

Cloud computing

Alessandro Galtieri, Senior Lawyer, Colt Technology
Services, London, UK

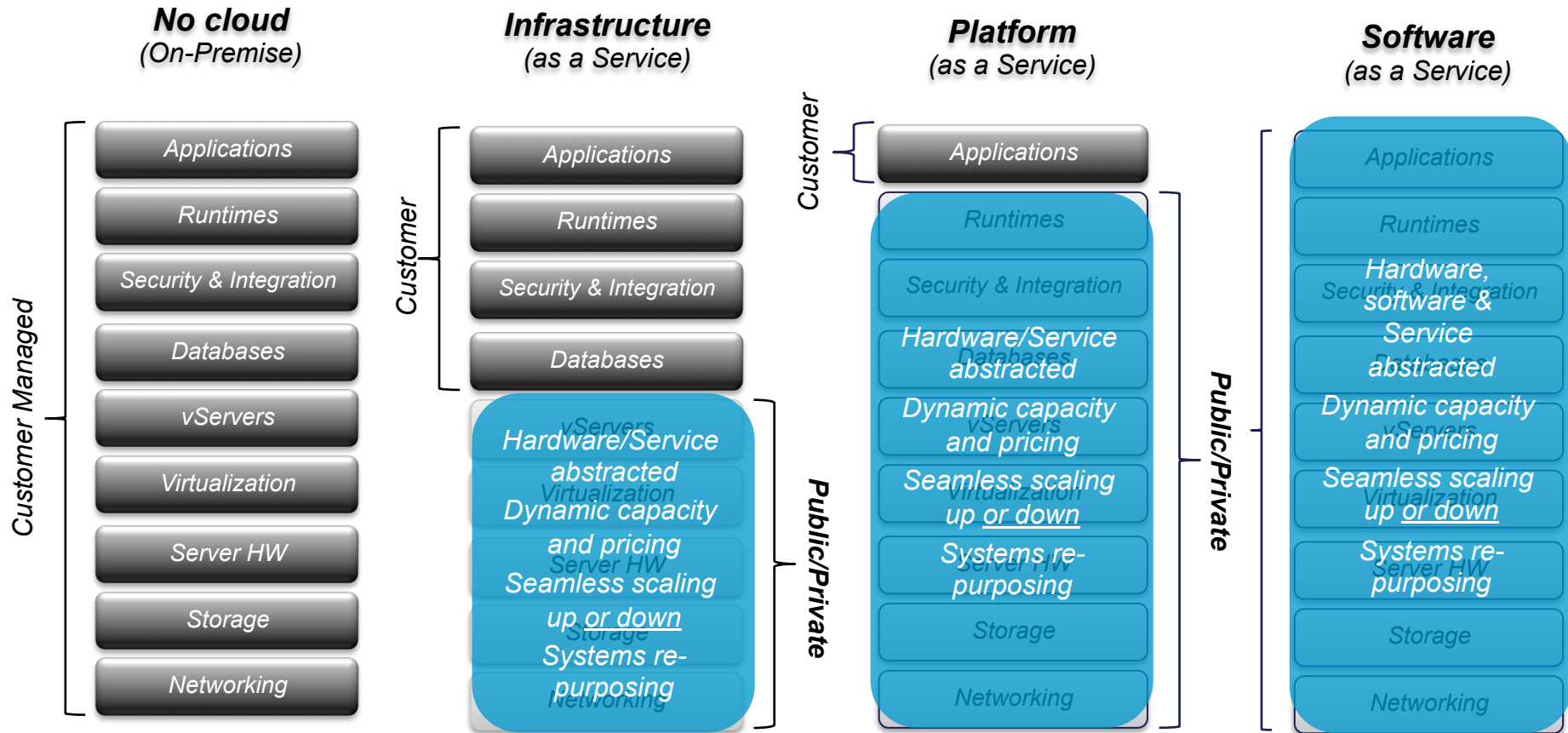
Pavel Klimov, General Counsel EMEA, Unisys, London, UK

Severin Loeffler, Assistant General Counsel, Central Eastern
Europe, Microsoft, Munich, Germany

Introduction – cloud and contracting

Alessandro Galtieri, Senior Lawyer, Colt Technology
Services, London, UK

Cloud computing – the basics



Cloud computing – the risks

- Loss of control (SRM)
- Data protection
- Data security and data segregation
- Vendor lock-in and Change management
- Resilience
- Termination and suspension
- Liability
- Regulation

Cloud computing – the trends

- Increased use of hybrid cloud (public for “burst” needs)
- More contract terms becoming negotiable
- Open standards becoming available
- Industry and government initiatives to provide technical and contractual standards/benchmarks.

Trust, transparency and control

Severin Loeffler, Assistant General Counsel, Central Eastern Europe, Microsoft, Munich, Germany



What should
customers ask cloud
service providers?

- *How do you protect my data?*
- *How do you use my data?*
- *How can you help me with my compliance needs?*
- *Where is my data, and who has access to it?*
- *What do you do in response to government demands for customer data?*

**Why should I
trust you?**



Perception v. Reality: Privacy & Security in the Cloud

Perceptions holding customers back from cloud services:

- *60% concerned about data security*
- *45% worried that using the cloud would result in a lack of control over their data*
- *42% doubted reliability of the cloud*

In contrast, for customers using the cloud:

- *94% have gained security benefits they didn't have with on-premise technology*
- *62% have seen increased levels of privacy protection*
- *75% have experienced improved service availability*

Data points provided by [Cloud Trust Study](#) conducted by TWC

Transparency

- *Clear and concise contract terms*
 - *Data location specificity*
 - *Use of data only to provide service*
 - *Subcontractors identified and notification of changes*
- *Report audit results*
- *Law Enforcement Request Report*

ISO 27018 – Born in the Cloud



Key Principles - Cloud providers must:

*Not use data for advertising or marketing unless express **consent** is obtained*

*Be **accountable** to determine if customer data was impacted by a breach of information security*

*Be **transparent** about data location and how data is handled*

***Communicate** to customers and regulators in the event of a breach*

*Provide customers with **control** over how their data is used*

*Have services **independently audited** for compliance with this standard*

“In short, when governments seek information from Microsoft relating to customers, we strive to be principled, limited in what we disclose, and committed to transparency.”

Brad Smith

*General Counsel & Executive Vice President
Microsoft Corporation*

*Customer data
≠
Microsoft data*

*Government
demand
↓
Customer*

*Data access
governed by law
where it rests*

Evolving the law

Cybersecurity and privacy

Pavel Klimov, General Counsel EMEA, Unisys, London, UK

Cloud – a friend of a foe to my data security?

- Key barriers to the adoption of Cloud
 - Security of data
 - Regulatory restrictions
 - Data transfers
 - Government access to data
- Key Benefits
 - Scalability
 - Lower costs
 - Agility
 - New capabilities

Data Security

- Holistic approach
 - Risk vs. benefit assessment
 - Technical solution evaluation
 - Legal/regulatory risks assessment
 - Contractual mitigation
 - Insurance cover
- Are these risks specific to the cloud?
 - Gap analysis vs. traditional solutions

Data Protection/Privacy

- Key issues
 - Loss/lack of control
 - Lack of visibility into processing
 - International data transfers
 - Governmental access to data
 - E-discovery

Q & A



Appendix 1 - checklist when purchasing cloud services (AG)



Pre-contract: internal approval

- In addition to a review of business requirements, a business case and proper risk and compliance analysis.
- There is a risk that staff at any level will circumvent your official procurement and approvals processes, particularly with 'click-wrap' and 'free' services.
- 'Free' services may involve payment for extras, or generate income from processing data about you. They can pose serious data protection, client confidentiality and information security risks.

1 **Liability**

- Cloud providers frequently exclude contractual liability for their customers' direct losses and even more frequently, indirect losses, as a result of service failure.
- It may not be possible to re-negotiate these terms. In practice the solution may be to choose a cloud provider with
 - a good track record
 - commitment to remain in the cloud computing market
 - a strong reputation to protect

2 Service levels and service credits /1

- Service levels should be objective, quantifiable, repeatable measures of matters within your cloud provider's responsibility.
- You should consider various aspects of service availability including:
 - **point of measurement:** availability of service provision or availability at the point of user consumption (with ancillary KPIs that matter to you: time to respond, time to repair, etc.)
 - **service measurement period:** even if a service boasts high availability 24/7, this could translate into relatively high downtime during normal working hours)
 - **application availability:** availability of particular applications may be just as important to you as general availability of a service

Service levels and service credits /2

- Cloud providers commonly offer service credit if they fail to meet their service level agreement. You should weigh up the relative merits of this regime against damages according to your jurisdiction.
- In general, service credit regimes offer certainty and keep risk to identifiable and manageable levels.
- You should however be careful before accepting that service credits are your sole and exclusive remedy. This will limit your right to sue for damages at large or terminate the contract.

3 Lock-in, termination and return of data

- Before entering a cloud computing contract, you should think about what will happen if you need to terminate it.
- You should ensure that if you need to migrate services to another cloud provider, or back to you, it can take place with minimal disruption.
- You should therefore define your requirements for exit at an early stage in negotiations, and ensure that the contract provides a clear exit strategy.
- You should consider removing contractual provisions permitting the cloud provider the right to exercise lien over your data and client data.

Change of terms (1): change of control, assignment, novation

- You should consider the risks associated with another entity obtaining control of your chosen cloud provider.
- Contractual approaches to managing this risk include:
- requiring the cloud provider to inform you in advance (subject to any listing rules of a relevant stock exchange) of any proposed change in control of the cloud provider
- having the right to terminate the contract if a change of control has occurred
- ensuring that any transfer of the cloud provider's rights and obligations under the contract to another entity (commonly referred to as 'assignment' in the case of rights and 'novation' in relation to rights and obligations) is subject to the prior written approval of the customer

- **Change of terms (2): other changes by the cloud provider**
- Some cloud computing contracts include clauses allowing the cloud provider to change the terms of the contract at any time without agreement by the customer. You should consider:
 - deleting the right or making the right subject to your agreement to any change
 - placing an obligation on your cloud provider to notify you in advance of any changes and give you the right to terminate the contract if you do not agree to the changes.

Other points (1): Subcontracting

- When determining your contractual approach to supply chain risk management, you should also consider:
 - Should subcontracting be permitted at all?
 - If subcontracting is permitted, should it be permitted in respect of the whole or part of the subject matter of the contract?
 - If subcontracting is permitted, on what basis can you withhold your consent?
 - Do you have the right to review the terms of the subcontract?
- You should also consider the various mechanisms you can use to allocate, manage or transfer the risks associated with subcontracting - for example, by ensuring that the cloud provider is fully liable for the performance of sub-contractors.

Other points (2): Suspension of services

- Cloud computing contracts frequently contain a right for the cloud provider to suspend services at its discretion. You should resist this. Alternative approaches include:
 - not permitting suspension
 - not allowing suspension for any reason other than non-payment, unless prior notice was given
 - not allowing suspension without prior written notice of non-payment, with an obligation on the provider to give a final notice, and a commitment to restore services within a certain number of days after payment
 - allowing suspension for material breach, but only after reasonable prior notice and good-faith consultation with you.

Appendix 2 – European Commission Expert Group on Cloud Computing Contracts (AG)

The screenshot shows the European Commission Justice website. At the top, there is a navigation bar with the European Commission logo and the word 'JUSTICE'. Below this is a breadcrumb trail: 'European Commission > Justice > Contract law > Cloud computing > Expert group'. The main content area features a search bar and a 'Share' button. On the left, there is a sidebar menu with categories like 'CONTRACT LAW', 'Common European Sales Law', 'Insurance Contract Law', 'Cloud Computing Contracts', and 'Expert Group'. The main content area is titled 'Expert Group' and contains the following text:

Expert Group on Cloud Computing Contracts

On 18 June 2013, the Commission set up an Expert Group on Cloud Computing Contracts.

The Expert Group was established to assist the Commission in identifying safe and fair contract terms and conditions for cloud computing services for consumers and small firms.

The group shall take account of existing best market practices in terms and conditions in cloud computing contracts and the protection of individuals with regard to the processing of personal data and on the free movement of such data (as required under of Directive 95/46/CEC).

Composition of the Group

The Expert Group is composed of practitioners and organizations representing cloud service providers and customers (especially individual/private consumers and small firms), as well as representatives of legal professions or academics with expertise in cloud computing contracts and in personal data protection issues relevant to cloud computing contracts.

The members of the Expert Group were selected following a call for application.












































Read more:
Press release – call for application

On the right side of the page, there is a section titled 'Policy in the making' with two sub-sections:

Call for applications regarding the Commission Decision of 18.6.2013 setting up the Commission Expert Group on Cloud Computing
More

Euronews: EU to simplify cross-border trade rules
Euronews episode of Right on takes a look at online shopping: Less than one in ten Europeans buy online from other EU countries. For both consumers and sellers, the process is simply too complicated... To boost cross-border trade, cut costs and give customers greater choice, the EU has drafted a Common European Sales Law.
More

Insurance Contract Law: Expert report pinpoints obstacles to cross-border trade
European Commission Press release Brussels, 27 February 2014 An expert group set up by the European Commission to examine barriers to cross-border trade in insurance law across Member States (IP/13/74) delivered its comprehensive report today.
More

- ▶ [Agenda](#)  (435 kB) 
 - ▶ [Discussion paper on "Data location and security"](#)  (242 kB) 
 - ▶ [Discussion paper on "Modifications of cloud computing contracts"](#)  (592 kB) 
 - ▶ [Discussion paper on "Unfair terms in cloud computing contracts"](#)  (446 kB) 
 - ▶ [Synthesis](#)  (196 kB) 
- Meeting of 27/28 March 2014
- ▶ [Agenda](#)  (423 kB)
 - ▶ [Discussion paper on "Availability of service"](#)  (744 kB) 
 - ▶ [Discussion paper on "Subcontracting"](#)  (750 kB) 
 - ▶ [Discussion paper on "Audit and reporting"](#)  (177 kB) 
 - ▶ [Discussion paper on "Data transfers in the cloud"](#)  (424 kB)
 - ▶ [Synthesis](#)  (355 kB) 
- Meeting of 9/10 April 2014
- ▶ [Agenda](#)  (425 kB) 
 - ▶ [Discussion paper on "Liability"](#)  (415 kB) 
 - ▶ [Synthesis](#)  (316 kB)  (including discussions on other topics)
- Meeting of 30 April 2014
- ▶ [Agenda](#)  (422 kB) 
 - ▶ [Discussion paper on "Control and use of content"](#)  (521 kB) 
 - ▶ [Discussion paper on "Data disclosure and integrity"](#)  (214 kB) 
 - ▶ [Synthesis](#)  (198 kB)  (including discussions on other topics)
- Meeting of 11/12 December 2014
- ▶ [Agenda](#)  (426 kB) 
 - ▶ [Working paper on "Availability"](#)  (234 kB) 
 - ▶ [Working paper on "Liability \(including remedies\)"](#)  (166 kB) 
 - ▶ [Working paper on "Control and use of content"](#)  (100 kB) 
 - ▶ [Working paper on "Switching - Transfer and deletion of data after the end of the relationship"](#)  (322 kB) 