



EVERYTHING MATTERS

Legal challenges in cloud computing

Maarten Truyens
DLA Piper Brussels



EVERYTHING MATTERS

1. Privacy & data protection

Privacy and data protection

- Applicable laws
 - EU Directive 95/46/EC
 - National implementations
 - e.g., the Belgian Act of 8 December 1992
 - Adopted in pre-Internet area, when centralised and limited processing was the rule
- EU rules are substantially more restrictive than rules from other countries (particularly US)



3

Privacy and data protection

- Cloud computing exposes the age, formality and complex application of the current laws
- Many legal issues are not yet resolved
- Reform of the current rules in the pipeline, but not for tomorrow



4

“Data controllers” and “data processors”

- Legislation makes fundamental distinction between:
 - **data controller:** party that defines the purpose and the means of the processing
 - **data processor:** “dumb performer”
- Distinction is crucial to know who is responsible
- Data controller is liable towards the “data subjects”
- Data controller must choose appropriate data processors, and must seek adequate contractual protection from them



5

Data protection issues in the cloud

- Severe issues when applied in cloud computing context:
 - both customer and — particularly — the hosting provider define the “means” of the processing
 - statutory assumption that the controller is entirely in control of the processing
 - cloud computing is all about reducing the level of direct control, while EU legislation is all about keeping control of data
 - what about “sub-processors”?



6

Applicable data protection law

- An EU Member State's national law will apply when:
 - establishment of EU-based controller located in its territory processes personal data
 - controller outside EU uses "equipment" within territory
- Applied to cloud computing:
 - using EU-based data centre = becoming subject to the very strict EU data protection rules?
 - most authorities interpret "equipment" in an extremely broad way (even browser cookies)



7

Transfer of data outside EU

- Principle: no transfer of data to countries outside the EU that do not offer an "adequate level of protection"
 - only Switzerland, Argentina and Canada
- Exceptions:
 - ask permission from every "data subject" involved
 - if transfer is *necessary* to execute contract with the data subjects
 - for US: subscribing to "safe harbour list"
 - "Binding Corporate Rules"
 - European Commission's model agreement



8

Transfer of data outside EU

- In practice:
 - only use cloud provider with data centre within EU
 - e.g. Amazon EC2: choice of location (US East, US West or Ireland)
 - or make sure that model agreement is concluded with the cloud provider



9



EVERYTHING MATTERS

2. Contracting issues

Small contract, big liability?

- Cloud computing services offer low barrier to entry and easy scaling possibilities
 - “click-wrap agreements” are legally enforceable!
- Many publicly available cloud computing contracts limit liability of hosting provider to a level that is not in line with the potential risk
- Cloud computing contracts resemble typical software licenses, although potential risk is much higher



11

Example

*We and our licensors **shall not be responsible for any service interruptions**, including, without limitation, power outages, system failures or other interruptions, including those that affect the receipt, processing, acceptance, completion or settlement of any payment services. (...)*

*Neither we nor any of our licensors **shall be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages**, including, but not limited to, damages for loss of profits, goodwill, use, data or other losses (...)*



12

Other contractual issues

- **Vendor lock-in**
 - There is no general legal requirement for a vendor to provide you with data export facilities. Everything depends on your contractual agreement.
- **Unilateral termination possibilities**
 - Cloud provider often reserves the right to unilaterally terminate its service provision
- **Involvement of multiple parties**
 - no single point of contact



13

Other contractual issues

- **Auditing requirements**
 - many contracts impose auditing possibilities that include physical inspection
 - how can these auditing requirements be complied with when geographically decentralised cloud services are used?
- **Applicable law & competent court**
 - if outside own country, any litigation can become prohibitively expensive
- What happens in case of **bankruptcy** of the provider?



14

Service Level Agreement

- Important in any service contract, crucial in a cloud computing context
- Points of attention:
 - How is the availability calculated by the provider?
 - *e.g. 10 outages of 6 minutes versus 1 outage of 1 hour*
 - Independent measurement of performance?
 - Are service credits the “sole remedy”?



15



EVERYTHING MATTERS

3. Liability for illegal data

Liability of cloud provider for illegal content

- In many jurisdictions, cloud providers can be held liable for the illegal data they may be hosting
- eCommerce Directive (2000/31/EC) introduced special liability protection for hosting providers:
 - no *liability* for services that “consist of” the storage of electronic information
 - under the condition that the provider has no knowledge or awareness of illegal nature...
 - ...and removes or blocks illegal data when it does gain knowledge or become aware of illegal nature (“notice and takedown”)



17

Liability of cloud provider for illegal content

- Issues:
 - special protection is focused on **storage**, and does not take into account **processing** activities
 - significant amount of (particularly French) case law does not offer protection when services do not consist *exclusively* of storage activities
 - liability protection does not prevent so-called injunctions, which can be as costly and time-consuming
 - no standard notice-and-takedown procedure
- Reform in the pipeline?



18



EVERYTHING MATTERS

Contact

maarten.truyens@dlapiper.com