EU Data Breach in the Cloud
cconcerns and business opportunities

Gloria Marcoccio - CSA Italy Chapter
CSA CEE Summit, 23 October 2013
Not-for-profit Association (registered in nov 2011)

- **104** regular members

- **9** Affiliations/Agreements:
  - Clusit
  - Assintel
  - AFCEA
  - NIC
  - ANORC
  - OWASP
  - (ISC)² Chapter
  - BSI

- **8** Sponsors:
  - Trend Micro
  - CA Technologies
  - ITWay
  - Allied Telesis
  - SafeNet
  - The Data Protection Company
  - Sentient
  - BSI

- **3** Collaborations: Oracle Community For Security

- **3** Research Areas: Translations, Portability-Interoperability-Application Security, Privacy & Legal in the Cloud – 5 WGs

- **>490 LinkedIn members**

G. Marcocci "EU Data Breach in the Cloud"  www.cloudsecurityalliance.it
What does the Commission mean by secure Cloud computing services in Europe?

*Press Releases: 15/10/2013*

Europe should aim to be the world's leading 'trusted cloud region'. Widespread adoption of cloud computing is essential for improving productivity levels in the European economy; but the spread of cloud could slow in light of recent revelations about PRISM and other surveillance programmes. These surveillance revelations have also led to calls for national or regional cloud computing initiatives.

Introduction

• Regulations on Data Breach are becoming more and more important in the networked & information society as well in the traditional sectors such as energy and transport.

• Data Breach as a specific case of Security Incident has several implications requiring a mix of technical, organizational and procedural measures, as well as proper set up and management of contractual relationships between the interested parties, specifically considering the impact from several, overlapping jurisdictional scenarios.
Introduction

- Data Breach issue represents one of the **important challenges** that the **cloud computing** ecosystem & industry have to face and transform in successful managed services.

- The Data Breach study made by CSA ITALY Chapter deals with the related existing EU legislation framework and proposes the cloud computing perspective in terms of area of concerns as well as business opportunity and it is aimed at promoting a common CSA focus also in view of the very recent EU new Data Breach Regulation, directly applicable in the EU member states without transposition into the 28 national legislative frameworks

The CSA Italy Chapter Data Breach study is available at: [http://cloudsecurityalliance.it/](http://cloudsecurityalliance.it/)
Why so much interest in EU Data Breach

Data breach is a security incident that has led to the personal data of individuals being compromised.

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.


Telcos and ISPs in the EU are obliged to set up appropriate security measures and Data Breach prevention/management/notification processes.
Why so much interest in EU Data Breach

The EU Data Breach requirements have significant implications for

- the EU Telcos and ISPs
  and also, specifically mentioned for the first time, very clearly:

- their “outsources”, to whom they entrust the provision of those services (in whole, in part)

Moreover the obligations concerning Data Breach now in force for the EU Telcos, ISPs and their outsources involved in electronic communication services publicly accessible:

should be of interest potentially to all data controllers, given that similar requirements may yet be introduced throughout the EU under the draft EU Data Protection Regulation.
The EU Civil Liberties Committee on Monday 21 October 2013 voted on the draft EU Data Protection new framework.

"This evening's vote is a breakthrough for data protection rules in Europe, ensuring that they are up to the the challenges of the digital age. This legislation introduces overarching EU rules on data protection, replacing the current patchwork of national laws", commented rapporteur for the general data protection regulation, Jan Philipp Albrecht after the vote.

The committee vote also sets out Parliament's mandate to start negotiations with national governments in the Council. Parliament aims to reach an agreement on this major legislative reform before the May 2014 European elections.

The negotiating mandate for the regulation was adopted by 51 votes to 1, with 3 abstentions.

Why so much interest in EU Data Breach

- Example:
  October 17, 2013

“The Dutch government proposes mandatory breach notification

The Netherlands government's proposal for mandatory data breach notification would require all organisations to inform the Dutch DPA of security breaches. According to law firm De Brauw Blackstone Westbroek in Amsterdam, a failure to notify would be punishable by a fine of a maximum of EUR 450,000.

Any breach of security measures that could reasonably be expected to have a negative impact on the protection of personal data which that entity processes would have to be notified. In addition, individuals whose data may has been compromised would have to be notified if their privacy is at risk, unless the data concerned had been encrypted.

The government also proposes a fine for non-cooperation. The DPA could impose a fine of up to EUR 450,000 on companies which do not fully cooperate during an investigation or audit.”

(Privacy Law & Business news – www.privacylaws.com)
Context of reference for describing EU laws with regards to Data Breach

- **Personal Data**
- **Other Data**
- **Information society services (content services)**, as such including any service consisting in one or both of the following:
  - the provision of material with a view to its being comprised in signals conveyed by means of an electronic communications network;
  - the exercise of editorial control over the contents of signals conveyed by means of such a network

example: a shopping portal or an online newspaper would be a content service, and not an electronic communications service.

- **Public communications services** are, in short, any electronic communications service that is provided so as to be available for use by members of the public, bearing in mind that an “electronic communication service” is any electrical, magnetic or electro-magnetic signals (including speech, music, sounds, visual images or data of any description) conveyed over a transmission system.
Context of reference for describing EU laws with regards to Data Breach

- Other business sector not necessarily available “on line”
- Preventive security measures in order to minimize the risk of data destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected
- Measures for detection of security incidents
- Security measures ex post (to be in place in case of security incident, to minimize the adverse effects)
- Measures for notifying security incidents to data subjects concerned and/or national competent Authorities
- Measures for managing security incidents (incident management processes)
## EU Data Breach Legislation in force

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Other Data</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Information society services (content services)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Public communications services</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Other business sector not necessarily available “online”</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Preventive security measures</td>
<td>X article 17</td>
<td>X article 4</td>
<td>X article 5 and Attachment II</td>
<td>X article 4</td>
</tr>
<tr>
<td>Measures for detection of security incidents</td>
<td>X article 4</td>
<td></td>
<td>X article 5 and Attachment II</td>
<td>X article 2(3)</td>
</tr>
<tr>
<td>Security measures ex post</td>
<td>X article 4</td>
<td></td>
<td>X article 5 and Attachment II</td>
<td></td>
</tr>
<tr>
<td>Measures for notifying security incidents to data subjects concerned and/or national competent Authorities</td>
<td>X article 4</td>
<td></td>
<td>X article 5 and Attachment II</td>
<td>X articles 2, 3, 5 and Attachments</td>
</tr>
<tr>
<td>Measures for managing security incidents</td>
<td>X article 4</td>
<td></td>
<td>X article 5 and Attachment II</td>
<td></td>
</tr>
</tbody>
</table>


EU proposed new directives concerning security incident and Data Breach

| Context of reference                                                                 | Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data \[1\] | Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union \[2\] |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Personal Data                                                                         | X                                                                                                                                       | X                                                                                                                                 |
| Other Data                                                                            | X                                                                                                                                       | X                                                                                                                                 |
| Information society services (content services)                                      | X                                                                                                                                       | X                                                                                                                                 |
| Public communications services                                                        | X                                                                                                                                       |                                                                                                                                  |
| Other business sector not necessarily available “on line”                            | X                                                                                                                                       | X                                                                                                                                 |
| Preventive security measures                                                          | X article 30                                                                                                                               | X article 14                                                                                                                   |
| Measures for detection of security incidents                                          | X article 31 (implied)                                                                                                                   | X article 14 (implied)                                                                                                          |
| Security measures ex post                                                             | X                                                                                                                                       | X article 14 (implied)                                                                                                          |
| Measures for notifying security incidents to data subjects concerned and/or national competent Authorities | X article 31 and article 32                                                                                                             | X article 14 (implied)                                                                                                          |
| Measures for managing security incidents                                              | X article 31                                                                                                                               | X article 14 (implied)                                                                                                          |


G. Marcoccio "EU Data Breach in the Cloud"
MAIN STANDARDS AND GUIDELINES

Focus on the management of security incidents

ENISA: European Union Agency for Network and Information Security:
  • “Data breach notifications in the EU”, January 13, 2011
  • “Good Practice Guide for Incident Management, 2010
  • “ENISA Threat Landscape”, 8 January 2013
  • “Critical Cloud Computing - A CIIP perspective on cloud computing services- Version 1.0”, December 2012

NIST: National Institute for Standards and Technology (U.S.)
  • “SP 800 61 Rev 2 Computer Security Incident Handling Guide”, August 2012

ISO: International Organization for Standardization
  • “ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management”

CSA: Cloud Security Alliance
  • “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0” (Domain #9)
**EU Regulation 611/2013:**

Essential timing, tasks and interactions between Outsourcer(s) and Provider for notification of data breach to national competent authority (DPA, Data Protection Authority) and, if any, to subscribers/individuals

*Entry into force in all the EU member states: August 25, 2013*

**Legenda**

Provider = provider of publicly available electronic communications services

Outsourcer = another provider contracted by Provider to deliver part of electronic communication service without having a direct contractual relationship with subscribers (example: in relation to billing or management functions)

---

[GLORY.IT s.r.l. all rights reserved 2013]

G. Marcoccio "EU Data Breach in the Cloud"
When a personal Data Breach is likely to adversely affect the personal data or privacy of a subscriber or individual?

Circumstances to take into account

• the Data Breach involves data concerning financial information, location data, internet log files, web-browsing histories, e-mail data, or itemized call lists

• the likely consequences of the personal Data Breach for the subscriber or individual concerned, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation

• where the data has been stolen or when the provider knows that the data are in the possession of an unauthorised third party

(Article 3 of EU Regulation 611/2013)
ESSENTIAL ROADMAP FOR THE OUTSOURCER

- Identify its Customers subject to the EU Regulations and Directives with regard to Data Breach
- Agree with them the services for which applies the Data Breach obligations
- Agree with them the criteria to detect a Data Breach within the service provided
- Negotiate with them bearing in mind that it will be at least necessary to:
  - Implement security measures
  - Assign appropriate contact persons
  - Develop and operate a process to detect a Data Breach
  - Develop and operate a process to inform the Customer about the Data Breach
  - Operate processes for supporting the Customer in case of request of further information as necessary for the case of Data Breach
  - Develop and operate appropriate information systems to retain information about the Data Breach and related management, able to provide proper reliable support in case of litigations or requests from the competent national authorities
- Implement the measures required
CLOUD PERSPECTIVE

Bearing in mind the EU legislation in force and the new proposed regulations and directives, cloud services providers should evaluate for their business areas:

1 Encryption

appropriate encryption strategy since Data Breach regulations consider encryption as a core measure

data breach obligations should not be considered as part of “ancillary requirements” because the EU approach in regulating data protection & privacy as well as security for infrastructure, specifically demands focus on the governance of risk, commensurate with the criticality of a business, and the governance in case of incidents
CLOUD PERSPECTIVE

2 Agreements

contractual obligations concerning Data Breach management, especially when the applicable law does not completely clarify the extent and repartition of liabilities.

Moreover the agreement should provide the route to clarify Data Breach aspects concerning multiple jurisdictional and applicable law items, typical heritage of a cloud computing service.

3 Incident management governance

appropriate to the end user expectations
compliant with the applicable Data Breach legislation,
it should be considered as one of the main enablers for a successful operation of a business.

In a cloud service context it probably represents one of the primary challenges to face, since it requires appropriate cloud service operation with built-in functions in terms of "anti- Data Breach by design" capabilities.
Thank you for your attention!

EU Data Breach in the Cloud
concerns and business opportunities

gloria.marcoccio@glory.it