Cloud Computing

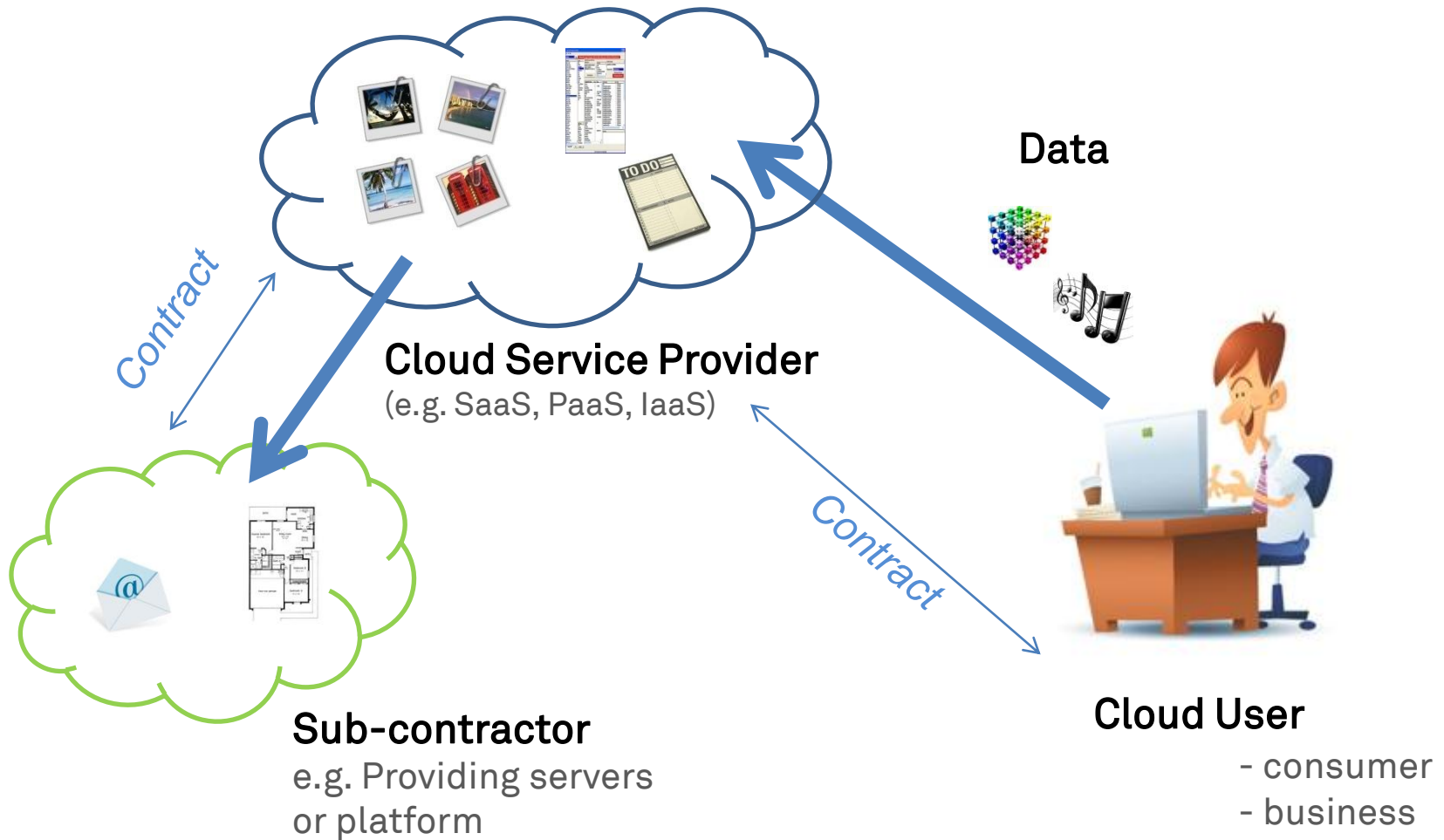# Hot topics in relation to security, liability and privacy

LORENZ | International lawyers

Cloud Computing : who and what is involved?

Cloud Service Provider
(e.g. SaaS, PaaS, IaaS)

Contract

Data

Contract

Sub-contractor
e.g. Providing servers
or platform

Cloud User
- consumer
- business

LORENZ | International lawyers

Hot Topics

- Cloud Computing Contracts

- Vendor Lock-in

- Liability for Data Security and Loss of Data

- Service Level Agreements

- Privacy Regulations

- Third Party Access

Cloud Computing Contracts

- Most of the time standard contracts -> No opportunity for customers to negotiate terms

Click-wrap agreements are binding!

By clicking the "I Agree" button I acknowledge that I have read and accept the terms of the above agreement.

I Agree   Cancel

- Sometimes contain extensive limitation of the Cloud Service Provider's liability

- Unilateral termination possibilities for Cloud Service Provider

- Outsourcing possibility for the Cloud Service Provider: what about liability?

- No audit of the cloud possible

Vendor Lock-in

Transfer of data

Compatibility

and

Interoperability

→ Vendor lock-in

What if the Cloud Service Provider goes bankrupt?

What happens with the Data after the termination of the agreement?

Liability for Data Security and Loss of Data

"as is" software performance warranty

Standard approach:
excluding liability for security of any data and provide that the customer retains full responsibility for data safety

Legal requirement to keep data secure

Consumer law: prohibition to inappropriately excluding or limiting the liability of the seller or supplier

Liability for data security and loss of data (2)

- Exclusion of certain types of damage
  - Indirect damage (loss of profits, reputational damage, loss of goodwill, etc.)
  - Direct damage (loss of data)

  → no exoneration for fraud!
  → exoneration for serious error or negligence is allowed if explicitly determined in the contract

- Cap on the amount of indemnities

- Limitation in time for indemnity claims

- Exclusion of financial compensation – only reparation

- Force majeure: (power cut, strikes, failure of telecom services, third party failure, *etc*)

  ↘*Not only natural disaster but often any event beyond control of Cloud Service Provider*

Service level agreements

-> often little room to negotiate SLA (depends on volume, own private cloud)

- Availability of the service

- Speed of the service

- Capacity

- Efficiency

- Availability of the help desk

- Maintenance time

- *Etc.*

Who determines whether the service level was met?

Compensation ?
- Service-credits
  (= credit on next invoice)
- Other indemnities?

Root cause analysis after any service failure?

Right to terminate?

<u>Privacy regulations</u>

Controller: determines the purposes and means of the processing
of personal data.

Processor: processes personal data on behalf of the controller.

→ triggers responsibilities and obligations

<u>Problem:</u> In the cloud computing context, the roles of controller
and processor become blurred

<u>Solution:</u> contract should clearly define the role of the provider and
the role of the customer and the associated liabilities

Privacy regulations (2)

Transfer of data outside the EU:

ONLY if the country in question ensures an adequate level of protection

Problem: Data that is stored in the cloud could be transferred outside the EC;
 location may be unknown

Solutions: - safe harbor and model data transfer clauses

 - consent by the data subject

 - ensuring adequate level of protection in the technology itself

<u>Third Party Access</u>

- Protection of trade secrets and privileged information

- Who has access?

- How is access protected?

- Can Cloud Service Provider accommodate audit trail or record hold requests and implement them?

- What will the Cloud server provider do in case of?
  - Subpoenas
  - Criminal investigations
  - Search warrants/possible seizures
  - E-discovery
  - > immediately contact Cloud User or allow access?

The Contract

1) Identification of the Cloud Service Provider: who, where, auditing, security certificates, outsourcing -> due diligence

2) Specification of the service
   I. Price
   II. SLA
   III. Remedies

3) Data protection and security
   I. Who is controller and who is processor of personal data?
   II. Interoperability and compatibility
   III. Backup of the data – data restoration
   IV. Access protection

4) Liability of the Cloud Service Provider: what is excluded?

5) Termination of the agreement
   I. By both parties?
   II. What happens with the data?

CONCLUSIONS

Until security, privacy and legal issues surrounding cloud computing are better settled, companies seeking the benefits of cloud computing may wish to utilize a more conservative approach, particularly for highly sensitive and personally identifiable data: contract with Cloud Service Providers that give sufficient contractual guarantees

LORENZ | International lawyers

QUESTIONS?

Lorenz
Steven De Schrijver
Regentlaan 37-40 Boulevard du Régent
1000 Brussels
T. 32 2 239 2000 - F. 32 2 239 2002
s.deschrijver@lorenz-law.com
www.lorenz-law.com