Cloud computing and personal data protection

Gwendal LE GRAND
Director of technology and innovation
CNIL
Data protection in Europe

- Directive 95/46/EC || Loi 78-17 du 6 janvier 1978 amended in 2004 (France)
- Definition of personal data
- **Principles**: Purpose limitation, proportionality, retention period, security, data subjects’ rights

### Cloud vs. data protection

<table>
<thead>
<tr>
<th>Topic</th>
<th>Cloud</th>
<th>Data protection (Directive)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control and security</td>
<td>Provider: “<em>We take care of everything</em>”</td>
<td>“<em>the processor shall act only on instructions from the controller</em>”</td>
</tr>
<tr>
<td>Data controllership</td>
<td>Provider: “<em>We take care of everything and we are not liable</em>”</td>
<td>“<em>controller</em>’ shall mean the entity which determines the purposes and means of the processing”</td>
</tr>
<tr>
<td>Location</td>
<td>Provider: “<em>We cannot guarantee the location of your data</em>”</td>
<td>“<em>transfer may take place only if (...) the third country in question ensures an adequate level of protection</em>”</td>
</tr>
<tr>
<td>Retention period</td>
<td>Retention policies are independent from the client or the processing</td>
<td>“<em>personal data is kept for no longer than is necessary for the purposes for which the data were collected</em>”</td>
</tr>
</tbody>
</table>
Snowden impact

- 88% decision-makers changing cloud buying behavior

- 5% of respondents believe location does not matter at all when it comes to storing company data

- 31% of ICT decision-makers are moving data to locations where it will be safe

- 62% of those not currently using cloud feel the revelations have prevented them from moving their ICT into the cloud

- ICT decision-makers prefer buying a cloud service located in their own region, esp. EU respondents (97%) and US respondents (92%)

- 16% are delaying or cancelling contracts with cloud service providers

Source: NTT Communications’ 2014 survey of 1,000 ICT decision-makers in France, Germany, Hong Kong, UK and USA
Outline

Part 1

- CNIL recommendations
  - Guidance with models of contractual clauses (2012)

- WP29 recommendations
  - Opinion 5/2012 on cloud computing

Part 2

- Cloud security alliance
  - Privacy Level Agreement Outline for cloud services in the EU
  - Star certification

- C-SIG draft code of conduct (EU level)
  - Opinion 2/2015 on C-SIG draft code of conduct

- ISO standards

Part 3

- GDPR
  - Adoption process
  - Certification
  - Processors
1. CNIL’s recommendations

**Process**
- Interviews
- Public consultation (end 2011)
- Consultation analysis
- Publication of recommendations (June 2012)

**Objectives**
- Help companies, *esp. SMEs*, decide
- Meet current **state of play**
- **practical tools:** method and model clauses
- Formal documents to support (security and legal) vs. finance
- Provide food for thought
1. CNIL’s recommendations

- **Process**
  - Interviews
  - Public consultation (end 2011)
  - Consultation analysis
  - Publication of recommendations (June 2012)

- **Objectives**
  - Help companies, esp. SMEs, decide
  - Meet current *state of play*
  - **practical tools:**
    - method and model clauses
  - Formal documents to support (security and legal) vs. finance
  - Provide food for thought

- **Key steps**
  - Identify data + processing operations which will be passed to Cloud
  - Define your requirements for technical and legal security
  - Carry out a risk analysis to identify the essential security measures for the company*
  - Identify the relevant type of Cloud
  - Choose a service provider offering sufficient guarantees*
  - Review the internal security policy
  - Monitor changes over time
1. CNIL’s recommendations: Risk analysis

- Information security risks + data protection and privacy risks
  - Both processes can be combined

Methodology for Privacy Impact Assessments

- For data controllers
- For data processors
1. CNIL’s recommendations: Risks

- 35 risks identified by ENISA¹

- **CNIL**: **10 risks with higher data protection relevance**
  - Loss of governance;
  - Vendor lock-in;
  - Isolation failure;
  - Legal requests, in particular by foreign authorities;
  - Supply chain failure;
  - Insecure or ineffective deletion of data, or too long retention period;
  - Improper access rights management;
  - Unavailability;
  - Cloud provider termination or acquisition;
  - Compliance challenges, especially on international transfers.

1. CNIL’s recommendations: A provider with sufficient guarantees

- **Determine CSP qualification:**
  - Processor OR joint controllership
  - Allocating liability

- **Facts analysis on public PaaS and SaaS:**
  - Low level of instructions
  - No monitoring capabilities
  - Standard offers
  - Standard contracts
  ⇒ Joint controllership (generally)

- **Model clauses – only models !**
  - But: “Service providers who do not offer these essential guarantees in their contracts and who refuse any negotiation with their potential customers should not be selected”

- **Controller must have access to all the technical and security information needed for risk analysis:**
  - Accessible security policy
  - Physical safety and security measures on the host site
  - Measures to ensure the availability, integrity, confidentiality;
  - System for reporting complaints and security breaches;
  - Reversibility/portability;
  - Traceability and reporting of incidents detected by the CSP;
  - Service Level Agreements

  ➢ Privacy commitments (e.g. clauses, CSA PLA)

- If the provider is data processor, the customer must be able to audit the provider’s system*

- **Role of Certifications (ex : ISO /IEC 27001)**

- **Compliance with data protection laws**, subcontractors, retention period, transfers (next slides), etc.
1. CNIL’s recommendations: Audit & Certification

**Right to Audit ?**
- from the right to audit the location of the servers where data are processed and stored ….
- …to the right to audit the security measures of the processor,

**CSP :**
- As a processor, you should accept audit from your controllers
- As a joint-controller, responsible of security.

**Controller :**
- You don’t HAVE TO audit your processors but you should BE ABLE TO.
1. CNIL’s recommendations: Transfers outside EU

- Clear and complete *indication of countries* hosting the service provider’s data centres;

- **Adequate protection abroad**
  - EC Standard contractual clauses
  - *Binding corporate rules* – “BCR“

- **1st transfer vs ulterior transfer**
  - Any transfer should be legally grounded
  - Add in your contract that clauses or BCR are mandatory to any ulterior transfer

- **Immediate information to the customer in case of a request** from a foreign administrative or judicial authority.

- **About Safe Harbor**
  - Safe Harbor is illegal since 6/10/2015
  - Any such transfers should be stopped

- **What can replace SH ?**
  - EC Standard contractual clauses ?
  - Binding corporate rules – “BCR“ ?
  - SH2 ?
2. Other actions

- **Contribution to ANSSI referential on qualification of Cloud provider**
  (« Prestataire de services sécurisés d’informatique en nuage »)

- **WP29 recommendations (WP196 – July 2012)** and [Opinion 2/2015](#) on C-SIG draft code of conduct

- **Participation to several international groups**
  - ISO [see next slide]
  - CSA : PLA (February 2013) and PLAv2 (May 2015)
2. C-SIG draft code of conduct

- **Cloud code of conduct (EU level)**
  - [Opinion 2/2015](#) on C-SIG draft code of conduct
    - Transition to GDPR; CoC vs enforcement by DPAs; governance of the code; Location of the processing; International transfers; liability; security; right to audit …

- **Next steps …**
2. ISO standards

- ISO/IEC 29100 Privacy framework
  Terminology and principles to be used in every privacy related standard

- ISO/IEC 29151 Code of practice for PII protection
  Catalogue of generic privacy controls, in addition to ISO/IEC 27002 (information security controls)

- ISO/IEC 27017 Code of practice for information security controls for cloud computing services based on ISO/IEC 27002
  Catalogue of information security controls specific to cloud computing, in addition to ISO/IEC 27002

- ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
  Catalogue of privacy controls specific to cloud computing, (theoretically) in addition to ISO/IEC 29151

- ISO/IEC 27001 Information security management system (ISMS)
  Requirements for the certification of information security management systems

- ISO/IEC 27009 Sector specific application of ISO/IEC 27001 – Requirements
  Requirements for the creation of sector-specific standards that would fit in the ISO/IEC 27001 framework

Next step: use ISO/IEC 27009 requirements to build the missing privacy requirements in a new standard, in order to be able to certify management systems including privacy and/or cloud computing specific aspects
3. The draft GDPR

- General purposes
  - Adapt to the Internet world
  - Harmonise across Europe
  - Simplify procedures
  - Accountability

- In practice
  - No prior notification but **extended data breach notification**
  - Joint responsibility for some services and security (art 24 & 30) → Cloud computing
  - Higher fines
3. GDPR: Certification (art.39)

- Different types
  - certification mechanisms, data protection seals and marks

- In effect
  - Demonstrate compliance with the Regulation of processing operations carried out.
  - Does not reduce the responsibility of the controller or the processor for compliance with the Regulation
  - Does not impact the tasks and powers of the supervisory authority
3. GDPR: processors

**Changes / clarifications. The processor:**

- shall not enlist another processor without consent of the controller;
- implements appropriate measures to ensure a level of security appropriate to the risks;
- makes available to the controller all information necessary to demonstrate compliance + allow for and contribute to audits conducted by the controller;
- informs the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions;
- shall notify the controller without undue delay after becoming aware of a personal data breach;
- may/shall designate a data protection officer.
Conclusion

- Several tools are useful in the cloud
  - DPA recommendations
  - Best practices
  - Certifications
  - Codes of conducts

- Different level of transparency and assurance

- GDPR as a game changer and opportunity to raise trust in CSPs
Useful references

- **CNIL’s recommendations**

- **CNIL’s guides**
  - Security (basics):
  - Privacy Impact Assessment:

- **WP29 Opinion on Cloud computing:**