

Legal Aspects of Cloud Computing

Dr. Susann Wolfgram & Ulrike Weinbrenner
Dr. Alexander Duisberg (Bird&Bird)

Agenda

- Cloud Computing Overview
- Role Play on Hot Topics
 - SAAS versus on-premise software licensing
 - SLAs
 - Data privacy
 - Data security
 - E-Discovery
- Q & A

Cloud Computing



1960ies
Mainframe



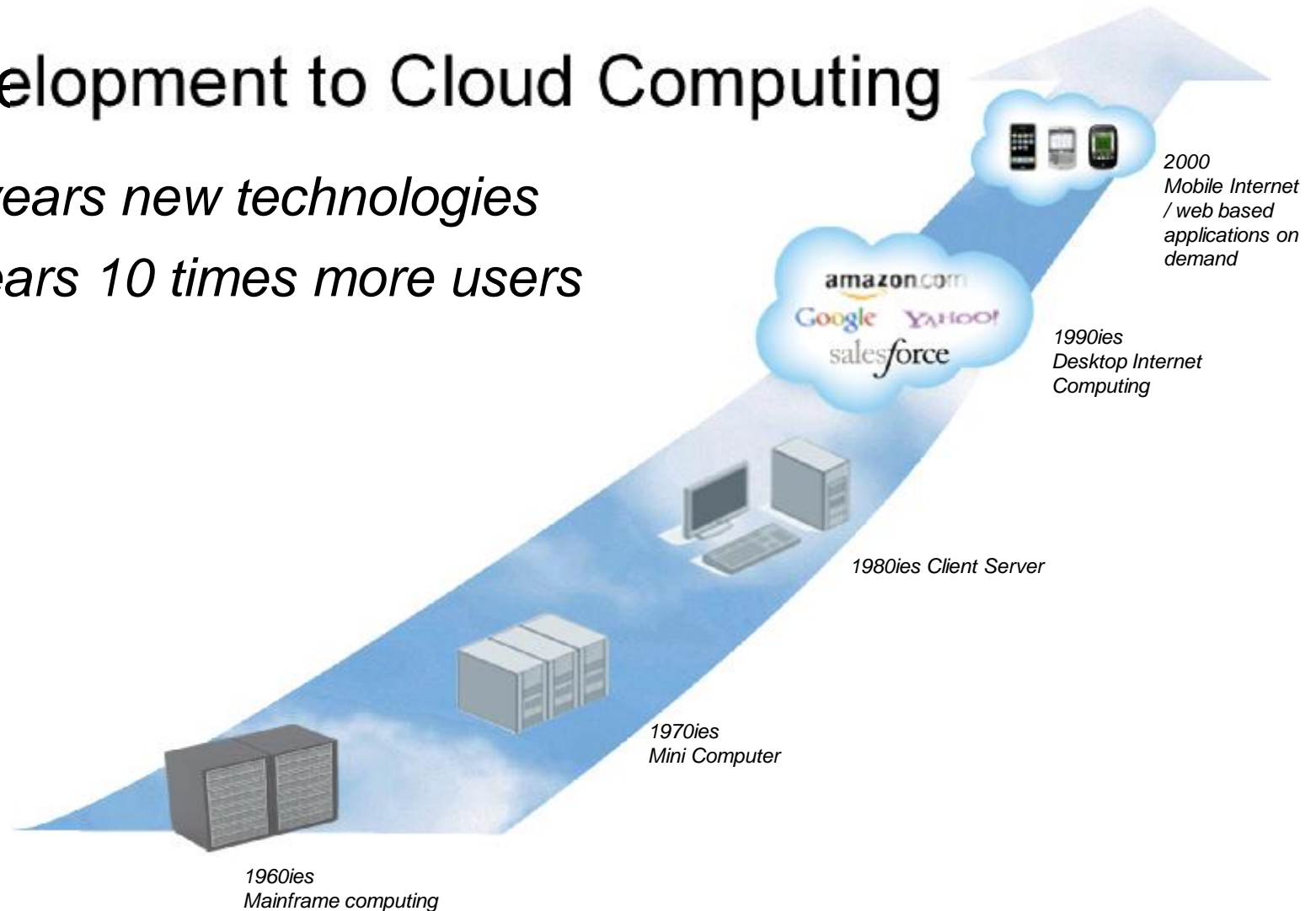
1980ies
Clientserver



Today
Cloud computing

Development to Cloud Computing

Every 10 years new technologies
Every 10 years 10 times more users



Cloud Computing Overview

- Front end: users access through the Internet/mobile device an application or service, e.g. to collect, process, organize, use or store data.
- Back end: Vendor provides such application / service through a ***MULTI-TENANT ARCHITECTURE***:
 - All customer data reside on the "same" system / hardware i.e. data center(s), (usually huge server farms) – however:
 - Customer instances / data are segregated on shared equipment
 - Updates / upgrades of applications are seamlessly provided to all customers / users at the same time
 - System security and availability is the same for every customer

Development of Cloud Computing



Low cost – fast - user friendly



collaboration – realtime - mobility



Transition from one Cloud to another Cloud

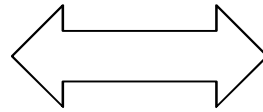
Upfront Considerations:

- Customer wants flexibility and does not want to "be locked" in with one single provider forever.
- How to achieve flexibility: "Portability" of consistent / structured data in good data quality to another vendor or in-house
- Agreements are concluded for a limited period for the subscription term – exit rights determined upfront.

Actual Transition Steps:

- Trigger: expiration or termination → return of Customer's data is key.
- Transition support from 1st provider may be provided for a limited time (pre-agreed [x] months), sometimes at additional costs
- Data format: Customer Data is often returned in .csv format.
- Vendor will confirm deletion of data in first cloud after transition.

Software as a Service



On Premise (in-house IT)

- § Service / Subscription based model, often per User
- § One fits all solution: same code base for all customers – software is configured not customized
- § All "Customer" Data resides on SaaS provider's systems
- § Same technical and organizational measures of SAAS vendor apply to every customer (multi-tenant architecture)

- § Software is installed at customer premises and often furnished with a perpetual enterprise license
- § Customization of software may be specific to a customer
- § Supported by internal customer IT department
- § Third party data processor involvement optional – otherwise full control over data

SaaS . . . Legal Challenges

Customer concerns:

- Losing or leaking of customer data
- Data access up to data migration (data portability in case of termination)
- Indemnity
- Warranty
- Limitation of liability
- Escrow

Vendor responses:

- Security and Privacy: technical and organizational measures
- Adequate level of data protection through Safe Harbor/ EU data center
- Indemnification for Third Party IP claims as well as for customer's use of the application ("lawful content")
- User identity – export regulations!
- Escrow often not meaningful

Service Level Agreements (SLA)

Customer concerns:

- How to measure?
- What to measure?
 - Service availability
 - Transaction times?
- Credits / penalties - missed SLAs for [x] consecutive months?
- What failure entitles to a termination for cause?

Vendor responses:

- Monthly reports on average availability of cloud (not customer specific)
- Email alerts for outages
- Customer has to also cooperate and file an incident
- Force majeure or external factors (no control over the internet)
- Side note: revenue recognition

Data Privacy (1)

Customer concerns:

- Where are data stored?
- Applicable law adequate? (EU data protection laws ./ US Safe Harbor principles?)
- What happens in case of breach of confidentiality or security?
- What if authorities want to access data?
- Use of subcontractors?
- Who answers data subjects?

Vendor responses:

- Depends – different models feasible and offered
- Customer preferences for EU jurisdictions may not be available
- Notification requirements for security breach to be discussed
- Cooperation with authorities
- Often required to use sub-contractors (pass-through obligations)
- Audit rights – what makes sense?

Data Privacy (2)

Customer = Data Controller

- Remains legally responsible
- Define scope of data processing (data categories) by Data Processor v. own data processing (from cloud to user)
- Check reliability of Data Processor and Subcontractors
- Check technical measures
- Initial audit?
- Check registration requirements with local DPAs

Vendor = Data Processor

- Must obey to lawful instructions (custom instructions limited in SaaS model)
- Reasonable controls by customers through external audit reports and/or certifications
- Maintain technical measures based on technological developments
- Check registration requirements as data processor

Data Privacy (3)


German Customer:

- Needs a written commissioned data processing agreement (Sec. 11 BDSG)
- Comply with increased control obligations under German law
- Check Safe Harbor Certification
- Cost savings as legitimate reasons to select vendor as long as no conflicting interests of data subjects
- Involve Works Council, if any

US Vendor:

- Possible to contractually agree on a data processing agreement that meets all legal requirements of German data protection law
- Facilitate controls through meaningful audit reports / availability of contracts / self-certifications / data secrecy
- Notice if status of Safe Harbor certification is likely to be lost
- Assist with ROI analysis

Proposal Bird & Bird (1)

- Standardized software offerings  contracting through standardized contract terms
- Select certified cloud service providers
- Define locations and subcontractors
 - Reproduction of data at any time
- Controller's directional rights
 - Clear-cut contractual obligations
 - Flexible termination (regulated industries)
- Information rights of data subjects?

Proposal Bird & Bird (2)

- Liability and Indemnity
 - Customer liability for incompliance at source
 - Vendor liability for incompliance in operation
- Exit and retransition
 - Data migration and data formats
 - Documentation
- Regulate data base rights (Article 7 Database Directive 96/9/EC) – a potential pitfall!

Data Security

Customer concerns:

- Loss of control over data – to what extent?
- What technical measures apply?
- Are they up to date? How do I learn of change?
- How does the vendor control measures taken?
- Do I get access to security audit reports?
- Breach notification?

Vendor responses:

- Access controls (physical/ intrusion/system, remote access)
- Transmission controls (encryption)
- Input control (log files)
- Job control (follow instructions)
- Availability / Disaster recovery
- Segregation of data
- External audits & Vulnerability / penetration tests / IT policies
- Data secrecy
- Training / background checks

Audit Rights to Check Data Center Security

Customer concerns:

- On-site audits required
- Legal requirements to be able to conduct on-site audits in certain countries and/or in some industries
- Additional requirements to prove or certify "state of the art" data center security
- Continuous technical developments

Vendor responses:

- Data Centers are NO "weekend destinations"
- On-site audit rights cannot be granted to all customers but only where legally required or for large customers
- Internationally recognized Security Standards (e.g. ISO 27001 or SAS 70) help customers to control vendor regularly

Proposal Bird & Bird

- Technical & organizational measures (TOM)
 - Assess Vendors' standard security policies
 - Regulators require to implement national standards
 - Details vary significantly (per country annexes?)
 - Stringent requirements e.g. in Germany, Italy, Spain
- Security breach provisions
 - Customer liability as data controller
 - Proactive response by Vendor (timelines!)
 - Indemnity by Vendor for incompliance
- Audit rights – address by delegation and certified standards
 - Approach tbc by regulators

EDiscovery – International dimension

Customer concerns:

- Foreign blocking statutes and data privacy regulations
- The Hague Convention and European Blocking Statutes may result in US sanctions
- Compliance with EDiscovery may lead to breach of EU Data Protection Law

Vendor responses:

- International legal conflict – no "one-fit-all" answers and varying interpretation of the law in EU jurisdictions
- The Hague Convention often inapplicable (country reservations)
- Article 29 WP in WP 158: need for reconciling requirements of US rules and EU privacy provisions

Proposal Bird & Bird

Upfront considerations on legitimacy of disclosure

- Balance of interest test
- Restrict disclosure to anonymized or pseudonymized data
- Filtering of irrelevant data by a trusted third party in the EU and only transfer a limited set of data
- Single transfer of all relevant information
- Significant amount of data to be transferred? Use of Binding Corporate Rules or Safe Harbor

EDiscovery – Data protection

Customer concerns:

- Need to show reasonable efforts to locate, preserve and produce electronically stored information (ESI)
- Lack of control
- Ability to find and process tremendous amount of ESI
- Vendor specific issues regarding data storage (format/archiving schedules/capabilities)?

Vendor responses:

- Make data processing, data-retention and back-up policies transparent and provide information on how data is maintained
- Procedures for locating information in the cloud
- Assist with implementation of legal hold, or return data
- Stored data can be returned without interfering with business operation

Proposal Bird & Bird (1)

Contractual provisions on

- **Locating** information
 - Vendors list on location of data
- Subcontractors
 - Transparency
 - Pass through of obligations
 - Audit rights
- **Accessing** information
 - Customer's access (represented by Vendor?) to all data centres at all times
 - Short notice access and collection of data

Proposal Bird & Bird (2)

- **Preserving** information
 - Separation from third party customer data
 - Legal hold and ensure immediate data collection
 - Vendor's retention policy – suspension of technical routine deletion cycles
- Vendor to commit to / provide global discovery policy
 - Legal hold, search, anonymizing, disclosure
- Assess potential risks from breach of data protection regulation
 - Purpose of EDiscovery
 - Limited and select access on a case-by-case basis
- Balance against risks under Blocking Statute rules
 - Assigned inspection within the EU?

QUESTIONS & ANSWERS

THANK YOU!

Backup Slides

Data privacy different perspectives

United States: "Privacy is the right to be left alone" - Justice Louis Brandeis

UK: "the right of an individual to be protected against intrusion into his personal life or affairs by direct physical means or by publication of information"

Germany: "Privacy is a fundamental human right and the reasonable expectation of every person"

"Two adversarial Principles of Protection"

- **Privacy and Data Protection Laws** in the EU promoted by governments
 - ➡ sanctions on infringements
- **Self-regulation** (Sectorial Laws) for fair information practices by codes of conducts promoted by businesses
 - ➡ sanctions only under certain circumstances

Increasing Regulation on Data Privacy

Selected Laws:

- 1970 First Data Protection Code in Germany
- 1978 French law "Loi relative à l'informatique"
- 1980 OECD Guidelines concerning the protection of privacy and transborder flows of personal data
- 1995 EC Directive on Data Protection (95/46/EC)
- 1996 US: Health Insurance Portability and Accountability Act (HIPAA)
- 2000: Safe Harbor Privacy Principles of the US Department of Commerce
- 2010: Charter of Fundamental Rights of the European Union, Article 8 "Protection of Personal Data"

Main Privacy Principles:

- Lawfulness and fairness
- Necessity of data collection and processing
- Purpose specification and purpose binding
 - There are no "non-sensitive" data
- Transparency
 - Data subject's right to information correction, erasure or blocking of incorrect / illegally stored data
- Supervision (= control by independent data protection authority) & sanctions
- **Adequate organizational and technical safeguards**

US Sectorial Laws

- No explicit right to privacy in the constitution
- Limited constitutional right to privacy implied in number of provisions in the Bill of Rights
- A patchwork of federal laws for specific categories of personal information
 - E.g., financial reports, credit reports, video rentals, etc.
- White House and private sector believe that self-regulation is enough and that no new laws are needed (exception: medical records)
- Leads to conflicts with other countries' privacy laws

EU: Adequate Level of Data Protection

- Any processing of personal data outside EU/EEA requires that the recipient of data provides for an "adequate level of data protection". The European Commission may find that a third country also ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.
- United States - Safe Harbor certification ensures also adequate level of data protection
- Data transfer also permitted with data subjects informed and voluntary consent; or under the Standard contractual clauses issued by EU or under approved Binding Corporate Rules (code of conduct)
- Go to http://ec.europa.eu/justice/policies/privacy/index_en.htm for more information

Safe Harbor Registration

US companies **voluntarily self-certify** to adhere to a set of privacy principles worked out by US Department of Commerce and Internal Market Directorate of the EU

- **Little enforcement**: A self-regulatory system in which companies merely promise not to violate their declared privacy practices
- **Criticized** by privacy advocates and consumer groups in both US and Europe
- **Recently** Düsseldorfer Kreis

Conclusion: Privacy and Contracts

Generally, Subscription Agreements mirror all of the standard Privacy law requirements, which provide. . .

- to process the Customer Data in accordance with the Agreement, Customer's instructions and applicable data protection laws and regulations;
- appropriate technical, organizational and security measures against unauthorized access to or unauthorized alteration, disclosure, destruction or loss of Customer Data;
- reasonable steps to ensure that employees are aware of and are suitably trained in such technical, organizational and security measures;
- to maintain the security and integrity of the Service and the Customer Data.

User Identity – why is this an issue?

Vendor's concerns:

- How do we know that customer is not in an embargoed country?
- How do we ensure that the application is used according to the laws of the respective country?
- How do we know that the user is not a "spying" competitor?

Customer's issues:

- Customer needs to warrant that the application provided is used according to the laws in the respective country where its USERS are.
- Customer must control the user access provisioning in light of export rules.

EDiscovery – Obligations and Sanctions

- Discovery involves identification, preservation, collection, review and production of relevant information in a party's possession
- Spoliation of evidence → sanctions, e.g.:
 - reverse of burden of proof
 - striking of pleadings
 - taking certain matters as proven
 - fines etc.
- Subject of discovery requirements: Customer not Vendor
- Reasonable efforts required → Blanket assertion that data in the cloud is inaccessible (Rule 26(b)(2)(B)) not acceptable

Hague Convention, Blocking Statutes and EDiscovery (1)

The Hague Convention (dated March 18, 1970): "Taking of Evidence Abroad in Civil or Commercial Matters"

- All EEA Member states ratified or accessed (except Austria, Belgium and Malta)
- Most EEA Member states have issued reservations or declarations under article 23 (pre-trial discovery) (except Lithuania, Slovakia, Slovenia and Czech Republic).
 - They may not (or only under certain conditions) execute letters of request issued for pre-trial discovery (e.g. France requires that request enumerates documents with specific link to dispute)
 - Conditions vary among EU member states

Hague Convention, Blocking Statutes and EDiscovery (2)

Is the Hague Convention exclusive and mandatory?

- US: no exclusive or mandatory procedure (Société National Industrielle Aérospatiale, US District Court, 482 U.S. 522 (1987)).
- Europe: will mainly depend on the existence and provisions of Blocking Statutes.
 - E.g.: French law No.68-678 of July 26, 1968, modified by law No.80-538 of July 17, 1980, sets forth a prohibition to communicate to foreign public authorities, documents likely to undermine the sovereignty, the security, the essential economic interests of France or the public order (Article 1)
 - Gather evidence for foreign judicial or administrative proceedings unlawful unless permitted by law or international treaties