Data Protection & Privacy

Data Privacy in Cloud environment

Kjell Ohlsson
7th March 2013
Who?

**Presenter:**
- Kjell Ohlsson - AstraZeneca

**Audience:**

**Timing:**
- 45 minutes including Q&A
Objectives

• Give basic understanding of Data Protection & Privacy + Cloud Computing

• Raise awareness around Data Privacy risks in Cloud environments
Basic understanding of Data Protection & Privacy + Cloud Computing
Data Privacy
Important Definitions

Data subject
(Den registrerade)

Identifiable natural person. I.e. not a legal entity.
# Data Privacy

## Important Definitions

<table>
<thead>
<tr>
<th>Personal Data (Personuppgift)</th>
<th>Sensitive Personal Data (Känslig personuppgift)</th>
</tr>
</thead>
<tbody>
<tr>
<td>------Examples------------------</td>
<td>------Examples------------------</td>
</tr>
<tr>
<td>• Name</td>
<td>• Health</td>
</tr>
<tr>
<td>• Identification numbers</td>
<td>• Labour relations</td>
</tr>
<tr>
<td>• Gender</td>
<td>• Racial or ethnic origin</td>
</tr>
<tr>
<td>• Age</td>
<td>• Political opinions</td>
</tr>
<tr>
<td>• Nationality</td>
<td>• Religious beliefs</td>
</tr>
<tr>
<td>• Language(s) spoken</td>
<td>• Criminal history</td>
</tr>
<tr>
<td>• Private/home address</td>
<td>• Sexual preferences</td>
</tr>
<tr>
<td>• Telephone number</td>
<td></td>
</tr>
<tr>
<td>• Email address</td>
<td></td>
</tr>
</tbody>
</table>

Data that makes the Data Subject identifiable
Data Privacy

Important Definitions

- **Data subject** (Den registrerade)
- **Personal Data** (Personuppgift)
- **Sensitive Personal Data** (Känslig personuppgift)

**Data Controller** (Personuppgiftsansvarig)
Typically a company
Data Privacy
Important Definitions

Data subject
(Den registrerade)

Personal Data
(Personuppgift)

Sensitive Personal Data
(Känslig personuppgift)

Data Controller
(Personuppgiftsansvarig)
Typically a company

Processor(s)
(Personuppgiftsbiträde(n))
Data Privacy Principles

Ensuring Transparency and Notification about intended data use
Data Privacy Principles

Using Personal Data for a known purpose only.
Keep usage in order and no “cheating”!
Data Privacy Principles

Ensuring Data Quality, meaning data is accurate and up-to-date
Data Privacy Principles

Retention. Don’t keep data longer than necessary

![Image of a person disposing of data]
Data Privacy Principles

Honouring individual’s rights. Data subjects must have right to access their data and if necessary, correct it.
Data Privacy Principles

Taking appropriate security measures to protect data from loss, damage and unauthorized disclosure
Data Privacy Principles

3rd parties must adopt appropriate security measures
Data Privacy Principles

Overseas Transfers must be controlled and data adequately protected
Data Privacy Principles

Sensitive Personal Data must be especially protected and only used with consent (if no exception applies)
Global Data Privacy Laws

as of October 2012

Cloud Computing

Introduction

Cloud computing is a style of computing in which "elastic" IT-enabled capabilities are delivered as a service to external customers using Internet technologies.

The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and/or computation.

Common examples of services include:
- Dropbox.com, iCloud.com, skydrive.live.com (e.g. for info-sharing)
- gmail.com, outlook.com, me.com (mail services)
- Netflix (streaming video)
Cloud computing
Value proposition (detailed in backup slides)

1. Elastic Capacity.
2. Quick and easy deployment.
3. No Capital expenditure, No initial investment.
4. Pay as you go, for what you use.
5. Focus on your business!
Cloud Computing

Deployment Models

Public Cloud
Infrastructure available to “anyone” via Internet. This is typically what is denoted “The Cloud”.

Private Cloud
Infrastructure dedicated to an individual organisation. Complicated. Doubtful financial and management savings.

Hybrid Cloud
Dedicated and publicly available infrastructure co-exist. This is most likely where most organizations will end up when “going for the cloud”.

Kjell Ohlsson  |  March 2013
Cloud Computing
Services (subset of “XaaS”=Anything as a Svc)
Cloud Computing
Services (subset of “XaaS”=Anything as a Svc)
Objectives

Data Privacy risks in Cloud environments
Data Privacy and Cloud Computing

Introduction
Data Privacy and Cloud Computing

Introduction
Cloud Computing
Privacy Risks Overview

There are 3 main Privacy related risks associated with Cloud Services:

• Lack of control over the Personal Data – Where is it? How is it? Can we get to it?

• Lack of information about the processing of the Personal Data – What is being done with it? By whom?

• Lack of, or insufficient ability to, influence the contract with the cloud service provider – Not trivial to do anything about the previous risks.
Cloud Computing

Privacy Risks – Lack of Control over Data

A cloud provider may use its physical control over data from different clients to link Personal Data.

Lack of isolation

Lack of availability

Lack of data subject rights

Lack of integrity

Lack of intervenability

Lack of confidentiality

E.g. due to weak interoperability because of vendor relying on proprietary technology, or due to lack of appropriate backup / Disaster Recovery arrangements.

E.g. due to sharing of resources – Personal Data emanating from a wide range of sources in terms of data subjects and organisations mean there could be conflicting interests/ different objectives.

E.g. due to law enforcement requests made directly to a cloud provider from foreign governments. (E.g. FISAAA in USA)

A cloud provider may not provide the necessary measures and tools to assist in responding to access, deletion or correction requests.

Due to the complexity and dynamics of an outsourcing chain.

Kjell Ohlsson | March 2013
Cloud Computing

Privacy Risks – Lack of Information about processing

• Insufficient information about a cloud service provider’s processing operations poses a risk to Data Controllers and Data Subjects. We may not be aware of potential threats and risks, and therefore can’t take measures to mitigate them.

• Potential threats include:
  • **Chain processing** is taking place involving multiple processors and subcontractors (sub-processors).
  • Personal Data are **processed in different geographic locations** within the EEA (=EU + Iceland, Liechtenstein & Norway) – this **impacts on the law applicable** to any data protection disputes which may arise between user and provider.
  • Personal Data is **transferred to 3rd countries outside the EEA**. 3rd countries **may not provide an adequate level of protection** and transfers may not be safeguarded by appropriate measures (e.g. standard contractual clauses / binding corporate rules) and therefore may be illegal.
Cloud Computing
Privacy Risks – Lack of Influence over Contract

• Under privacy legislation in many countries, Company X will remain the data controller of the personal data and therefore will be liable for any privacy breaches caused by any 3rd party processors.

• Despite this, Company X may not have the ability to negotiate the contractual terms of the cloud service as standardised contracts are a feature of many cloud service providers (e.g. Google, Amazon and Apple).

• It is also difficult to ensure that any contracts between the cloud service provider and their sub-contractors have appropriate protection for Personal Data.
To summarize

• Basic concepts of Data Protection & Privacy + Cloud Computing

• Reasoning around Data Privacy in Cloud environments and the risks introduced
Questions?
Backup slides

- Privacy/Cloud Information from Swedish Data Inspection Board (Datainspektionen)
- Article about legislation that affects privacy
- Detailed “Value proposition” for Cloud computing
Attached documentation

• Data Inspection Board (Datainspektionen) information material

• Article about legislation that potentially affects privacy
1. Elastic capacity

- Scaling up and down in minutes
- No need to provision
- Optimize resources based on your needs
- Can easily manage unexpected peaks
2. Quick deployment

- IT infrastructure is no longer a barrier
- Easier to test different solution
- No need to wait for provisioning
- Shorter development cycles
3. No Capital expenditure

- No initial investment needed
- No commitments
4. Pay as you go

- Clear pricing models
- Pay for compute power by the hour
- Pay for storage by the gb
- Pay for transfer per gb
- Pay per end user

- ....pay as you go...

- Remember, this is all elastic. Easy to turn on/off resources
5. Focus on business

• No need to build from scratch,
• Services are out there to "reuse"
• Much is automated – no waiting

• You can spend more time on value add activities