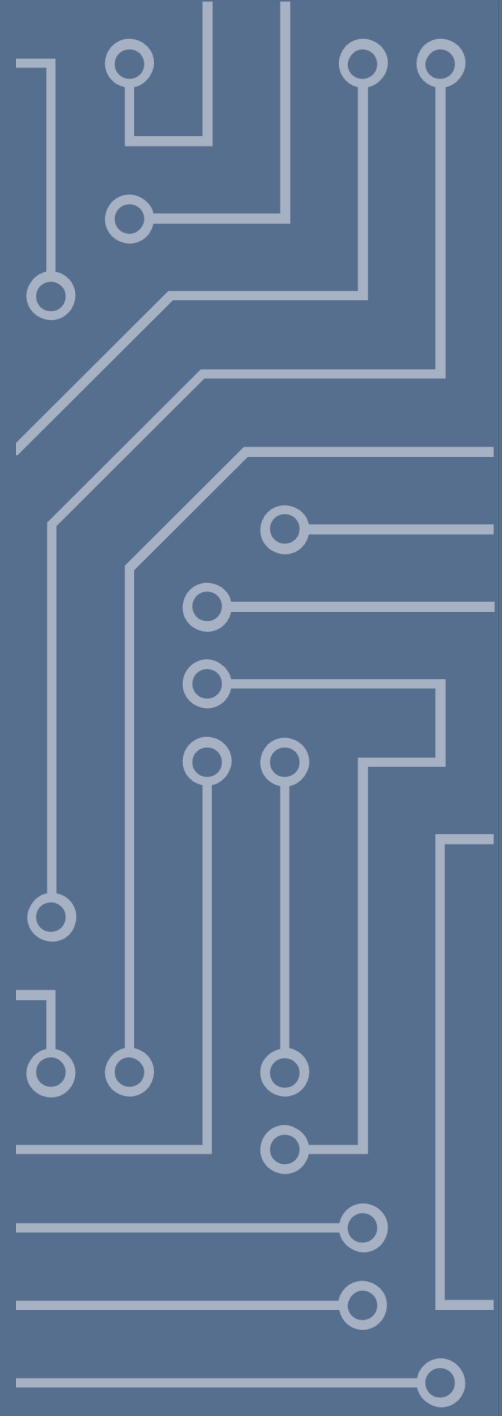
- Nietzsche, Friedrich, Zur Genealogie der Moral



LUCENTUM
Privacy and Technology Law

Key Takeaway #4

There is no absolute security, there is always a balance between security, value and cost



Information Security – Example

Heartbleed

Information Security – Example

Risk Assessment

LUCENTUM
Privacy and Technology Law

Risk Assessment

RISK ASSESSMENT		Consequence				
		Insignificant (1) No injuries / minimal economical loss	**Lesser (2)** First Aid necessary / Mid range economical loss	**Average (3)** Medical Aid required / High economical loss	**Larger (4)** Hospital Aid required / Larger economical loss	**Catastrophical (5)** Deaths / Enormous economical loss (Bankruptcy)
Likelyhood	**Almost Certain (5)** Often / Once a week	**Mid (5)**	**High (10)**	**High (15)**	**Catastrophical (20)**	**Catastrophical (25)**
	Likely (4) Likely to happen / Once a month	**Mid (4)**	**Mid (8)**	**High (12)**	**Catastrophical (18)**	**Catastrophical (20)**
	Possible (3) Could happen / Once a year	**Low (3)**	**Mid (6)**	**Mid (9)**	**High (12)**	**High (15)**
	Unlikely (2) Has not happened but could / Once in a decade	**Low (2)**	**Mid (4)**	**Mid (6)**	**Mid (8)**	**High (10)**
	Rare (1) Possible but only in special circumstances / Once in a century	**Low (1)**	**Low (2)**	**Low (3)**	**Mid (4)**	**Mid (5)**

Example: The Electrical Grid

- First documented hacker attack in 2015, when Russian state-controlled hackers managed to cut electricity in Ukraine for hundreds of thousands of people for six+ hours in the middle of the winter. It was repeated in 2016.
- That operation was called Dragonfly 1.0, and later followed Dragonfly 2.0. The latter managed to affect a handful US grids, one in Turkey and two in Ukraine.
- Five confirmed hacker attacks followed the next 24 months.

Largest threats

Attacker	Number of successful attacks
Squirrels	879
Birds	434
Snakes	83
Racoons	72
Rats	36
Martens	22
Beavers	15
Jellyfish	13
Hackers	5

Example: The Electrical Grid

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels."

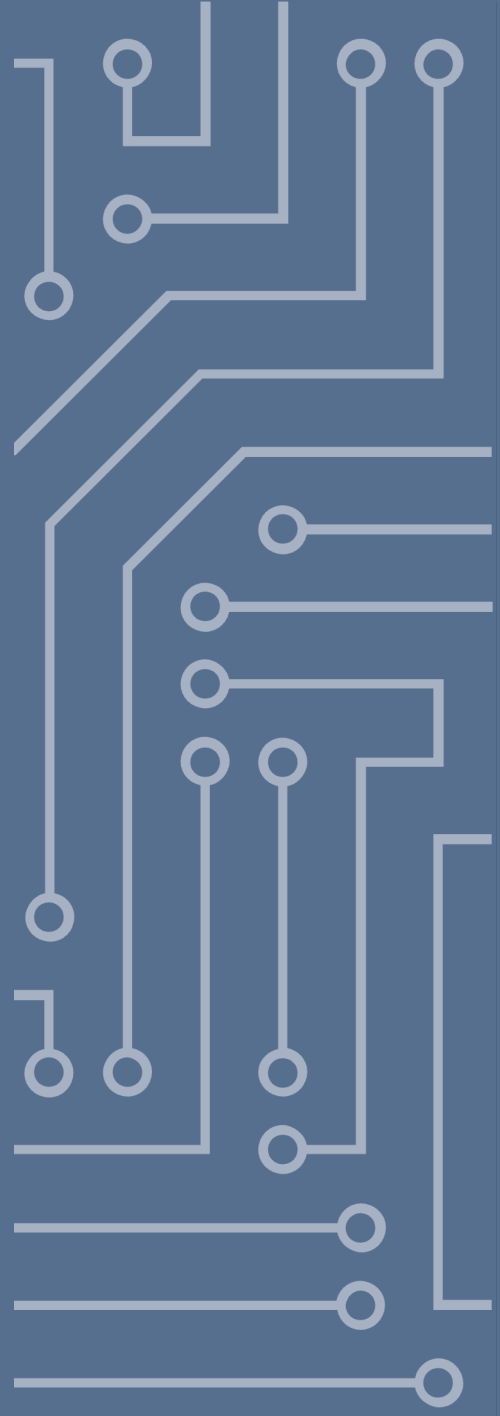
– John C. Inglis, Former Deputy Director, National Security Agency 2015.07.09

Key Takeaway #5

Real threats and popular perception often stand far apart, you job is to correctly assess the real risks

Key Takeaway #6

What is to be defined as a real threat changes a lot over time.



Example: BCP and DRP

- Business Continuity and Disaster Recovery
- In the 1990's, focus was on loss of electricity or loss of data
- After 9/11 and Fukushima Daiichi, things changed
- Now focus is on how to carry on if the office simply does not exist, many employees are dead, or the area of business is inaccessible

Why Business Models?

LUCENTUM
Privacy and Technology Law

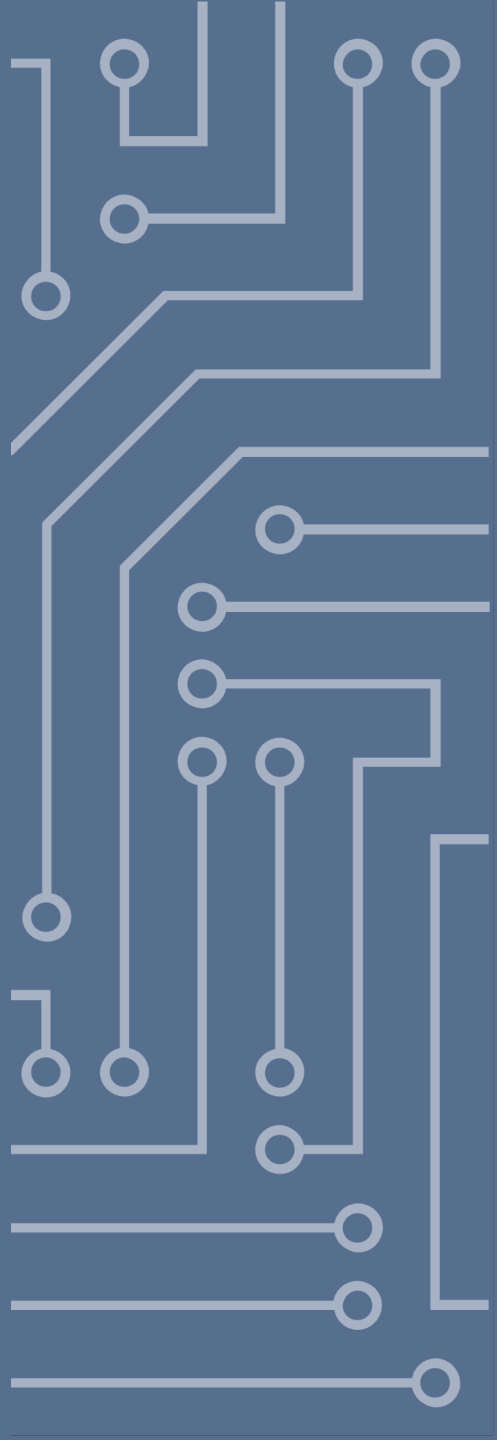
Purpose of Business Models

- Defining the Chain
- Provide Contents
- Defining the Market
- Determining Company Actions
- Understanding Positioning And Competition
- Mitigate Risks

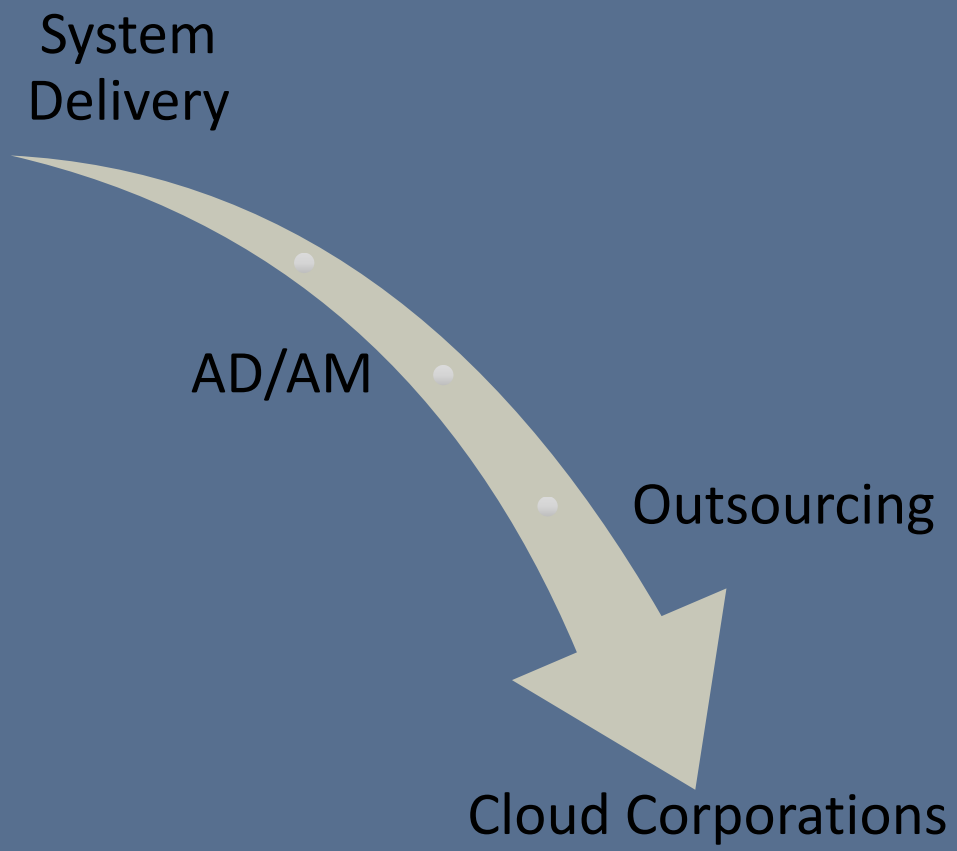
Purpose of Business Models and Contracts

Adherence to a standard business model has several benefits:

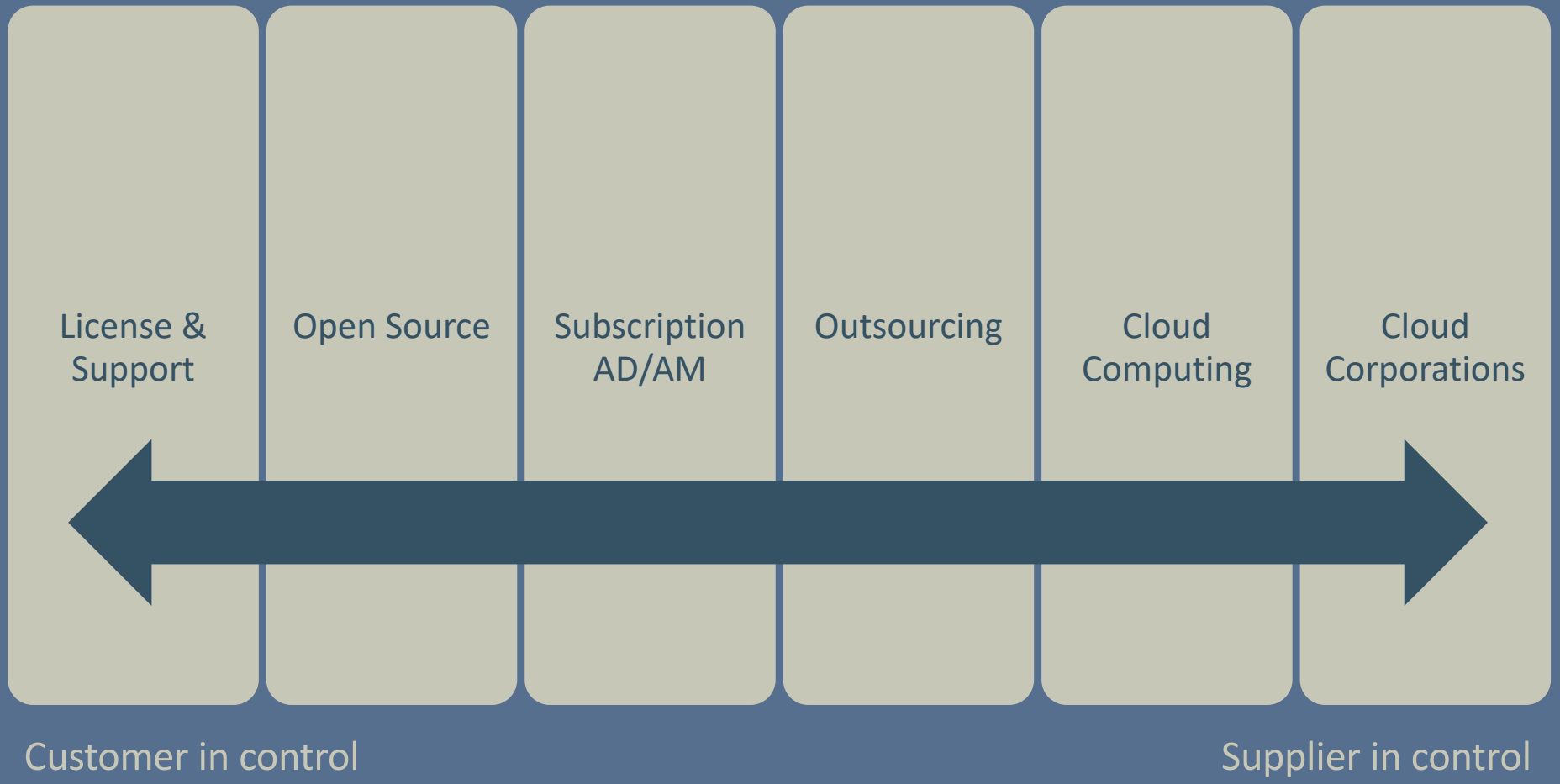
- Clear allocation of responsibility
- Clear allocation of risks
- Clear principles of roles for the various parties
- Standardised revenue and cost structure



Control Progression



Our Business Models



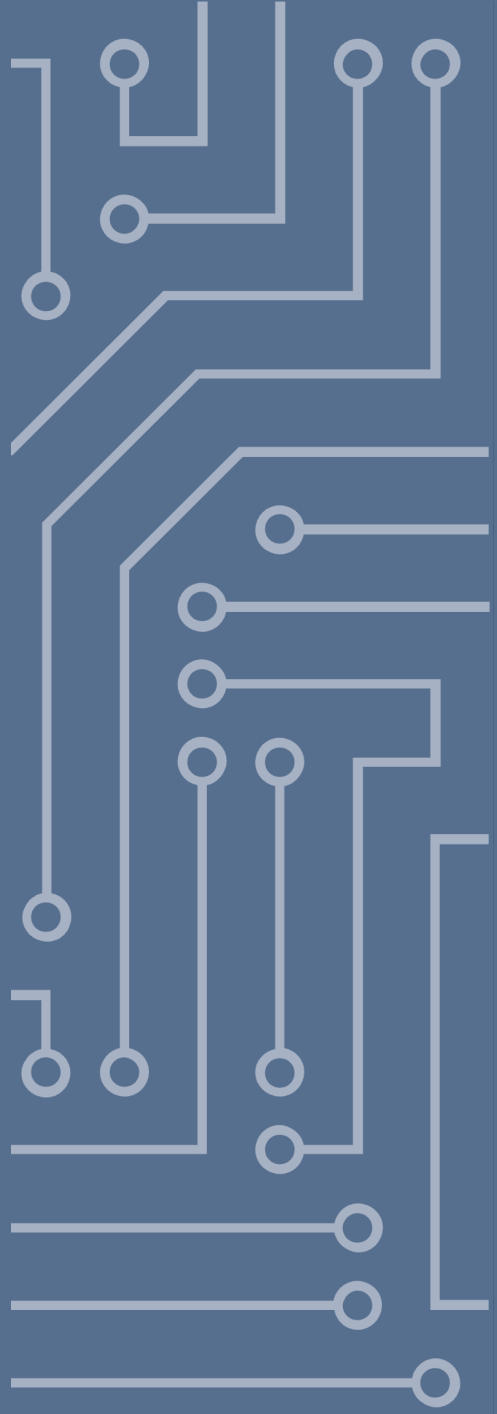
LUCENTUM
Privacy and Technology Law

Common Business Models

LUCENTUM
Privacy and Technology Law

In-House IT and Development

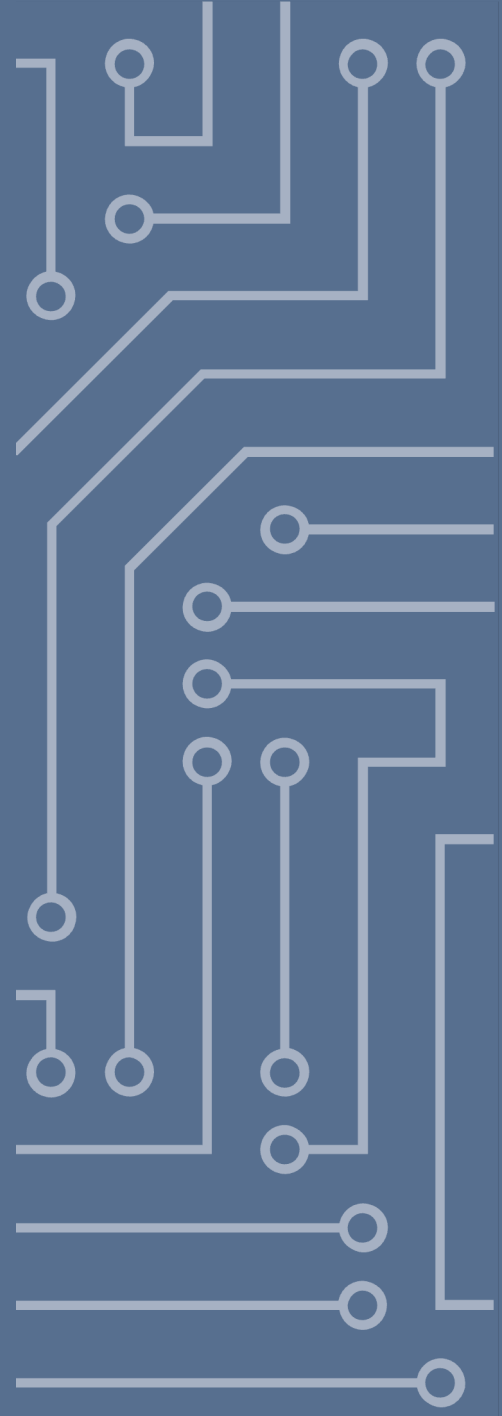
- Own employees
- LTC
- Consultants



License and Support (1/3)

- There are several sub-types to this business model, such as:
  - COTS (Commercial of the Shelf)
  - System Development
  - System Delivery

- Two primary development method categories:
  - Waterfall
  - Agile



License and Support (2/3)

- The software is usually installed in the Customer's premises
- License (a legal concept) is in focus conferring limited rights
  - Limits in time
  - Limits in use
  - Limits in geography
- There might be both Support and Maintenance contracts connected to the license

License and Support (3/3)

- Benefits include:
  - Control of the Environment
  - Control of Supplier's Involvement
- Risks include:
  - Dependency on a Supplier for Continued Improvement
  - Dependency on Internal Resources for Everything Else

Open Source (1/4)

Open Source Definition by OSI

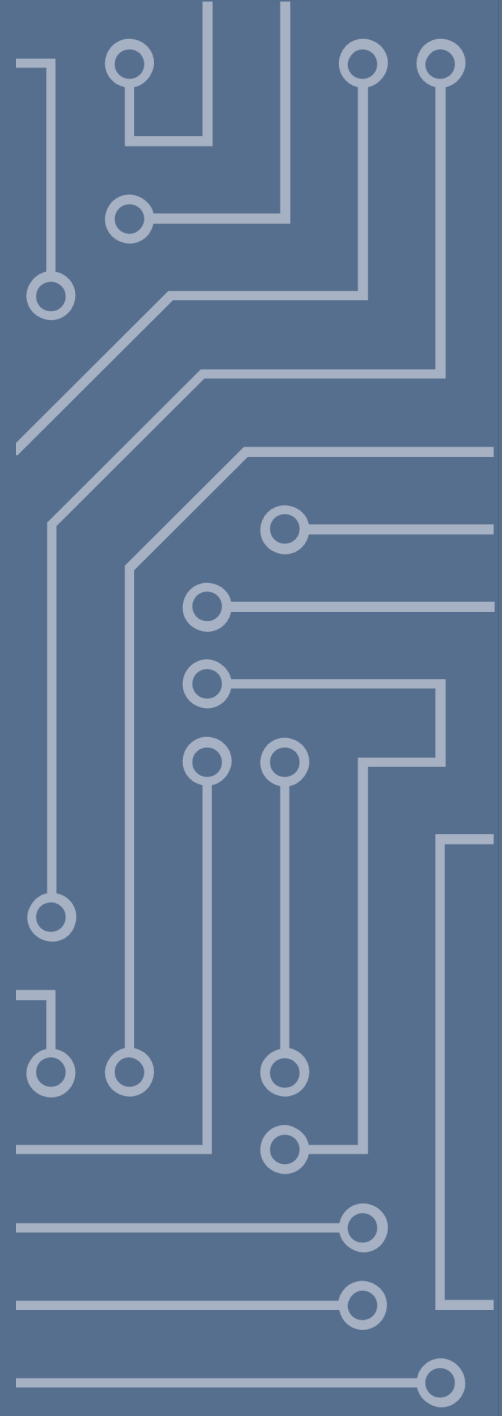
① Free Redistribution
② Source Code
③ Derived Works
④ Integrity of the Author's Source Code
⑤ No Discrimination Against Persons or Groups
⑥ No Discrimination Against Fields of Endeavour
⑦ Distribution of License
⑧ License Must Not Be Specific to a Product
⑨ License Must Not Restrict Other Software
⑩ License Must Be Technology-Neutral

Open Source (2/4)

- There are several business models associated with open source
  - Dual-licensing (as in both open source and proprietary)
  - Delayed open-sourcing
  - Selling professional services
  - Selling support and maintenance
  - Selling of certificates and trademark use
  - Selling software as a service
  - Selling of optional proprietary extensions

Open Source (3/4)

- Strong Copyleft
  - GPL
- Weak Copyleft
  - EPL / MPL / LGPL
- No Copyleft
  - BSD / MIT



Open Source (4/4)

- Benefits include:
  - Less Risk if Supplier Disappears
  - Ability and Right to Alter the Software
- Risks include:
  - IPR Infringement Issues
  - No Single Responsible Entity

Subscription & Application Development / Maintenance (1/2)

- Subscription is the business model where the Customer purchases software through a subscription, often bundling license, support and maintenance
- AD/AM are the business models where the Customer purchases, either software development or software maintenance, or both
- Often structured as bulk hours per year

Subscription & Application Development / Maintenance (2/2)

- Benefits include:
  - Larger Professional Team Handling Development and Support
- Risks include:
  - Dependency on a Supplier
  - Customer Must Have a Clear Plan

Outsourcing

LUCENTUM
Privacy and Technology Law

Outsourcing – Overview

- Basically taking a unit and placing it with a supplier
- Often structured in two transactions:
  - Asset Transfer
  - Service Delivery
- AD/AM is a common area to outsource
- BPO (Business Process Outsourcing) is growing rapidly
  - E.g. outsourcing of salary handling etc.
- Outsourcing can be both tactical and strategic

Outsourcing – What?

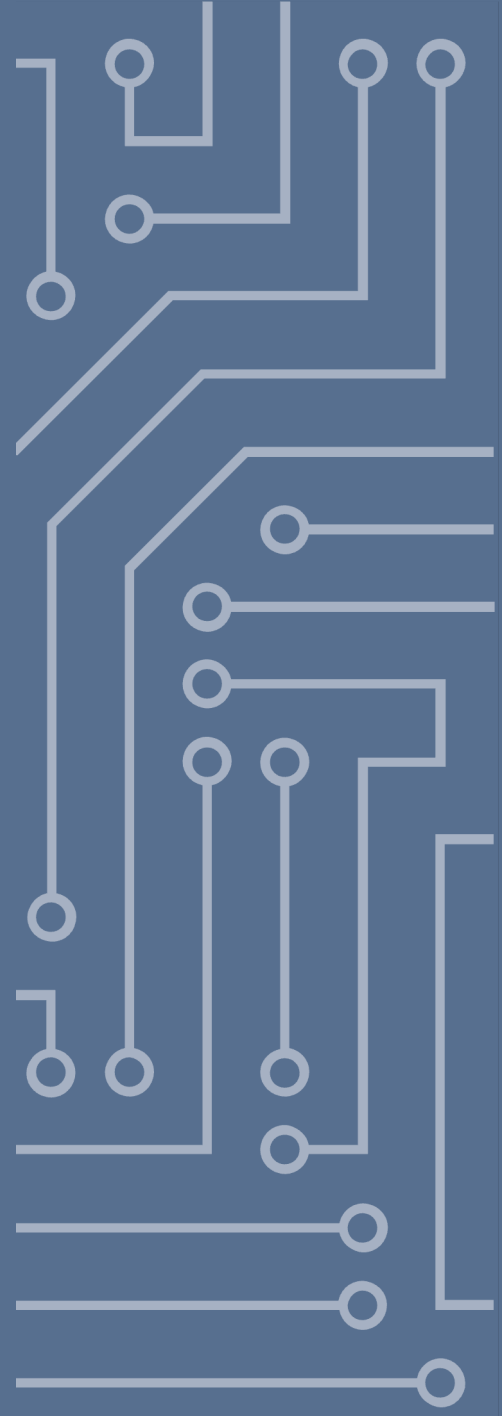
1. Category of IT contracts (for our purposes)
2. Business model for supply of functions (customer)
3. Business model for provision of services (supplier)
4. Partnership Model
5. Way to build corporations

➢Outsourcing v. Sourcing?

Outsourcing – Models

Common Models

- Staff augmentation
- Project-based Outsourcing
- Out-tasking/Contracting
- Managed Services
- Offshoring

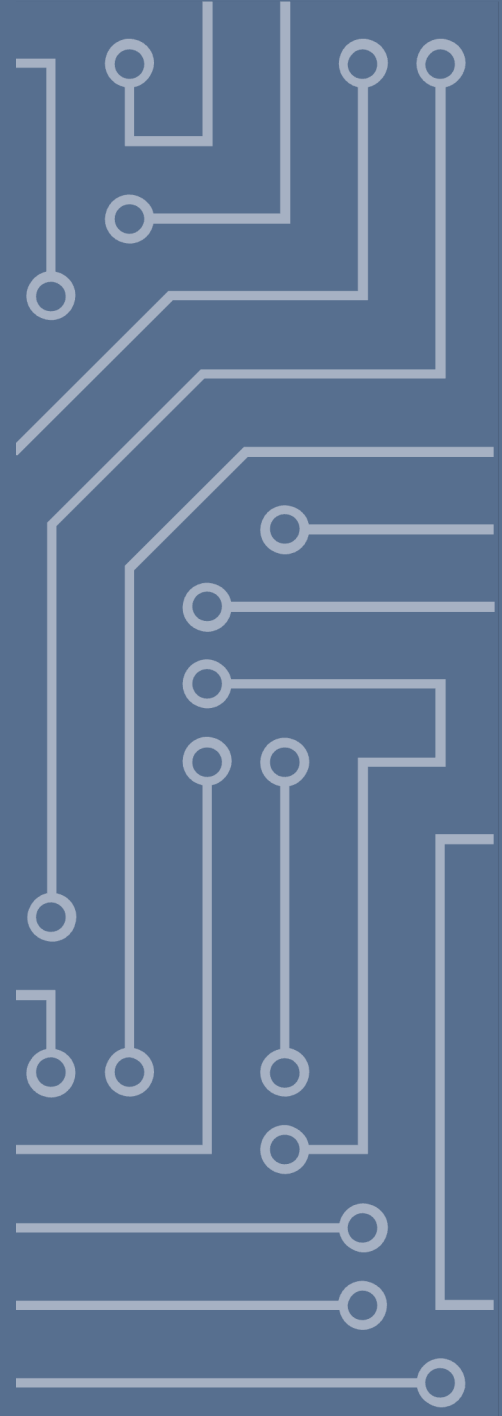


Outsourcing – As IT Contracts

- Long term agreements
- Often two contracts in one deal
  - Asset Transfer Agreement
  - Master Services Agreement
- Often Complex Contracts

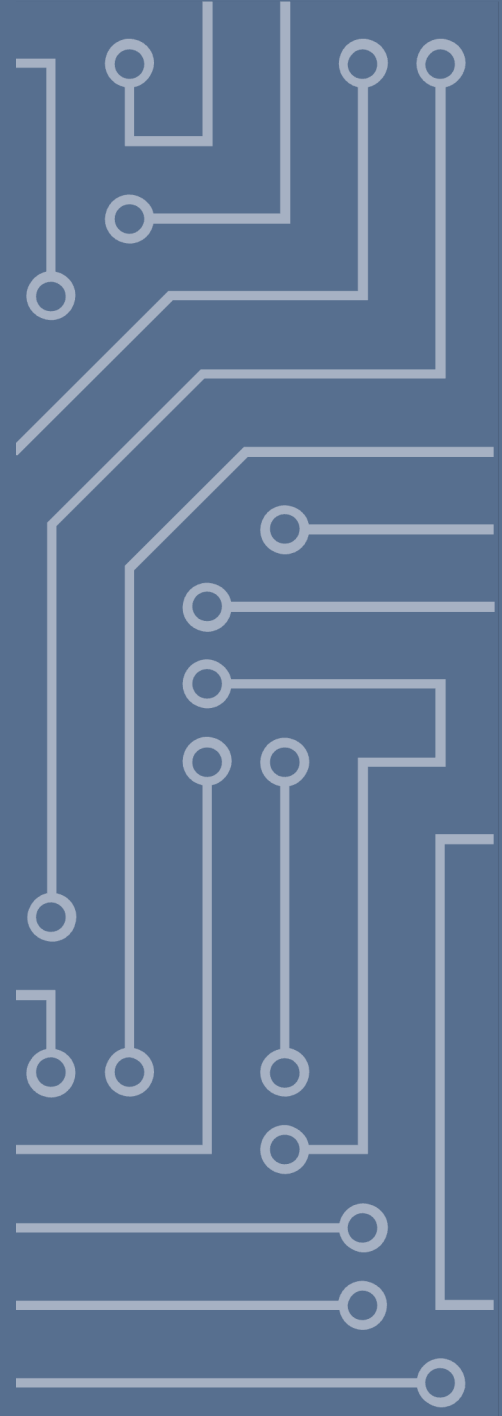
Outsourcing – Benefits

- Customer able to focus on core business
- Larger Professional Team Handling Development and Support
- Economies of scale could reduce cost
- Off-shoring could reduce cost
- Opex instead of Capex

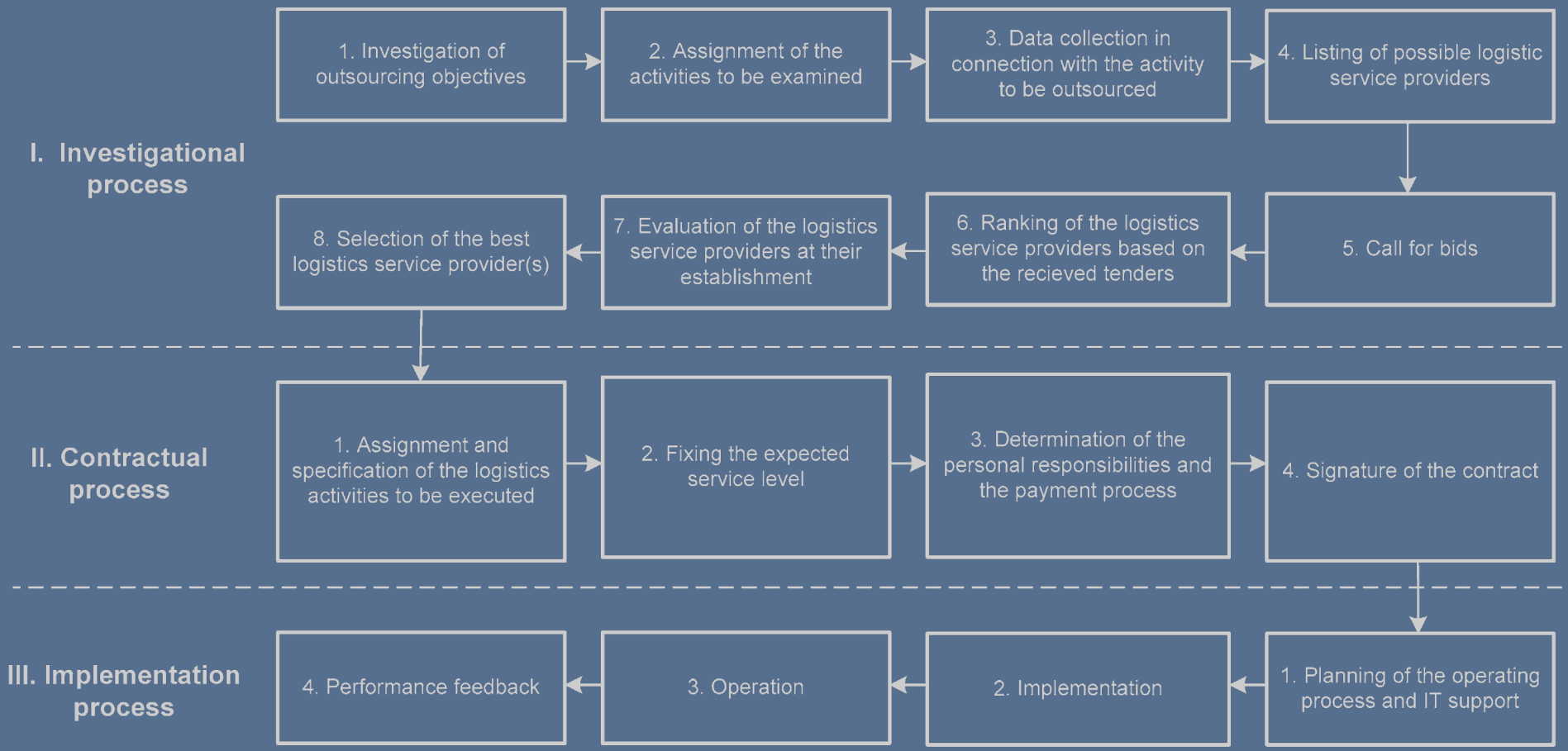


Outsourcing – Risks

- Dependency on a Supplier
- Reduced in-house knowledge base
- Decreased control over vital functions
- Security risks
- Regulatory and Compliance



Outsourcing – Process



LUCENTUM
Privacy and Technology Law

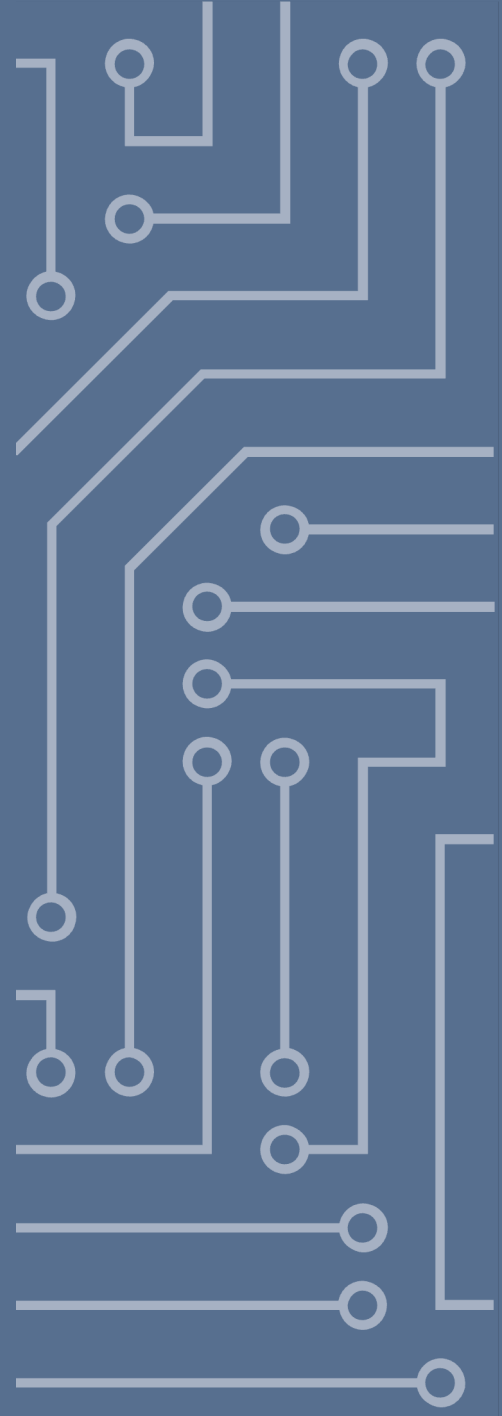
Cloud Computing

LUCENTUM
Privacy and Technology Law

NIST's Cloud Computing Definition (1/3)

<u>Essential Characteristics</u>

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

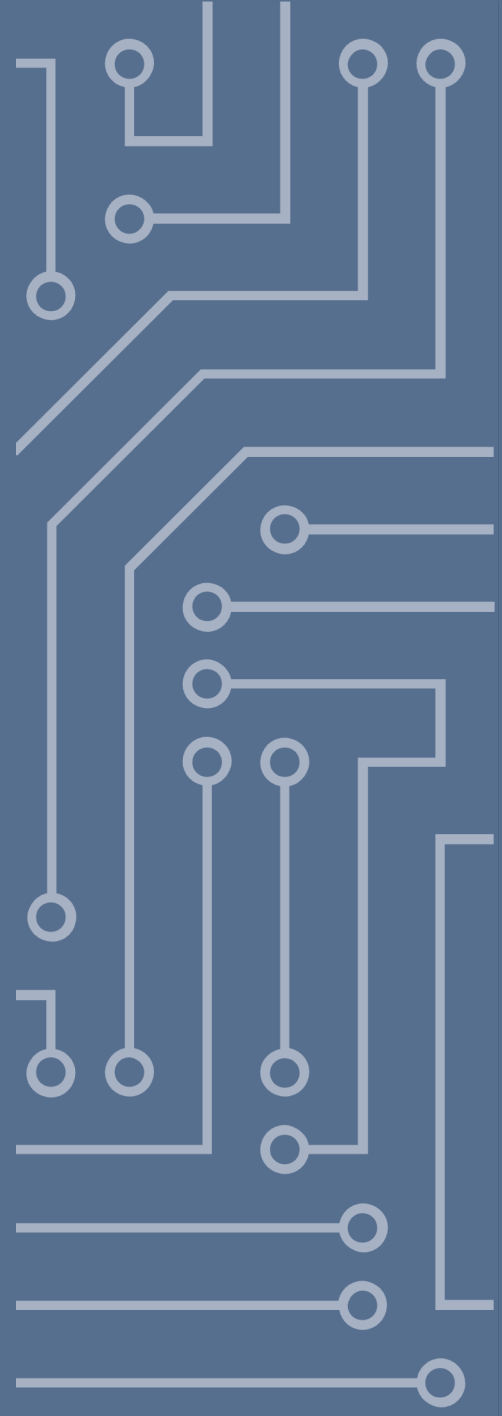


NIST's Cloud Computing Definition (2/3)

Service Models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

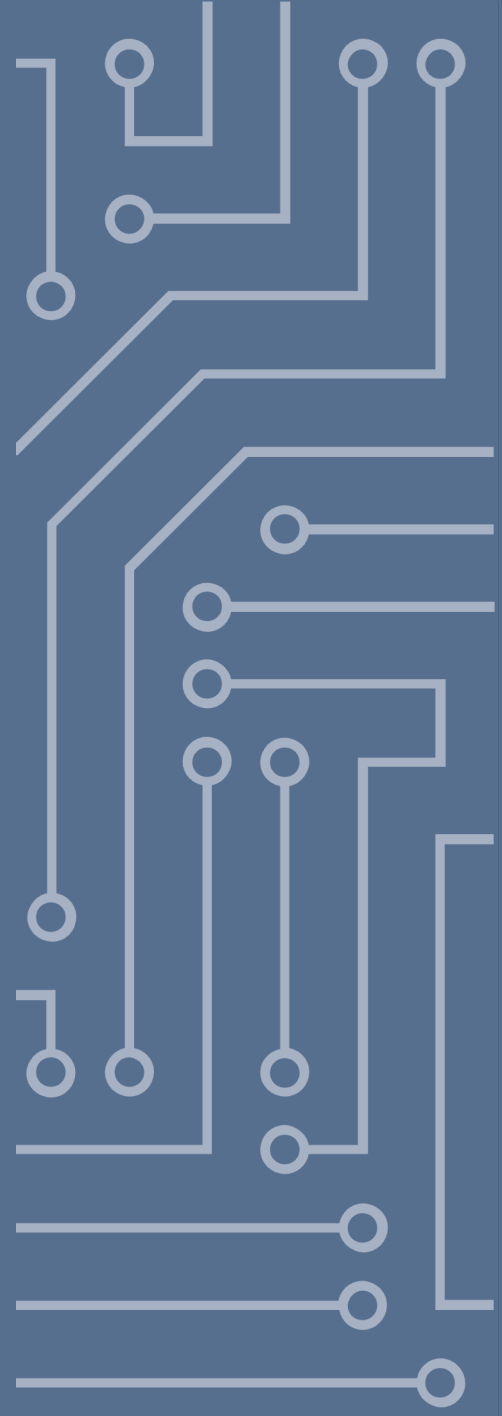
- X as a Service



NIST's Cloud Computing Definition (3/3)

<u>Deployment Models</u>

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud



Primary Risks in Cloud Computing

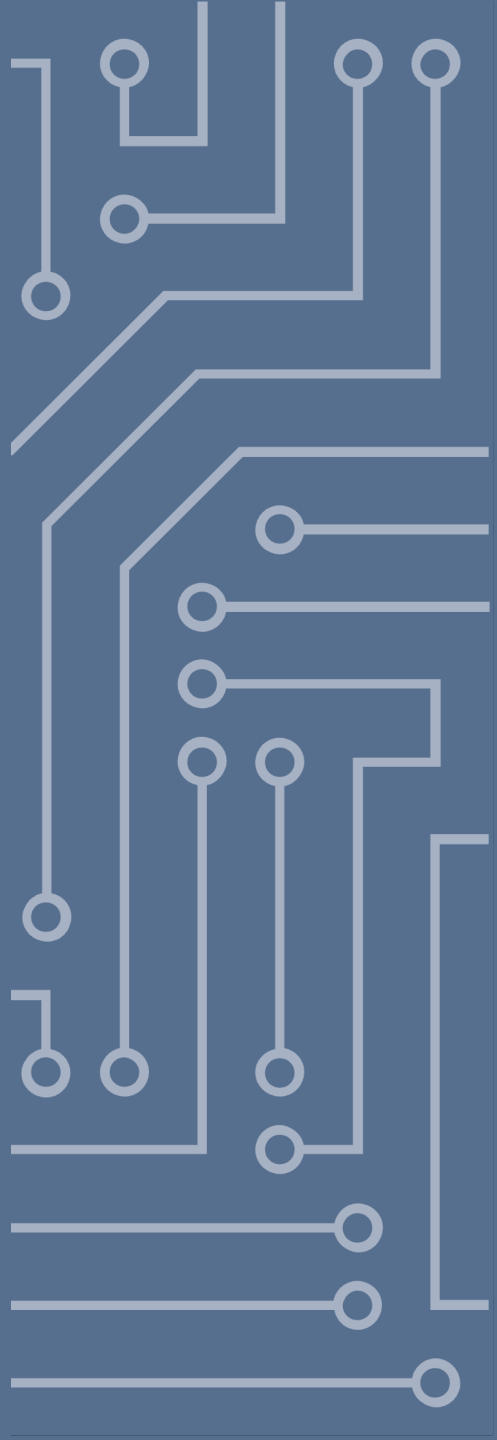
- The Cloud Service does not fulfil our needs (utility)
- The Cloud Service does not perform as needed (warranty)
- Lock-In Effects (the Hotel California syndrome)
- Loss of Data
- Security Issues
- Legal Risks

Benefits and Risk of Cloud Computing

- Benefits include:
  - Larger Professional Team Handling Development and Support
  - “Pay as You Go” Model Might Reduce Cost
  - Elasticity Provides Instant Flexibility
- Risks include:
  - Dependency on a Supplier
  - Regulatory and Compliance

Cloud Corporations

- Building a business through connecting various cloud providers
- Can be very cost efficient in a start up phase
- Scalability can be a complex issue
- Many suppliers can be difficult to track or replace
- Lock-in must be avoided



The Cloud Agreement

LUCENTUM
Privacy and Technology Law

AWS Cloud Contract

1. Use of the Service Offerings
2. Changes
3. Security and Data Privacy
4. Your Responsibilities
5. Fees and Payment
6. Temporary Suspension
7. Term; Termination
8. Proprietary Rights
9. Indemnification
10. Disclaimers
11. Limitations of Liability
12. Modifications to the Agreement
13. Miscellaneous
14. Definitions

AWS EC2 SLA (excerpt)

General Service Commitment
AWS will use commercially reasonable efforts to make the Included Services each available for each AWS region with a Monthly Uptime Percentage of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Services do not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Service Credits
Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for the individual Included Service in the affected AWS region for the monthly billing cycle in which the Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	30%
Less than 95.0%	100%

Central Clauses

- Supplier's responsibility
- Service description
- Service levels
- Third-party applications
- Customer's responsibility
- Price and payment
- Data Protection
- IPR
- Customer data
- Confidentiality
- Security
- Termination of the agreement
- Transitional services
- Liability and limitations of liability
- Choice of law and dispute resolution

Legal Challenges

LUCENTUM
Privacy and Technology Law

Overview of Legal Challenges

- Governing law and jurisdiction
- Processing of personal data
- Intellectual Property Rights
- Rights to and in Data
- Security
- Liability

LUCENTUM
Privacy and Technology Law

Governing Law and Jurisdiction

- Identifying governing law and jurisdiction can be difficult, especially outside of a contract
  - Governing Law = The country or nations laws that will apply to a case
  - Jurisdiction = Court of law or arbitral institute with competence to adjudicate

- In most cases the parties to a contract may decide; however…
- There are instances where the parties are not free to decide
  - E.g. Data Protection Regulations

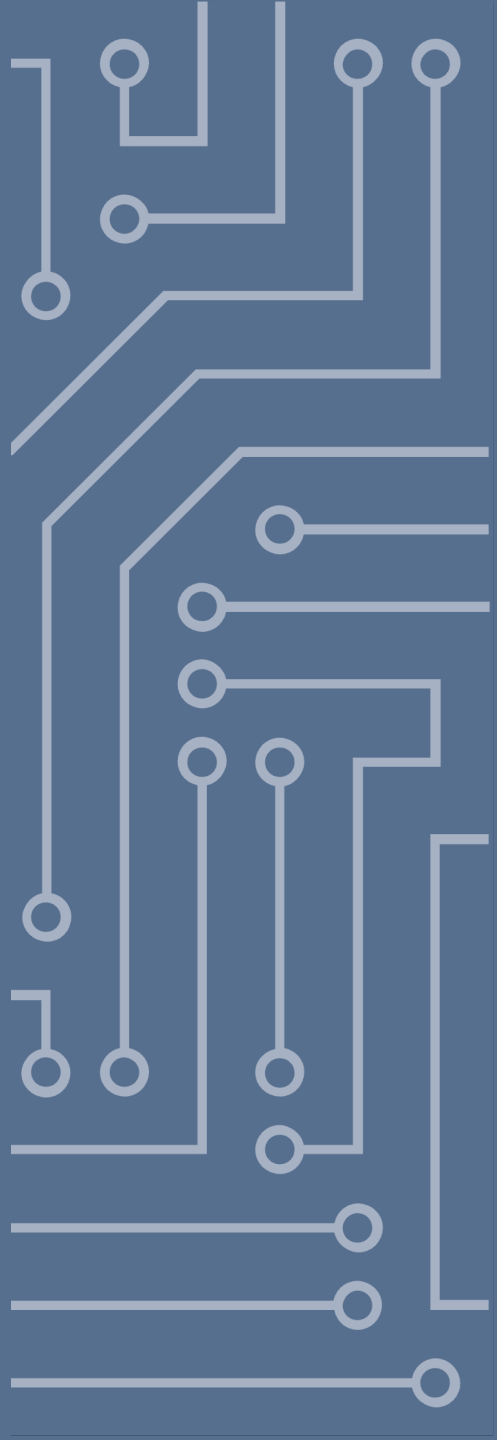
Processing of Personal Data (1/4)

Objectives of the GDPR (Art. 1)

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Processing of Personal Data (2/4)

- Identified as one of the major obstacles for cloud adoption
- The new EU Regulation (GDPR) brings a maximum penalty of 4% of the global turn-over or EUR 20 million (whichever is higher)



Processing of Personal Data (3/4)

Fundamental Rights of Data Subjects

- The right to know if my personal data is being processed, which personal data that is being processed and the purposes for which they are processed
- Certainty that my personal data is only processed based on consents or other defined legal basis
- Certainty that the data controller shall take the technical and organizational information necessary to protect my data
- Safeguards to protect my data from being sent outside the EU, unless I consent or there is clear legal basis

Processing of Personal Data (4/4)

- The Customer is the Data Controller
- The Supplier is the Data Processor
- The Customer is fully responsible for the Data Processing
- The Customer must ensure the protection of the Data Subjects rights through agreement with the Supplier

- The Data Processing Agreement is key
  - It must be in writing [Art. 17(4)] and
  - conforming to certain requirements [Art. 17(2) and 17(3)].

Intellectual Property Rights

- Copyright
  - Can the Customer place its data and software with the Supplier or in the Cloud?
  - Who is liable for infringement in third party's rights?
  - Who owns the IPRs created in the course of using the services?
- Software Licensing Issues
  - Does the license agreement allow for transfer to the Supplier or the Cloud?
- Open Source Issues
  - GPL v AGPL

Right to and in Data

- Who owns the data?

- There are no direct right *in rem* to data
- Limited rights exist through a patchwork of legislation
- Must be handled through contractual obligations

- Oxford v. Moss (1979) 68 Cr App Rep 183

Right to and in Data

- Existing legal framework is a patchwork, no generic ownership in data:

- Privacy laws protects processing of data but do not touch upon ownership
- Copyright law protects the expression of an idea but provides only limited rights
- Trade secrets laws require all information to be kept secret to afford protection
- Etc.

Key Takeaway #7

There is no real ownership of data.

Security

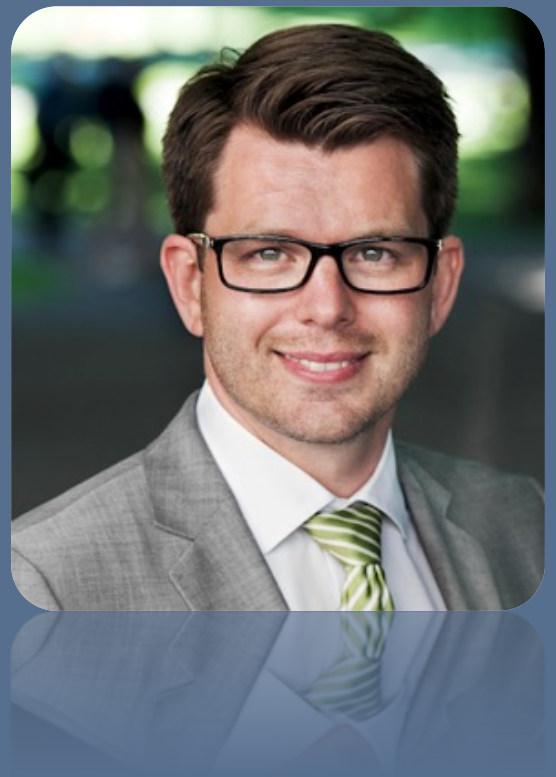
- There are many aspects to Security
  - Physical Security
  - Logical Security
  - Disaster Recovery and Business Continuity
  - Regulatory Compliance
- Security is both positive and negative
  - E.g. prevent access to data for all unauthorized entities while providing ease of access for all authorized entities
- Draft and enforce (i.e. by contract) a security policy handling the above areas

Liability

- Liability and Limitation of Liability clauses distributes risks
  - Only affective between parties to a contract
  - Cannot distribute criminal liability or regulatory penalties
  - Can only indirectly handle third party claims

- Liability clauses in contracts decides who will assume the economic effects of breach, damage or loss in the end

LUCENTUM
Privacy and Technology Law



Questions?

tobias.edvardsson@lucentum.se
Linkedin.com/in/tobiasedvardsson